

Blockchain : nouveau Web ou nouveau Wap ?

Sylvain Colin, Florent Robic

▶ **To cite this version:**

Sylvain Colin, Florent Robic. Blockchain : nouveau Web ou nouveau Wap ?. Sciences de l'Homme et Société. 2017. hal-01813452

HAL Id: hal-01813452

https://minesparis-psl.hal.science/hal-01813452

Submitted on 12 Jun 2018

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

MÉMOIRE 3A CORPS DES MINES

Blockchain : nouveau Web ou nouveau Wap ?



Sylvain Colin et Florent Robic

Sous le pilotage de Françoise Trassoudaine

Remerciements

Nous souhaitons en premier lieu remercier notre pilote Françoise Trassoudaine, pour son écoute attentive et ses nombreux conseils tout le long de l'année. En particulier sur nos présentations, qu'elle a su grandement améliorer.

Nous remercions également les membres de la CTP pour leurs retours lors de nos présentations et leur soutien.

Merci aussi aux nombreux professionnels et chercheurs qui ont accepté de nous recevoir et prendre de leur temps pour nous expliquer leur point de vue sur le sujet. En particulier, Jean-Yves Rossi, professeur de droit aux mines de Paris, et son cabinet de conseil CANTON Consulting qui nous a ouvert les portes du W3C et donné accès à plusieurs acteurs internationaux à la pointe du domaine.

Introduction

Le *buzz word* technologique de l'année 2017 sera sans doute « blockchain », il succède ainsi à ses illustres ancêtres « Webinar », « Web 2.0 », « Big Data », « Data mining », « Cloud », *etc.* pour certains déjà oubliés. Mais qu'en est-il vraiment : La « disruption » ultime ? Le nouvel Internet ? La technologie qui va révolutionner la banque et l'assurance ? Ou bien plutôt un feu de paille, le nouveau terme à la mode dont tout le monde s'empare ? Sur la blockchain, comme sur de nombreuses technologies informatiques, les avis divergent, entre thuriféraires promettant la révolution et sceptiques patentés, qui vouent aux gémonies toute nouvelle technologie présentée comme l'innovation ultime. Comme souvent, l'informatique intrigue, et chacun y va de sa prédiction quant aux changements qu'une technologie pourrait induire.

Depuis son invention en 2008, comme la technologie sous-jacente au bitcoin, la Blockchain a su démontrer sa solidité en permettant à la monnaie de fonctionner avec des enjeux financiers de plus en plus élevés. Depuis bientôt 10 ans, elle permet à tous les utilisateurs du bitcoin et de centaines d'autres crypto-monnaies de s'accorder sur les montants possédés par chacun en gardant la trace de toutes les transactions.

Pour rendre possible la création d'une monnaie virtuelle, la blockchain a su résoudre un problème qui avait résisté jusqu'alors aux informaticiens : le transfert de titre de propriété sans intervention d'un tiers de confiance. Elle le fait en permettant à un réseau d'ordinateurs de s'accorder sur un livre de compte commun qui respecte la propriété de chacun sans qu'aucun des participants n'ait à faire confiance à aucun autre.

Beaucoup de questions méritent d'être posées au sujet de cette nouvelle technologie, les acteurs sont en droit de se demander comment cela fonctionne, si différentes versions existent, si celles-ci proposent toutes les mêmes fonctionnalités, quels en sont les différents avantages et défauts, quels nouveaux usages cette technologie permet-elle ? Le régulateur doit se poser ces questions et doit également se positionner pour répondre aux attentes des acteurs de son domaine. Comment s'assurer de toujours remplir sa mission dans un contexte changeant, quelle posture doit-il adopter ? doit-il encourager ou proscrire cette innovation ?

Nous espérons que ce mémoire pourra donner quelques pistes à nos lecteurs afin de répondre à ces questions. Il serait souhaitable notamment que le régulateur envisage une régulation « neutre technologiquement » guidée par des principes généraux. Cette idée de neutralité présente dans la régulation des télécoms depuis plusieurs années permet de laisser les technologies évoluer en évitant de les brider par un cadre trop restrictif.

En effet, il ne faut pas perdre de vue que la Blockchain, aussi intéressante soit-elle, n'est qu'une variante plus évoluée d'une base de données distribuée, elle pourrait être surpassée dans quelques années par d'autres technologies. Ainsi un régulateur qui définirait un cadre trop spécifique dédié à la blockchain prendrait le risque de figer l'innovation.

Table des matières

Remerciements **2**

Introduction **3**

1 Explications : histoire, mécanismes **6**
1.1 L'éclosion du bitcoin **6**
1.2 Le fonctionnement de bitcoin **8**
1.3 De 2009 à nos jours **13**
1.4 Le contrat intelligent **15**
1.5 50 nuances de blockchain **16**

2 Les blockchains, une évolution technique et applicative **18**
2.1 Alice (et Bob) au pays des blockchains **18**
2.1.1 Blockchains publiques et privées 18
2.1.2 Minage et système de consensus 19
2.1.3 Nature des données 22
2.1.4 Confidentialité 23
2.1.5 Réversibilité des données 24
2.1.6 Tiers de confiance 25
2.1.7 Synthèse et sémantique 26
2.2 Panorama d'applications potentielles **27**
2.2.1 Quelques usages des blockchains publiques 27
2.2.2 Quelques applications des DLT 29
2.3 Limites des DLT **30**
2.3.1 Sécurité des DLT 30
2.3.2 La question de la confiance 30
2.3.3 Utilité réelle du système ? 31
2.3.4 Synthèse 31
2.4 Limites des blockchains publiques **31**
2.4.1 Coût du système et consommation énergétique 32
2.4.2 Cadre légal 33
2.4.3 Fiabilité du système 35
2.4.4 Souveraineté du système 37
2.4.5 Un enjeu d'éducation aux risques numériques 38
2.4.6 Décentralisation et protection des consommateurs 39
2.4.7 Quelques limites techniques 40
2.4.8 Synthèse 41
2.5 Une première réponse technique : les *sidechains* **42**
2.5.1 Fonctionnement 42
2.5.2 Intérêts et limites 43

3 Cas d'usage détaillés **46**
3.1 Les applications financières **46**
3.1.1 Les crypto-monnaies : monnaie ou actif ?, le cas bitcoin 46
3.1.2 Gérer les transactions sur la blockchain, le cas FundsDLT 49
3.2 Les autres usages **51**
3.2.1 La gestion de l'identité, le cas *dock.io* 52
3.2.2 Traçabilité et *supply chain*, le cas everledger 53

4 Impacts prévus, cadre réglementaire et recommandations **55**
4.1 Blockchains publiques et gouvernance **55**
4.1.1 Statut des crypto-monnaies 55

4.1.2 Blockchains publiques et gouvernance 56
4.1.3 Synthèse 57
4.2 Régulation et réglementation des blockchains : l'exemple du secteur financier 58
4.2.1 Préambule : quelques principes de régulation financière 58
4.2.2 Blockchains et secteurs financiers 59
4.2.3 Quelle vision pour le régulateur ? 61
4.2.4 Blockchains et réglementation, l'exemple des titres non cotés 63
4.2.5 Synthèse 64
4.3 Recommandations et ouvertures sur la régulation 65
4.3.1 La réglementation doit être technologiquement neutre ! 65
4.3.2 Réguler les blockchains n'est pas une urgence ! 67
4.3.3 Quelques pistes d'ouverture 68
4.3.4 Synthèse 71
4.4 Quel avenir pour les blockchains ? 71
4.4.1 Quelques remarques générales 72
4.4.2 L'avenir des blockchains publiques 73
4.4.3 L'avenir des blockchains privées 75
4.4.4 Synthèse 76
5 Bibliographie 78

1 Explications : histoire, mécanismes

Avant de pouvoir étudier la blockchain, il est nécessaire de comprendre le fonctionnement du bitcoin. C'est la plus célèbre des crypto-monnaies qui a inventé le mécanisme dont il est ici question. L'idée de stocker des données sous la forme de chaînes de blocs (*blockchain*) se retrouve dans des protocoles informatiques antérieurs. C'est par exemple le cas du célèbre gestionnaire de version « git » utilisé par de très nombreux développeurs. C'est seulement lors de la publication du code source de bitcoin en janvier 2009 qu'apparaît la première occurrence des mots « *block chain* » dans leur sens « moderne ». Ce n'est pas encore le mot composé que nous utilisons et il désigne alors la structure qui stocke le registre des transactions de la monnaie. Pour comprendre ce qu'apporte cette technologie, nous proposons d'étudier son mécanisme initial, c'est-à-dire le fonctionnement de la chaîne bitcoin.

1.1 L'éclosion du bitcoin

En résumé

Plusieurs monnaies virtuelles ont été créées avant que le bitcoin soit inventé. Cependant toutes avaient en commun de reposer à divers degrés sur un acteur central. Cette centralisation rendait ces technologies peu robustes, l'exemple de l'*e-gold,* fermé par le FBI en raison de sa trop grande utilisation par des trafiquants, l'illustre parfaitement. La saisie de ses serveurs a suffi à arrêter complètement son fonctionnement.

En 2008, Satoshi Nakamoto, un pseudonyme, propose une nouvelle monnaie appelée le bitcoin. Cette fois-ci, le protocole sous-jacent est décentralisé. Il permet de transférer de façon sûre la propriété entre deux utilisateurs sans l'intervention d'un tiers de confiance ou d'un quelconque acteur central. Cette propriété est la grande innovation de cette nouvelle monnaie.

L'idée d'une monnaie entièrement virtuelle n'est pas apparue avec le bitcoin. Dès 1983, David Chaum proposait un tel système à la conférence CRYPTO (1), une des conférences les plus prestigieuses dans le domaine de la cryptographie. Son constat était le suivant :

- les transactions électroniques d'un individu sont toutes enregistrées ;
- la connaissance par un tiers de toutes les transactions d'un individu est extrêmement intrusive ;
- il est facile d'en déduire sa religion, ses opinions politiques, son style de vie, ses déplacements, *etc.* ;
- les autres moyens de paiements ne sont pas satisfaisants.

En effet, les moyens de paiements anonymes de l'époque comme la monnaie fiduciaire et les chèques au porteur peuvent être volés ou falsifiés. De plus, les preuves de paiement sont difficiles à produire et ils peuvent faciliter la corruption, les marchés noirs, *etc.* Le système décrit dans son article répondait à ces problématiques.

Pour pallier cette situation et appliquer son idée, il crée quelques années plus tard la société *Digicash* pour la mettre en œuvre, cependant elle ne survivra pas à l'éclatement de la bulle internet au début des années 2000. D'autres monnaies cherchant à répondre à ce besoin de protection de la vie privée furent créées par la suite, une des plus célèbres est e-gold. Cette monnaie numérique était garantie par l'or et permettait à ses utilisateurs de rester anonymes. Plébiscitée pour un certain nombre d'activités illégales, le FBI saisit en 2005 l'intégralité de ses actifs.

Aussi différentes que puissent-être toutes ces monnaies, elles reposaient sur un principe commun : l'existence d'un tiers de confiance. Selon les différentes monnaies, celui-ci pouvait avoir une vision plus ou moins complète des transactions, de l'identité des participants, *etc.* mais sa

présence et la confiance des utilisateurs étaient incontournables. Il en est de même pour toutes les autres monnaies plus classiques. Les monnaies nationales sont garanties par les banques et les états. Un exemple plus original : l' « or » présent dans certains jeux vidéo en ligne. Cette monnaie est vendue contre de l'argent « réel » puis l'« or » virtuel est géré par le développeur qui se porte garant de la bonne tenue du système.

C'est ce tiers de confiance que propose de supprimer Satoshi Nakamoto lorsqu'il publie en octobre 2008 : *bitcoin: A Peer-to-Peer Electronic Cash System* (2) qui jette les bases du protocole *bitcoin.* Avant de s'intéresser au fonctionnement de cette monnaie, il est intéressant de noter que Satoshi Nakamoto est un pseudonyme et qu'à ce jour son identité réelle n'est toujours pas connue. Plusieurs pistes s'affrontent mais aucune d'entre elles ne semble en mesure d'apporter de preuves de leur véracité. Satoshi pourrait même être un groupe de personnes à l'image de Nicolas Bourbaki. Le site bitcoin.fr référence les différentes pistes sur son identité (3).

Le protocole inventé par Satoshi est conçu de manière à ce qu'un utilisateur n'ait besoin d'avoir confiance en aucun autre en particulier. Il doit seulement croire qu'aucune coalition majoritaire ne travaille (dans un sens précisé ultérieurement) contre lui. Pour supprimer cet acteur qui paraissait jusqu'alors indispensable, *bitcoin* propose un système pair-à-pair[1] décentralisé, transparent capable de s'autoréguler. Le fonctionnement de bitcoin est transparent à plusieurs titres, premièrement le protocole et le code informatique sous-jacent sont libres, n'importe quel utilisateur peut l'expertiser ; deuxièmement, le système s'apparente à un grand registre des transferts, permettant à tous de vérifier la balance des comptes et la validité des transactions. Les utilisateurs peuvent également participer activement à la validation des nouveaux transferts par le biais du « minage ».

[1] Un réseau pair-à-pair est un réseau d'ordinateurs où tous les membres peuvent agir à la fois comme clients et comme serveurs. Chaque ordinateur du réseau est susceptible de communiquer avec tous les autres.

1.2 Le fonctionnement de bitcoin

En résumé

Bitcoin fonctionne grâce à un réseau d'ordinateurs. Ceux-ci partagent entre eux une base de données appellé blockchain. Chaque utilisateur peut librement créer des comptes sur la blockchain. La blockchain est organisée en blocs successifs permettant de connaître l'historique de toutes les transactions entre les différents comptes depuis la création de la chaîne. Toutes les 10 minutes environ, un nouveau bloc est ajouté contenant toutes les nouvelles transactions ayant été lancées durant cette période. C'est à ce moment qu'elles sont alors inscrites dans le registre et considérées comme effectuées.

Pour publier les blocs, les ordinateurs du réseau sont en compétition pour résoudre un problème algorithmique. La difficulté de ce problème est automatiquement ajustée en fonction de la puissance de calcul du réseau de sorte que le résoudre demande environ 10 minutes. La solution de ce problème dépend des transactions ayant eu lieu durant la période et du bloc précédent. Ainsi, à chaque fois qu'un bloc est ajouté il certifie également les blocs précédents. En effet pour introduire une modification dans un bloc ancien, il faut être en mesure de résoudre de nouveaux tous les problèmes des blocs suivants.

Les participants à ce processus sont appelés « mineurs » par analogie avec les chercheurs d'or. Lorsqu'un bloc est ajouté à la chaîne, le « mineur » ayant trouvé la solution du problème et publiant le bloc reçoit en récompense les frais de transactions ainsi que des nouveaux bitcoins. C'est le seul mécanisme permettant l'introduction de nouveaux bitcoins. Cette récompense diminue régulièrement de sorte que le nombre de bitcoins en circulation sera limité à 21 millions.

Comme expliqué ci-dessus, bitcoin est un système autorégulé qui permet le transfert de propriété numérique. Jusqu'à l'invention du bitcoin, le problème du transfert de propriété numérique n'avait pu être résolu sans l'intervention d'un tiers garantissant les échanges et effectuant donc à divers degrés la tenue de compte. Dans le monde numérique, copier un objet est extrêmement facile. Dès lors s'assurer que lors d'un échange un transfert de propriété a bien eu lieu est beaucoup plus complexe que dans le monde physique.

Pour fonctionner bitcoin utilise plusieurs mécanismes cryptographiques connus (signatures, hash et arbres de Merkle, horodatage, preuve de travail, réseau pair-à-pair) et les organise ingénieusement pour remplir son objectif.

Dans le système bitcoin, l'équivalent d'un compte est représenté par une paire de clefs. L'une dite publique qui va être l'identifiant de l'utilisateur sur le réseau, l'autre dite privée sert à prouver qui est le détenteur légitime du compte. Il est possible pour chaque utilisateur de posséder autant de comptes que souhaités car l'utilisateur est lui-même responsable de la génération des clefs. Il est intéressant de remarquer que de ce fait, l'utilisateur devient l'unique responsable de ses comptes, si un utilisateur perd ses clefs privées il perdra l'argent associé comme l'illustre ce malchanceux gallois qui a jeté un vieux disque dur en oubliant de copier les clefs préalablement (4).

Les pièces bitcoin peuvent ensuite être regardées comme une chaîne de signatures. Le propriétaire ordonne un transfert en signant avec la clef privée une référence à une transaction précédente dont il était le bénéficiaire et indique la clef publique du nouveau propriétaire. Tous les utilisateurs peuvent vérifier que la clef privée qui signe l'ordre de transfert correspond bien à la clef publique du précédent détenteur. Pour plus de détails sur les transactions, voir l'encadré.

« Compte » bitcoin

Pour pouvoir utiliser bitcoin, les utilisateurs doivent s'identifier sur le réseau. Il ne s'agit pas de dévoiler son identité ou de choisir un véritable pseudonyme, il faut se créer un identifiant

Pour cela Alice doit générer une paire de clefs asymétriques appelées : « clef publique » et « clef privée ». Ces deux clefs sont complémentaires, un message chiffré à l'aide d'une clef publique ne peut être déchiffré que par la clef privé correspondante et inversement.

Comme son nom l'indique la « clef publique » peut être publiée. C'est cette clef qui représente Alice sur la blockchain. La clef privée par contre ne doit jamais être diffusée, c'est le « mot de passe » de son compte.

Effectuer un transfert

Si Alice souhaite envoyer un bitcoin à l'adresse de Bob, elle doit envoyer un ordre de transfert sur le réseau. Elle utilise sa clef privée pour signer cet ordre en le chiffrant, ainsi les utilisateurs du réseau peuvent vérifier que le propriétaire légitime est bien à l'origine de l'ordre en utilisant sa clef publique, celle-ci étant publiquement associée au bitcoin qui doit être transféré.

En effet, cette clef publique est capable de déchiffrer la signature, prouvant que le détenteur de la clef privée est bien à l'origine de la transaction.

L'ordre de transfert contient plusieurs informations :

- la clé publique de Bob, c'est le nouveau « portefeuille » qui détiendra le bitcoin ;
- le portefeuille d'origine des bitcoins, la transaction est signée avec la clef privée lui correspondant permettant de s'assurer de la légitimité du donneur d'ordres ;
- la récompense donner au mineur qui validera cette transaction, ceux sont les frais de transactions ;
- le montant transféré (en réalité c'est le montant non transféré qui est indiqué, la monnaie).

Encadré 1 : Les transactions

Il faut ici remarquer que le bitcoin, est tout comme l'euro, une monnaie divisible, il n'est pas nécessaire de transférer un minimum de 1 bitcoin. Un bitcoin peut être divisé par 10000000, un dix-millionième de bitcoin, la plus petite unité, est appelé un satoshi en hommage à son créateur.

En l'état, il est cependant impossible de vérifier que la pièce n'est pas déjà été dépensée sans se mettre d'accord sur un historique des transactions précédentes. C'est usuellement ici qu'intervient le tiers de confiance qui se charge de « garder le livre de compte » et s'assurera que la même pièce n'est pas dépensée deux fois. Pour contourner ce problème, bitcoin met en place un registre distribué à travers le réseau d'utilisateurs et organisé en forme de chaîne de blocs.

Ce registre est en première approche similaire à un livre dont une nouvelle page est publiée toutes les 10 minutes. Celle-ci contient toutes les transactions effectuées durant cette période (en réalité les pages ne sont pas infinies et par conséquent certaines transactions peuvent mettre plus de temps à être traitées) ainsi qu'une référence à la page précédente permettant de garder le livre ordonné. Ces pages sont les fameux blocs de la blockchain.

Ce livre partagé entre tous les utilisateurs permet de se mettre d'accord sur un historique des transactions et éviter les problèmes de double dépense. Lorsqu'un utilisateur reçoit une transaction, il peut comme nous l'avons vu s'assurer que son interlocuteur possède bien la clef pour débloquer les fonds mais également s'assurer en lisant le livre que les fonds reçus n'ont pas été déjà dépensés et une fois la transaction écrite savoir que les fonds lui appartiennent de manière irrévocable. Dans les faits l'utilisateur n'a pas à vérifier lui-même la cohérence de la transaction, le réseau acceptera une nouvelle page si et seulement si celle-ci est cohérente avec le reste du livre,

interdisant de fait toutes fraudes apparentes. Pour en savoir plus sur l'organisation interne des blocs et les arbres de Merkle, vous pouvez vous reporter à l'encadré correspondant.

La difficulté est de permettre un consensus entre l'ensemble du réseau sur un seul livre, une seule chaîne. Comment choisir qui publiera le prochain bloc ? Comment s'assurer qu'une seule version ne persiste ? Comment s'assurer que le livre ne sera jamais modifié ? Plutôt que de placer un acteur central pour assurer ce travail, le protocole opère par tirage au sort.

La première solution qui vient à l'esprit serait de choisir un compte au hasard et le charger de la vérification. Mais ce procédé engendrerait plusieurs problèmes. Le propriétaire est-il connecté/actif ? Comment effectuer ce tirage ? Plus problématique, comme il est très facile de créer un « compte », comment s'assurer que le jeu ne soit pas truqué ?

Le mécanisme proposé par Satoshi Nakamoto pour répondre à ces questions est celui de la preuve de travail. Avec ce système les chances de gagner à la « loterie » sont proportionnelles à la puissance de calcul investie. La participation à ce processus de validation est libre et les personnes qui y participent sont appelées les mineurs. Ils récupèrent les transactions diffusées sur le réseau, vérifient leur validité et utilisent leur puissance de calcul pour résoudre un problème. Ce problème dépend des données du bloc et est donc unique à chaque nouveau bloc. Il est conçu pour que le seul algorithme existant pour le résoudre consiste à essayer des combinaisons au hasard jusqu'à trouver une combinaison satisfaisante.

En pratique, ce problème fait appelle à une fonction de *hashage* cryptographique. Une fonction de *hashage* cryptographique est un programme informatique qui associe à une entrée quelconque un nombre entre 0 et une borne max (dans le cas du bitcoin 2^{256}) de telle sorte qu'il ne soit pas possible de retrouver grâce à ce nombre les données d'entrée. Ce mécanisme permet de créer des empreintes de données. Il est par exemple très utile pour stocker de façon sécurisée des mots de passe. En stockant l'empreinte du mot de passe plutôt que le mot de passe lui-même on protège le mot de passe de l'utilisateur même en cas de piratage. Ce système est aussi utilisé pour vérifier l'intégrité des fichiers. Après avoir téléchargé un fichier de grande taille, l'utilisateur peut calculer son empreinte si elle correspond à celle du fichier initial le transfert s'est effectué correctement, dans le cas contraire le fichier a été corrompu.

L'encyclopédie collaborative *Wikipedia* définit une fonction de hashage cryptographique comme étant :

« une fonction de hachage qui, à une donnée de taille arbitraire, associe une image de taille fixe, et dont une propriété essentielle est qu'elle est pratiquement impossible à inverser, c'est-à-dire que si l'image d'une donnée par la fonction se calcule très efficacement, le calcul inverse d'une donnée d'entrée ayant pour image une certaine valeur se révèle impossible sur le plan pratique. Pour cette raison, on dit d'une telle fonction qu'elle est à sens unique. »

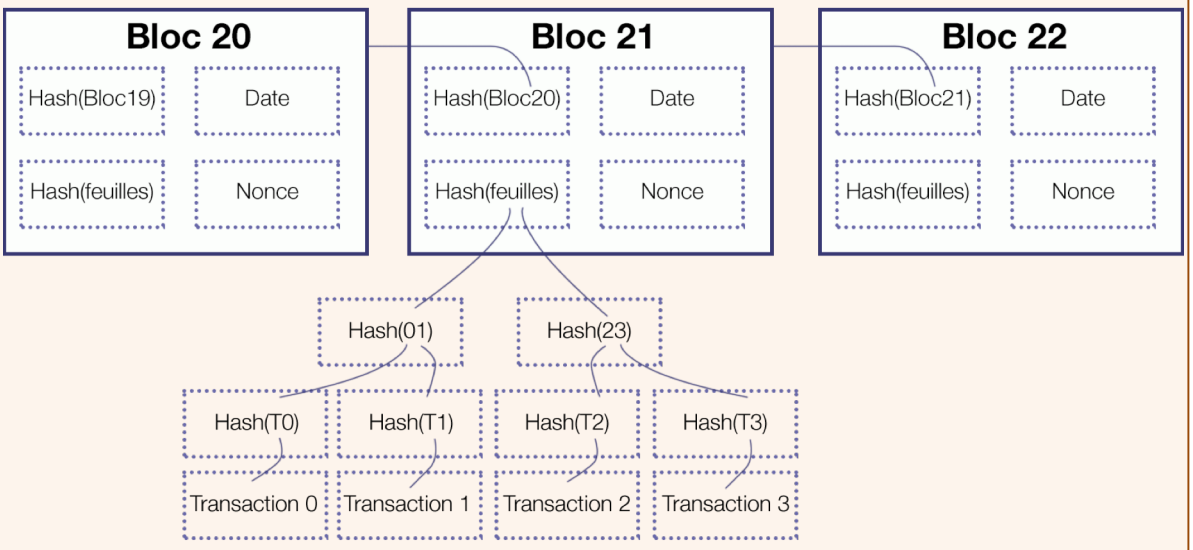
Un exemple d'une telle fonction est la fonction SHA-256, elle convertira le titre de ce mémoire en la chaîne de caractères suivante :

28de7a6cd416c38b345b427eeb388f256dab276bb453ec136c48a15eabcfb2b7

Changer un seul caractère dans le titre changera complètement cette empreinte (également appelée « *hash* »), ces empreintes numériques sont très utiles pour s'assurer rapidement de l'intégrité de données.

```
blockchain → ef7797e13d3a75526946a3bcf00daec9fc9c9c4d51ddc7cc5df888f74dd434d1
Blockchain → 625da44e4eaf58d61cf048d168aa6f5e492dea166d8bb54ec06c30de07db57e1
```

Les blocs d'une blockchain utilisent de nombreuses fois ce type de fonction, comme le montre la structure des blocs expliquée par le schéma ci-dessous :



Cette structure arborescente, appelée « arbre de Merkle » permet de vérifier rapidement l'intégrité de l'ensemble des transactions. Combinée à la structure chaînée des blocs, l'organisation de la blockchain rend très complexe la modification d'une transaction ancienne puisque celle-ci aurait des répercussions sur tous les blocs avals. Le « nonce » permet de s'assurer que tout changement d'une transaction de la chaîne demandera un temps de calcul rédhibitoire. La structure arborescente permet aussi de se séparer d'une partie de l'historique des transactions en n'en conservant seulement la signature si celles-ci n'ont plus d'utilité.

Encadré 2 : Organisation des blocs

Le premier « mineur » qui trouve une solution diffusera son bloc dans le réseau. Sa probabilité de trouver dépend du nombre de tentatives et donc directement de la puissance de calcul mobilisée. Pour s'assurer qu'une solution émerge en moyenne toutes les 10 minutes la

difficulté est régulièrement et automatiquement réajustée. Une fois un bloc reçu, les mineurs commencent à travailler sur le bloc suivant.

Pour résoudre le problème de minage, les ordinateurs consomment des quantités importantes d'électricité. C'est une des limites de ce protocole qui sera évoquée plus en détail à la partie 2.4.1.

Pour rémunérer les mineurs qui investissent de l'énergie dans la résolution du problème deux systèmes sont mis en place. Premièrement la création monétaire, lorsque qu'un bloc est ajouté une transaction spéciale est incluse offrant un certain nombre de bitcoins au mineur l'ayant créé. Cette récompense est divisée par deux tous les 210,000 blocs (soit un peu moins de 4 ans). Initialement de 50 bitcoins, elle est aujourd'hui de 12,5 bitcoins. Ces nouveaux bitcoins sont inscrits comme une transaction par le mineur dans le bloc qu'il publie. Ce système de création monétaire limite le nombre maximum de bitcoins en circulation qui est de 21 millions. En sus de cette récompense, le mineur perçoit aussi des frais de transactions fixés librement par les utilisateurs. Ces frais représentent actuellement en moyenne un peu plus de 15% de la rémunération des mineurs. Le « salaire » des mineurs oscillent aujourd'hui aux alentours de 1% du volume de transactions.

Un dernier problème peut se poser : que se passe-t-il si deux mineurs différents publient au même moment un nouveau bloc ? Une partie du réseau recevra le premier tandis que l'autre recevra le second. Qui doit alors recevoir la récompense ? Quelles sont les transactions valides, celles du bloc 1 ou du bloc 2 ? Le protocole prévoit que chacun doit travailler pour créer la suite du bloc qu'il a reçu en premier, une des deux « équipes » publiera un bloc en premier et cette chaîne deviendra la chaîne de référence puisque le protocole prévoit de toujours privilégier la chaîne la plus longue. Ce cas n'est pas la norme mais il se produit cependant plusieurs fois par mois. Il est extrêmement rare que deux chaînes persistent plus de 3 blocs, l'une finissant toujours par l'emporter rapidement. Pour être prudent il est cependant recommandé d'attendre qu'une transaction soit « recouverte » par 6 blocs (environ 1 heure) pour la considérer comme irrévocable. Il serait hautement improbable que deux chaînes concurrentes se maintiennent sur une durée aussi longue. De plus, si un attaquant souhaite annuler cette transaction, il devrait alors publier une chaîne de 6 blocs et donc recalculer seul des preuves de calcul extrêmement coûteuses.

Ce système garantit donc bien toutes les propriétés minimales souhaitées pour une monnaie. Il est impossible pour un attaquant de voler l'argent des propriétaires légitimes, les transactions inscrites sont toutes valides (présence des fonds chez le débiteur) et il est impossible de produire de la fausse monnaie. De plus toutes ces conditions sont remplies par un protocole entièrement distribué, sans asymétrie protocolaire entre les utilisateurs. Son existence sans problème majeur depuis plus de 8 ans montre la solidité du système. Particulièrement depuis que son cours s'est envolé, un attaquant qui parviendrait à attaquer la chaîne obtiendrait une gratification significative. Si dans cette présentation nous nous sommes concentrés sur les transactions financières, nous remarquons déjà que le protocole peut s'adapter facilement au transfert d'autres objets, en conservant ces propriétés. De plus, le protocole décrit ici est simplifié, certaines fonctionnalités n'ont pas été décrites. Par exemple chaque transaction peut être accompagnée d'un message, cela permet déjà d'utiliser la blockchain de bitcoin pour d'autres usages que le transfert monétaire notamment afin de certifier la date de création d'un document. Une transaction est également écrit comme un script informatique, dans un langage volontairement limité, préfigurant ce qui est aujourd'hui appelé « *smart-contracts* ».

1.3 De 2009 à nos jours

En résumé

Initialement, la communauté bitcoin n'était composée que de cryptographes, elle s'est cependant rapidement élargie.

Entre 2011 et 2013, le bitcoin se fait connaitre du très grand public en étant tout d'abord associé à des usages peu recommandables. Dans le même temps des blockchains alternatives commencent à apparaître.

À partir de 2016, la technologie de la blockchain commence à intéresser de plus en plus de secteurs.

Les premières années de bitcoin ne sont pas très mouvementées mais la communauté grossit et s'organise. Les premières plateformes d'échanges se créent et le minage commence à rechercher l'efficacité.

Intrinsèquement parallélisables, les algorithmes de minage sont adaptés pour pouvoir tourner sur des cartes graphiques plus performantes que les processeurs sur ce type de tâche, le minage commence sa professionnalisation. En 2010 deux failles sont repérées dans l'implémentation du protocole, elles sont rapidement corrigées.

Plusieurs événements se produisent en 2011 sur le plan des usages de bitcoin, en particulier l'ouverture de la plateforme *Silkroad* sur le réseau Tor. Cette plateforme, surnommée le supermarché de la drogue, permet à des utilisateurs de se procurer des substances illicites en échange de bitcoins. Elle opérera jusqu'à sa fermeture par le FBI en octobre 2013. Quasi-simultanément la parité bitcoin / euro est pour la première fois dépassée en février 2011.

C'est aussi durant cette année que les premières blockchains alternatives apparaissent. En particulier *Namecoin* (4), premier *fork* de bitcoin, qui propose de se servir de la technologie blockchain non pas simplement comme une crypto-monnaie mais pour enregistrer des noms de domaine en *.bit* de façon décentralisée et indépendante.

Les noms de domaine comme *mines-paristech.fr* permettent de donner aux sites web des adresses facilement mémorisables. L'enregistrement se fait auprès d'organismes et des tables font ensuite le lien entre ceux-ci et les adresses IP des serveurs hébergeant le contenu. Dans le cas précédant nous sommes redirigés vers *194.214.158.58*.

Namecoin propose de supprimer les organismes attribuant les noms de domaines et les serveurs s'occupant de rediriger correctement les internautes par une blockchain. Dans la pratique, l'initiative n'a pas eu le succès escompté. Un des principaux écueils a été le cyber-squattage, cette pratique consiste à enregistrer le nom de domaine d'une organisation avant que celle-ci n'ait le temps de le faire. Pour s'en protéger les sociétés enregistrent aujourd'hui souvent très en amont des annonces les noms des sites web qui seront utilisés pour un nouveau projet. En proposant l'enregistrement de domaine à un coût très bas et en n'offrant aucun recours pour les victimes *Namecoin* a trop facilité cette pratique, pénalisant ainsi son propre succès.

Quelques mois plus tard un autre fork est effectué, c'est la création de la blockchain *Litecoin.* Aujourd'hui cette crypto-monnaie est la quatrième en terme de capitalisation totale représentant 2 milliards soit environ 5 % de bitcoin. L'idée de ces concepteurs était d'essayer d'améliorer certains aspects de bitcoin qu'ils jugeaient problématiques. En premier lieu, l'avantage pour les mineurs d'utiliser du matériel spécifique. Comme nous l'avons évoqué, au cours de l'année 2010 le minage s'améliore : la première étape a été de remplacer les processeurs par des cartes graphiques plus adaptées au calcul de la preuve de travail bitcoin. Cependant les cartes graphiques ne sont qu'une

première étape et pour aller plus vite les mineurs les ont remplacées par des circuits intégrés spécifiquement conçus pour la preuve de travail de bitcoin. Avec cette escalade matérielle, il n'est plus possible pour un utilisateur lambda de miner des bitcoins en étant rentable, les seuls mineurs véritablement actifs sont des fermes de calculs gérées par des entreprises. Litecoin propose donc de changer la fonction supportant la preuve de travail par une fonction équivalente du point de vue fonctionnel mais ne pouvant pas bénéficier des mêmes optimisations matérielles. Ainsi Litecoin espérait éviter la concentration du minage entre quelques grands acteurs. C'est aussi en 2012, qu'une alternative à la preuve de travail, la preuve d'enjeu est proposée (5). Elle a pour but de résoudre le problème de la consommation énergétique posée par la preuve de travail.

La popularité de bitcoin ne se démentira pas l'année suivante, le cours dépasse pour la première fois les 1 000 $. De nombreuses banques centrales commencent à regarder le sujet avec des avis rendus assez divers. C'est aussi durant l'année 2013, que la blockchain commence à être regardée par de plus en plus d'acteurs pour des usages autres que les crypto-monnaies comme un registre notarié ou pour suivre des actifs réels.

À la suite de ce premier pic le cours chuta fortement durant l'année 2014, ceci dû en particulier à la fermeture pour fraude de Mt. Gox, principale plateforme d'échange à l'époque. Malgré ces turpitudes le développement de bitcoin et de la blockchain suit son cours. Le code de bitcoin est mis à jour pour faciliter des usages non monétaires de la blockchain. La communauté se saisit de plus en plus des enjeux de passage à l'échelle avec la continuation du débat sur la taille des blocs ou la naissance des *sides-chains*. Pour plus d'informations à ce sujet, nous vous conseillons la lecture du chapitre 3 de l'ouvrage « *Blockchain et autres registres distribués : quel avenir pour les marchés financiers ?* » (6), ainsi que la partie 2.5 de ce mémoire.

En juillet 2015, la blockchain qui est aujourd'hui la deuxième plus importante en terme de capitalisation est créée. Il s'agit d'ethereum (7). Une de ses principales nouveautés vis-à-vis de bitcoin est de permettre la création de *smart-contracts*. Les *smart-contracts sont* des instructions informatiques, des algorithmes, dont l'exécution est automatisée et certifiée par la blockchain (voir partie suivante), beaucoup plus expressifs que ceux disponibles sur *bitcoin*. Depuis la popularité de la blockchain ne s'est pas démentie et a même atteint un public beaucoup plus large comme le montre l'évolution des requêtes sur le sujet.

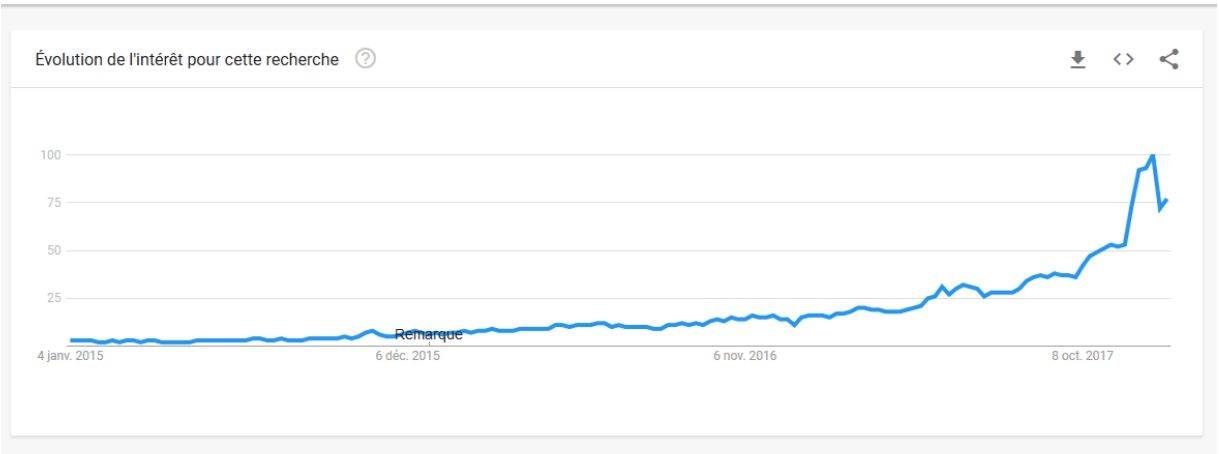


Figure 1 : Popularité du terme blockchain sur Google

1.4 Le contrat intelligent

En résumé

Les *smart-contracts* sont des programmes informatiques s'exécutant sur une blockchain. Ils permettent d'automatiser certaines tâches. Par exemple, le déclenchement d'un paiement lorsque plusieurs conditions sont réunies.

Nous avons évoqué précédemment qu'une différence fondamentale entre la blockchain ethereum et la blockchain bitcoin était la présence de *smart-contracts* plus complets. Mais qu'est-ce qu'un *smart-contract* ?

Un *smart-contract* (dans le contexte des blockchains) est un programme informatique dont l'exécution est assurée et vérifiée par le réseau. C'est à dire qu'une fois lancée sur le réseau le contrat s'exécutera irrémédiablement comme il a été programmé. Le but est d'éviter les litiges sur le contrat et d'automatiser la résolution selon les termes prévus, sans recours possible. En étant distribué sur la blockchain un *smart-contract* en acquiert les propriétés de robustesse et d'immuabilité. Ils permettent en outre de signer des contrats avec des parties qui n'ont pas notre confiance, celles-ci ne pouvant s'opposer à la réalisation de leur partie du contrat. Les exemples les plus simples seraient des paiements conditionnés à la réalisation d'un événement, la sécurisation d'un dépôt, etc.

Si l'idée des *smart-contracts* a pris de l'ampleur récemment, notamment grâce à la plateforme ethereum, ces contrats étaient déjà présents dans bitcoin sous une forme plus simple. L'exemple minimal est celui d'une simple transaction qui peut déjà être vue avec le prisme *smart-contract*. L'argent peut être dépensé si l'émetteur prouve son identité à l'aide d'une clé privée. Cet exemple peut-être complexifié pour devenir un système multi-signatures, c'est-à-dire : l'argent pourra être dépensé si deux clefs sont données, ou encore un exemple un peu plus complexe, si deux clefs parmi trois sont données. Le dernier exemple a de multiples applications comme gérer automatiquement des problèmes de gouvernance où l'accord d'une majorité est nécessaire pour débloquer des fonds.

Les contrats bitcoins étaient cependant limités par le langage de programmation. C'est une des raisons qui a motivé la création de la blockchain ethereum. Les *smart-contracts* ethereum sont dits *Turing Complet*, il est possible de programmer tout ce qui est programmable en utilisant ce langage (ce qui n'était pas le cas pour *bitcoin*). Il est ainsi possible d'imaginer implémenter des contrats aussi complexes que souhaités sur la blockchain, cependant quelques bémols sont à soulever même en négligeant l'aspect légal de ce type de contrat.

Rédiger un contrat en langage informatique ou formel n'est pas immédiat et formaliser le langage et même plus spécifiquement le langage juridique est aujourd'hui un sujet de recherche. De plus, une fois rédigées de cette manière, les clauses du contrat ne peuvent plus faire l'objet d'interprétation, supprimant la souplesse pouvant être nécessaire à l'obtention d'un accord.

La programmation dans un langage complet implique également une plus grande surface aux attaques et aux bugs. Lorsque l'on dit que le contrat s'exécute de façon sûre, cela n'implique pas qu'il s'exécute selon le souhait des parties. L'exemple de *The DAO* le démontre. Lorsqu'une faille dans le code est découverte il est alors très difficile pour les contractants de s'en protéger (8). De plus se pose des questions d'ordre plus philosophique, la faille présente dans le contrat fait-elle parti de celui-ci ?

L'exécution sur une blockchain implique que l'évaluation soit répliquée par un grand nombre d'ordinateurs (l'ensemble du réseau validant les blocs). Cela limite donc l'aspect intelligent de ces contrats. À l'heure actuelle, un contrat évaluant un sinistre avec l'appui d'une intelligence artificielle semble inatteignable. Pour fonctionner un contrat sur ethereum utilise des ethers, la monnaie de la

blockchain. Le parallèle avec un carburant est très clair : plus un contrat est long à exécuter plus il va nécessiter de gaz pour fonctionner.

Toutes ces raisons nous poussent à affirmer que contrats automatisés seraient aujourd'hui une dénomination plus appropriée pour les contrats intelligents. Dans tous les cas, ces systèmes laissent de nombreuses questions ouvertes. D'un côté, l'« informatisation » du langage juridique, en le formalisant d'avantage, ouvre des pistes intéressantes sur l'autocorrection et la détection automatique d'erreurs (9) dans les contrats. Elle lui enlève, cependant, la souplesse de l'appréciation pouvant être nécessaire lors de la négociation et permettant de se protéger des erreurs manifestes.

1.5 50 nuances de blockchain

Dans cette partie nous avons principalement étudié le fonctionnement de bitcoin et dans une moindre mesure d'ethereum qui sont les deux plus grandes blockchain (en terme de capitalisation tout du moins). Mais le bestiaire des blockchains est très loin de si limiter. Aujourd'hui, plus de 150 crypto-monnaies *blockchain* ayant des capitalisations théoriques supérieures à 10 000 000 d'euros sont à dénombrer. Celles-ci présentent des caractéristiques potentiellement très différentes de la blockchain bitcoin. La diversité est encore plus grande lorsque l'on examine les blockchain hybrides ou privées destinées à fonctionner dans un environnement plus restreint. Dans ce contexte aucune taxonomie ne s'est encore imposée.

Comme le souligne Laurent Leloup dans son ouvrage (10), désigne-t-on la même chose lorsque nous parlons de *blockchain* et de chaînes de blocs ? La réponse est : pas nécessairement. D'une part les mécanismes communément admis sur le fonctionnement d'une *blockchain* vont plus loin que la simple chaîne de blocs qui lui préexistait ; d'autre part certaines *blockchains* présentent des structures plus complexes. C'est par exemple le cas d'IOTA qui organise ses blocs en forme de graphe acyclique orienté, une structure plus complexe dont la chaîne n'est qu'un cas particulier.

En assemblant différentes parties de ces différentes monnaies, il semble possible de reconstituer une « blockchain » ne partageant aucun des principes de la technologie initialement proposée par bitcoin. C'est pourquoi dans la prochaine partie nous essayerons de donner un guide de lecture permettant d'identifier les différentes caractéristiques de ces projets.

Ce qu'il faut retenir

1. Au départ, une *blockchain* est un système distribué permettant de réaliser des transactions de titre de propriété numérique dont l'authenticité ne peut être remise en cause. Ces transactions peuvent être effectuées sans avoir recours à un tiers de confiance. Cette absence de tiers de confiance dans un système d'échange numérique est la principale nouveauté apportée par cette technologie.
2. La blockchain bitcoin est une structure autorégulée et organisée en blocs, chaque bloc peut être vu comme une page d'un livre de compte résumant les transactions de la journée. Les blocs sont liés grâce à des mécanismes cryptographiques rendant la modification de l'historique des transactions par un attaquant hautement improbable.
3. Les transactions peuvent contenir toutes sortes de données, permettant d'adosser aux blockchains monétaires des usages variés.
4. En particulier, cette structure peut être enrichie par des *« smart-contracts »,* des programmes informatiques dont l'exécution est assurée par la blockchain, pour permettre d'accomplir des tâches plus complexes que des transactions dans le même cadre.
5. Cette complexité n'est pas sans risque et si les mécanismes de bases de la blockchain sont aujourd'hui éprouvés, ces contrats offrent des garanties techniques plus faibles particulièrement lorsque ceux-ci deviennent complexes.
6. Enfin, propulsées par l'engouement autour de la technologie, il existe aujourd'hui un grand nombre de types différents de blockchain.
7. En particulier, de nombreuses crypto-monnaies ont été créées. Elles présentent divers degrés d'innovation par rapport à la chaîne bitcoin. Mais attention, si certaines sont très intéressantes, d'autre semblent d'avantage compter sur la crédulité des internautes pour obtenir de l'argent.
8. Il existe également de nombreux projets privés utilisant leurs propres blockchains internes. Ces blockchains dites « privées » peuvent être assez éloignées du projet initial.

2 Les blockchains, une évolution technique et applicative

En s'appuyant sur des principes de cryptographie et un assemblage astucieux de briques techniques, bitcoin a fait émerger un nouveau modèle de paiement mais également une technologie nouvelle : la blockchain. Cette technologie est désormais l'objet de nombreux projets ou déclarations et de multiples entreprises affirment vouloir mettre en oeuvre des blockchains dans des secteurs aussi variés que la banque, le commerce ou l'industrie. Cette variété d'applications se caractérise également par une grande diversité dans la manière même d'envisager la technologie. Se développent ainsi derrière ce terme des systèmes aux caractéristiques techniques variées, loin pour certaines des principes cardinaux de l'esprit bitcoin. Nous nous proposons ici de dresser un portrait de ces technologies par le prisme de certaines de ces caractéristiques techniques, en faisant émerger les raisons qui ont présidé à ces évolutions techniques et les applications qu'elles permettent ou pourraient permettre.

2.1 Alice (et Bob) au pays des blockchains

Explorons donc dans un premier temps quelques grandes caractéristiques, techniques ou conceptuelles, qui distinguent actuellement les projets blockchains existants. Il nous apparaît que derrière le terme blockchain se cachent désormais des technologies aux propriétés bien disparates.

2.1.1 Blockchains publiques et privées

En résumé

Blockchains publiques	Blockchains privées
- Utilisation ouverte à tous - Données publiques - Code informatique public	- Système interne à une organisation ou partagé entre des organisations - Accès restreint au code et aux données

La distinction majeure aujourd'hui entre les différentes blockchains nous semble être la séparation entre les blockchains dites publiques et les blockchains dites privées ou hybrides. Cette distinction fait apparaître deux familles de technologie extrêmement différentes, aux applications bien distinctes, qui ont été à l'origine d'évolutions techniques importantes.

Comme leur nom l'indique, les blockchains publiques sont ouvertes à tous, à savoir que tout le monde peut utiliser le système. Bitcoin en est l'exemple le plus emblématique : n'importe qui peut créer une adresse bitcoin et réaliser des transactions sur la blockchain. Ces blockchains publiques sont soutenues par deux populations : les utilisateurs et les mineurs. Si l'on revient sur l'exemple de bitcoin, les mineurs sont tous utilisateurs dans le sens où ils doivent posséder une adresse bitcoin, *a minima* pour pouvoir recevoir leur récompense et les frais de transaction s'ils parviennent à valider un bloc. En revanche, on peut être utilisateur de bitcoin, détenir une adresse et réaliser des transactions, sans pour autant réaliser d'opération de minage. Mais l'un des principes fondamentaux de bitcoin reste l'ouverture du système : tout le monde peut devenir utilisateur ou mineur. Au-delà de la question de l'accès au système, le code et les données de la blockchain bitcoin sont également publics. Le code est en libre accès sur GitHub et peut être copié afin de créer sa propre blockchain. De plus, toutes les transactions sur la blockchain sont publiques. On peut ainsi trouver sur Internet le contenu des blocs (transactions, *hash*, mineur qui a validé le bloc) et des transactions qu'ils contiennent (adresses de départ et d'arrivée, montant de la transaction et des frais de transactions). Il en est de même pour ethereum, une autre blockchain publique.

À l'inverse, les blockchains privées et hybrides sont des systèmes fermés créés entre un nombre restreint d'acteurs. Une blockchain privée est un système interne à une organisation, partagée entre des acteurs de cette organisation. Une blockchain hybride est un système partagé entre plusieurs organisations. Ces deux types de blockchains sont assez similaires et, par souci de simplification, nous utiliserons la terminologie de blockchains privées pour désigner les deux technologies. En effet, ces systèmes sont comparables à des bases de données distribuées et partagées entre utilisateurs, organisées sous la forme d'une chaîne de blocs contenant des données, par exemple un registre de transactions (nous verrons l'exemple de Funds DLT un peu plus loin). Contrairement à des blockchains publiques, seuls quelques acteurs y ont accès et peuvent voir les données sur la chaîne. Nous verrons également que les systèmes de minage y sont généralement absents, remplacés par des mécanismes de consensus beaucoup plus simples. Le réseau fonctionne la plupart du temps sans mineur, la validation des blocs étant effectuée par les utilisateurs mêmes.

Cette distinction entre blockchains publiques et privées est sans doute la plus cruciale et la plus discriminante. L'ouverture du système nécessite en effet des mécanismes de consensus complexes, mis en oeuvre à l'aide de principes cryptologiques et d'un écosystème astucieux. A l'inverse, les blockchains privées résultent la plupart du temps d'un accord entre acteurs qui souhaitent développer un système commun qu'ils ont un intérêt à faire fonctionner correctement, ce qui implique une forme de confiance entre les parties prenantes. Nous verrons que cela a un impact majeur sur la nature de la technologie, tant est si bien qu'émergent des débats sémantiques pour déterminer si ces blockchains privées peuvent réellement être considérées comme des blockchains. Certains leur préfèrent l'appellation de DLT (*Distributed Ledger Technology*). Mais laissons pour le moment ce débat et tâchons de mieux comprendre les raisons d'une telle interrogation en explorant d'autres variations techniques autour de la technologie blockchain.

***NOTA BENE** : S'il existe une distinction entre blockchains privées (internes à une organisation) et hybrides (partagées entre plusieurs acteurs), nous regroupons ces deux familles de technologie très similaires sous l'appellation de blockchains privées, celles-ci étant avant tout des systèmes fermés.*

2.1.2 Minage et système de consensus

En résumé

Preuve de travail	Preuve d'enjeu	Blockchains privées
- Poids proportionnel à la puissance de calcul - Incitation économique car mécanisme coûteux - Risque d'une attaque des 51% - Coût énergétique	- Poids proportionnel à la quantité de monnaie - Risque limité d'une attaque des 51% - Envisagée sur la blockchain ethereum	- Confiance entre les acteurs - Mécanismes de consensus simplifiés

S'il nous semble que bitcoin n'est pas à proprement parler une innovation technologique majeure - mais plutôt un assemblage astucieux de briques techniques qui préexistaient à son invention -, on peut en revanche affirmer qu'elle a introduit un système totalement novateur qui a cassé bien des codes dans le domaine du paiement. A ainsi été créé un système sans gouvernance centralisée, où le contrôle est distribué au sein d'un réseau de mineurs. Plus fort encore, les nœuds du réseau ne se connaissent pas et n'ont aucun besoin de se faire confiance ! S'il existe un mécanisme crucial dans le système bitcoin, qui a permis d'atteindre cet objectif, il s'agit sans nul doute de la preuve de travail (*Proof of Works, PoW*). Rappelons que, dans une blockchain utilisant la preuve de travail, l'objectif d'un mineur consiste à trouver un nonce, à savoir une chaîne de

caractères, qui, lorsqu'il sera haché avec les données du bloc, renverra un *hash* qui satisfait certaines conditions. Cette recherche du bon nonce ne peut se faire qu'en essayant successivement des chaînes de caractères de manière aléatoire. La capacité à valider un bloc est donc proportionnelle à la capacité à calculer des *hashs*, donc à la puissance de calcul du mineur. En introduisant un *incentive* économique (récompense et frais de transaction), le système bitcoin encourage les tenants du système à fournir ce travail informatique consistant à calculer des *hashs* afin de faire fonctionner la Blockchain. Les mineurs ont donc un intérêt économique à fournir ce travail, d'autant qu'il leur coûte d'un point de vue énergétique. Surtout, ce mécanisme semble idéal pour faire émerger un consensus autour de données fiables. En effet, il encourage les mineurs à ne valider que des transactions licites, sous peine que le bloc soit rejeté par la majorité du réseau et que le mineur ne perçoive donc pas la récompense liée à la validation du bloc incriminé. De manière similaire, il favorise le consensus car tous les mineurs ont un intérêt à travailler sur la chaîne la plus longue et éviter ainsi les *forks* intempestifs, car seule la chaîne principale est considérée comme valide et permettra là-encore de toucher une récompense. Le risque majeur réside dans le fait qu'un mineur détienne la majorité de la puissance de calcul, auquel cas il aurait un contrôle absolu sur la blockchain. Nous reviendrons sur cette limite du système de manière plus détaillée par la suite.

Ceci étant posé, la preuve de travail est-elle le mécanisme de consensus idéal ? Pas nécessairement. D'une part, un mineur pourrait en effet contrôler la blockchain en détenant plus de 50% de la puissance de calcul. Bitcoin, qui génère aujourd'hui près de cinq millions de Terahashs chaque seconde, nécessite une puissance de calcul gigantesque et il paraît difficile à croire qu'un mineur puisse à lui seul fournir la moitié de cette puissance. Ceci étant, les mineurs du réseau sont aujourd'hui en nombre assez restreint et sont essentiellement de gros consortiums. Ainsi, une entente entre quelques consortiums seulement pourrait théoriquement leur permettre de prendre le contrôle de la blockchain. Surtout, on voit aujourd'hui apparaître de petites blockchains publiques sur lesquelles la puissance de calcul fournie est bien moindre et où il est donc nettement plus aisé pour un acteur mal intentionné de prendre le contrôle du système.

Au-delà de ce risque systémique, la preuve de travail est un mécanisme extrêmement énergivore. Nous présenterons par la suite quelques calculs plus détaillés sur le coût engendré par le système mais celui-ci s'élève à plusieurs centaines de millions de dollars. Surtout, ce coût est dépensé pour calculer des *hashs* qui ne servent à rien d'autre qu'à prouver que l'on a fait fonctionner des processeurs et fourni un « travail » informatique. Ainsi, les mineurs, en quelque sorte, dépensent de l'énergie simplement pour prouver qu'ils sont prêts à en assumer le coût, ce qui s'apparente à une dépense assez peu raisonnable.

Ces deux constats - sécurité et coût énergétique - ont conduit certains chercheurs à développer des mécanismes de consensus alternatifs à la preuve de travail. Le plus prometteur semble être le mécanisme de la preuve d'enjeu (*Proof of Stake, PoS*) (5). Alors que la preuve de travail offre une probabilité de valider un bloc proportionnelle à la puissance de calcul du mineur, la preuve d'enjeu considère que cette probabilité est proportionnelle à la quantité de crypto-monnaie détenue par le mineur. Ici, donc, pas de travail à fournir, tant est si bien que le processus n'est, par analogie, pas considéré comme du minage mais comme du forgeage. L'idée sous-jacente consiste donc à considérer que, plus un forgeur possède de monnaie, plus il a intérêt à ce que le système fonctionne correctement et de manière fiable. On lui donne donc d'autant plus de poids qu'il a d'enjeu à maintenir le système fonctionnel.

La première conséquence est que tout utilisateur peut devenir forgeur sans besoin matériel quelconque. Comme il n'y a plus de travail demandé par le système, il n'y a plus besoin d'incitation économique et, ce faisant, il n'y a plus de création monétaire afin de récompenser les forgeurs. Ceci implique que la quantité de monnaie sur une blockchain utilisant la preuve d'enjeu est ainsi fixée à l'avance et qu'il n'existe plus de mécanisme continu de création monétaire. Autre conséquence majeure de la disparition du « travail » informatique : il n'y a plus besoin de dépenser de l'énergie massivement, ce qui est bien l'un des objectifs majeurs de ce nouveau mécanisme.

Analysons désormais les intérêts (11) (12) d'un tel système en termes de sécurité. *A priori*, le système demeure robuste dans le sens où un acteur ayant du pouvoir sur la blockchain est un acteur qui y détient une quantité importante de monnaie et qui a donc une forte incitation à ce que le système soit stable. Ainsi, un acteur détenant plus de la moitié de la quantité de monnaie aurait un contrôle sur la blockchain mais sans doute aucun intérêt à faire s'effondrer le système. Pour autant, la preuve d'enjeu induit un premier problème important pour obtenir un consensus, appelé *Nothing-at-Stake problem* (le problème du Rien-à-Perdre). Cela signifie qu'en cas de *fork*, c'est-à-dire en cas de développement parallèle de plusieurs chaînes, un forgeur peut tenter de valider des blocs sur les deux chaînes en compétition avec la même probabilité que s'il tentait de ne valider un bloc que sur la chaîne la plus longue, supposée être la chaîne principale. Avec un mécanisme de preuve de travail, le mineur peut certes répartir sa puissance de calcul entre les deux chaînes concurrentes mais il divise alors sa puissance sur chacune des chaînes et diminue ainsi ses chances d'y valider un bloc. Un deuxième problème concerne la valeur des crypto-monnaies sur une blockchain fonctionnant avec de la preuve d'enjeu. En effet, si l'on utilise la preuve de travail, la monnaie est créée pour récompenser les mineurs pour le travail qu'ils ont fourni. Cette création monétaire a donc un coût, celui du minage, c'est-à-dire celui de l'électricité utilisée pour valider les blocs. La valeur de la monnaie est donc liée à des paramètres extérieurs, tels que le prix de l'électricité. A l'inverse, avec la preuve d'enjeu, la monnaie est créée *a priori* et sans travail, ce qui en fait avant tout un actif sans valeur en soi, qui ne prend de la valeur que parce que les utilisateurs acceptent de lui en donner. De plus, la preuve d'enjeu présente le désavantage de lier intérêts technique et économique, dans le sens où l'influence d'un acteur sur le système est proportionnelle à sa capacité à valider des blocs, donc ici proportionnelle à la quantité de monnaie qu'il détient. La preuve de travail présente l'intérêt de mieux séparer les deux intérêts. Un mineur détenant une grande part de la puissance de calcul aura une grande influence technique mais ne détiendra pas nécessairement une grande quantité de monnaie, et n'aura donc pas nécessairement de grands intérêts économiques sur le système. En revanche, la preuve d'enjeu paraît plus sécurisée que la preuve de travail, dans le sens où acquérir la moitié de la masse monétaire en circulation sur une blockchain a un coût plus élevé qu'acquérir la moitié de la puissance de calcul des mineurs. L'attaque des 51%, sur laquelle nous reviendrons ultérieurement, apparaît donc plus complexe avec la preuve d'enjeu qu'avec la preuve de travail.

Notons qu'ethereum envisage très sérieusement de passer à un système de consensus par preuve d'enjeu au cours de l'année 2018, avec la volonté notamment de réduire le coût énergétique du système. Pour lutter contre des acteurs qui utiliseraient leur masse monétaire pour tenter de prendre le contrôle du système, out tout du moins pour effectuer des transactions illicites ou allant à l'encontre des intérêts de la blockchain, les créateurs d'ethereum ont créé un système, appelé Casper. Celui-ci est finalement assez simple : pour pouvoir utiliser leur masse monétaire à des fins de validation de blocs (forgeage), les utilisateurs doivent déposer une partie de leur argent sur un compte à part. L'argent sur ce compte sera bloqué tant que l'utilisateur participera à la validation des blocs. Casper intègre alors des mécanismes destinés à vérifier les blocs que tente de valider l'utilisateur. Si le système considère que l'un des blocs est illicite, l'argent déposé sur le compte séparé sera récupéré par ethereum et sera définitivement perdu par l'utilisateur. Il y a donc une incitation économique pour les forgeurs à ne valider que des transactions licites, et donc à garantir la stabilité du système.

Enfin, pour une blockchain privée, il n'est pas nécessaire de mettre en oeuvre des mécanismes de consensus complexes et coûteux. La mise en place d'une telle technologie, soit en interne au sein d'une entreprise, soit comme système partagé entre plusieurs acteurs, présuppose que les acteurs ont des intérêts convergents et se font confiance pour partager un système dans lequel tous ont un intérêt. Le nombre restreint d'acteurs favorise également la mise en place de mécanismes simplifiés. Par exemple, les acteurs peuvent voter de manière simple pour valider ou non une transaction, qui sera inscrite sur la blockchain si une condition simple est remplie (vote à l'unanimité ou à une majorité définie à l'avance par exemple).

2.1.3 Nature des données

En résumé		
Crypto-monnaies	**Registres**	***Smart-contracts***
- Blockchain comme registre de transactions - Nécessaire au fonctionnement du système	- Registre de transactions - Registre de biens	- Contrats automatisés

Si bitcoin a été pensée comme un système monétaire parallèle, on voit aujourd'hui émerger des projets blockchains dans des secteurs divers, avec des applications variées. Nous aurons par la suite l'occasion de dresser un portrait rapide de différents cas d'usage, puis de revenir de manière détaillée sur certains d'entre eux. Nous nous proposons ici de nous intéresser à la nature générale des données qui semblent pouvoir être hébergées sur une blockchain. Naturellement, une blockchain est, d'une certaine manière, une base de données, et pourrait donc être potentiellement utilisée pour stocker tout type d'information. Pour autant, il nous semble que l'on peut grossièrement regrouper les différentes blockchains en quelques grandes catégories par nature des données.

La première utilisation d'une blockchain est bien sûr la mise en oeuvre de monnaies virtuelles, ou crypto-monnaies. Toutes les blockchains publiques tournent aujourd'hui autour de ce principe et sont pensées avant tout comme des registres de transactions monétaires. On peut même affirmer qu'aucune blockchain publique ne peut actuellement faire l'économie d'une crypto-monnaie. En effet, les deux mécanismes de consensus majeurs que sont la preuve de travail et la preuve d'enjeu nécessitent l'existence d'une telle monnaie virtuelle. Ainsi, la preuve de travail fonde le système sur des incitations économiques matérialisés par une récompense et des frais de transaction, lesquels sont bien évidemment versés dans la devise virtuelle. La preuve d'enjeu, elle, est directement liée à la monnaie puisqu'elle lie la capacité à valider un bloc à la quantité d'argent détenue. Sans crypto-monnaie, il n'y a donc pas de mécanisme de consensus, ce qui est le fondement cardinal d'une blockchain publique.

De manière plus générale, une blockchain peut héberger un système de *tokens*, à savoir des jetons virtuels ayant une certaine valeur marchande. Un *token* peut s'échanger dans l'économie réel contre de la monnaie d'État (on a alors une crypto-monnaie) ou encore contre un bien matériel ou encore un service.

Si la blockchain bitcoin est un registre de transactions monétaires, on peut alors utiliser une blockchain pour tenir un registre de manière beaucoup plus générale. On peut ainsi, par exemple, tenir un registre de transactions de manière plus large. Nous examinerons en détail l'exemple de Funds DLT, qui tient un registre de transactions d'actifs financiers. La Direction Générale du Trésor française a également lancé une consultation pour explorer la possibilité d'utiliser des blockchains afin de tenir des registres de titres non cotés. Toujours dans l'idée des registres, on peut également tenir sur une blockchain des inventaires de biens matériels. Citons l'exemple d'Everledger, une blockchain qui recense au niveau mondial les diamants afin de mettre en oeuvre un système fiable et robuste permettant de lutter contre les trafics.

Enfin, on voit également se développer des projets blockchain autour de la notion de *smart contracts*. Il s'agit de contrats totalement dématérialisés, rédigés dans du code informatique, qui s'exécutent de manière automatisée. Ainsi, les contrats ne sont détenus par aucune autorité et ne peuvent être contestés. Un cas d'application éventuel pourrait être ce que l'on appelle les *cat bonds*. Il s'agit de contrats financiers destinés à couvrir des risques climatiques. Imaginons ainsi qu'un

particulier habitant dans une zone présentant des risques de crues souscrive à un tel contrat pour être indemnisé en cas d'inondation. Si une telle crue se produit, on peut alors imaginer qu'un organisme indépendant de confiance valide le fait qu'il y a eu une crue , enclenchant ainsi l'exécution du contrat sans que les parties prenantes n'aient quelque action que ce soit à effectuer. On appelle un tel organisme indépendant un oracle, c'est-à-dire un tiers extérieur se portant garant d'une information destinée à enclencher l'exécution du contrat.

2.1.4 Confidentialité

En résumé

Pseudonymat	Anonymat	Blockchains privées
- Contenu des transactions public (montant, parties prenantes) - Identité masquée - Exemple : bitcoin	- Contenu des transactions privées - Exemple : ZCash, Monero	- Utilisateurs identifiables

Si l'on en croît l'imaginaire collectif, bitcoin serait un paradis pour les trafics en tous genres, permettant à des marchés peu scrupuleux de faire florès dans l'anonymat le plus total. On ne peut nier que bitcoin a été associé à plusieurs affaires, comme la plateforme Silk Road, réputée pour vendre des stupéfiants sur le *dark net*, ou encore, plus récemment, la propagation à grande échelle du rançongiciel WannaCry, qui a braqué les projecteurs sur bitcoin, qui était le seul moyen de paiement possible pour les rançons. Cependant, l'anonymat sur bitcoin n'est pas si évident. En effet, bitcoin n'est pas une blockchain anonymisée. Elle se base sur un système de pseudonymat, à savoir que l'intégralité des transactions sont publiques, mais chaque utilisateur apparaît sous la forme d'un pseudonyme, à savoir sa clé publique. Il est ainsi possible de tracer l'intégralité des transactions liées à une clé et, si l'on parvient à lier la clé à une identité réelle, retracer l'historique des transactions réalisées par cette personne à l'aide de cette clé. Bien que cela soit une tâche difficile, il a été prouvé par le passé que c'était tout à fait possible. Ainsi, le FBI est parvenu à tracer nombre de transactions bitcoin réalisées par le fondateur de Silk Road en identifiant sa clé publique.

Certaines blockchains aujourd'hui prétendent aller plus loin dans l'anonymisation des données et proposer un service totalement anonyme. On peut citer l'exemple de Zcash, qui permet de réaliser des transactions totalement anonymes, dont ne sont rendus publics ni les adresses ni le montant. La vérification des transactions se fait grâce à un procédé cryptographique dit *zero-knowledge proof*, qui permet de vérifier la validité des transactions sans pour autant avoir accès à l'intégralité des informations les concernant. Un tel système présente un avantage, qui est d'ailleurs le slogan de la blockchain Zcash : « all coins are created equal ». En effet, l'anonymisation des transactions empêche de tracer l'historique d'une unité de monnaie, contrairement à bitcoin. Ainsi, certains bitcoins, ayant par exemple été utilisés dans des transactions frauduleuses, peuvent être d'une certaine manière marqués par leur histoire, leur conférant une valeur moindre que des bitcoins « propres ». On peut également citer l'exemple de Monero, une autre blockchain anonymisée qui utilise une technologie dite de « signature de cercle », l'idée étant qu'une transaction est signée non par un utilisateur mais par un cercle d'utilisateurs, ce qui permet de noyer en quelque sorte l'identité réelle dans une masse d'utilisateurs.

Enfin, il existe des blockchains dont les transactions ne sont pas anonymisées, à savoir que les utilisateurs impliqués sont tout à fait identifiables. Cela est notamment le cas dans certaines blockchains privées. En effet, si le système a été conçu comme une base de données partagée où

tous les acteurs ont besoin de pouvoir accéder aux données, il n'est pas nécessaire d'anonymiser les transactions, d'autant que la blockchain n'est accessible qu'à un nombre restreint d'acteurs.

2.1.5 Réversibilité des données

En résumé

Blockchains publiques	Blockchains privées
- Irréversibilité théorique des transactions - The DAO : illustration d'un retour en arrière particulièrement complexe	- Réversibilité possible car consensus plus simple - Réversibilité nécessaire dans certains secteurs (banque par exemple)

Rappelons en préambule que l'un des objectifs majeurs du système bitcoin est de garantir l'irréversibilité des transactions, rendant donc impossible d'annuler une transaction une fois celle-ci validée sur le réseau. En pratique, on considère qu'une transaction est totalement validée au bout d'environ une heure, ce qui revient à attendre qu'elle ait été publiée sur la blockchain et que cinq à six blocs aient été validés par la suite. Ceci garantit, à défaut qu'il soit impossible de revenir en arrière, qu'annuler le bloc contenant la transaction nécessite une puissance de calcul considérable, rendant fortement improbable l'hypothèse du développement d'une chaîne plus longue ne contenant pas ce bloc. Ainsi, une fois la chaîne suffisamment longue pour rendre techniquement impossible tout retour en arrière, les transactions peuvent être considérées, *de facto*, comme irréversibles. Evidemment, cette caractéristique est absolument nécessaire pour garantir le bon fonctionnement d'un système de transactions comme bitcoin. On ne pourrait utiliser un moyen de paiement s'il existait un risque qu'une transaction puisse être annulée à n'importe quel moment. Bien entendu, ceci est possible sur un système de paiement traditionnel mais la décision d'annulation est alors entre les mains d'une autorité centrale de contrôle telle qu'une banque ou la justice. Sur un système décentralisé comme bitcoin, dont la substantifique moelle réside justement dans la disparition de toute autorité de contrôle, on ne saurait accepter qu'une transaction puisse être annulée sans pénaliser fortement la confiance que l'on a dans le système.

Pourtant, si des mécanismes d'annulation de transactions existent dans les systèmes de paiement traditionnels, c'est bien évidemment parce qu'il y a un intérêt à ne pas avoir un système trop rigide qui ne supporte aucun retour en arrière. Par exemple, si un compte bancaire est victime d'une attaque informatique qui vise à détourner des fonds, il existe des moyens d'annuler certaines transactions afin de protéger le consommateur. Cette notion de protection est absente d'une blockchain comme bitcoin. Ainsi, même en se tournant vers la justice pour constater l'illégalité d'une transaction, il est techniquement impossible de l'annuler par la suite sur la blockchain sans consensus des mineurs. ethereum en a fait l'amère expérience avec la plateforme *The DAO (Decentralized Autonomous Organization)*. Cette plateforme implémentée sur ethereum avait vocation à lever des fonds auprès de particuliers dans le but de financer des projets d'entreprises, à mi-chemin donc entre *crowdfunding* et *venture capital*. La plateforme était gérée à l'aide de *smart contracts*, qui ont été à l'origine d'un détournement massif de fonds. En effet, le code informatique des *smart contracts* contenaient une faille permettant notamment de répéter des retraits de fonds sans vérifier la disponibilité du solde demandé. Cela a permis à un acteur malveillant de détourner près de cinquante millions de dollars, soit environ 3% de la masse monétaire totale en ethers à l'époque. Cette affaire pose bien évidemment la question de la sécurité des fonds détenus sur une blockchain. Surtout, elle a marqué un tournant incontestable en ce qui concerne la question de la réversibilité des transactions. En effet, à la suite de l'attaque, il a été décidé de revenir sur ces transactions et donc d'opérer pour la première fois l'annulation de transactions sur une blockchain. La difficulté d'une telle opération réside dans le fait qu'elle nécessite le consensus des mineurs, qui

seuls ont le contrôle de la blockchain et de l'écriture des blocs. Or, ce consensus n'a pas été atteint, certains mineurs refusant de revenir en arrière, au nom justement du principe cardinal de non réversibilité des transactions. Cet état de fait a conduit à un *hard fork*, à savoir que la blockchain ethereum s'est scindée en deux blockchains parallèles. Sur la première, les fonds détournés ont été bloqués puis remboursés, alors que la deuxième blockchain (appelée aujourd'hui ethereum Classic) a gardé en l'état les soldes de tous les comptes impactés par l'affaire. Tout détenteur d'ethers détenait alors de la monnaie sur les deux blockchains, mais les cours de l'ether et de l'ether classique se sont effondrés. Aujourd'hui, la valeur d'un ether est d'environ dix fois celle d'un ether classique.

Si cet exemple a mis en lumière l'intérêt d'un système permettant d'annuler des transactions, aucune blockchain publique majeure n'a mis en oeuvre un tel mécanisme. En effet, la décision d'annuler une transaction, à défaut de pouvoir être prise par une autorité de contrôle, ne peut être prise que par les mineurs, et obtenir l'unanimité sur une telle décision est impossible, certains restant farouchement attachés à l'esprit initial de bitcoin, qui prône la réversibilité la plus complète. Cette caractéristique technique fait là-encore émerger une scission majeure entre blockchains publiques et blockchains privées. D'une part, une blockchain privée créée entre quelques acteurs de confiance peut tout à fait aisément trouver des consensus pour réécrire des transactions, sans la difficulté de mettre d'accord un réseau de mineurs ne se connaissant pas. D'autre part, et nous explorerons par la suite plus en détail quelques cas d'usage potentiels, on peut penser utiliser des blockchains dans des secteurs régulés tels que la banque ou l'assurance. Dans une telle hypothèse, il est inenvisageable de faire l'économie de tels mécanismes de retour en arrière, car cela contredirait certains principes cardinaux de protection des consommateurs.

2.1.6 Tiers de confiance

En résumé

bitcoin	Réintroduction du tiers de confiance
- Système décentralisé - Aucune autorité de contrôle	- *Smart contracts* : oracles, garants juridiques - Régulation sur une blockchain privée

Nous terminons notre tour d'horizon général des différentes blockchains avec une dernière propriété extrêmement importante de bitcoin : l'absence de tiers de confiance. L'idée de créer un système monétaire décentralisé va de pair avec celle de développer un système sans aucun tiers de confiance qui serait le garant à la fois de l'argent détenu mais aussi du bon déroulement des transactions. L'idée, donc, est bien de créer un écosystème monétaire sans banque ni autorité de contrôle. Ces tiers de confiance traditionnels sont ici remplacés par des mineurs et par la notion de consensus, en considérant que la majorité des mineurs sont honnêtes et souhaitent le bon fonctionnement du système. Ce qui, finalement, revient à déplacer la confiance depuis des tiers agréés vers le bon sens d'une majorité d'acteurs inconnus. Jusqu'à présent, ce système a prouvé sa fiabilité, sans pour autant que l'on puisse totalement se départir de la notion de confiance.

Pour autant, on voit des blockchains se créer en réintroduisant des tiers de confiance. Revenons par exemple sur la notion de *smart contracts* présentée précédemment et plus précisément sur l'exemple des *cat bonds*. Nous disions que ces contrats pourraient être exécutés lorsqu'un acteur tiers viendrait valider sur la blockchain qu'un événement climatique défini à l'avance s'est bien produit. Cet acteur ne serait pas nécessairement lui-même un utilisateur de la blockchain. Il s'agit bien ici d'un tiers de confiance qui aurait un rôle sur la bonne exécution des contrats. Cependant, il existe une petite nuance par rapport à un système de confiance plus

traditionnel, où par exemple une banque est le garant du système de paiement : ici, le tiers de confiance n'a aucun contrôle sur le bon fonctionnement du système en lui-même, il est uniquement une source d'information. De plus, contrairement à une banque, il n'est pas lui-même un acteur impliqué du système dans lequel il aurait des intérêts. A défaut de garantir sa probité, cela constitue au moins un gage qu'il n'a pas d'intérêt personnel à fournir de mauvaises informations. De manière plus générale, et nous y reviendrons un peu plus tard, ces *smart contracts* présentent des problèmes légaux. Un contrat d'assurance français, par exemple, doit contenir un certain nombre de clauses de protection des consommateurs. A ce titre, un *smart contract* ne saurait être considéré, d'un point de vue juridique comme un contrat d'assurance. Si l'on veut pouvoir inscrire ces contrats dans un cadre légal conventionnel, l'une des pistes pourrait être d'attacher à chaque contrat électronique un contrat « littéraire », rédigé bien que dématérialisé, qui pourrait être validé d'un point de vue légal par un tiers de confiance comme un juge ou un avocat.

Enfin, si l'on s'intéresse aux blockchains privées, il apparaît que la question de la confiance est bien différente de celle qui se pose sur les blockchains publiques. Comme nous l'avons déjà dit, une blockchain privée résulte la plupart du temps soit de la mise en place d'un projet interne à une entreprise, soit d'une volonté commune entre plusieurs acteurs de mettre en oeuvre un système partagé. Ces acteurs se connaissent, ont des intérêts convergents et ont donc toutes les raisons de se faire confiance. Il en résulte des mécanismes de consensus simplifiés. Nul besoin ici d'un système débarrassé de tous tiers de confiance car là n'est pas l'intérêt du système. On peut d'ailleurs parfaitement imaginer des tiers de confiance ayant des rôles spécifiques sur des blockchains privées. Imaginons ainsi un système bancaire où le back-office serait basé sur des blockchains. La forte régulation et les nécessaires mécanismes de protection des consommateurs pourraient impliquer l'intervention de tiers de confiance, tels que la justice, pour pouvoir éventuellement invalider des transactions.

2.1.7 Synthèse et sémantique

Nous avons donc exploré quelques grandes évolutions de la technologie blockchain par rapport à l'esprit initial de bitcoin. Nous avons commencé notre exploration par une distinction fondamentale entre blockchains publiques et blockchains privées. Il s'agit sans doute de la distinction la plus discriminante, qui fait émerger aujourd'hui deux familles technologiques assez différentes.

D'un côté, donc, les blockchains publiques, comme bitcoin ou ethereum pour ne citer que les deux plus importantes. Elles sont majoritairement destinées à héberger des crypto-monnaies ou des *tokens* de manière plus générale, certaines ajoutant à cela une surcouche applicative comme l'implémentation de *smart contracts*, qui existent tant sur bitcoin que sur ethereum, bien qu'ils soient beaucoup plus développés sur cette dernière. Si différents systèmes de preuve peuvent être envisagés, tous ont un même objectif : parvenir à une forme de consensus sur la validité des blocs, en considérant qu'une majorité du réseau est honnête. La preuve de travail est aujourd'hui le système de référence, malgré ses limites. Sur ces blockchains, les données sont irréversibles une fois validées sur la blockchain. Revenir en arrière demande un consensus qu'il paraît difficile à trouver et la seule solution adoptée jusqu'à présent a été un *hard fork*, qui n'a rien d'une solution satisfaisante. Enfin, le principe de ces blockchains consiste à créer un système totalement décentralisé, contrôlé par un réseau pair-à-pair sans autorité de contrôle ni tiers de confiance (sauf éventuellement comme source externe d'information mais pas comme garant du bon fonctionnement du système). Même si ces différentes blockchains peuvent différer sur certains points (système de preuve, confidentialité, fonctionnalités, …), elles n'en demeurent pas moins une famille de technologies assez cohérente.

Cette famille de technologies semble pour autant assez éloignée de celle des blockchains privées. Ici, pas de minage ou de forgeage mais des systèmes de vote simplifiés, car nul besoin de mécanismes de consensus complexes lorsque l'on se fait confiance. La différence majeure est sans

doute là : d'un côté, la foi en le bon sens de la majorité pour éliminer toute dépendance à un acteur central ; de l'autre, des acteurs se faisant confiance qui ont des intérêts communs à créer un système partagé. L'objectif est radicalement différent, et les technologies également. Exit, donc, les mécanismes complexes de consensus, loin des blockchains publiques, dont l'essence même repose sur l'idée du consensus et du contrôle distribué. Ces blockchains, loin de l'esprit bitcoin, n'ont pas de raisons de faire de l'irréversibilité un principe de confiance, ou de refuser toute idée de tiers de confiance. Ainsi, ces systèmes s'apparentent plus à des bases de données partagées et distribuées, avec comme avantage une certaine robustesse offerte par le chaînage des données et les mécanismes cryptographiques sous-jacents. Certains leur refusent donc l'appellation de blockchains et préfèrent les considérer comme des DLT (*Distributed Ledger Technology*), c'est-à-dire des technologies de registres distribués. L'appellation fait sens et permet de distinguer deux familles de technologies aux caractéristiques finalement bien différentes.

2.2 Panorama d'applications potentielles

Nous nous proposons désormais de dresser un panorama assez général de quelques cas d'usage potentiels des blockchains publiques et des DLT. Nous reviendrons par la suite de manière plus détaillée sur quelques applications et exemples qui nous paraissent particulièrement pertinents.

2.2.1 Quelques usages des blockchains publiques

En résumé

Crypto-monnaies

- Système monétaire sans autorité centrale

Smart contracts

- Exemple de l'assurance
- Gestion de l'identité et des données personnelles

Plateformes bifaces

- Désintermédiation
- Réduction voire suppression des frais de transaction
- Absence de service client

Registres

- Registre robuste et partagé
- Exemple du cadastre

Le premier usage des blockchains publiques, tant d'un point de vue historique que de celui des applications actuelles, est sans aucun doute celui des crypto-monnaies. La blockchain est initialement née avec bitcoin, dont l'objectif consistait à créer un système monétaire parallèle totalement décentralisé, ne nécessitant ni autorité de contrôle (par exemple, une banque centrale en charge de l'émission de la monnaie) ni tiers de confiance en charge du bon fonctionnement du système (tel que les banques de dépôt, chargées de stocker la monnaie détenues par les personnes et de réaliser les transactions monétaires). Ceci a été rendu possible par la création d'un réseau pair-à-pair où chaque nœud possède une copie du registre des transactions. La fiabilité du système est portée par le mécanisme de consensus, qui garantit que, si le réseau est composé majoritairement de nœuds honnêtes, la chaîne principale sera composée de transactions valides.

Une autre application des blockchains publiques que l'on voit se développer concerne l'implémentation de *smart contracts*. Nous avons déjà évoqué ce sujet en citant l'exemple des *cat bonds*, mais il est possible d'envisager de multiples applications. On a ainsi vu se créer un projet destiné à assurer les passagers contre des retards dans les trajets en avion. L'idée consiste à souscrire un contrat permettant une indemnisation en cas de retard. Ces contrats sont placés sur une blockchain, et le système est connecté directement aux panneaux d'affichage des aéroports. Un

retard peut donc être remboursé automatiquement puisqu'il existe un accès direct à l'état du trafic aérien. On remarque alors que l'on réintroduit par là-même l'idée d'un tiers de confiance, appelé oracle, fournissant une information pour enclencher l'exécution du contrat, à l'image de l'aéroport qui partagerait les données de décollage de ses vols. Cependant, ce tiers de confiance n'est en rien impliqué dans la transaction et n'y a aucun intérêt, se contentant de fournir une information. On peut également utiliser les *smart contracts* comme une couche de protection au-dessus d'un système monétaire. Ainsi, on peut imaginer assurer une transaction grâce à des *smart contracts*, l'intégralité du processus se passant sur la blockchain, sans besoin d'autorité quelconque. Comme la blockchain permet un système monétaire sans banques, les *smart contracts* peuvent implémenter des systèmes d'assurance sans compagnies d'assurance. On trouve déjà des *smart contracts* très développés sur ethereum, le langage informatique étant Turing-complet, ce qui permet la rédaction d'objets informatiques complexes. Bitcoin implémente également un système de *smart contracts*, moins développé.

On peut également penser que la blockchain puisse permettre le développement d'applications collaboratives. Citons par exemple OpenBazaar, qui s'apparente à un site comme leboncoin.fr, en offrant une plateforme d'échange entre particuliers. La différence majeure se situe dans les systèmes sous-jacents à chacune des deux technologies. Ainsi, leboncoin.fr est une plateforme web qui gère les transactions pour les utilisateurs. À l'inverse, OpenBazaar est un système pair-à-pair qui permet d'interconnecter directement les utilisateurs les uns aux autres. Pour utiliser le service, un utilisateur doit charger un logiciel pour intégrer un réseau sur lequel il est connecté directement aux autres utilisateurs. Les transactions se font alors sur la blockchain bitcoin, réduisant considérablement les frais de transaction par rapport à certaines plateformes de commerce en ligne plus traditionnelles. De manière générale, on peut imaginer des blockchains offrant des fonctionnalités similaires à certaines plateformes bifaces existantes, telles qu'Airbnb ou Uber. Certains vont même jusqu'à évoquer l'idée qu'un système tel qu'Airbnb pourrait être totalement dématérialisé. L'idée sous-jacente serait de mettre en œuvre des systèmes basés sur des *smart contracts* complexes qui remplaceraient certaines interactions humaines. Par exemple, est évoquée l'idée d'intégrer un système aux portes des logements loués permettant de les déverrouiller à l'aide d'un QR code, enclenchant automatiquement le paiement de la location sans que le propriétaire ait besoin d'être présent. Cependant, cela nous semble tout à fait hypothétique, nombre de situations étant difficiles à automatiser avec des *smart contracts*. Par exemple, comment gérer un dysfonctionnement du système intégré à la porte ou, pire encore, un cas de dégradations causées par le locataire ? Qui viendrait enclencher un *smart contract* permettant au propriétaire d'être dédommagé et qui paierait les indemnités ? L'intérêt d'une plateforme intermédiaire réside en effet également dans le fait d'avoir un service client permettant de gérer les conflits, et donc un intermédiaire vers qui se tourner en cas de problème. Cependant, l'intérêt d'un système décentralisé comme une blockchain pour remplacer des plateformes bifaces réside dans le fait qu'il peut être utile de se passer d'une plateforme centrale gérant les transactions. En particulier, cela permet de ne plus avoir à faire confiance à un service de transactions, mais surtout d'offrir un service sans intermédiaire et donc sans frais de transactions. Si l'on peut imaginer que des frais puissent être payés pour récompenser les mineurs, ils paraissent pouvoir être considérablement réduits comme pour OpenBazaar. Il serait également envisageable de créer des systèmes sur lesquels les utilisateurs eux-mêmes seraient les nœuds du réseau de minage. Ainsi, si les mineurs ne sont autres que les utilisateurs eux-mêmes, il n'y aurait pas de frais à payer mais il leur serait simplement demandé de consacrer un peu de puissance de calcul pour faire fonctionner le système en échange du droit à pouvoir l'utiliser.

Enfin, il nous paraît possible d'utiliser des blockchains pour tenir des registres publics accessibles à tous. Si bitcoin en est un exemple comme registre de transactions, on peut imaginer d'autres exemples de registres de manière plus générale. L'une des applications envisageables serait celle de la tenue des cadastres, à savoir le registre des terrains fonciers et des titres de propriété. Ces données pourraient être stockées sur une blockchain avec un double intérêt. D'une part, un tel

système serait robuste, extrêmement difficile à falsifier, ce qui pourrait amener une évolution majeure dans certains pays où de tels registres ne sont pas tenus correctement voire sont falsifiés du fait de la corruption. D'autre part, toutes les transactions sur une blockchain étant horodatées et les blocs dans l'ordre chronologique, il serait très facile de déterminer l'antériorité d'un titre de propriété par rapport à un autre et ainsi résoudre d'éventuels conflits quant à la possession d'un terrain.

2.2.2 Quelques applications des DLT

En résumé

Registres de transactions

- Système bancaire
- Transfert d'actifs

Supply chain

- Améliorer la traçabilité

Registres de biens

- Exemple d'Everledger

En ce qui concerne les blockchains privées, ou DLT, les applications envisageables paraissent similaires mais pourraient avoir lieu dans des domaines ou à des échelles bien différentes. Ainsi, on pourrait imaginer utiliser des DLT pour tenir des registres de transactions dans les domaines financiers ou assurantiels. Notons par exemple que le système SWIFT, qui gère aujourd'hui les transactions bancaires au niveau mondial, est vieillissant et que nombre de banques envisagent de le remplacer. On pourrait ainsi tenir le registre des transactions bancaires sur une blockchain privée partagée entre les banques. Un consortium de banques, R3, avait été créé pour réfléchir à l'utilisation d'une blockchain à cet effet, mais ces réflexions n'ont jusqu'à présent pas été concluantes. Plus généralement, des DLT pourraient être utilisés pour tenir des registres de transactions financières. Nous présenterons un peu plus tard l'exemple de FundsDLT dans la partie 3.1.2, qui opère dans le secteur des actifs financiers. Cet exemple illustre également l'intérêt d'un tel système pour résoudre des problèmes de désintermédiation. En effet, en mettant en place un système décentralisé pair-à-pair, on permet la mise en interaction entre des acteurs qui n'étaient pas nécessairement connectés directement, favorisant la diminution des processus intermédiaires, potentiellement sources de coût et d'inefficacité.

Est également évoquée la possibilité d'utiliser des DLT au sein des chaînes d'approvisionnement de certaines usines. Plusieurs entreprises ont communiqué autour du sujet même si peu d'applications semblent aujourd'hui fonctionnelles. L'idée d'utiliser des DLT permettrait d'améliorer la traçabilité de certains produits ou encore de lutter contre la contrefaçon grâce à un système robuste et décentralisé, où les informations sont partagées entre les acteurs.

Enfin, si l'on évoquait la possibilité de tenir des registres sur des blockchains publiques, cette idée s'applique également aux blockchains privées, au-delà du secteur financier et des registres de transactions. Citons ainsi l'exemple d'Everledger, une blockchain tenant un registre des diamants au niveau mondial. L'intérêt d'un tel système consiste à avoir un système robuste et fiable permettant de tracer les diamants afin de lutter contre certains trafics.

Ainsi, dans ces différentes applications, l'intérêt principal est souvent d'avoir une technologie tout à fait robuste, difficile à falsifier, mais également décentralisée et présentant des intérêts en termes de désintermédiation. Pour autant, la blockchain n'est pas la solution miracle à tous les problèmes et il nous semble aujourd'hui que beaucoup de projets blockchains sont brandis comme des gages de modernité, au même titre que la volonté de développer des projets de *big data* ou de *cloud*. Ces termes très à la mode sont vendeurs mais il paraît nécessaire d'être prudent pour

séparer le bon grain de l'ivraie. La blockchain aura sans doute des applications utiles mais n'est pas l'alpha et l'oméga de toute entreprise. En particulier, il est envisageable que les applications les plus pertinentes soient des applications internes à certaines entreprises, permettant d'optimiser le back-office, sans que cela n'ait d'impact ou de visibilité auprès du grand public.

2.3 Limites des DLT

Ainsi, les DLT peuvent présenter un intérêt indéniable dans certains secteurs où il peut être utile de se munir d'un système robuste de registre ou de base de données, qui soit partagé entre différents acteurs. Cependant, il apparaît que ces systèmes présentent également des limites, malgré l'emballement médiatique qui peut exister autour d'eux.

2.3.1 Sécurité des DLT

La première limite des blockchains privées réside sans doute dans la sécurité de ces systèmes. En soi, une blockchain n'a aucune raison de présenter plus de failles de sécurité qu'un autre système tel qu'une base de données plus classique. Le développement de blockchains privées fera sans doute émerger des systèmes plus ou moins sécurisés, de manière similaire à n'importe quelle autre technologie. En revanche, la blockchain présente un risque supérieur dans le sens où il s'agit d'une technologie décentralisée et partagée. Le fait que tous les acteurs détiennent une copie de la blockchain augmente les risques de piratage et pose une question de cyber-sécurité. La sécurité d'un système informatique étant égale à celle de son maillon le plus faible, il suffit que l'un des acteurs n'ait pas assez sécurisé son système d'information pour que la blockchain devienne vulnérable. Une telle technologie paraît ainsi moins sécurisée qu'une base de données hébergée par exemple chez un prestataire externe spécialisé.

2.3.2 La question de la confiance

Au-delà du risque de sécurité, il convient de noter que se pose sur une blockchain privée la question de la confiance. Plus qu'une limite, il s'agit de constater que les blockchains privées ont un esprit bien différent de leurs homologues publiques. La force majeure de bitcoin réside dans la capacité à avoir mis en place un système sans autorité de contrôle et sans confiance aucune entre les acteurs. Seule la force du nombre garantit la robustesse du réseau, car un acteur malhonnête, noyé dans le réseau des mineurs, ne peut agir de manière illicite qu'en détenant la majorité de la puissance de calcul, ce qui paraît improbable. Les blockchains privées, au contraire, fonctionnent entre des acteurs qui ont des intérêts communs et donc une incitation naturelle à se faire confiance. L'esprit est radicalement différent et pose la question de savoir si le terme de blockchain est bien adapté pour désigner ces systèmes, alors que l'absence de confiance est un élément cardinal dans le système bitcoin. D'un point de vue fonctionnel, cette question de la confiance peut être une limite si apparaissent des intérêts divergents entre les acteurs, où des groupes se forment qui soient en capacité de prendre le contrôle de la blockchain. En effet, les blockchains privées sont naturellement partagées sur un réseau bien plus restreint que les blockchains publiques. Par conséquent, le poids d'un acteur dans la validation des transactions est mécaniquement plus important que sur un système ouvert. Si des intérêts divergents apparaissent, il n'est donc pas à exclure que le système devienne non fonctionnel, le poids d'un groupe d'acteurs « divergents » pouvant leur permettre potentiellement de bloquer certaines transactions pourtant licites, surtout avec des mécanismes de vote voire d'unanimité.

2.3.3 Utilité réelle du système ?

Enfin, il nous semble aujourd'hui que certaines blockchains privées sont développées essentiellement à des fins de communication. Nous évoquions la volonté de certains d'apparaître en phase avec les enjeux du monde numérique, en abusant parfois des termes techniques les plus à la mode comme *big data*, *machine learning*, *cloud computing*, on encore, donc, *blockchains*. Cet effet de mode pousse certaines entreprises à vouloir à tout prix développer des projets blockchains à des fins de communication, sans en avoir réellement l'utilité. On voit également fleurir des projets de start-ups qui parviennent à lever des fonds, sans doute parce que certains fonds de venture capital craignent de passer à côté d'une révolution majeure, alors même que les projets qu'ils financent ne semblent pas nécessairement en mesure de devenir des applications majeures de la blockchain. Cet engouement ne sert pas nécessairement la technologie, dont les réelles potentialités semblent parfois masquées par le nuage de fumée assez opaque qui entoure le terme, du fait du développement de multiples projets finalement assez creux.

On peut également noter que la blockchain a un effet d'accélérateur à certains niveaux. La simple utilisation du mot et de la technologie aux sein de certaines entreprises semble favoriser le développement de projets qui n'auraient peut-être jamais pu évoluer avec des moyens plus traditionnels. Nous avons pu ainsi échanger avec certains chefs de projet, qui ont mentionné que, si la blockchain n'apparaissait pas nécessairement comme le système le plus adapté, l'utilisation de cette technologie, par l'engouement qu'elle suscite auprès des décideurs, a permis de développer des projets de manière beaucoup plus rapide, plus flexible et moins coûteuse. Si l'on peut se réjouir que la blockchain favorise ainsi la modernisation et la numérisation de certains secteurs, on peut déplorer que, dans certains cas, elle y contribue plus par l'emballement qu'elle suscite que par son potentiel technique, d'autant qu'elle se substitue alors à des systèmes qui seraient sans doute plus adaptés.

2.3.4 Synthèse

Les DLT apparaissent comme des systèmes robustes, présentant un véritable intérêt par le fait qu'ils soient partagés sur des réseaux pair-à-pair, permettant notamment de connecter des acteurs et faire de la désintermédiation ou encore de mettre en place des systèmes de registre ou de bases de données sur lesquels un acteur ne pourrait saisir des données de manière unilatérale mais aurait besoin d'un consensus de ses pairs.

Pour autant, ces systèmes posent la question du risque cyber, du fait que les données sont partagées entre plusieurs acteurs, multipliant ainsi le risque de piratage. Le partage des données nécessite également une certaine confiance entre les acteurs, ce qui pourrait mettre en péril le système en cas d'intérêts divergents. Enfin, les blockchains privées semblent victimes d'une forme d'engouement qui favorise l'émergence de projets pas toujours pertinents. Certains acteurs semblent, à des fins de communication, vouloir faire du développement d'un projet blockchain un but en soi, plutôt qu'un moyen destiné à implémenter un système répondant à un besoin identifié. Pour partager un registre entre plusieurs utilisateurs de confiance des solutions plus simples existent. Il en va de même si un unique acteur est entièrement maître du système.

2.4 Limites des blockchains publiques

Les blockchains publiques, quant à elles, présentent également de multiples limites, tant dans l'aspect technique que dans l'esprit qui les anime. L'absence de toute gouvernance centralisée est un vrai frein au déploiement de tels systèmes sur certains secteurs, qui posent également des questions de souveraineté et de protection des utilisateurs. D'un point de vue technique, le coût énergétique et la fiabilité des blockchains publiques apparaissent comme de réelles limites, tout

comme certaines caractéristiques techniques actuelles (temps de latence, volume de transactions, …).

2.4.1 Coût du système et consommation énergétique

En résumé	
Consommation énergétique - Preuve de travail : calcul de *hashs* - Calculs non productifs en eux-mêmes	**Estimation de la consommation** - Une dizaine de milliards de kilowattheures par an sur bitcoin - Équivalent à la production d'une tranche de centrale nucléaire - Équivalent à la consommation électrique de la Lituanie

Du fait du mécanisme de la preuve de travail, bitcoin apparaît aujourd'hui comme un gouffre énergétique. Pour rappel, ce mécanisme de consensus consiste à appliquer une fonction de hachage à un bloc auquel on adjoint un nonce, c'est-à-dire une chaîne de caractères aléatoire, et ce de manière répétée afin de trouver un nonce qui permettra d'obtenir un *hash* respectant une certaine propriété mathématique. Concrètement, il s'agit donc de faire fonctionner un processeur en continu pour lui faire calculer des *hashs* jusqu'à parvenir à valider un bloc. Le mineur prouve ainsi qu'il a fourni un « travail » informatique. Plus il dispose de puissance de calcul, plus il est en mesure de valider des blocs et donc de percevoir une récompense. Le système offre ainsi une incitation à fournir de la puissance de calcul pour faire fonctionner la blockchain. Pour autant, ce « travail » a un coût, car faire tourner des processeurs est un procédé gourmand en énergie. Cette consommation en énergie, si elle est nécessaire pour soutenir le mécanisme de la preuve de travail et donc offrir un système fiable sur lequel les mineurs ont des intérêts à publier des blocs licites, peut tout de même s'apparenter à une gabegie énergivore dans le sens où cette consommation est, en soi, totalement improductive. En effet, les *hashs* calculés ne présentent, en eux-mêmes, aucun intérêt mais ne servent qu'à prouver, dans un sens, que le mineur est prêt à dépenser de l'énergie et en payer le coût pour parvenir à valider un bloc. Le résultat de la fonction de hachage importe finalement assez peu, ce qui compte étant simplement la capacité à effectuer le calcul et non son résultat.

Certains sites ont proposé diverses estimations de la consommation en électricité nécessaire pour faire fonctionner la blockchain bitcoin. Citons par exemple le calcul effectué par le site bitcoin.fr (13), qui estime la consommation de bitcoin entre 2,15 et 5,4 milliards de kilowattheures par an, soit une puissance comprise entre 0,25 et 0,62 gigawatts. A titre de comparaison, si l'on se réfère aux données fournies par l'EIA (*Energy Information Administration*) quant à la consommation d'électricité en 2014 (14), une consommation de 2,15 milliards de kilowattheures est équivalente à la consommation électrique totale du Gabon, alors que le Honduras a une consommation proche des 5,3 milliards. Le calcul de la consommation électrique du minage sur bitcoin est fondé sur trois valeurs : la consommation du matériel de minage, sa puissance de calcul et le nombre de *hashs* calculés sur le réseau bitcoin, estimé à environ deux millions cinq cent mille terahashs par seconde. Cette estimation prend en compte le nombre de *hashs* calculés en moyenne au début de l'année 2017. Or, si l'on observe l'évolution du nombre de *hashs* (cf. encart), on constate que celle-ci suit une croissance exponentielle et atteint au mois de juin 2017 une moyenne comprise entre cinq millions et cinq millions et demi de terahashs par seconde. L'estimation de l'énergie consommée a donc doublé en six mois et devrait continuer à augmenter. A titre de comparaison, une tranche nucléaire produit en moyenne environ huit milliards de kilowattheures par an, ce qui semble de l'ordre de grandeur de la consommation actuelle du minage sur bitcoin. Une consommation d'une

dizaine de milliards de kilowattheures par an est équivalente à la consommation d'un pays comme la Lituanie ou le Paraguay.

Le calcul prend en compte deux matériels de minage différents : le *AntMiner S7*, qui consomme dix watts pour une puissance de calcul de 4,86 terahashs par seconde ; et le *AntMiner S9*, qui consomme 1 375 watts pour une puissance de calcul de quatorze terahashs par seconde. On peut ainsi estimer la puissance requise par chacune des deux machines pour effectuer la totalité des calculs de *hashs* sur le réseau bitcoin, la fourchette étant donnée par une estimation pour chacun des deux matériels. Ces deux matériels étant les plus utilisés et les plus récents de la gamme, l'estimation paraît assez fiable.

Encadré 3 : Consommation des matériels

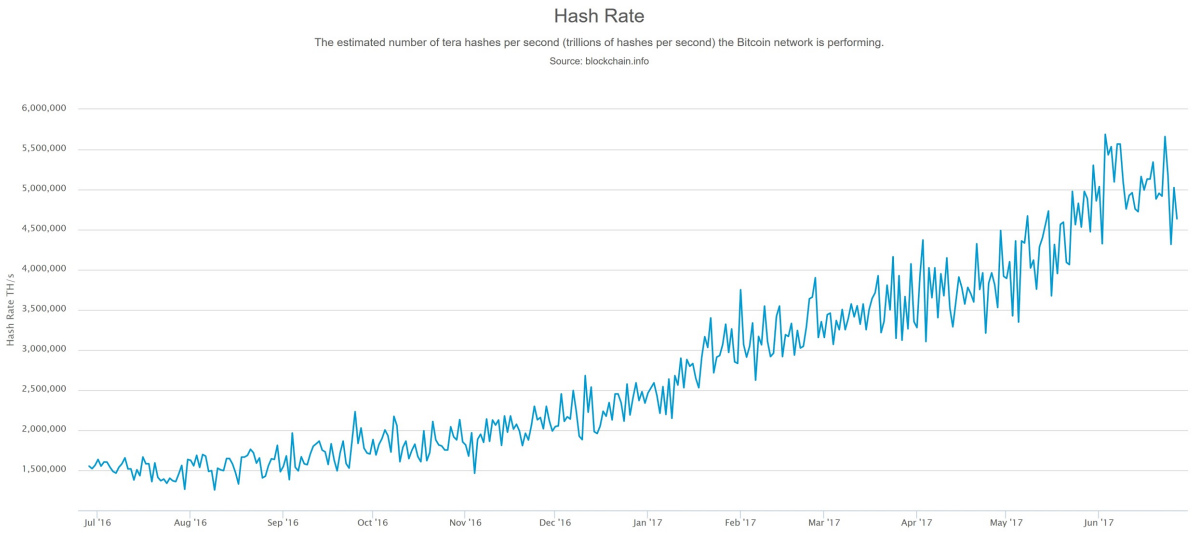


Figure 2 : Evolution de la puissance de calcul du réseau bitcoin (15)

2.4.2 Cadre légal

En résumé

***Smart contracts* et assurance**

- Quelle expertise pour rédiger de tels contrats ?
- Question de la protection des consommateurs
- Inapplicable à un domaine régulé en l'absence de tiers de confiance juridique

Crypto-monnaies

- Monnaies virtuelles non reconnues par les États
- Actifs de spéculation, forte volatilité
- Peu attractif pour le grand public

Les blockchains et certaines de leurs applications présentent également des limites d'un point de vue réglementaire. Citons tout d'abord l'exemple des *smart contracts*, souvent évoqués comme de possibles révolutions, notamment sur le marché de l'assurance. Les plus enthousiastes n'hésitent pas à penser que les compagnies d'assurance sont vouées à disparaître, remplacées par des contrats automatisés sur des blockchains. Notons une première limite à cette affirmation, qui

est qu'une compagnie d'assurance est tout de même une entreprise qui accepte de prendre le risque de devoir vous indemniser en cas de problème. Même si l'assurance venait à être révolutionnée par les blockchains, il demeurerait nécessaire de trouver une partie extérieure prête à assumer un tel risque. Si l'assurance collaborative est évoquée, avec un système où chaque souscripteur cotiserait et participerait ainsi à constituer une caisse destinée à payer les indemnisations, ceci reste tout de même assez théorique. De plus, les contrats d'assurance sont des objets juridiques complexes, qu'il paraît difficile d'automatiser complètement. D'une part, la rédaction d'un tel contrat nécessite une expertise et une technicité forte, que seuls des juristes spécialisés sont en mesure d'avoir. Pour s'inscrire dans le cadre légal, la rédaction de *smart contracts* dans le domaine de l'assurance n'échapperait pas à une rédaction supervisée par un expert juridique, ce qui pourrait s'apparenter à l'intervention d'une forme de tiers de confiance. De plus, évaluer un dommage peut être une tâche difficile qui nécessite l'intervention d'un expert, capable d'estimer le préjudice de manière plus nuancé qu'un contrat automatisé dont l'analyse serait plus binaire. A ce titre, si l'on peut envisager automatiser des contrats simples tels que les *cat bonds*, la majorité des contrats d'assurance nous semble trop complexes et trop soumis à l'interprétation humaine pour considérer qu'ils puissent être automatisés. Enfin, il nous paraît nécessaire de rappeler que l'assurance est un domaine régulé où les contrats sont soumis à une réglementation stricte. En particulier, ils doivent contenir un certain nombre de clauses destinées à protéger les consommateurs. Pour garantir la validité juridique d'un *smart contract* d'assurance, il faudrait donc à la fois que les blockchains publiques soient reconnues comme des systèmes fiables par le régulateur et que lesdits contrats soient reconnus comme de vrais contrats d'assurance, ce qui impliquerait qu'ils s'inscrivent dans un cadre légal bien défini. Aucune des deux conditions ne semblent remplies aujourd'hui. A titre d'exemple, l'anonymisation ou la pseudonymisation de certaines blockchains est un frein majeur, tant il est inenvisageable qu'un contrat d'assurance passé entre deux entités n'ayant aucun moyen de s'identifier puisse être reconnu légalement, ne serait-ce que pour garantir la possibilité d'une action en justice en cas de non application du contrat. Une solution qui nous paraît envisageable nous paraît être de lier à chaque *smart contract* un contrat rédigé traditionnel qui permettrait de réintroduire le contrat dans le cadre réglementaire existant. Cela nécessiterait en revanche de réintroduire des tiers de confiance juridiques tels que des juges ou des avocats, afin de garantir la légalité des contrats. Il apparaît délicat aujourd'hui qu'une telle solution s'applique, tant certains mineurs, très attachés à l'esprit insufflé par bitcoin, semblent réticents à accepter toute idée d'un tiers de confiance ou d'une autorité externe.

Un autre exemple de limite légale concerne le statut des crypto-monnaies. Celles-ci ne sauraient être considérées comme des monnaies au sens légal du terme. En particulier, elles ne sont émises par aucun État, n'ont aucun pouvoir libératoire (à savoir qu'un créancier peut exiger un paiement en espèces et, symétriquement, ne peut s'y opposer), ne permettent pas de payer l'impôt ou encore ne bénéficient d'aucune garantie d'État. Ces limites en font des moyens de paiement limités et risqués pour les utilisateurs. Par ailleurs, elles sont extrêmement volatiles du fait notamment d'une forte spéculation, ce qui en fait un objet spéculatif intéressant et risqué mais surtout un moyen de paiement peu attractif. On observe ainsi des cycles de croissance et décroissance très fréquent et de grande amplitude. Une monnaie comme bitcoin est également non fongible, c'est-à-dire que tous les bitcoins, d'une certaine manière, ne se valent pas. En effet, il est aisé de reconstituer l'histoire d'un bitcoin particulier, qui n'existe sur la blockchain que sous la forme d'un historique de transactions. Ainsi, il est facile de tracer les bitcoins ayant servis à des transactions notoirement illégales, ce qui peut rendre ces bitcoins moins attractifs que des bitcoins « propres ». Notons que certaines blockchains implémentent des crypto-monnaies fongibles, notamment par l'anonymisation des transactions. Cependant, il nous apparaît que les crypto-monnaies ne seront jamais reconnues comme des monnaies pleines et entières car elles ne sauraient tomber sous le contrôle d'un État sans perdre tout ce qui en fait la substantifique moelle. Pour autant, cela ne signifie pas qu'elles ne seront jamais des systèmes de paiement utilisés par le grand public. Cependant, nous en doutons fortement, tant les limites qui les entourent nous

semblent importantes. Tout d'abord, leur utilisation est aujourd'hui restreinte à quelques marchés de niche et elles ne sont acceptées comme moyen de paiement que très rarement. De plus, leur forte volatilité est un frein à l'investissement. Surtout, il nous semble qu'un citoyen privilégiera toujours une monnaie d'état (tant que celle-ci reste suffisamment forte mais il paraît peu probable que toutes les monnaies mondiales se dévaluent conjointement tant qu'il demeurera des États de droit stables et fiables) avec toutes les protections qu'elle garantit à un système un peu anarchique reposant qui plus est sur une technologie mal comprise et assez opaque.

2.4.3 Fiabilité du système

En résumé

Attaque des 51%

- Si plus de la moitié de la puissance de calcul est détenue par des acteurs malhonnêtes
- Attaque peu probable car les mineurs ont intérêt à garder le système fiable
- Coût d'une telle attaque estimé à quelques centaines de millions de dollars

Attaque des 25% ou des 33%

- Permet à un groupe d'acteurs d'augmenter ses gains en publiant plus de blocs
- Nécessairement efficace avec un tiers de la puissance de calcul

Attaque par déni de service

- Inonder le réseau avec des transactions volontairement lourdes à traiter
- Attaques déjà observées sur ethereum

Pérennité du système

- Diminution de la récompense et de l'incitation au minage
- Risque de désertion de mineurs en cas d'inadéquation entre coût du minage et récompense

SI bitcoin apparaît comme un système fiable, il n'en présente pas moins des limites. Rappelons que l'idée initiale consistait à mettre en oeuvre un système permettant de valider des transactions dans un environnement sans confiance, en l'absence d'une autorité de contrôle. Cela est permis par le développement d'un mécanisme de consensus au sein d'un réseau de mineur, en considérant que la chaîne de blocs principale est celle sur laquelle travaille la majorité des mineurs ou, du moins, la majorité de la puissance de calcul. Si la majorité de la puissance de calcul est détenue par des mineurs honnêtes, alors les transactions validées sur la chaîne ont toutes les raisons d'être licites. Pour autant, il existe bien un risque qu'un acteur malveillant puisse prendre le contrôle du système. Ainsi, si un mineur ou un groupe de mineurs possède plus de la moitié de la puissance de calcul, il pourra valider des blocs plus rapidement que le reste du réseau, créant ainsi la chaîne la plus longue qui sera donc considérée comme la chaîne principale. Ce risque, s'il peut paraître improbable, n'en est pas moins réel. Un argument qui vient relativiser ce risque est qu'un mineur, par le fait qu'il perçoit des bitcoins lorsqu'il valide un bloc, est un détenteur de bitcoins qui a tout intérêt à ce que le système fonctionne correctement pour ne pas risquer que ses fonds soient dévalués. Pour autant, il n'est pas totalement inenvisageable d'imaginer qu'un acteur ait un intérêt supérieur à faire s'effondrer le système, malgré le coût que représenterait la puissance de calcul nécessaire à prendre le contrôle de la chaîne. Imaginons dans un exercice de politique fiction un État au sein duquel bitcoin serait devenu une valeur refuge dévaluant fortement la monnaie nationale. Il pourrait être intéressant pour cet État de faire tomber le système, quitte à en payer le coût. Ce coût apparaît difficile à estimer de manière exacte mais on peut en donner une estimation. Nous proposons un calcul un peu simpliste, qui chiffre le coût d'une telle attaque à quelques centaines de millions de dollars, ce qui est évidemment une somme extrêmement importante, que seul un acteur tel qu'un État puissant pourrait investir.

Des chercheurs de l'université Cornell ont même montré qu'il était possible de mener une attaque contre la blockchain avec seulement 33% de la puissance de calcul. Il ne s'agit pas ici de prendre le contrôle à proprement parler en publiant des blocs plus vite que le reste du réseau. En revanche, il existe une stratégie, dite de *selfish mining*, qui permet à un groupe de mineurs d'augmenter sa probabilité de gains par rapport à des acteurs honnêtes. Cette stratégie consiste, pour un groupe de mineurs, à ne pas publier immédiatement un bloc que l'on vient de miner. Ainsi, le reste des mineurs continue à travailler sur une chaîne de blocs de plus petite taille, en minant sur une chaîne ayant un risque de ne jamais devenir la chaîne de référence, ce qui revient à dépenser de la puissance de calcul de manière inutile, pendant que les mineurs « égoïstes » travaillent sur la chaîne qui deviendra la chaîne de référence. S'il peut apparaître difficile pour un mineur seul de réunir le tiers de la puissance de calcul, des groupements pourraient se créer entre des mineurs ayant un intérêt à mener ensemble une telle stratégie, qui serait plus lucrative à condition de s'entendre. Cela nécessiterait cependant de rendre l'attaque plus ou moins publique pour attirer autant de mineurs que possible et atteindre le seuil des 33%, ce qui peut être un frein à l'efficacité d'une telle stratégie.

Si l'on considère aujourd'hui qu'environ cinq millions de terahashs sont calculés sur bitcoin chaque seconde, il serait nécessaire, pour prendre le contrôle de la Blockchain, de fournir une puissance de calcul équivalente pour détenir un peu plus de la moitié de la puissance de calcul totale. Considérant qu'un *AntMiner S9* permet de calculer quatorze terahashs par seconde, il faudrait donc investir dans l'achat d'environ 360 000 machines. On les trouve actuellement sur Internet à un prix d'environ 2 000$ sur Amazon, mais nous sommes parvenu à trouver un site proposant un tarif de 1 099$. Nous utiliserons cette fourchette basse pour notre estimation, sans présumer en rien de la capacité du site à fournir une telle quantité de matériel à un attaquant potentiel ! Nous obtenons à ce tarif un investissement matériel de près de quatre cent millions de dollars. Il faudrait ajouter à cela la location d'un local climatisé permettant d'installer ces machines en évitant la surchauffe, mais il paraît difficile d'estimer le coût d'une telle location. Enfin, il est nécessaire de dépenser de l'électricité pour faire fonctionner le parc d'*AntMiner S9* pendant un temps suffisant pour casser la blockchain, normalement de l'ordre de quelques heures. Partons du principe qu'il suffit d'une journée pour que l'attaque fonctionne. Il faudrait alors faire fonctionner nos 360 000 machines consommant 1 375 watts pendant vingt-quatre heures, soit près de douze millions de kilowattheures. Si l'on se réfère au site Eurostat, le coût d'un kilowattheure en France est d'environ 0.089€ (20), soit une dizaine de centimes de dollars, d'où un coût énergétique de près de cent vingt mille dollars. Nous obtenons donc au total plus de cinq cent millions de dollars, en omettant un certain nombre de coûts. Cela n'est en rien une estimation précise mais elle permet de considérer l'ordre de grandeur du coût d'une telle attaque, de l'ordre de plusieurs centaines de millions de dollars (21).

Encadré 4: Coût d'une attaque à 51%

Il est également possible de mener sur une blockchain des attaques par déni de service. Rappelons que, pour vérifier une transaction, il faut vérifier l'historique des bitcoins utilisés afin de s'assurer que ceux-ci sont bien en possession du débiteur et qu'il n'y a pas de double dépense. Une transaction peut donc être plus ou moins longue à valider selon le nombre de bitcoins (en pratique, de fractions de bitcoins) à vérifier ainsi. Un moyen de ralentir le système consiste donc à chercher à valider une transaction utilisant des bitcoins aux origines très différentes, car la transaction sera longue à valider. Un acteur malveillant prêt à payer pour attaquer le système peut ainsi passer sur le réseau un grand nombre de telles transactions, avec en sus des frais importants pour inciter les mineurs à traiter ces transactions en priorité. Une telle stratégie permet, en quelque sorte, d'occuper les mineurs, les empêchant ainsi de vérifier d'autres transactions. Cela peut créer un fort ralentissement du système, et augmenter les temps de validation des transactions. D'autres attaques plus simples peuvent également être envisagées. Par exemple, sur une blockchain implémentant des *smart contract*, il est possible de ralentir très fortement le système en passant des

contrats volontairement très longs à exécuter voire exécutant une boucle à l'infini. De telles attaques par déni de service ont déjà été menées, en particulier sur ethereum.

Les chercheurs (19) ont montré qu'avec 33% de la puissance de calcul, la stratégie de *selfish mining* est nécessairement gagnante dans le sens que les mineurs « égoïstes » publieront plus de blocs et donc recevront plus en récompense que s'ils publiaient leurs blocs de manière transparente, et ce quel que soit le comportement des mineurs honnêtes. De plus, si en cas de compétition entre la chaîne publiée par les mineurs « égoïstes » et une chaîne publiée par un autre mineur, les mineurs honnêtes choisissent de manière indifférenciée la chaîne sur laquelle ils cherchent à publier le bloc suivant, la stratégie devient toujours gagnante avec seulement 25% de la puissance de calcul (18).

Encadré 5 : Attaque à 33%

Enfin, on peut se poser la question de l'intérêt pour un mineur de valider des blocs si l'incitation économique devient trop faible. Rappelons que, sur bitcoin par exemple, les mineurs sont récompensés lorsqu'ils valident un bloc car on leur donne quelques bitcoins (actuellement douze et demi) et ils récupèrent les frais des transactions publiées sur le bloc. Or, la récompense est vouée à disparaître, ce qui pourrait entraîner une augmentation des frais de transactions, sans exclure pour autant que l'intérêt de miner des blocs devienne beaucoup plus faible qu'aujourd'hui. Or, au vu du coût énergétique du minage, il n'est pas à exclure que certains mineurs finissent par abandonner, car leur revenu deviendrait trop faible par rapport à leur dépense énergétique. Une désertion d'un grand nombre de mineurs risquerait d'affaiblir le système, qui est d'autant plus sécurisé qu'il mobilise une forte puissance de calcul et un grand nombre de mineurs. En cas d'abandon massif de nombreux mineurs, on pourrait envisager qu'une attaque des 51%, par exemple, devienne beaucoup plus accessible.

2.4.4 Souveraineté du système

En résumé

La question de la confiance

- Confiance en la majorité des mineurs
- Quelle stratégie pour les consortiums de mineurs ?
- Concentration de consortiums chinois sur bitcoin

État des lieux des mineurs sur bitcoin

- Quelques consortiums détenant la majorité de la puissance de calcul
- Risque d'émergence d'un consortium trop puissant

Il apparaît également que les blockchains publiques peuvent présenter un certain nombre de limites en termes de souveraineté. A titre d'exemple, la plupart des mineurs sur bitcoin sont désormais des consortiums chinois, du fait d'un prix assez faible de l'électricité en Chine. Par ailleurs, les intentions à long terme de ces consortiums ne sont pas nécessairement claires et il n'est pas à exclure qu'il y ait également une volonté politique chinoise d'avoir une présence forte sur un système comme bitcoin. Lorsque l'on prétend qu'une blockchain est un système fonctionnant sans confiance, c'est oublier un peu vite que celui-ci ne fonctionne pas de manière indépendante et désincarnée, mais est bien le reflet de la volonté des mineurs de valider ou non certaines transactions. Il y a donc nécessairement une forme de confiance de la part des utilisateurs, dirigée en particulier vers les mineurs. Or, ceux-ci sont la plupart du temps méconnus, et leurs intentions peu claires. Se pose donc la question de la volonté de développer des applications grand public sur un tel système et d'y mettre, potentiellement, des données critiques. Il y a, au-delà de l'idéal d'un

monde sans confiance, des enjeux de souveraineté qui pourraient se poser, en regard notamment de la forte présence chinoise sur une blockchain comme bitcoin.

Il est par ailleurs arrivé dans l'histoire de bitcoin que certains consortiums aient atteint une taille suffisamment importante pour faire craindre une trop grande emprise sur le réseau, provoquant la méfiance. Ces consortiums se sont alors scindés en plusieurs consortiums indépendants dans le but de rassurer les utilisateurs. Cependant, il n'est pas à exclure que certains consortiums puissent, à un moment, travailler de concert. Alors que le nombre de consortiums possédant une part non négligeable de la puissance de calcul est finalement assez restreint, une entente pourrait favoriser l'émergence d'un groupe détenant, si ce n'est la majorité de la puissance, du moins une part suffisamment importante pour influencer le bon fonctionnement du système.

2.4.5 Un enjeu d'éducation aux risques numériques

En résumé

Gestion des clés privées

- Mauvaises pratiques sur les mots de passe
- Pas de récupération possible en cas de perte de sa clé privée

Systèmes de protection des utilisateurs

- Exemple de Ledger
- Sécurisation des transactions
- Mécanismes de récupération des fonds

La blockchain met également en lumière un enjeu important de la révolution numérique : l'éducation du grand public aux problématiques de sécurité numérique. Aujourd'hui, la plupart des particuliers utilisant des systèmes numériques font montre de mauvaises pratiques, notamment en ce qui concerne la gestion des mots de passe. Beaucoup de personnes utilise des mots de passe peu sécurisés, soit car trop simplistes et habituels (tel que le très utilisé « azerty »), soit parce que trop souvent réutilisés. Au-delà du choix personnel des mots de passe, certaines plateformes semblent sous-estimer les risques en termes de cybersécurité en requérant des mots de passe aux formalismes beaucoup trop simplistes. Ainsi, une banque oblige ses clients à choisir des mots de passe constitués de six chiffres, ce qui est une aberration pour une application aussi sensible, malgré tous les mécanismes de protection qui ont pu être créés. De telles mauvaises pratiques auraient des conséquences désastreuses sur une blockchain comme bitcoin où il n'existe aucun mécanisme de récupération de mot de passe. Or, perdre sa clé privée revient à perdre définitivement l'accès à l'intégralité de ses fonds en bitcoins. L'enjeu de sensibiliser le grand public à ces problématiques apparaît donc comme crucial.

Pour pallier à ces risques, on voit par ailleurs émerger des produits visant à sécuriser les portefeuilles en bitcoin des particuliers, tel que le système français Ledger (16). Une photo du nouveau président français Emmanuel Macron tenant un appareil Ledger a d'ailleurs agité la communauté blockchains, qui y a vu un signe que la politique du président élu pourrait favoriser le développement des nouvelles technologies et en particulier des blockchains. Ledger est un portefeuille numérique permettant de stocker des bitcoins de manière sécurisée, avec des mécanismes de protection destinés au grand public. L'idée de Ledger part de plusieurs constats. Tout d'abord, la gestion des clés privées est un réel problème, alors même qu'il s'agit de l'élément le plus crucial et potentiellement le plus exposé à des risques de piratage. De plus, il n'existe pas de mécanisme pour récupérer l'accès à ses bitcoins en cas de perte de sa clé privée. Enfin, si votre appareil est infecté, il peut être possible d'accéder à vos saisies clavier et donc ainsi de récupérer votre clé privée lorsque vous la tapez pour valider une transaction. Ledger offre donc un système permettant de remédier à ces problèmes. L'idée consiste à utiliser une clé USB spéciale, appelée *wallet*, pour réaliser ses transactions. Cette clé USB contient la clé privée de votre compte bitcoin, sécurisée par des mécanismes cryptologiques. Lorsque vous voulez réaliser une transaction, il vous

suffit d'insérer la clé USB et de rentrer un code PIN, directement sur la clé. Les mécanismes de validation des transactions sont ensuite faits directement sur le système intégré à la clé USB et non sur votre ordinateur, ce qui permet d'utiliser un *wallet* Ledger y compris sur un ordinateur infecté, puisque tout est géré directement depuis le système sécurisé intégré au *wallet*. Ainsi, vous n'avez plus à retenir votre clé privée mais un simple code PIN et vous pouvez utiliser vos bitcoins sans crainte que votre compte soit piraté par l'utilisation d'un logiciel malveillant. Certes, un simple code PIN paraît moins sécurisé qu'une clé privée, mais son utilisation nécessite d'avoir l'accès au *wallet* Ledger. Enfin, Ledger inclut des mécanismes permettant de récupérer l'accès à son compte en cas de perte de son *wallet* ou de son code PIN, de manière similaire à un système de récupération de mot de passe.

2.4.6 Décentralisation et protection des consommateurs

En résumé

Deux visions opposées

- Enthousiasme pour un système assez libertarien
- Pragmatisme : intérêt d'un organe de contrôle

L'intérêt d'un service client

- En cas de vol sur un compte bancaire
- Mécanisme de remboursement impossible sans autorité centrale

Au fil de nos lectures sur le sujet des blockchains, il nous est apparu que deux visions s'opposent sur l'intérêt d'un système décentralisé. Certains thuriféraires y voient une opportunité de développer un système sans aucune autorité de contrôle, sur lequel chacun sera maître de ses données et de ses actions, renouant avec l'idée d'un internet émancipateur, outil d'une forme de libération vis-à-vis de certaines prérogatives de l'État. L'absence de gouvernance centralisée et de contrôle apparaît comme un idéal qui avait émergé avec l'apparition d'internet, et qui a pu s'essouffler face notamment à la prise en main du système par des acteurs privés exploitant la moindre donnée personnelle. Pour autant, cet enthousiasme, s'il peut être partagé pour certaines applications (en particulier, nous évoquerons plus tard la gestion de l'identité numérique), nous paraît parfois trop extrême. Souvent, l'autorité et le contrôle nous semblent avoir des intérêts indéniables. Dans nombre d'applications, ces autorités ou tiers de confiance sont également des interlocuteurs qui ont un rôle de service clients. Considérons par exemple le secteur bancaire. Si certains semblent rêver aujourd'hui d'un système sans banque, il nous paraît bien utile et confortable de pouvoir nous tourner vers notre banquier en cas de problème, pour être remboursé en cas de vol de carte bancaire ou pour faire opposition à une transaction. Sur bitcoin, il n'existe aucun mécanisme similaire. L'affaire de la plateforme *The DAO* sur ethereum a permis de prendre conscience de cette problématique. Revenir sur les transactions malveillantes a été particulièrement difficile tant les mineurs étaient incapables d'atteindre un consensus sur la nécessité ou non de rembourser les personnes flouées. Si la blockchain principale a finalement vu un remboursement effectué, cela s'est fait au détriment d'un *hard fork* et d'un effondrement du cours de l'ether. Les limites de la décentralisation totale sont alors apparues en pleine lumière.

2.4.7 Quelques limites techniques

En résumé

Standardisation des blockchains publiques

- Une blockchain principale : concentration de la puissance de calcul, robustesse
- Plusieurs blockchains principales : plus de flexibilité pour de nouvelles fonctionnalités

Temps de latence

- Une heure pour valider une transaction sur bitcoin
- Incompatible avec des systèmes à grande échelle

Volume de transactions

- Faibles volumes
- Passage à l'échelle technique difficile
- Des solutions : augmenter la taille des blocs, créer des *sidechains*

Changements structurels

- Difficulté à implémenter des changements structurels
- Nécessité d'un consensus entre mineurs

Citons tout d'abord une problématique qui, sans être une limite, pourrait conditionner l'avenir de la technologie des blockchains publiques. Se pose aujourd'hui la question de savoir comment la technologie va se standardiser, avec deux options possibles. Soit la technologie va être phagocytée par une blockchain majeure sur laquelle se développeront potentiellement de nouvelles fonctionnalités, soit vont émerger en parallèles plusieurs blockchains, aux caractéristiques différentes, comme cela semble être le cas aujourd'hui, bien que bitcoin continue à être la blockchain la plus importante, tant en terme de puissance de calcul qu'en capitalisation boursière. Chacune des deux hypothèses présente des inconvénients et des avantages. Si une blockchain majeure venait à se développer, elle concentrerait la puissance de calcul, ce qui en augmenterait la robustesse, rendant plus difficile la possibilité de contrôle la moitié de cette puissance. Pour autant, il apparaît alors que bitcoin serait sans doute la blockchain la plus à même de devenir cette blockchain majeure, ce qui n'est pas sans faire apparaître un certain nombre de limites, bitcoin n'étant pas la blockchain la plus avancée sur certaines fonctionnalités (anonymisation, développement des *smart contracts*, …). De plus, faire évoluer structurellement la blockchain est un exercice délicat, comme nous le verrons très prochainement, et l'implémentation de nouvelles fonctionnalités n'en sera que plus complexe. A l'inverse, développer plusieurs blockchains en parallèle permettrait de créer des systèmes différents et sans doute plus flexibles pour s'adapter aux différentes fonctionnalités requises, mais la puissance de calcul risque alors de se diviser entre les blockchains, les rendant plus vulnérables et créant potentiellement de la concurrence entre les différents systèmes.

Si l'on se concentre plus spécifiquement sur bitcoin, qui demeure la blockchain réalisant le plus de transactions, on observe également une limite technique majeure : le temps de latence pour valider les transactions. Un bloc étant validé en moyenne toutes les dix minutes, cela représente le temps minimal à attendre avant qu'une transaction que l'on vient de réaliser soit écrite sur la blockchain. Pour autant, il est recommandé d'attendre environ une heure, afin que cinq à six blocs aient été validés, rendant *de facto* quasiment impossible qu'une chaîne plus longue se développe et devienne la chaîne principale au risque d'invalider la transaction. Cependant, un temps de latence d'une heure avant d'être assuré qu'une transaction a été passée est une vraie limitation technique. Ceci n'est pas un frein au développement de systèmes d'échanges impliquant de grosses transactions, mais il paraît difficile d'envisager faire du paiement à grande échelle ou du micropaiement avec un tel temps de validation. Imaginons que l'on veuille payer une baguette en bitcoin à la boulangerie. Il paraît alors absurde de devoir attendre une heure avant de pouvoir repartir avec son pain ! Aujourd'hui, certains commerces acceptent le bitcoin mais prennent le risque de laisser partir le client sans avoir la certitude absolue que le paiement sera correctement

effectué. La limite paraît trop importante pour que le paiement en bitcoin se généralise. Cette limite est encore plus rédhibitoire lorsque l'on considère des applications plus complexes, tel que du trading haute fréquence, où il est nécessaire d'avoir des systèmes en temps réel. Si l'on peut envisager réduire les temps de validation des transactions (en particulier, nous étudierons l'exemple des *sidechains*), il paraît impossible d'implémenter des systèmes en temps réel. Le système blockchain, fondé sur l'idée d'un contrôle des transactions par un réseau, nécessitera toujours un certain temps de latence permettant aux acteurs de valider les transactions. Même si ces mécanismes de validation peuvent être rapides, il existe un temps incompressible nécessaire à la vérification de la licéité des transactions.

Il apparaît également que le système bitcoin est aujourd'hui un système qui réalise un nombre finalement assez faible de transactions. Ainsi, sont réalisées environ une dizaine de transactions chaque seconde, très loin des vingt mille transactions par seconde de moyenne que l'on observe sur le système bancaire traditionnel. Si bitcoin ou une autre blockchain publique venait à développer des applications grand public nécessitant un changement d'ordre de grandeur dans le nombre de transactions réalisées, un passage à l'échelle technique serait nécessaire. Aujourd'hui, et au vu du paramétrage de bitcoin (taille des blocs, fréquence de validation, …), un tel passage à l'échelle est impossible car le système n'aurait pas la capacité de traiter toutes les transactions reçues. L'une des solutions pourrait être de créer un système de *sidechains*, mais nous reviendrons dessus plus en détail dans la section suivante. Une autre solution pourrait être d'augmenter la taille des blocs, ce qui nécessiterait l'accord tant des mineurs que des utilisateurs, consensus loin d'être évident aujourd'hui.

Plus largement, se pose d'ailleurs la question de la possibilité de faire évoluer une technologie comme bitcoin. Si l'on veut réaliser des changements structurels sur une blockchain publique, un consensus des mineurs est obligatoire afin que ceux-ci acceptent d'utiliser les nouvelles fonctionnalités ou caractéristiques implémentées. C'est là l'une des limites d'un système totalement décentralisé sans autorité de contrôle : toute évolution doit être acceptée par le réseau faute de quoi les mineurs continueront à utiliser une version antérieure du code qui aurait leur préférence. Or, obtenir ce consensus des mineurs paraît être une tâche potentiellement compliquée. Prenons l'exemple de l'affaire *The DAO*. Suite au détournement des fonds de certains particuliers, s'est posée la question de savoir s'il fallait revenir ou non sur les transactions malhonnêtes, ce qui nécessitait de réécrire des transactions sur des blocs déjà validés. La communauté des mineurs s'est divisée, certains acceptant une telle réécriture quand d'autres l'ont refusée, au nom de l'irréversibilité des transactions sur une blockchain. Cette incapacité à trouver un consensus a conduit à un *hard fork*, créant deux blockchains ethereum parallèles. Ceci illustre la difficulté à trouver un consensus au sein du réseau de mineurs, ne serait-ce que pour annuler une transaction manifestement illégale. Une telle difficulté pourrait également advenir s'il était décidé de procéder à des changements structurels majeurs sur une blockchain publique.

2.4.8 Synthèse

Les blockchains publiques présentent donc de multiples limites qui nous semblent être un frein à leur développement. D'un point de vue technique, d'abord, ces systèmes sont extrêmement énergivores, en tout cas ceux fonctionnant avec la preuve de travail comme mécanisme de consensus. Malgré une robustesse certaine, il existe également bien des risques qu'un mineur ou plus vraisemblablement un groupe de mineurs puisse prendre le contrôle du système avec une important puissance de calcul. De plus, la nature des mineurs peut poser question, en termes de souveraineté et de confiance que l'on peut avoir dans un système fortement contrôlé par des consortiums, pour la plupart chinois, et aux intentions quelque peu opaques. Toujours d'un point de vue technique, les blockchains publiques offrent aujourd'hui des performances assez moyennes en termes de temps de latence ou de volumes possibles de transactions, et apparaissent comme des systèmes encore peu standardisés et peu matures.

Par ailleurs, l'esprit même des blockchains publiques est un vrai frein à leur développement auprès du grand public. L'absence d'encadrement légal empêche de pouvoir imaginer des applications larges dans des secteurs régulés comme l'assurance. De plus, il nous semble que le grand public aura toujours peu d'appétence pour des systèmes sans autorité et sans garantie car dépourvus de mécanismes de protection des utilisateurs. Enfin, si ces systèmes venaient malgré tout à être utilisés par le grand public, il nous apparaît nécessaire de bien alerter les consommateurs sur les risques, en particulier sur la question de la gestion des clés privées, tant on observe de mauvaises pratiques en termes de risques cyber auprès de la population.

2.5 Une première réponse technique : les *sidechains*

Une première solution à ces limites techniques (temps de latence, passage à l'échelle, difficultés à effectuer des changements structurels sur une blockchain publique) pourrait résider dans la mise en place d'un écosystème à base de *sidechains* (17). Nous nous proposons ici d'introduire cette technologie et de voir comment elle pourrait aider à résoudre une partie des limites évoquées.

2.5.1 Fonctionnement

En résumé

Ecosystème	**Principe**
- Une blockchain principale - De multiples petites blockchains parallèles : les *sidechains*	- Mécanismes de change monétaire entre la blockchain principale et les *sideschains*

Le principe général des *sidechains* consiste à avoir un écosystème au sein duquel se développent de multiples blockchains essentiellement de petite taille, en parallèle d'une blockchain majeure, qui pourrait être par exemple bitcoin. On met ensuite en place des mécanismes permettant de réaliser des transactions entre la blockchain principale et les blockchains parallèles afin de pouvoir déplacer des fonds de l'une vers les autres et réciproquement. Les *sidechains* s'analysent donc par rapport à une blockchain centrale de référence, autour de laquelle elles gravitent. Notons qu'une *séchai* pourrait tout à fait avoir ses propres *sidechains*.

Prenons l'exemple d'un système centré autour de bitcoin. Ce système contiendrait de multiples blockchains parallèles destinées à des applications diverses. Il serait possible d'envoyer des bitcoins depuis la blockchain bitcoin vers les blockchains parallèles et réciproquement. Plus précisément, les *sidechains* utiliseraient sans doute chacune leur propre crypto-monnaie, que nous pouvons appeler de manière générique les sidecoins. Des mécanismes existent donc pour convertir des bitcoins en sidecoins sur une *sidechain* et vice-versa.

L'idée d'un tel mécanisme est relativement simple. A cet effet, on crée un format spécial de transactions sur bitcoin permettant de bloquer des bitcoins sur la blockchain pour débloquer en conséquence des sidecoins sur la *sidechain*. Ainsi, un détenteur de bitcoins peut demander à en bloquer une partie sur la blockchain. Ceux-ci demeurent alors sur la blockchain bitcoin mais ne sont plus accessibles ni par l'utilisateur, ni par qui que ce soit d'autre. Une fois la transaction validée et les bitcoins bloqués, des sidecoins sont libérés en contrepartie sur la *sidechain*, par un mécanisme similaire utilisant une transaction spéciale. La transaction de blocage sur bitcoin fournit une preuve cryptologique à la *sidechain* pour garantir que les bitcoins ont été bloqués et que les sidecoins peuvent être libérés en conséquence. L'utilisateur peut alors effectuer des transactions sur la

sidechain et ses bitcoins ne sont plus accessibles. Un mécanisme similaire permet de faire le transfert inverse, en bloquant des *sidecoins* pour débloquer des bitcoins sur la blockchain principale.

2.5.2 Intérêts et limites

En résumé

Temps de latence

- Création d'une *sidechain* de micropaiement
- Mécanismes de validation accélérés
- Change monétaire entre bitcoins et sidecoins

Nouvelles fonctionnalités

- Implémentées sur des *sidechains* spécifiques, flexibles
- *Sidechains* connectées à une blockchain principale, mécanismes de change
- Exemple de Liquid, développé par Blockstream

Limites

- Retour à de multiples systèmes fermés
- Risque de dilution de la monnaie entre les *sidechains*
- Blocage d'une partie de la masse monétaire

Comment un tel écosystème peut-il aider à résoudre les limites techniques évoquées précédemment ? Commençons par revenir sur la question de la standardisation et de l'émergence d'une blockchain principale ou de multiples systèmes. L'idée des *sidechains* consisterait justement à conserver une blockchain principale, certes rigide, mais autour de laquelle se développeraient d'autres systèmes plus flexibles. L'idée serait bien de conserver une blockchain de référence et des petits systèmes gravitant autour.

Pour revenir sur la limite des temps de latence, les *sidechains* pourraient être une vraie solution à ce problème. Si l'on identifie un cas d'usage nécessitant des temps de latence très réduits par rapport à ce qui existe sur bitcoin, on peut créer des blockchains spécifiques, restreintes à un secteur sur lequel s'exprime ce besoin Ces blockchains peuvent être pensées avec des mécanismes de validation des transactions simplifiés et très largement accélérés. Certes, le mécanisme de consensus ne se fera sans doute jamais en temps réel, mais l'on peut imaginer des mécanismes ne prenant guère plus de quelques secondes. Une fois cette blockchain créée, avec des caractéristiques techniques adaptées au problème, on peut ensuite la relier à une blockchain comme bitcoin avec ces mécanismes de transaction entre blockchain principale et *sidechain*. Cela permet de créer un système de change entre la monnaie bitcoin et les *sidecoins*, change qui peut être fixé comme paritaire. Ainsi, il sera possible de réaliser des micropaiements directement avec des équivalents de bitcoin sur des *sidechains* spécifiques.

De manière plus générale, si l'on veut tester une nouvelle fonctionnalité, il n'est pas nécessaire de tenter de l'implémenter sur une blockchain comme bitcoin, particulièrement rigide. Il suffit de créer une petite blockchain, beaucoup plus flexible, avec des caractéristiques techniques plus adaptées à la fonctionnalité voulue. Il est ensuite possible de connecter cette blockchain à une blockchain principale comme bitcoin. L'intérêt consiste donc à conserver une blockchain principale robuste, destinée à de faibles volumes de transactions, autour de laquelle graviteraient des systèmes beaucoup plus flexibles, permettant l'implémentation de nouvelles fonctionnalités, avec des caractéristiques techniques ciblées sur un cas d'usage précis. Notons qu'a été lancée récemment une première *sidechain* adossée à bitcoin. Cette *sidechain*, nommée Liquid et implémentée par la société Blockstream, s'adresse aux organismes de change, tels que Kraken ou Bitfinex, qui

permettent d'échanger des bitcoins contre de la monnaie « réelle ». Il sera donc possible pour ces organismes de réaliser des transferts monétaires directement sur la *sidechain* Liquid, ce qui présente un intérêt en termes de temps de latence. En effet, la validation est considérablement accélérée, grâce à un système de consensus très simplifié. Ici, tous les acteurs, appelés *functionaries* votent (de manière automatisée grâce à des algorithmes internes de vérification) et une transaction est validée si onze *functionaries* sur dix-huit ont accepté la transaction. Le temps de validation moyen est d'environ sept secondes, ce qui est bien évidemment plus rapide que sur bitcoin.

Pour autant, cette notion de *sidechains* présentent encore un certain nombre de limites. Les *sidechains* auront finalement des fonctionnement qui leur seront propres, voire seront, comme Liquid, des systèmes fermés. On peut alors se poser la question l'intérêt d'un tel système par rapport à un simple développement interne sans lien avec bitcoin ou toute autre blockchain publique. Dans certains cas, l'intérêt est évident, comme pour Liquid où l'objectif est de réaliser des transactions bitcoin plus rapidement, par l'intermédiaire d'une crypto-monnaie intermédiaire, un peu comme une banque peut réaliser rapidement des transactions entre plusieurs de ses comptes alors que ne s'effectuent des transactions interbancaires que plus rarement, en regroupant plusieurs transactions pour faire la somme de ce que chaque banque doit à l'autre. Si l'on revient à notre idée de micropaiement, on pourrait se poser la question de lier une telle *sidechain* à un système comme bitcoin plutôt que de créer des mécanismes permettant d'échanger directement des euros en *sidecoins*. Par exemple, sur une blockchain partagée sur un réseau de commerçants, on pourrait imaginer que chaque commerçant fasse de l'achat et de la vente de *sidecoins* auprès du public, sans passer par une blockchain principale. Pour autant, les deux mécanismes ne sont pas incompatibles et pourraient cohabiter. Se pose malgré tout le risque qu'un utilisateur bitcoin n'ait à diluer sa crypto-monnaie entre de multiples *sidechains* dont il aura l'usage, au risque de s'y perdre. D'autant que l'utilisateur devra bien choisir la quantité de monnaie à déplacer sur chaque *sidechain*, ce qui est nettement moins confortable qu'un système unique sur lequel regrouper l'intégralité de son argent. Par ailleurs, le fonctionnement d'un tel système consiste à bloquer de l'argent sur la blockchain principale pour en débloquer sur la *sidechain*, et réciproquement. Mécaniquement, il en résulte qu'une grande partie de la masse monétaire, tant sur la blockchain principale que sur les *sidechains*, sera bloquée voire définitivement inutilisable. En effet, un utilisateur ayant bloqué des bitcoins et dépensé l'intégralité des sidecoins ainsi obtenus ne pourraient plus récupérer les bitcoins bloqués, qui seraient donc totalement inutilisables. Cela apparaît comme une vraie limite, d'autant que la masse monétaire sur bitcoin a vocation à être limitée.

Ce qu'il faut retenir

9. Les blockchains forment un ensemble de technologies assez diversifié, le terme étant finalement assez mal défini et regroupant des systèmes aux caractéristiques bien différentes.

- Une distinction majeure : blockchains publiques (accessibles à tous, code informatique et données publiques) / blockchains privées et hybrides (accessibles à un nombre restreint d'acteurs, eux seuls ayant accès au code et aux données).
- Différents systèmes de consensus : preuve de travail (des mineurs fournissent de la puissance de calcul, système robuste mais coûteux en termes d'énergie) / preuve d'enjeu (des forgeurs valident des blocs en fonction de la quantité de monnaie qu'ils détiennent) / votes simples (pour des blockchains privées) :
- Différentes natures de données : crypto-monnaies / registres / *smart contracts.*
- Confidentialité : pseudonymat (bitcoin) / anonymat (ZCash, Monero) / identifiable (blockchains privées).
- Réversibilité des données : transactions irréversibles en théorie sur les blockchains publiques, en pratique très difficiles à inverser (*The DAO*) / réversibilité plus facile sur des blockchains privées.
- Tiers de confiance : aucun tiers de confiance dans l'esprit initial / oracles pour les *smart contracts* / tiers de confiance juridiques sur des blockchains privées.

10. Bien que peu de blockchains aient émergées actuellement, plusieurs cas d'usages apparaissent possibles et sont évoqués :

- Blockchains publiques : crypto-monnaies / plateformes bifaces / registres publics.
- Blockchains privées : registres de transactions / registres de biens / *supply chain.*

11. Les blockchains privées, ou DLT, apparaissent comme des systèmes robustes, difficiles à falsifier. Ils présentent également un intérêt dans le sens où ce sont des registres partagés, sur lesquels un acteur ne peut rien écrire sans l'accord de ses pairs. Pour autant, ces systèmes présentent quelques limites :

- Sécurité du système : risque systémique lié au fait que les données sont partagées entre plusieurs acteurs, potentiellement vulnérables.
- La question de la confiance : le système peut s'effondrer si apparaissent des intérêts divergents entre les acteurs.
- L'emballement médiatique : certains projets semblent plus résulter d'une volonté de communication que d'un besoin réel. La blockchain est trop souvent une fin en soi plutôt que le moyen de développer un projet répondant à un besoin réel.

12. Les blockchains publiques présentent également de multiples limites, techniques et conceptuelles, qui sont de véritables freins à leur développement notamment auprès du grand public.

- Cadre légal : absence de contrôle centralisé incompatible avec le développement d'applications grand public / pas de mécanismes de protection des utilisateurs / nécessité d'alerter sur les risques liés à une mauvaise gestion des clés privées.
- Question de la fiabilité du système : attaque des 51%, des 33% / attaque par déni de service / pérennité des blockchains publiques.
- Question de souveraineté : méconnaissance des mineurs et de leurs intérêts.
- Coût de la preuve de travail : consommation énergétique du minage sur bitcoin équivalente à la production d'une tranche de centrale nucléaire.
- Limites techniques : temps de latence / volumes de transactions.

13. Les *sidechains* pourraient apporter des réponses à certaines limites techniques.

- Fonctionnement : une blockchain principale autour de laquelle gravitent des *sidechains* parallèles / mécanismes de transaction entre ces blockchains.
- Intérêt : *sidechains* beaucoup plus flexibles, permettent l'implémentation de plus de fonctionnalités.

3 Cas d'usage détaillés

Tout d'abord limité à bitcoin et à des usages de crypto monnaies, nous avons vu dans la partie précédente que la technologie de la blockchain a depuis considérablement évolué et s'est diversifiée. Dans cette partie nous allons regarder plus précisément, le fonctionnement et les usages de quelques applications de la technologie. Grâce à ces quelques cas d'usage précis, nous souhaitons illustrer les points forts et les limites évoqués dans la partie précédente. En particulier, le niveau de décentralisation « en pratique » souvent plus faible que celui annoncé notamment concernant les blockchains privées mais aussi pour les blockchains publiques.

3.1 Les applications financières

Les applications au domaine de la finance sont celles les plus souvent citées dans les médias. Sans doute car la blockchain a été inventée pour créer une crypto-monnaie, faisant de la finance son domaine naturel d'application. Dans cette sous-partie, nous tacherons d'analyser deux cas d'usage tout d'abord celui des crypto-monnaies, celles-ci étant devenues aujourd'hui bien trop nombreuses, nous vous proposons dans une première sous-partie de se focaliser sur le bitcoin.

3.1.1 Les crypto-monnaies : monnaie ou actif ?, le cas bitcoin

En résumé

Monnaie ou actif ?

- Un temps de paiement élevé : actif
- Des frais de transactions élevés : actif
- Solutions de type *sidechains* : monnaie
- Volatilité : actif

Le problème de la centralisation

- Pool de minages : centralisé
- Développeurs bitcoin : centralisé
- Portefeuille en ligne : centralisé
- Minage P2P : décentralisé
- Services décentralisé : décentralisé

Comme nous l'avons vu, la blockchain bitcoin est une blockchain publique. Tous les utilisateurs peuvent devenir des « mineurs », envoyer des ordres de transfert ou simplement en télécharger une copie. Souvent présenter comme une monnaie, nous chercherons d'abord à déterminer quels sont ces usages. Nous montrerons ensuite à travers le cas précis du bitcoin les limites des blockchains publiques discutées en partie 2.4 en nous intéressant tout particulièrement à la question de la décentralisation.

Pour la majorité de ces partisans les plus convaincus, le bitcoin est une monnaie. Pour eux, le bitcoin a vocation à devenir une monnaie utilisable au jour le jour comme l'euro, le dollar et le renminbi. Cependant le protocole initial semble souffrir de nombreuses limites empêchant un tel usage.

Par construction, le délai moyen pour obtenir la confirmation d'un paiement sur la blockchain bitcoin ne peut descendre en dessous de 5 minutes. Cela provient de l'organisation de la blockchain qui ne publie un bloc que toutes les 10 minutes. Ce délai a toutefois tendance à s'allonger pour deux raisons. Comme nous l'expliquions dans la première partie pour être certain qu'une transaction ne pourra pas être annulée il est préférable d'attendre que plusieurs blocs soient validés. Les défenseurs d'un usage monétaire du bitcoin rétorqueront que pour une transaction de faible envergure la probabilité d'un acte malveillant est nulle et que se prémunir contre ce risque d'annulation est absurde. En outre, la taille des blocs étant limitée, une transaction peut attendre quelques heures avant d'être inscrite dans la chaîne faute de place. Ce problème touche d'avantage les transactions proposant des récompenses faibles, les mineurs inscrivant en priorité les transactions les plus rentables afin de maximiser leur gain.

Le deuxième obstacle majeur à l'usage monétaire est le coût des transactions. Pour espérer que son paiement soit validé dans le prochain bloc, c'est-à-dire en moins de 10 minutes, les frais de transactions sont de quelques dollars. Ce prix s'explique par la taille limitée des blocs, si le nombre de transactions en attente est supérieur à la taille du bloc, les mineurs choisissent en priorité les transactions les plus rentables. Si un utilisateur choisit de ne mettre que quelques centimes de frais pour la validation de sa transaction, celle-ci pourrait ne jamais être validée. Une augmentation de la taille des blocs par exemple pourrait permettre de résoudre au moins partiellement ce problème. Mais dans les conditions actuelles, il est difficile d'imaginer qu'une carte de paiement bitcoin soit en mesure de concurrencer une carte de paiement classique.

Ces deux obstacles ne sont cependant pas infranchissables. S'ils sont présents sur la blockchain bitcoin, des crypto-monnaies alternatives proposent des délais de validation de blocs plus courts ainsi que des frais de transaction moins élevés. Même sur la blockchain bitcoin des solutions construites par-dessus celle-ci offrent des solutions à ces deux problèmes. C'est par exemple le cas du « Lightning Network » développé par *Blockstream*, le système construit à l'aide de *smart-contracts,* permet d'effectuer des micropaiements entre plusieurs utilisateurs en s'affranchissant des contraintes précédemment citées. Il respecte les principes de bitcoin en proposant une architecture pair-à-pair et en fonctionnant sans tiers de confiance. Ce type de solution complexifie l'usage des bitcoins mais rende une exploitation monétaire plus crédible.

Cependant, les délais et les frais de transactions ne sont pas les deux seuls obstacles à l'utilisation monétaire du bitcoin. La volatilité du cours reste trop importante pour l'établir en tant que monnaie de référence. Sur ces cinq dernières années le cours du bitcoin a pu être multiplié ou divisé par 10 en l'espace d'un mois à plusieurs reprises. De telles variations ne permettent pas d'envisager un usage non spéculatif.

Dernier obstacle à son utilisation monétaire, le manque d'établissement acceptant les paiements en bitcoin. Quelques grands noms dans l'industrie du jeux vidéo acceptent toutefois les bitcoins. Il est également possible de les utiliser sur quelques plateformes de vente en ligne néanmoins le phénomène reste ultra-minoritaire. De plus, à notre connaissance, l'ajout de cette possibilité a été plus souvent motivé par les potentielles retombées publicitaires de l'annonce du support de bitcoin que par un réel intérêt pour le système. Selon un grand site web les acceptant, les usagers ont également toujours été aux abonnés absents. Cependant deux exceptions notables permettant l'usage monétaire de bitcoin peuvent être citées :

- Wikipedia accepte depuis 2014 les dons en bitcoins, son fondateur soutenant l'idéologie sous-jacente ;
- tous les usages illégaux profitant du pseudonymat offert par bitcoin.

Une étude récente de l'université de Sydney (18) estime que la part de transactions illégales sur le réseau bitcoin est de 45%. Pour cela les chercheurs se sont appuyés sur deux grandes sources de données : les saisies effectuées par le FBI et les adresses bitcoin des plateformes illégales et de

leurs utilisateurs. À partir de ces données et grâce à la transparence des transactions ils ont pu parvenir à cette estimation.

À noter que des boutiques bien réelles ont également su profiter de l'exposition médiatique du bitcoin. À Paris dans le passage du Grand Cerf vous pouvez de dépenser des bitcoins. Mais de l'aveux même des propriétaires, le principal impact est médiatique (18). L'usage ne suit pas.

Après analyse des différentes caractéristiques pratiques du bitcoin, il semblerait que le bitcoin ressemble plus à un actif qu'à une monnaie. Un dernier argument en faveur de cette théorie provient d'une étude des variations du prix et des volumes de transactions. Cette étude a été effectuée par quatre chercheurs de l'université de Goethe à Francfort (19), en analysant ces deux informations, le constat de leur modèle est sans appel : les nouveaux utilisateurs de bitcoin l'utilisent comme un actif et non comme une monnaie.

Dans le cas pratique de bitcoin il est également instructif d'étudier en pratique la décentralisation du système. Sur le papier la monnaie est totalement décentralisée : tout le monde peut devenir mineur et participer aux vérifications, le code source est libre et tout le monde peut l'expertiser. Mais qui décide du futur de bitcoin ? Comment les décisions sont-elles prises ? Est-ce que le principe de décentralisation est respecté jusqu'au bout ? Arthur Gervais et ses co-auteurs proposent de répondre à cette question (21). Dans cet article les auteurs analysent les grandes sources de centralisation et de décentralisation en allant au-delà du protocole.

Plusieurs éléments concrets tendent à montrer une forte centralisation du bitcoin, en dépit d'un protocole initial décentralisé. En premier lieu, l'apparition des grands *pools* de minage est une des principales sources de centralisation. Le protocole bitcoin fonctionne grâce à la preuve de travail. L'idée initiale était que tous les ordinateurs du réseaux puissent participer à ce mécanisme de validation. Comme la majorité d'entre eux est honnête, aucune coalition majoritaire ne peut menacer la chaîne et par conséquent la sécurité du réseau est assurée. Cependant, miner des bitcoins pouvant être très lucratif l'activité s'est alors organisée. Le minage est effectué via des *pools* de minage, sortes de coopératives groupant à la fois *datacenters* professionnels et individus et répartissant les gains entre ses membres en fonction de leur investissement. Faire partie d'un *pool* est aujourd'hui le seul moyen réaliste d'obtenir une récompense. Aujourd'hui, les 6 plus gros « *pools* » publient plus de 75% des blocs. S'ils décidaient de s'entendre, ils pourraient prendre le contrôle de la chaîne.

Deux autres sources de centralisation proviennent des utilisateurs eux-mêmes. Pour éviter de devoir installer des clients *bitcoin* complets s'occupant de la vérification des transactions et demandant un espace de stockage important et de la puissance de calcul, certains utilisateurs préfèrent choisir des portefeuilles en ligne ou des clients *bitcoin* utilisant le mode SPV. Dans le premier cas, l'utilisateur se dessaisit totalement de la propriété de ses bitcoins : le portefeuille en ligne détient la clef de ses bitcoins et agit donc comme un tiers de confiance. Dans le second cas, l'utilisateur garde le contrôle mais il choisit de ne pas participer à la sécurité du réseau et fait confiance à quelques nœuds pour assurer les vérifications.

Les mises à jour de bitcoin constituent également un point de centralisation important. Les développeurs de bitcoin peuvent influencer son avenir. L'article de l'université de Francfort cite l'exemple de la mise à jour 0.8 de bitcoin, cette version n'étant pas totalement interopérable avec la version précédente un bloc v0.8 a été rejeté par les clients non mis à jour. Possédant plus de puissance de calculs à ce moment la chaîne compatible 0.7 est devenue la plus longue, c'est à ce moment que les développeurs sont intervenus pour convaincre les gros *pools* de minage de ne pas suivre les règles et de ne pas miner la chaîne la plus longue et ainsi valider le bloc rejeté. L'article souligne que cet exemple prouve bien le manque de décentralisation de bitcoin :

> *« This decision comes at odds with the claim that bitcoin is a decentralized system and that the majority of the computing power regulates bitcoin. Less than 10 entities took a decision to outvote the majority of the computing power in the network. »*

Les développeurs bitcoin possèdent également une clef leur permettant de diffuser un message d'alerte à l'ensemble des membres du réseau. Si cela peut sembler anodin, une application directe est celle des pièces tachées « *tainted coins ».* Comme l'ensemble des transactions bitcoin sont publiques il est possible de suivre l'argent et de bannir une ou plusieurs adresses. Les entités centrales précédemment citées jouent un rôle prépondérant dans ce système. La plateforme MtGox, plus grande plateforme d'échange avant sa fermeture, avait par exemple décidé de bloquer les comptes ayant échanger avec certaines adresses bitcoins associées à une affaire de hack. Si les développeurs bitcoin décidaient d'envoyer un message à tous les clients recommandant le bannissement de certaines adresses, ils pourraient certainement bloquer des fonds.

Les chercheurs notent cependant que tout n'est pas noir et que des initiatives visent à respecter la décentralisation du système. Il existe par exemple des *pools* de minage fonctionnant grâce à un système pair-à-pair ne donnant pas un pouvoir de décision au coordinateur. De même, des sociétés proposent de simplifier l'expérience du portefeuille de bitcoin tout en protégeant l'utilisateur. La conclusion reste cependant que le système est bien moins décentralisé qu'on ne le pense et que la majorité des décisions sur l'avenir du système sont prises entre quelques décideurs : l'équipe de développement de bitcoin et les responsables des grands *pools* de minage.

3.1.2 Gérer les transactions sur la blockchain, le cas FundsDLT

En résumé

Un gain en efficacité

- Le développement d'interface API moderne est à lui seul un gain important
- La blockchain est une structure partagée qui est un support naturel de transactions
- Cette solution permet aux acteurs de s'impliquer à différents degrés dans le processus

Une base de données comme une autre

- FundsSquare est un acteur central, il développe les APIs, contrôle le Hub KYC, etc.
- Les acteurs ont tous une confiance dans la Bourse du Luxembourg qui pourrait offrir ce service directement

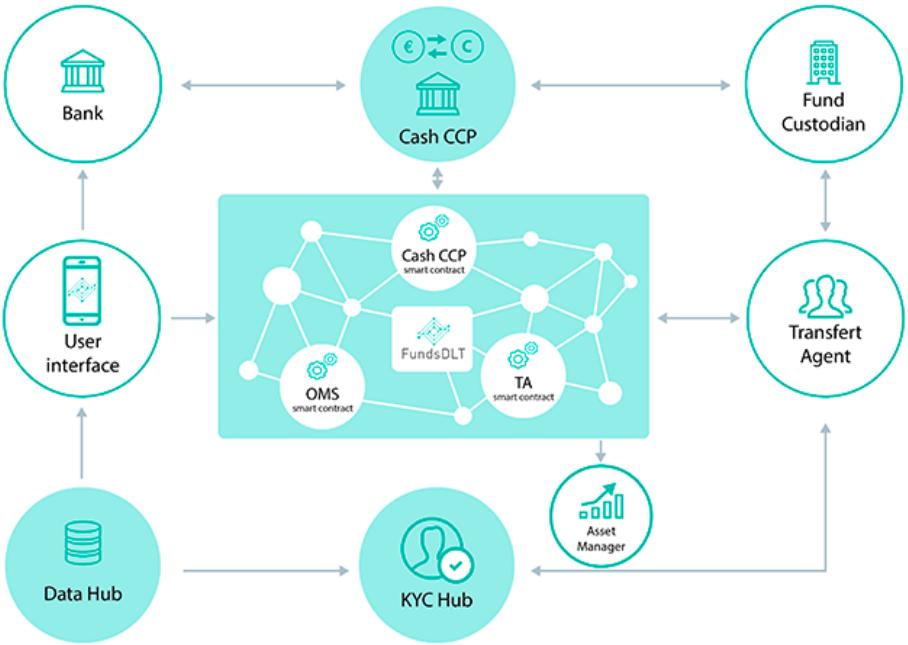
FundsSquare est une entreprise créée par la Bourse de Luxembourg, InTech et KPMG. Elle a pour but de créer une blockchain privée (un DLT) FundsDLT permettant de fluidifier la gestion d'actifs pour les clients finaux comme pour les entreprises du domaine. Cette blockchain est construite sur le modèle de la blockchain ethereum. Cette blockchain est souvent choisie comme base pour les blockchains privées car ses *smart-contracts* plus complets que ceux de bitcoin offrent de nombreuses possibilités. Elle vise à proposer des interfaces modernes à l'ensemble des acteurs du marché, des clients finaux aux chambres de compensation en passant par les entreprises

spécialisées dans le B2B pour permettre des gains de temps importants, une rationalisation des contrôles administratifs et une automatisation des tâches.

Aujourd'hui le monde de la gestion des titres est complexe. De nombreux acteurs interviennent dans l'écosystème : l'investisseur et l'*asset manager*, le distributeur, le dépositaire central de titres, l'agent de transfert, etc. Cela crée des délais de traitement importants, par exemple un transfert peut prendre jusqu'à 6 jours. Ceci est principalement dû à une succession d'étapes obligatoires qui n'ont pas su développer des interfaces efficaces. Chaque passage d'un acteur à l'autre ajoutant une durée incompressible.

Par exemple, les démarches de vérification administratives utiles et nécessaires, en particulier pour la lutte contre le blanchiment, sont souvent répétées inutilement par l'ensemble des acteurs de la chaîne à cause d'un manque de communication de l'information.

FundsDLT propose de résoudre ces problèmes en proposant des APIs (interface de programmation) à l'ensemble des acteurs du marché des actifs permettant d'effectuer toutes les opérations dans un environnement unique. Cet environnement est celui d'une blockchain privée accessible à tous les acteurs financiers le souhaitant. Elles proposent un ensemble de *smart-contracts* permettant d'opérer les actions sans valeurs ajoutées automatiquement et garder une base de données commune facilitant le suivi en temps réel des investissements. Adossé à cette blockchain, un module *« Know Your Customer »* permet de stocker l'ensemble des informations utiles sur les clients et évite de dupliquer les demandes et les contrôles.



Encadré 6 : Organisation de FundsDLT

Le produit gagne toute sa valeur en intégrant l'ensemble des acteurs de la chaîne à qui elles proposent des interfaces modernes. À la différence de bitcoin, la blockchain FundsDLT ne propose pas de transactions transparentes mais différencie les flux pour chaque gestionnaire de fonds afin de protéger le secret des affaires. Les acteurs peuvent choisir d'installer un nœud sur leur propre infrastructure ou être hébergés directement par FundsSquare.

Les limites de la décentralisation sont ici touchées. Se pose la question de savoir si un tiers de confiance a vraiment été supprimé. Avions-nous besoin d'une blockchain pour réaliser ce projet ? Il est vrai que celui-ci en garde beaucoup de caractéristiques :

- la nécessité d'avoir une sécurité élevée est une évidence et la blockchain s'adapte bien à ce cadre ;
- la nécessité de proposer un mécanisme ouvert ou tout le monde peut venir se greffer est là encore tout à fait aligné avec les principes d'une blockchain ;
- enfin l'idée de données partagées est une fois encore au cœur de la blockchain.

Cependant la blockchain ne semble pas nécessaire à la réussite de ce projet. Bien entendu, c'est une structure qui fonctionne dans ce cas et une étude plus poussée pourrait peut-être même montrer qu'elle est la structure la plus adaptée. Mais un projet équivalent aurait pu être développé en utilisant d'autres technologies bien avant.

En effet, le projet est en partie centralisé. La partie *KYC* du projet n'est pas stockée directement sur la blockchain mais sur un service annexe opéré par FundsSquare. Il aurait été donc possible de développer ce service indépendamment, il aurait permis d'éviter une redondance administrative coûteuse en temps sans avoir recours à une blockchain. D'une manière générale, et cela rejoint les critiques formulées à propos des développeurs de bitcoin, la société FundsSquare développe seule FundsDLT. Elle a donc toute latitude pour modifier le protocole selon ses intérêts. Les acteurs décidant d'utiliser son service lui font donc confiance. FundsSquare propose d'ailleurs d'héberger les activités des sociétés participant à la blockchain.

Il nous semble que le gain principal apporté par FundsDLT soit de proposer des interfaces modernes à l'ensemble des acteurs de la place, un traitement automatisé de certaines tâches et un partage intelligent de données entre les acteurs. Tous ses services ne requièrent pas l'usage d'une blockchain et aurait pu être proposer dans des conditions identiques de sécurité avant même l'invention de celle-ci.

De ce que nous avons pu voir de cette blockchain privée, et nous suspectons que ça soit le cas de nombreux projets sérieux, si elle constitue une grande amélioration par rapport au système existant, cette amélioration aurait été possible sans blockchain. D'un point de vue strictement technologique, la blockchain n'est pas l'élément clé qui a permis au projet de fonctionner. Cependant comme tout concept informatique à la mode, elle a pu faciliter la prise de décisions dans des institutions désireuses de paraître modernes et si elle n'était pas nécessaire cela ne veut pas dire qu'elle n'était pas adaptée.

3.2 Les autres usages

Les applications de la blockchain ne sont pas limitées aux cryptomonnaies. Deux grands domaines d'application pressentis sont la gestion de l'identité et la gestion d'une *supply-chain*. Dans cette partie nous illustrons chacun de ces deux utilisations. Dock.io est une plateforme permettant de centraliser les différents profils d'un utilisateur sur les plateformes professionnelles comme *linkedIn* dans un profil unique adossé à la blockchain ethereum. Everledger est une blockchain privée, de la galaxie *hyperledger*, assurant la traçabilité des diamants.

3.2.1 La gestion de l'identité, le cas *dock.io*

En résumé

La gestion d'identité (pour les réseaux professionnels)

- Des données stockées sur la blockchain ethereum
- Une plus grande fluidité pour l'utilisateur qui peut transférer ses données d'un service à l'autre
- Une gestion facilitée pour l'utilisateur avec une mise à jour unique

Décentralisée

- Le protocole est protégé contre les changements unilatéraux
- Le protocole est robuste et pourrait survivre à une faillite de dock.io

Protection de la vie privée

- Rien n'empêche les plateformes de garder les données
- L'intervention du législateur sera toujours nécessaire pour rééquilibrer une relation par nature déséquilibrée

Une décentralisation limitée

- Un projet possible sans la blockchain
- Dock.io garde une position centrale malgré toutes ses précautions

Dock.io souhaite devenir la plateforme/protocole unique pour gérer nos données professionnelles. Elle propose à ses utilisateurs de stocker, collecter, synchroniser et gérer leurs données entre les différentes applications et réseaux professionnels présents sur internet. Elle s'appuie sur la blockchain ethereum pour stocker et partager les données.

Une fois inscrit sur le site internet de dock.io, l'utilisateur trouve une interface unique pour gérer ses données professionnelles et données qu'il peut choisir de partager comme il le souhaite avec les différents autres services. Cela lui permet de garder ses différentes informations à jour facilement et de s'inscrire rapidement sur n'importe quel nouveau service sans avoir à remplir de fastidieux formulaires.

Pour les plateformes professionnelles, proposer une connexion via dock.io c'est proposer à ses futurs utilisateurs un parcours d'inscription sur leur plateforme simple tout en accédant immédiatement aux données de ces nouveaux utilisateurs.

Aujourd'hui les grandes plateformes d'internet essayent d'occuper cette place centrale. Google, Facebook et LinkedIn proposent toutes des modules de « *login* » sur des sites tiers à l'aide du compte de l'utilisateur. Dock.io promeut un modèle plus ouvert et décentralisé dans lequel la base de données centrale n'est pas possédée par la grande plateforme du domaine (Facebook pour les réseaux sociaux, LinkedIn pour la sphère professionnelle et Google pour le reste de l'univers) mais par l'utilisateur lui-même. L'utilisateur peut donc plus facilement migrer entre les plateformes et contrôler ses données. Pour appuyer plus son idéologie, dock.io fait le choix d'utiliser une blockchain publique pour le stockage des données. Ce système de stockage lui permet de ne pas se retrouver en possession des données et limite son pouvoir puisqu'il ne définit que la société ne définit que le protocole permettant d'interagir avec ces données.

Le système semble cependant admettre quelques limites pointées pour la plupart dans le livre blanc de la plateforme (23). LinkedIn étant déjà une plateforme dominante, son intérêt à devenir interopérable est limité, il peut donc contraindre dock.io a utilisé son protocole. De plus, stocker les données sur la blockchain n'offre aucune garantie supplémentaire sur le respect des règles par les plateformes une fois qu'elles sont en possession de vos données. Ce dernier cas est également valable pour le site dock.io lui-même, si le protocole ne requiert pas cette étape, il

semble que *de facto* les utilisateurs utiliserons le site web dock.io qui aura donc accès à l'intégralité des données de ses utilisateurs.

Dans ce cas précis la blockchain nous semble quand même apporter deux atouts majeurs au protocole. Premièrement, il le rend extrêmement robuste. Même en cas de faillite de dock.io le protocole pourra continuer à être utilisé. Secondement, si dock.io voulait changer contre l'avis de tous le fonctionnement de son système, rien n'empêcherait alors les utilisateurs et les applications de continuer à utiliser l'ancien protocole. Pour ajouter un bémol, il nous semble encore une fois que comme les utilisateurs interagiront majoritairement via le site dock.io en cas de fermeture de celui-ci il faudrait qu'une solution alternative équivalente soit rapidement déployée pour permettre au protocole de continuer à fonctionner, ce qui reste hypothétique.

À l'inverse, si l'adossement à la blockchain ethereum rend le protocole très robuste, il rend le coût de celui-ci du système dépendant du cours du gaz (monnaie de la blockchain ethereum servant à exécuter des *smarts-contracts*). Les développeurs sont bien conscients de ce risque et ils proposent en alternative, si jamais le cours du gaz venait à s'envoler, de créer leur propre version de la chaîne pour permettre au protocole de continuer. Ils précisent cependant être opposés à cette solution, sauf en cas de force majeur.

Avant de conclure, il nous faut faire remarquer que dock.io n'est pas la première initiative du genre. Son originalité repose sur l'utilisation de la blockchain. En 2014, le MIT Media Lab proposait un protocole cherchant à répondre en partie aux mêmes problèmes. Il s'agit d'OpenPDS (24). À la différence de dock.io, ce protocole ne propose pas de stocker les données sur la blockchain mais chez un tiers de confiance. Ce tiers agit comme un coffre-fort numérique intelligent. L'utilisateur n'a alors pas à donner un accès direct aux données aux différentes applications sur lesquelles il se connecte, le coffre-fort intelligent réalise les calculs nécessaires sur les données brutes et les communique ensuite aux applications. Nous pensons qu'un tel protocole gagnerait encore plus à être utilisé en coopération avec une blockchain publique puisqu'elle permettrait alors de s'affranchir du tiers de confiance tout en garantissant une protection optimale des données contre les partages abusifs d'une plateforme finale mal intentionné.

Malgré les défauts de cette première version, nous pensons que ce type de protocoles de gestion d'identité est une piste très intéressante d'usages non-monétaires des blockchains. Nous espérons donc que les travaux du *community group* du W3C sur le sujet (auxquels nous avons pu participer sous l'étiquette Canton Consulting) pourront porter leurs fruits (25).

3.2.2 Traçabilité et *supply chain*, le cas everledger

En résumé

Le suivi de la *supply chain*

- Une tâche naturellement effectuée sur une blockchain
- Demande la coopération de tous les maillons de la chaîne

Un système très éloigné des principes du bitcoin

- Un serveur blockchain central
- Aucune des innovations de la blockchain nécessaire à la réalisation du projet

Everledger propose une blockchain, Diamond Time-lapse, permettant de suivre les diamants tout au long de leur parcours depuis la mine jusqu'en bijouterie. Elle est basée sur la technologie hyperledger d'IBM. Elle appartient donc à la galaxie des blockchains privées. Lorsqu'un utilisateur veut connaître la provenance d'un diamant, il entre son identifiant et obtient ainsi tout son parcours

détaillant sa mine d'origine, l'ensemble des artisans l'ayant manipulé à chaque étape de fabrication ainsi que ses différentes caractéristiques après chaque étape (poids, couleur, type de coupe, pureté et taille).

La société Everledger propose à chaque acteur de la chaîne de fabrication de s'intégrer dans le dispositif afin de renseigner toutes les informations nécessaires pour pouvoir fournir une fiche résumée complète du produit au client final à faible coût. Cette transparence a cependant ses limites. Chaque membre de la chaîne peut décider de restreindre les informations passées à son successeur pour éviter notamment de divulguer le nom de son fournisseur à ses clients. Seules quelques données doivent obligatoirement être publiques comme le lieu d'extraction.

Ce type de suivi peut être très facilement effectué dans une blockchain. En effet, il suffit de remplacer le mot bitcoin par diamant et le protocole décrit par Satoshi Nakamoto permet d'effectuer ce suivi. Néanmoins une question se pose, quel problème cherche-t-on à résoudre en utilisant une blockchain ? Dans ce cas, l'apport intrinsèque de la blockchain n'est pas clair.

Le protocole proposé semble faiblement distribué, selon le site internet d'Everledger les données seront stockées sur le serveur blockchain dont le fonctionnement est assuré par IBM. S'il est question que les données soient également inscrites dans une blockchain publique pour que le système soit transparent, cette blockchain ne participera pas de manière active à la certification. Au sujet de la gouvernance, il est dit que le conseil d'administration sera composé des divers parties prenantes mais rien n'est précisé au sujet du fonctionnement de la blockchain. Les fonctions mises en avant sont la synchronisation automatique avec les outils usuels de ce marché et l'automatisation de certaines étapes d'authentification. Toutes ces tâches ne dépendent pas d'une structure blockchain.

À notre connaissance, le protocole utilisé ici ne dépend absolument pas d'une structure blockchain. La société everledger pourrait proposer n'importe qu'elle autre structure pour stocker les données sur son serveur et publier une partie des informations en temps réel pour en assurer la transparence. Une blockchain ne garantit pas comme par magie une meilleure confidentialité ou transparence que d'autres structures de données. Elle a été conçue pour permettre de résoudre le problème de la double dépense en l'absence de contrepartie. Ici ce problème ne se pose pas. De même il n'est pas question de robustesse du système, en effet entretenir un tel système représente un coût très faible pour les grands acteurs du secteur. Pour nous, cette utilisation de la blockchain est plus justifiée par un effet de mode technologique que par un besoin impérieux.

4 Impacts prévus, cadre réglementaire et recommandations

En tant que fonctionnaires, nous avons cherché à aller au-delà de l'aspect technique et applicatif des blockchains et nous poser la question de la vision qu'a l'État de cette technologie émergente. La création de bitcoin fut une vraie révolution en termes de gouvernance en faisant émerger un système sans autorité centrale, ce que nous souhaitions analyser sous un angle étatique, en cherchant à savoir notamment comment le régulateur se positionne vis-à-vis d'une telle technologie et comment la réglementation peut s'adapter aux principes portés par bitcoin.

4.1 Blockchains publiques et gouvernance

Constatons tout d'abord que bitcoin fût un coup de pied dans la fourmilière du monde bancaire, par la suppression de multiples principes de gouvernance : émission de la monnaie par une autorité, fongibilité ou encore contrôle des transactions par les banques. Nous nous proposons dans cette section d'explorer quelques limites des crypto-monnaies, qui apparaissent comme l'une des briques indispensables au fonctionnement des blockchains publiques, avant d'évoquer la question de la gouvernance de ces systèmes, qui nous paraît être le frein majeur au développement de celles-ci.

4.1.1 Statut des crypto-monnaies

En résumé

L'importance des crypto-monnaies pour les blockchains publiques

- Application principale et aspect historique
- Nécessaires au fonctionnement des mécanismes de consensus

Les limites des crypto-monnaies

- Le statut légal, monnaies virtuelles non reconnues par un État
- Peu attractives auprès du grand public

Les crypto-monnaies sont bien plus qu'un cas d'usage des blockchains publiques, elles apparaissent comme un véritable moteur du système. Rappelons tout d'abord que celles-ci sont avant tout l'application historique de cette technologie et, à ce jour, encore la seule parmi les blockchains les plus connues, à l'exception des *smart contracts*, qui sont en revanche à un degré de maturité peu avancé. La blockchain est née, avec bitcoin, de la volonté de mettre en place un système monétaire décentralisé et sans autorité centrale. Les crypto-monnaies sont surtout aujourd'hui un pilier du fonctionnement des blockchains publiques. Les mécanismes de consensus sont ainsi tous fondés sur les crypto-monnaies. La preuve de travail nécessite que des mineurs fournissent de la puissance de calcul afin de valider les blocs. Cette puissance de calcul est évidemment coûteuse et les mineurs ne participent au fonctionnement de la blockchain que parce qu'ils y ont un intérêt économique, du fait de la rémunération qu'ils perçoivent lorsqu'ils parviennent à valider un bloc, ainsi que des frais de transaction payés par les utilisateurs. Il sera par ailleurs intéressant d'observer si les frais de transaction augmentent lorsqu'il n'y aura plus de récompense versée aux mineurs. Si les frais restent minimes, l'incitation à fournir de la puissance de calcul diminuera car l'intérêt économique sera réduit. Il apparaît donc que, sans crypto-monnaie, la rémunération des mineurs disparaîtrait et avec elle toute incitation à miner des blocs. Sans crypto-monnaie, la preuve de travail ne peut donc exister. Il en va de même pour la preuve d'enjeu, où la probabilité de valider un bloc est directement proportionnelle à la quantité de monnaie détenue. Ce mécanisme présuppose donc l'existence d'une crypto-monnaie, l'idée sous-jacente étant qu'un acteur détenant beaucoup de monnaie a un intérêt à garder le système stable et donc à se comporter de manière honnête. Ainsi, imaginer des mécanismes de consensus sans incitation

économique paraît être un vœu pieu, tant est si bien qu'il apparaît difficile d'imaginer des blockchains publiques qui n'implémenteraient pas de telles monnaies virtuelles.

Or, il nous semble que les crypto-monnaies présentent bien trop de lacunes pour véritablement trouver un écho favorable auprès du grand public. Soulignons tout d'abord que ces monnaies numériques ne sont en rien, d'un point de vue légal, reconnues comme des monnaies. En particulier, elles n'ont pas de pouvoir libératoire, ne sont pas garanties par l'État, ne permettent pas de payer l'impôt, … Nous avons évoqué ces limites précédemment et il nous apparaît que le statut des crypto-monnaies est un véritable frein à leur utilisation à grande échelle. Le grand public privilégiera toujours une monnaie d'État, bien plus sûre, tout du moins dans un contexte qui exclut des situations exceptionnelles (crise financière extrêmement grave, guerre, …). Certes, l'implémentation de fonctionnalités autres que les crypto-monnaies pourrait se voir comme une surcouche applicative de la technologie, réduisant les crypto-monnaies à leur rôle d'incitation économique pour le système de consensus. Pour autant, une telle situation présente à nos yeux deux limites. Tout d'abord, les crypto-monnaies sont, tout du moins actuellement, des actifs particulièrement volatils, soumis à une forte spéculation. La volatilité de ce qui est un pilier du fonctionnement du système est clairement une limite car elle fragilise la blockchain, qui pourrait être gravement menacé si sa crypto-monnaie s'effondre, rendant caduque l'incitation économique à miner les blocs. D'autre part, il paraît dur à envisager que les crypto-monnaies ne soient utilisées que pour le système de minage sans aucun lien avec les fonctionnalités implémentées sur la blockchain. En effet, une telle crypto-monnaie apparaîtrait comme un actif sans grande valeur, utilisé uniquement entre les mineurs, et sans application concrète. Cela rendrait la crypto-monnaie faible et donc peu incitative.

4.1.2 Blockchains publiques et gouvernance

En résumé

Blockchains publiques et gouvernance - Gouvernance décentralisée, sans autorité de contrôle - Idéal de liberté ou limite rédhibitoire ?	**Les limites de tels systèmes** - Incompatibilité avec une économie réaliste et réglementée - Absence de protection des utilisateurs et fragilité du système - La confiance en un système opaque et potentiellement faillible

Au-delà des crypto-monnaies, il nous semble que le grand public aura toujours du mal à faire confiance à un système dépourvu de toute gouvernance centralisée, ce que sont par nature les blockchains publiques. Ainsi, bitcoin ne nous apparaît pas tant comme une révolution technologique - il s'agit avant tout d'un assemblage, certes astucieux, de briques techniques qui préexistaient à son invention - que comme une révolution en termes de gouvernance. Ainsi, la blockchain a permis la création d'un système monétaire totalement décentralisé, dépourvu de toute autorité de contrôle qui émet la monnaie ou gère et contrôle les transactions. Il s'agit donc d'un système sans autorité, son fonctionnement étant intégralement décentralisé. La gouvernance d'un tel système s'établit par des mécanismes de consensus fondés sur la puissance de calcul ou la possession monétaire, mais sans qu'émerge un décideur ou un « chef » sur le système. Comme évoqué précédemment, cela peut être perçu de deux manières radicalement opposées et parfois extrêmes. Certains voient dans cette disparition de toute autorité le retour à l'idéal d'un Internet de liberté absolue, sans contrôle, quand d'autres y voient l'émergence d'un système totalement anarchiste. Avoir un système fiable malgré l'absence de contrôle peut bien évidemment avoir des intérêts, par exemple dans la gestion

de l'identité numérique, permettant à chacun de reprendre le contrôle sur ses données numériques. Pour autant, cela fait apparaître à notre sens deux limites majeures.

D'une part, si certaines applications pourraient bénéficier de tels systèmes sans gouvernance, il nous semble que de tels principes sont incompatibles avec bon nombre de principe d'une économie réaliste et ancrée dans un cadre législatif. Si des systèmes comme bitcoin peinent à convaincre le grand public, c'est avant tout parce que les principes prônés paraissent à la plupart totalement opposés à ce qu'ils cherchent dans un système monétaire, à savoir une forme de stabilité et des garanties de sécurité. Comme nous avons cherché à le montrer, un système comme bitcoin n'offre ni l'un ni l'autre, tant il est volatil et tant l'absence de toute autorité est un obstacle majeur au développement de mécanismes de protection des utilisateurs. Bitcoin est ainsi devenu le repaire d'informaticiens fascinés par la prouesse technique et de spéculateurs qui y voient un actif à même de leur faire gagner des millions.

D'autre part, il n'est pas sûr qu'il soit compatible d'avoir un système fiable et sans autorité. Nous avons mis en avant quelques limites des blockchains publiques qui ne semblent pas aller dans ce sens. L'absence de mécanismes de protection des utilisateurs est par exemple un véritable frein. L'affaire *The DAO* a mis en lumière la difficulté à gérer les conséquences d'un détournement de fonds. De plus, nous avons également mis en lumière quelques limites techniques qui nous font douter de la fiabilité et de la stabilité des blockchains publiques. Ainsi, il n'est pas inenvisageable qu'un acteur puisse prendre le contrôle de la blockchain (attaque des 51% voire des 33%), ou que celle-ci soit la cible d'attaques par déni de service. Si bitcoin semble fonctionner de manière stable, le système n'en est pas moins fragile sur certains points.

Enfin, il nous semble qu'affirmer que les blockchains sont des systèmes sans confiance est, sinon une aberration, du moins une grave exagération. Certes, les mineurs n'ont pas besoin de se faire confiance pour que le système fonctionne. Certes, la décentralisation du système fait que l'utilisateur n'a pas à remettre sa confiance entre les mains d'une autorité centrale. Cependant, l'utilisateur, s'il utilise la blockchain, fait confiance au système lui-même, c'est-à-dire à la fois au code informatique et à l'écosystème qui l'entoure, à savoir le réseau des mineurs. Si le code de bitcoin semble jusqu'à présent ne pas avoir révélé de faille, l'exemple de *The DAO* a démontré que les systèmes informatiques n'étaient pas infaillibles, même si la faille se situait dans le code des *smart contracts* et non dans celui de la blockchain même. Les mineurs, quant à eux, ne sont la plupart du temps pas identifiés et leurs intérêts sont mal connus. Pour revenir à l'exemple du système monétaire, il n'est pas certain que le grand public préférera faire confiance à un système informatique opaque et mal compris, contrôlé par des mineurs non identifiés et pour la plupart chinois, qu'à une banque qu'ils connaissent, qui leur fournit un service client, et qui présente des garanties d'État. La blockchain n'est donc pas un système sans confiance mais un système où la confiance est placée dans des acteurs différents et non traditionnels.

4.1.3 Synthèse

Si bitcoin a été une vraie révolution en termes de gouvernance, le système demeure aujourd'hui le repaire de quelques informaticiens fascinés ou autres trafiquants et spéculateurs. Le grand public, lui, se désintéresse encore massivement de ces systèmes à la gouvernance trop incertaine et qui présentent, à ses yeux, trop de limites et trop peu de garanties. Si l'absence de contrôle est un idéal de liberté pour certains, il est surtout rédhibitoire pour la plupart des gens, qui préfèrent des systèmes sur lesquels ils peuvent identifier une autorité, qui leur offre garanties et protection.

Cela est en partie illustré par l'utilisation finalement assez peu répandue des crypto-monnaies comme le bitcoin ou l'ether. Ces monnaies virtuelles, trop volatiles, inquiètent plus qu'elles n'attirent, et apparaissent avant tout aujourd'hui comme des objets de spéculation. Or, elles sont un pilier fondamental de la technologie blockchain, sous-tendant les mécanismes de

consensus, tant est si bien qu'il est difficile d'envisager l'avenir des blockchains sans se poser la question de l'évolution de ces monnaies virtuelles.

4.2 Régulation et réglementation des blockchains : l'exemple du secteur financier

La blockchain est évoquée régulièrement dans les secteurs de la banque et de l'assurance. Les *smart contracts* sont souvent présentés comme de vrais opportunités dans le secteur assurantiel, car ils permettraient l'automatisation d'un certain nombre de contrats. Comme évoqué précédemment, il nous semble que seuls des contrats assez simples pourraient ainsi se développer, mais que le domaine de l'assurance reste trop complexe à automatiser pour imaginer un développement à grande échelle des *smart contracts* d'assurance. De plus, un certain nombre de freins réglementaires existent, que nous aborderons dans cette partie. De même, la banque est un secteur au sein duquel la blockchain est régulièrement citée. Un consortium de banques, R3, s'est même développé dans l'idée d'analyser ce phénomène et de tenter de trouver des cas d'usage à la technologie dans le domaine bancaire. Les conclusions actuelles du consortium ne paraissent pas aller dans le sens d'une révolution par la blockchain mais quelques cas d'usage pourraient émerger.

Cette partie est destinée à présenter quelques enjeux en termes de régulation sur des domaines financiers principalement, et notamment sur les secteurs bancaires et assurantiels, régulés en France notamment par l'ACPR (Autorité de Contrôle Prudentiel et de Résolution), avec qui nous avons pu échanger autour de la question de la régulation de cette technologie nouvelle.

4.2.1 Préambule : quelques principes de régulation financière

En résumé

Lutte contre le blanchiment

- Connaissance des clients pour lutter contre la fraude
- Lutte contre le financement du terrorisme

Protection des consommateurs

- Garantie des fonds bancaires
- Droit à l'oubli, confidentialité

Stabilité du système financier

- Limiter la contagion en cas de crise

Nous souhaitions rappeler en préambule quelques grands principes de régulation financière qui guident l'action du régulateur et qui fourniront un cadre d'analyse pour analyser la position de celui-ci par rapport à l'émergence des blockchains sur les secteurs de la banque et de l'assurance.

L'un des principes cardinaux qui président à l'action du régulateur concerne la protection des utilisateurs. Tout projet bancaire ou assurantiel doit ainsi présenter un certain nombre de garanties auprès des consommateurs, tels que la protection des données, la confidentialité ou le droit à l'oubli. Ces droits doivent être pris en compte dans le déploiement de structures informatiques destinées à héberger des informations confidentielles concernant les clients. De plus, tout contrat bancaire ou assurantiel doit respecter un certain nombre de garanties juridiques destinées à protéger les consommateurs, qui bénéficient de plus de garanties fournies par l'État lui-même. Ainsi, notons que les dépôts bancaires bénéficient d'une garantie d'État, à savoir que les détenteurs d'un compte bancaire auprès d'un établissement agréé peuvent être indemnisés en cas d'incapacité de leur banque à rembourser leurs dépôts. De tels mécanismes sont destinés à instaurer une confiance dans le système bancaire et une forme de stabilité.

Un autre grand principe de régulation concerne la lutte contre le blanchiment et contre le financement du terrorisme, qui est un sujet particulièrement pertinent au vu de l'actualité mondiale et française. Pour cela, certaines règles doivent être respectées par les organismes bancaires et

assurantiels. Une première problématique concerne la connaissance des clients. Les banques et assurances doivent ainsi être en mesure d'identifier de manière certaine leur client, permettant notamment d'identifier les personnes ayant des pratiques frauduleuses. Les flux financiers doivent également être traçables, ce qui peut par exemple se traduire par une conservation des transactions bancaires afin de pouvoir identifier des flux suspects. Enfin, le régulateur participe à la lutte contre le développement d'économies parallèles frauduleuses dans son domaine de compétence, tel que, pour l'ACPR, le développement de contrats d'assurance par des organismes non agréés.

Enfin, le régulateur a également pour mission de garantir la stabilité du système financier, et donc de limiter toute contagion en cas de crise majeure, pour éviter tout effondrement du système. Les garanties d'État sont par exemple un mécanisme pour accroître la confiance dans le système bancaire et lutter contre tout mouvement de panique en cas de défection d'un acteur bancaire.

4.2.2 Blockchains et secteurs financiers

En résumé

Trois cas d'usages envisagés

- En interne, optimisation du *back office*
- Système partagé, désintermédiation
- Applications destinées au grand public

État actuels des projets blockchains

- Beaucoup de communication
- Globalement, état d'avancement assez faible
- Effet de mode très important

Sur les secteurs bancaires et assurantiels, le régulateur considère actuellement trois grands types de cas d'usage possibles des blockchains. Le premier consiste en l'utilisation de blockchains pour des applications internes à une banque ou une assurance. L'idée générale consisterait à utiliser des blockchains privées pour optimiser certaines applications de *back office*, de manière interne à un unique acteur. Un deuxième cas d'usage consisterait à mettre en place un système partagé de type blockchain hybride entre plusieurs acteurs. L'intérêt principal consiste à connecter des acteurs qui ne l'étaient pas nécessairement, à des fins de désintermédiation. Une illustration de ce type d'applications est bien évidemment fournie par l'exemple de FundsDLT, sur lequel nous nous sommes penchés de manière détaillée plus en amont dans ce mémoire. Un autre exemple pourrait être de changer le système de gestion des transactions bancaires, SWIFT, qui apparaît comme vieillissant. Le consortium R3 semble s'être penché sur le sujet mais a l'air de se détourner de la technologie blockchain comme solution potentielle à la mise en œuvre d'un nouveau système. Enfin, un troisième cas d'usage envisagé serait la volonté d'une banque ou d'une assurance de développer un système directement adressé aux utilisateurs finaux sur une blockchain. Il ne nous est cependant pas apparu qu'il existe actuellement de tels projets directement orientés vers un segment B2C dans les domaines de la banque ou de l'assurance.

De manière générale, il nous est apparu difficile d'appréhender l'état de développement de projets blockchains sur ces secteurs. À titre d'exemple, nous avons échangé avec une compagnie d'assurance, qui nous a assuré développer des projets autour de cette technologie, mais sans vouloir nous en révéler plus pour des raisons de confidentialité. Il nous semble aujourd'hui que, si certains acteurs ont atteint un degré de maturité sur le sujet pour envisager des usages pertinents, un certain nombre d'entreprises ont communiquent autour de cette technologie du fait d'un effet de mode important, sans pour autant développer de projet sérieux dans l'immédiat. Nos échanges avec l'ACPR semblent aller dans ce sens. Ainsi, il apparaît que se développent d'une part quelques projets ambitieux, voire trop ambitieux. Certains acteurs prônent aujourd'hui une dérégulation totale des blockchains, ou formulent le souhait de pouvoir utiliser directement sur un tel système des monnaies banque centrale. Ces idées paraissent pour le moment inapplicables en l'état. En

particulier, la régulation paraît tout à fait nécessaire pour garantir *a minima* une protection des consommateurs. Certains projets se développent à un rythme moins effréné et avec moins d'ambitions mais il apparaît que, dans les secteurs bancaires et assurantiels, la plupart des acteurs en soient au stade des discours, des déclarations d'intentions ou des preuves de concept. Seuls quelques acteurs pourraient être prêts rapidement. Ceci nous apparaît plutôt sain, tant la technologie manque de maturité. Surtout, entre blockchains publiques et privées, chacune détenant ses caractéristiques propres, définir le système le plus adapté et les cas d'usage les plus pertinents ne doit pas être fait dans la précipitation. Il nous apparaît en revanche assez problématique qu'il existe autour de cette technologie une forme d'agitation qui accapare l'attention de multiples acteurs qui, ne voulant pas être dépassés en cas de révolution majeure, prétendent s'intéresser à cette technologie sans en ressentir nécessairement l'intérêt. Rappelons cette citation de Dan Ariely sur le *big data*, qui pourrait s'appliquer tout autant à la blockchain :

> *« [it] is like teenage sex: everyone talks about it, nobody really knows how to do it, everyone thinks everyone else is doing it, so everyone claims they are doing it »*

En clair, chacun regarde son voisin avec la crainte qu'il développe un projet lui conférant un réel avantage compétitif, et préfère donc mettre quelques moyens sur le sujet pour limiter les risques sans pour autant y voir un réel intérêt. Ce jeu de dupe crée un effet de mode autour de la blockchain, mais nous doutons qu'elle soit à l'origine d'une révolution majeure, tout du moins dans un avenir proche.

Quelques expérimentations ont pu être lancées en production, c'est le cas du projet MADRE de la banque de France. Il s'agit d'une Blockchain hybride qui permet aux banques de générer automatiquement des identifiants créanciers SEPA. Ces identifiants sont nécessaires aux entreprises souhaitant émettre des prélèvements.

Cette Blockchain, construite sur le modèle d'ethereum, permet de diminuer grandement le temps nécessaire à l'émission de ces identifiants qui est passé de plusieurs jours à quelques heures, grâce à des vérifications automatisées par des *smart-contracts*.

Cette expérimentation a permis à la banque de France de monter en compétences dans le domaine des blockchains, cependant pour cet usage précis on peut s'interroger sur la pertinence de l'utilisation d'une blockchain.

En effet la banque de France aurait pu informatiser ce processus en se posant comme l'acteur central, puisque :

- premièrement, elle garde, de toute façon, le contrôle sur le processus ;
- secondement, tous les participants (les banques) ont confiance dans l'institution.

Malgré ces objections, la structure naturellement décentralisée de la Blockchain a permis au système de gagner en robustesse tout en facilitant le partage des coûts. Les acteurs du système supportant naturellement, en ayant leur propre copie de la Blockchain, une partie des coûts du système.

Encadré 7 : Projet MADRE, Banque de France

4.2.3 Quelle vision pour le régulateur ?

En résumé

Sur les blockchains publiques

- Beaucoup de prudence du régulateur
- Incompatibilité avec les principes de régulation
- Trop de limites techniques pour une utilisation sur les secteurs bancaires et assurantiels
- Interdiction pour un acteur régulé d'utiliser des blockchains publiques pour des applications grand public

Sur les blockchain privées

- Pas d'interdiction d'utilisation
- Nécessité d'un contrôle des risques opérationnels
- Blocages internes dans certaines entreprises

Nos discussions avec l'ACPR nous ont permis d'appréhender le point de vue du régulateur (18) sur le sujet des blockchains, sur les secteurs bancaires et assurantiels. Mettons tout de suite de côté les acteurs qui considèrent que les blockchains ne devraient faire l'objet d'aucune régulation ou souhaiteraient mettre en oeuvre des systèmes assurantiels sans aucun agrément. En effet, la banque et l'assurance sont des secteurs régulés et l'apparition d'une technologie nouvelle ne doit pas être le prétexte pour développer des systèmes de manière anarchique en omettant tous les principes de régulation. De manière plus pragmatique, le point de vue de l'ACPR est avant tout fondé sur une approche par les risques, qui *de facto* distingue de manière assez radicale les blockchains publiques et privées.

Ainsi, le point de vue du régulateur sur les blockchains publiques est pour le moment tout à fait suspicieux. De nombreuses limites s'opposent actuellement à l'utilisation de blockchains publiques dans des secteurs régulés. Nous citions comme grand principe de régulation la protection des données, la confidentialité ou le droit à l'oubli. Il semble évident que de tels principes sont actuellement incompatibles avec des systèmes publics, ouverts à tous. Nous avons également cité un certain nombre de limites en termes de protection des consommateurs : absence de service client, absence de garantie d'état ou de garantie de convertibilité sur les crypto-monnaies, … Nous évoquions également les limites des blockchains pseudonymes ou anonymes, notamment dans l'exemple des *smart contracts*. La difficulté voire l'impossibilité d'identifier les deux parties contractantes apparaît comme un vrai frein au développement de tels contrats. En cas de litige, comment pourrait-on par exemple mener une action en justice si l'on ne peut pas identifier la partie mise en cause ? De manière plus générale, la question du pseudonymat ou de l'anonymat pose de vrais problèmes en termes de ce que l'on appelle le KYC (Know Your Customer), à savoir la connaissance des clients, nécessaire notamment dans les secteurs bancaires et assurantiels pour lutter contre la fraude et le blanchiment. L'exemple de Silk Road a prouvé qu'il était possible de lutter contre un certain nombre de trafics sur bitcoin mais que cela était difficile, d'autant que la tâche sur une blockchain anonymisée serait plus ardu encore. Pour rappel, Silk Road était une plateforme de vente, entre autres, de drogues et d'armes. Le FBI est parvenu à retracer les transactions bitcoin du fondateur de la plateforme, en identifiant sa clé publique avant de remonter à son identité. Ses fonds ont alors pu être saisis en s'emparant de ses clés privées, en mettant la main sur son matériel informatique. Si un tel exemple est une réussite, il illustre aussi la difficulté de lutter contre les trafics. De nombreuses limites peuvent s'opposer à l'identification d'un trafiquant : utilisation de multiples clés publiques rendant difficile la traçabilité des transactions, difficultés à remonter à l'identité de la personne, impossibilité de saisir son matériel et de récupérer les clés privées, *etc.* De manière évidente, les blockchains publiques représentent donc un vrai défi en

termes de lutte contre le blanchiment et les trafics. D'autres limites, techniques, s'opposent au développement des blockchains dans les secteurs bancaires et assurantiels. A titre d'exemple, le volume de transactions ou les temps de latence sont de véritables freins au développement de projets, comme nous l'avons déjà montré. L'irréversibilité des transactions est également contraire à la régulation, car elle empêche *de facto* tout recours pour annuler une transaction *a posteriori*. Une autre limite aux yeux du régulateur vient de la difficulté d'auditer des systèmes totalement décentralisés tels que les blockchains publiques. Faudrait-il auditer chaque mineur, chaque utilisateur, voire même le code informatique lui-même ? Qui serait susceptible d'être sanctionné en cas de dérives ? Ces problèmes apparaissent d'autant plus difficiles à résoudre que les blockchains publiques sont par nature sans frontière, ce qui rend les questions légales encore plus complexes en l'absence de réglementation internationale.

Ces limites paraissent trop nombreuses et rédhibitoires pour que se développent des projets bancaires ou assurantiels sur les blockchains publiques. Le point de vue de l'ACPR est donc aujourd'hui extrêmement simple : une banque ou une compagnie d'assurance n'est pas autorisée à utiliser une blockchain publique comme un support informatique sur lequel on puisse implémenter des applications destinées au grand public. Les risques pour les utilisateurs est considéré comme trop important. Cependant, un tel point de vue, s'il clarifie la situation pour les acteurs traditionnels, laisse un certain nombre de questions ouvertes. Ainsi, si tout acteur régulé, ayant reçu un agrément, ne peut utiliser ces systèmes, d'autres acteurs développent des applications de paiement ou d'assurance sur des blockchains publiques, l'exemple le plus simple étant le système bitcoin lui-même ou toute autre crypto-monnaie qui, sans être des monnaies reconnues, n'en demeurent pas moins des systèmes de paiement, bien que limités. Il semblerait que l'ACPR réfléchisse à la définition d'un statut pour bitcoin, ce qui nous paraît nécessaire. En effet, il paraît difficile pour le régulateur de laisser se développer un système contrevenant aux principes de régulation sur un secteur régulé. Pour autant, la difficulté à définir un tel statut est réel, ne serait-ce que du fait qu'il n'existe aucun interlocuteur sur un tel système décentralisé. En attendant qu'un tel statut puisse éclaircir les choses, les blockchains publiques peuvent être utilisées, mais les utilisateurs doivent en assumer le risque.

Si les banques ou les compagnies d'assurance ne peuvent utiliser de blockchains publiques, rien ne les interdit en revanche de développer des blockchains privées, en interne ou entre acteurs. De manière générale, de tels systèmes ne contreviennent en effet pas aux principes de régulation. Les systèmes étant fermés et partagés, en principe, entre des acteurs régulés, les données clients demeurent confidentielles et protégées, tout autant qu'avec les systèmes actuels. De plus, les blockchains privées sont assez flexibles et permettent tout à fait la mise en oeuvre de mécanisme de réversibilité, de contrôle des transactions, ou encore de KYC. L'ACPR ne bloquerait ainsi pas le déploiement de projets blockchains, à la condition que ceux-ci présentent des garanties en termes de risques opérationnels. Ceci n'est cependant pas spécifique à la blockchain mais est un prérequis nécessaire avant le déploiement de tout système informatique sur un secteur régulé. Si nous avons montré que les blockchains privées pouvaient présenter des risques en termes de sécurité numérique, notamment du fait de la duplication des données, cela ne semble pas être un frein rédhibitoire à l'utilisation de tels systèmes. Lors de nos discussions avec l'ACPR, il est même apparu que les blocages majeurs n'émanaient pas du régulateur mais des entreprises elles-mêmes. En effet, les blockchains apparaissent comme des systèmes à même de favoriser la désintermédiation et donc de rendre obsolètes un certain nombre d'acteurs, comme l'illustre l'exemple de FundsDLT. Certains y voient donc une menace pour l'emploi, ce qui crée en interne des blocages, notamment syndicaux, au développement de projets blockchains.

De manière générale, la blockchain pose un certain nombre de questions que la réglementation devra trancher à l'avenir. Par exemple, les *smart contracts* devront sans doute évoluer pour prétendre être utilisés dans des domaines comme l'assurance. Le principe est particulièrement intéressant sur certains domaines. Citons par exemple le cas des transports, où il

serait aisé d'automatiser l'exécution de contrats de remboursements en cas de retard. Cependant, il demeure un certain nombre de limites, à commencer par le fait que le consommateur doit savoir sur quoi il s'engage, ce qui n'est pas évident sur des contrats rédigés dans un langage informatique. Une solution pourrait être d'attacher à chaque *smart contract* un contrat écrit, signé par les deux parties, reprenant les clauses d'exécution du *smart contract*. Il faudrait alors une preuve que les deux formes du contrat ne sont pas contradictoires, preuve qui pourrait être fournie par un garant juridique (juge, avocat, …), ce qui nécessiterait de faire confiance à un tiers. L'avenir des blockchains dans les secteurs régulés passe d'ailleurs sans doute par la réintégration de tiers de confiance et d'autorités de contrôle, ce qui paraît tout à fait possible sur des systèmes privés mais totalement à l'encontre de l'esprit des blockchains publiques.

4.2.4 Blockchains et réglementation, l'exemple des titres non cotés

En résumé

Consultation de la Direction Générale du Trésor

- Initiée par la loi Sapin II
- Ouvre la porte à l'utilisation de DLT sur le marché des titres non cotés
- Création d'une zone de test pour éprouver la technologie et la réglementation

Contenu de la consultation

- Adressée aux acteurs du secteur
- Identification des besoins techniques, applicatifs et réglementaires

Réponse de Paris Europlace

- Blockchains surcalibrées pour les titres non cotés
- Nécessité d'un statut de preuve pour les DLT
- Adaptation de la réglementation existante, pas de nouveau cadre réglementaire

Au-delà des marchés bancaires et assurantiels, la réglementation cherche également à appréhender l'émergence de cette nouvelle technologie. Une bonne illustration en est la consultation publique (20) lancée par la Direction du Trésor sur l'application des DLT au marché des titres non cotés. Cette initiative a pour origine l'article 120 de la loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, dite loi Sapin II. Celle-ci autorise le Gouvernement à *« réformer le droit applicable aux titres financiers afin de permettre la représentation et la transmission au moyen d'un dispositif d'enregistrement électronique partagé (en anglais, distributed ledger technology, ou DLT) des titres financiers qui ne sont pas admis aux opérations d'un dépositaire central ni livrés dans un système de règlement et de livraison d'instruments financiers »*. En clair, elle ouvre la porte à l'utilisation de blockchains privées sur le marché des titres non cotés - c'est-à-dire des actions d'entreprise non échangeables sur un marché boursier car vendues directement auprès des investisseurs sans appel public à l'épargne - et des parts détenus par les OPC (Organismes de Placement Collectif), à savoir les fonds d'investissement. L'intention sous-jacente consistait à identifier un marché de taille restreinte, sans risque systémique majeur, afin de l'utiliser comme zone de test sur laquelle adapter le cadre réglementaire pour favoriser le développement de projets blockchains. L'objectif poursuivi est double : éprouver l'intérêt de la technologie ainsi que la pertinence de la réglementation.

Les blockchains sont envisagées comme solution de complément ou de substitution aux comptes titres, à savoir les registres listant les titres détenus par un investisseur. Les DLT pourraient être utilisés comme des copies numériques, dématérialisées, de ces comptes titres. Surtout, il est également envisageable d'aller plus loin qu'une simple copie numérique de ces titres et de donner une véritable valeur juridique à ces DLT, en considérant qu'une écriture dans un DLT pourrait faire

office de preuve de propriété d'un point de vue juridique. Si une telle technologie était utilisée, il resterait à savoir entre quels acteurs ce registre serait partagé, ainsi que la forme qu'il prendrait : registre de titres ou registre de transactions.

Suite à la loi Sapin II, la Direction du Trésor a ouvert une consultation auprès des acteurs du marché des titres non cotés, l'objectif étant d'identifier plus précisément la position de ces acteurs quant à un éventuel déploiement de solutions blockchains. La consultation invite ainsi les acteurs à s'exprimer sur de nombreux sujets, tels que les cas d'usages les plus pertinents, la nécessité ou non de développer un nouveau cadre réglementaire, ou encore des questions plus techniques sur l'architecture du système et les propriétés les plus adaptées. Cette consultation ouvre la porte à une véritable évolution de la réglementation et les questions couvrent à la fois les aspects applicatifs, législatifs et techniques. La consultation a pris fin au 19 mai, et fixe la date du 9 décembre 2017 comme objectif temporel pour la création d'un cadre réglementaire adapté au développement de projets blockchains.

A l'heure où nous rédigeons ces lignes, peu d'informations ont été publiées quant aux réponses reçues par la Direction du Trésor à cette consultation. Notons tout de même quelques commentaires émis par Paris Europlace (20), à commencer par la remarque que la blockchain est sans doute surcalibrée par rapport à un marché de petite taille comme celui des titres non cotés, mais qu'elle aurait un intérêt réel sur le marché des OPC. Surtout, la place financière de Paris estime que le développement de projets blockchains n'aurait de sens que si les DLT ainsi conçus avaient une véritable valeur juridique, et qu'une écriture puisse être reconnue comme un titre de propriété sans avoir besoin d'inscrire le titre dans un registre matériel. Enfin, Paris Europlace estime que le développement de projets blockchain doit se faire au maximum dans le cadre réglementaire en place, la blockchain étant une technologie peu mature et susceptible d'évoluer, rendant potentiellement caduque un cadre législatif trop précis, ciblé sur la technologie telle qu'elle est aujourd'hui. Ce point nous paraît tout à fait important et rejoint la position que nous tenons vis-à-vis de toute réglementation de la blockchain, que nous défendrons dans la section suivante. Enfin, la place financière ne souhaite se prononcer sur l'intérêt d'une blockchain privée plutôt que d'une blockchain publique, considérant que la réglementation doit fixer des règles générales mais être « axiologiquement neutre » quant à la technologie utilisée.

4.2.5 Synthèse

Le régulateur regarde donc avec attention l'émergence des technologies blockchains, avec notamment un regard critique sur les blockchains publiques, qui font émerger des systèmes sans contrôle, totalement décentralisés. En particulier, le régulateur des banques et assurances, en gardant en tête trois grands principes de régulation (protection des consommateurs, lutte anti-blanchiment et stabilité financière), envisage trois grands cas d'usage pour les blockchains : développement en interne d'applications visant à optimiser le *back office*, développement de systèmes partagés entre acteurs à des fins de désintermédiation et développement d'applications sur un segment B2C.

Fort de ces grands principes, le régulateur interdit pour le moment à tout acteur régulé d'utiliser des blockchains publiques pour développer des applications ayant un impact sur le consommateur, considérant que ces systèmes présentent trop de limites en termes de gouvernance et de protection des utilisateurs. En revanche, une banque ou une assurance peut tout à fait utiliser des blockchains privées, à condition d'effectuer un contrôle poussé des risques opérationnels. Cependant, il ne nous semble pas aujourd'hui qu'émergent beaucoup de projets matures et concrets.

Enfin, la réglementation cherche à s'adapter aux blockchains. A ainsi été lancée une consultation sur le marché des titres non cotés, le but étant d'identifier les freins réglementaires et

techniques, afin de favoriser par la suite le développement de projets blockchains et ainsi éprouver l'intérêt de la technologie mais aussi la robustesse du cadre réglementaire.

4.3 Recommandations et ouvertures sur la régulation

Nous avons donc vu comment la régulation pouvait chercher à s'adapter à la technologie blockchain, avec aujourd'hui nombre d'interrogations et une approche par les risques qui exclut de fait les blockchains publiques, considérées comme présentant trop de limites. La réglementation cherche également à tenir compte de cette technologie et à en éprouver l'intérêt. Nous nous proposons ici de formuler quelques recommandations quant à quelques principes qui nous paraissent importants lorsqu'il s'agira de créer un cadre réglementaire autour des blockchains. En particulier, nous prônons un principe de neutralité technologique de la réglementation et nous incitons les pouvoirs publics à ne pas se précipiter pour réglementer une technologie aujourd'hui peu mature.

4.3.1 La réglementation doit être technologiquement neutre !

En résumé

Principe de neutralité technologique de la réglementation	**Il faut mener une réflexion globale sur les enjeux du numérique**
- Pas de réglementation spécifique à la blockchain - Un cadre réglementaire généraliste - Réglementer l'applicatif et non la technologie sous-jacente	- Réflexion alimentée par des problématiques posées par de multiples technologies - Neutralité de la rédaction du cadre réglementaire - Compatible avec une réflexion sur les besoins des acteurs sur la blockchain

Rappelons en préambule l'un des points soulevés par la place financière de Paris dans sa réponse à la consultation de la Direction du Trésor. Celle-ci s'est exprimée sur l'intérêt d'un système privé ou d'un système public, en prônant une ordonnance « axiologiquement neutre », à savoir un texte qui ne spécifie pas nécessairement que les projets doivent s'articuler autour d'un format de blockchains plutôt qu'un autre. A notre sens, ce point est tout à fait pertinent et nous proposons d'aller plus loin encore. Selon nous, la réglementation ne doit pas être spécifique à une technologie mais au contraire tout à fait généraliste. En effet, si la blockchain est aujourd'hui victime de l'effet *buzz word* qui est à l'origine de l'émergence de nombreux projets, elle n'en demeure pas moins - ou tout du moins elle devrait demeurer - un moyen et non une fin en soi. Il nous semble donc que la blockchain ouvre des perspectives applicatives et que ce sont ces applications qui doivent faire l'objet d'une réglementation. Imaginons ainsi que, sur un projet précis, la blockchain soit en concurrence avec une autre technologie pour développer un cas d'usage similaire. Cela n'aurait alors pas de sens que la blockchain puisse être soumise à des contraintes spécifiques qui pourraient empêcher l'implémentation de certaines propriétés, qui seraient en revanche possible avec une autre technologie. Osons une comparaison un peu simpliste : si l'État veut lutter contre les excès de vitesse, il peut réglementer sur le positionnement des radars et certains prérequis techniques pour de tels systèmes de détection de vitesse (réglementation sur la précision du système en termes de marges d'erreur par exemple) mais cela n'aurait pas de sens de préciser quel matériel technique ou quels algorithmes de traitement des données devraient être utilisés ! Il nous semble que le rôle de l'État consiste à fixer des limites quant à ce qu'un acteur économique peut faire ou non, mais pas à lui imposer les moyens techniques à mettre en oeuvre tant qu'il est en mesure de respecter les

règles qui lui ont été fixés. D'autant que l'expertise technique est plutôt du côté des acteurs que du côté de l'État. Une autre limite à la création d'un cadre réglementaire spécifique à la technologie vient de la difficulté à définir la technologie elle-même. Qu'est-ce réellement qu'une blockchain ou un DLT ? Nous espérons vous avoir convaincu que la réponse était loin d'être évidente tant ces terminologies regroupent des systèmes bien différents. L'État devrait-il alors formuler sa propre définition de ce qu'est une blockchain ? Cela ne nous paraît pas devoir être le rôle de l'État que de fixer la définition et les standards techniques d'une technologie. Cela pourrait ouvrir également la porte à des abus, certains cherchant à contourner la réglementation par quelques points de détail techniques permettant d'éviter l'appellation de blockchain. L'intérêt d'un cadre généraliste est de s'intéresser uniquement aux applications et aux caractéristiques globales de la technologie, sans rentrer dans des détails techniques qu'il appartient aux acteurs économiques d'optimiser.

Il nous semble que, plutôt que de réglementer de manière spécifique une technologie, il serait plus pertinent de mener une réflexion globale sur les enjeux et les risques du numérique. Cette réflexion pourrait déboucher sur un cadre réglementaire tout à fait généraliste, en incorporant des sujets et des questions inspirées par de multiples problématiques et technologies. Bien évidemment, cette réflexion peut être inspirée par des questions qu'ouvre l'émergence de la technologie - voire plutôt les technologies - blockchain. Citons par exemple la notion de *smart contracts*, que nous avons présentés comme incompatibles avec certaines applications auprès du grand public, en particulier parce que cela pose la question de la connaissance par le souscripteur de ce à quoi il s'engage en acceptant un contrat totalement dématérialisé rédigé en langage informatique. Nous citions comme solution le fait de lier à chaque *smart contract* un contrat écrit reprenant les conditions d'exécution du *smart contract*. Imposer un tel mécanisme ne nécessite pas de parler de blockchains ou même de *smart contracts*. On pourrait tout à fait imaginer une compagnie d'assurance automatiser en interne l'exécution de contrats très simples (encore une fois, les retards de transport paraissent intéressants en ce sens) sans pour autant les implémenter sur une blockchain mais simplement sur une base de données standardisée en interne. L'État doit donc, à ce sujet, simplement réglementer les conditions d'acceptabilité, en termes de risques pour les consommateurs notamment, qui doivent s'appliquer pour l'automatisation de l'exécution d'un contrat.

Cela n'interdit pas, en revanche, de commencer à identifier les besoins des acteurs pour favoriser le développement des blockchains, notamment en termes de réglementation, comme le fait très bien la consultation de la Direction du Trésor. Cependant, il nous semble qu'une telle consultation ne doit pas aboutir à la création d'un cadre réglementaire spécifique à la blockchain mais plutôt à un cadre aussi généraliste que possible, qui ne cible pas de manière spécifique la blockchain mais qui apporte des réponses à des problématiques plus générale, en formulant certains principes de manière aussi neutre que possible.

4.3.2 Réguler les blockchains n'est pas une urgence !

En résumé

Pas de précipitation à réglementer la blockchain

- Technologie peu mature, non standardisée
- Risque de brider les développements de la technologie en France
- Cadre existant *a priori* suffisant pour protéger les consommateurs

Peu de risques réglementaires actuellement

- Les blockchains publiques fonctionnent sur des marchés de niche
- Utilisateurs conscients des risques et prêts à les assumer

Alléger le cadre réglementaire

- Dans le but de favoriser l'émergence de projets
- L'exemple des titres non cotés

Tout comme le préconise la place financière de Paris, il nous paraît également nécessaire de ne pas se précipiter dans la rédaction d'un cadre réglementaire adapté à la blockchain. Rappelons que cette technologie n'est pas encore mature et pourrait évoluer, tant d'un point de vue technique que applicatif. A ce titre, adapter la réglementation en réaction à certaines limites actuelles des blockchains pourrait être contre-productif et brider le développement de cette technologie, tout du moins en France, nous affaiblissant potentiellement vis-à-vis de certains pays concurrents. Nous prônons également un développement de la blockchain à droit aussi constant que possible. Il nous apparaît que le droit actuel a été pensé comme un moyen de protection des utilisateurs et est donc adapté pour prévenir les risques les plus importants liés au déploiement d'une technologie comme la blockchain. L'exemple des secteurs bancaires et assurantiels montrent que le droit actuel est suffisant pour lutter contre les risques majeurs, en mettant de côté les blockchains publiques, trop risquées pour les utilisateurs. Selon nous, il n'est donc pas nécessaire de s'emparer en urgence des problématiques de la blockchain mais plutôt de se focaliser dans l'immédiat sur deux questions : combler, si besoin, des failles réglementaires permettant le développement de technologies risquées pour les utilisateurs, et alléger le cadre réglementaire pour favoriser le développement de projets blockchains tout en respectant les grands principes de régulation, à commencer par la protection des utilisateurs.

En ce qui concerne le premier point, il ne nous apparaît pas qu'il y ait aujourd'hui de grandes failles qui mettent potentiellement en danger les consommateurs. On peut bien sûr s'inquiéter de voir naître des systèmes tels que bitcoin, offrant des moyens de paiement sans autorité de contrôle et sans mécanismes poussés de protection. Pour autant, ces systèmes demeurent aujourd'hui concentrés sur des marchés de niche, et ne s'apparentent pas à des systèmes de paiement à grande échelle. Pour caricaturer, on peut aujourd'hui distinguer trois types de population utilisant les crypto-monnaies telles que bitcoin. Le premier groupe contient des passionnés de technologie, friands de nouveaux concepts techniques ou attachés à une vision libertarienne de l'Internet. Cette population est donc soit consciente du fonctionnement du système et donc en mesure d'en appréhender les risques, soit simplement attachée à toute forme d'indépendance, fût-elle au détriment d'une forme de sécurité. La deuxième population regroupe des gens à la recherche d'un actif spéculatif risqué en mesure de fluctuer fortement et rapidement. Ils sont donc conscients des risques du système car c'est précisément ce qu'ils recherchent. Enfin, il existe une troisième population composée d'acteurs malhonnêtes en quête d'un système opaque favorisant des opérations de blanchiment ou de trafic. En conclusion, il nous apparaît que les utilisateurs actuels des crypto-monnaies sont des gens conscients des risques et tout à fait enclins à les prendre. A ce stade de développement, les blockchains publiques sont donc des systèmes certes risqués, mais sur

des marchés de niche. A ce titre, s'il paraît judicieux pour l'État de réfléchir à la définition d'un statut pour ces crypto-monnaies, qui vivent actuellement plus ou moins en dehors de la réglementation, elles ne présentent pas un risque majeur pour la population et il n'y a pas urgence à définir un tel statut.

Le deuxième axe de développement de la réglementation devrait être d'identifier certains points réglementaires qui peuvent être allégés sans pour autant augmenter les risques de manière inacceptable, et qui auraient un véritable impact positif sur le développement de projets blockchains. Pour revenir sur l'exemple du marché des titres non cotés, reconnaître la validité d'une écriture électronique comme une preuve de la propriété d'un titre permettrait de donner un véritable intérêt au développement de blockchains sur le marché. Il faudrait bien sûr déterminer des conditions d'acceptabilité, notamment en termes de sécurité numérique ou encore sur les acteurs impliqués dans une telle écriture. Cependant, reconnaître toute forme de registre dématérialisé respectant certaines règles comme l'équivalent d'un compte titre traditionnel serait une vraie incitation à développer des systèmes numérisés, et en particulier des DLT.

En conclusion, l'État ne doit pas se précipiter pour réglementer les blockchains, en réaction à des inquiétudes face à une technologie nouvelle et radicalement libertarienne dans sa forme primitive. Le cadre réglementaire actuel nous semble présenter suffisamment de garde-fous pour empêcher le développement de projets manifestement risqués, et il nous paraît donc plus pertinent d'identifier au contraire les rigidités de la réglementation qui pourraient être allégées sans augmenter les risques, afin de favoriser le développement de projets qui, potentiellement, pourraient avoir un impact positif tant pour les consommateurs que pour le développement technologique en France.

4.3.3 Quelques pistes d'ouverture

En résumé

Sur la régulation et la réglementation

- Quelle régulation sur les secteurs autres que la banque et l'assurance ?
- Faut-il une réglementation mondiale ? Est-ce réaliste ?
- L'émergence des standards : standards de fait ou décrétés par une autorité ?

Quel rôle pour l'État ?

- Développer des projets blockchains ? Uniquement en cas de besoin réel.
- Quel contrôle un État peut-il exercer sur une blockchain publique ?
- Comment développer la technologie en France ? Aider les start-ups, ouvrir des projets d'État, impulser des travaux de recherche et d'enseignement…

Nous proposons ici quelques pistes de réflexion, quelques ouvertures sur des questions qu'il nous semble bon de poser mais sur lesquelles nous ne prétendons pas nécessairement avoir de réponses. En particulier, nous avons beaucoup évoqué le secteur financier, et en particulier les marchés bancaires et assurantiels, comme exemple de régulation. Bien entendu, la blockchain pourrait avoir des implications dans d'autres secteurs régulés. Citons pêle-mêle des secteurs comme le notariat (certains évoquent la possibilité de mettre sur une blockchain les cadastres), la médecine (pour partager des données médicales entre médecins et patient, avec des données en accès restreint sur un modèle similaire à ce que nous avons présenté en matière de gestion d'identité), ou encore les marchés de l'électricité et du gaz sur lesquels la blockchain est parfois évoquée. Il sera intéressant de constater quels choix seront faits sur ces marchés, en particulier sur la question de la protection des données.

Nous avons certes évoqué la question de la régulation et de la réglementation, mais en conservant le point de vue du droit français. Or, par nature, les blockchains publiques sont des systèmes sans frontière, de par l'identité des mineurs, des utilisateurs, mais aussi par le caractère universel des applications, en particulier les crypto-monnaies. A ce titre, il pourrait être judicieux de définir des règles communes sur de tels systèmes, notamment car ceux-ci prétendent justement s'affranchir de toute réglementation. Une vision partagée, notamment en termes de protection des utilisateurs, auraient donc d'autant plus de poids. Cependant, cela nous apparaît comme un vœu pieux, tant les intérêts des différents acteurs divergent lorsque l'on évoque les nouvelles technologies. A titre d'exemple, les lois en termes de gestion des données personnelles sont radicalement différentes en France, où les utilisateurs sont très protégés, et aux États-Unis, où la liberté d'utilisation des données est beaucoup plus importante. Sur le sujet uniquement de la blockchain, les intérêts divergent également. Si la France semble voir ces systèmes d'un œil suspicieux, la Chine semble s'y intéresser, de par la forte concentration de mineurs chinois sur le réseau bitcoin (du fait aussi de prix de l'électricité extrêmement bas). Enfin, la nouvelle administration des États-Unis a vu arriver un certain nombre de figures ouvertement favorables aux crypto-monnaies, et il sera intéressant de constater si ces positions personnelles se traduiront par des prises de position officielles sur le sujet.

Nous évoquions également le fait que la blockchain apparaît, tant dans sa forme publique que dans sa forme privée, comme une technologie pas encore totalement standardisée. De tels standards pourraient mettre plusieurs années à émerger et il sera intéressant d'observer la manière dont il se construiront. Seront-ils des standards fixés par une autorité ou plutôt des standards de fait, construits par une convergence entre les acteurs sur une technologie commune ? Il nous semble que ce n'est pas le rôle de l'État que de déterminer les standards techniques, d'autant que la dimension internationale de la blockchain rendrait l'exercice difficile. Comme pour de nombreuses technologies du numérique, les standards seront sans doute déterminés par les projets des acteurs, et en particulier les premiers projets qui parviendront à émerger comme les plus pertinents. On peut également imaginer que des organismes tels que le W3C, regroupant divers acteurs du numérique, puisse se saisir de la définition de ces standards, tels qu'il le fît notamment sur la définition de certains standards du Web.

Enfin, notre statut de fonctionnaire nous invite également à nous poser la question du rôle que l'État doit tenir vis-à-vis de la blockchain. Doit-il lui-même développer des projets blockchains ? Cela ne nous semble ni nécessaire, ni particulièrement pertinent. Le développement de blockchain ne doit surtout pas être en fin une soi (comme cela semble pourtant parfois être le cas au sein de certaines entreprises) mais plutôt un moyen si la technologie apparaît comme pertinente sur un cas d'usage précis sur lequel on identifie un besoin. Lançons par exemple une bouteille à la mer et évoquons le cas de la dématérialisation des registres électoraux. Les élections présidentielles de 2017 ont été marquée par la double inscription d'environ un demi-million d'électeurs sur les listes électorales. La coordination entre les listes des différentes villes et des différents bureaux de vote est donc apparue comme insuffisante. On pourrait imaginer un système dématérialisé, partagé entre les mairies et les bureaux de vote, qui permettraient de lutter contre les doubles inscriptions. Une blockchain permettrait d'avoir un système où l'inscription sur une liste serait soumise à validation des autres bureaux de vote. En particulier, un bureau où la personne est déjà inscrite pourrait bloquer l'inscription sur une autre liste dans les mécanismes de consensus. Il serait même envisageable de créer des systèmes de *smart contracts* qui permettraient de rayer automatiquement d'une liste électorale un électeur ayant été inscrit sur une autre liste. Un tel système permettrait de déléguer les inscriptions au niveau local sans que cela soit centralisé au niveau du ministère de l'intérieur. Bien évidemment, un système central avec une base de données qui vérifierait l'absence de toute inscription double serait tout aussi fonctionnel, et la blockchain n'est ni l'unique solution ni nécessairement la meilleure, mais elle pourrait présenter une alternative crédible et justifiée en cas de volonté de dématérialiser les listes électorales.

Nous avons également évoqué le fait que le régulateur se pose actuellement la question du statut à donner aux blockchains publiques. Ces systèmes apparaissent en effet comme de véritables enjeux pour l'État. L'absence d'interlocuteur est un véritable frein à toute tentative d'auditer ou de faire évoluer ces systèmes vers plus de protection. De plus, l'esprit insufflé par bitcoin d'un système sans contrôle, et en particulier sans contrôle d'État, rend quasiment impossible toute influence étatique. Pour autant, de véritables questions se posent. Citons par exemple le principe de l'irréversibilité des transactions. Si la justice d'un État venait à annuler une transaction sur bitcoin, il serait pour autant quasiment impossible en pratique de revenir sur cette transaction sur la blockchain car les mineurs s'y opposeraient. Sauf à saisir la clé privée de la personne ayant bénéficié de la transaction pour pouvoir effectuer une transaction inverse, il serait impossible d'appliquer la décision de la justice. De plus, la dimension internationale du système rend le problème plus difficile encore car bitcoin ne relève, en soi, d'aucune juridiction. Si l'on a vu que le FBI était parvenu à mettre la main sur les fonds du créateur de Silk Road, cet exemple ne signifie pas pour autant qu'il ait exercé un quelconque contrôle sur la blockchain mais simplement qu'il est parvenu à saisir les clés privés de la personne incriminée. Si l'État apparaît impuissant face à de tels systèmes sans contrôle, le constat n'est pas satisfaisant et il paraît nécessaire, *a minima*, d'alerter les utilisateurs sur les risques encourus, voire de limiter le développement des blockchains publiques tant qu'elles ne respecteront pas certains principes de protection. A titre d'exemple, certains commerces commencent à accepter les paiement en bitcoin, ce qui en soi est avant tout un risque pour le commerçant. Cependant, une telle publicité pour des systèmes risqués est-elle vraiment à encourager ?

Enfin, si l'État estime que la blockchain, et en particulier les blockchains privées, sont véritablement porteuses d'avenir (certains candidats à la présidentielle portaient dans leur programme l'idée qu'il faille faire de la France un précurseur sur cette technologie), il peut être intéressant de se poser la question de comment l'État peut en pratique favoriser le développement de cette technologie. Plusieurs idées se présentent alors. La première serait d'identifier des projets d'État sur lesquelles cette technologie aurait un intérêt réel et y développer des projets concrets, en interne ou avec l'aide d'entreprises françaises. Nous avons évoqué la question des listes électorales dématérialisées. Nous pouvons également nous interroger sur le rôle que l'État français pourrait avoir sur le développement d'un système de gestion d'identité numérique. Il paraît quelque peu contradictoire d'évoquer un tel système comme une manière pour le citoyen de récupérer le contrôle de ses données mais on pourrait envisager un travail en bonne intelligence avec des développeurs privés, notamment le W3C, permettant l'émergence d'un système public sans autorité de contrôle, mais où les États pourraient se porter garants de la validité des données d'état civil des utilisateurs et utiliseraient le système sur leurs propres applications, tels que les systèmes de paiement d'impôts en ligne, ou encore d'inscription sur les listes électorales. Une autre piste pour l'État concerne les incitations à la création de start-ups autour de la thématique blockchains. L'État pourraient ouvrir un certain nombre de sujets qui sont aujourd'hui de son ressort pour travailler en collaboration avec des jeunes entreprises, favorisant ainsi le développement de projets dans lesquels il a des intérêts, ainsi que le développement technologique et économique en France. L'État pourrait également favoriser les rencontres entre start-ups et grandes entreprises, qui pourraient déboucher sur des partenariats favorables aux deux entités. Enfin, il est intéressant de se poser la question du développement de la technologie elle-même, par des travaux de recherche, académiques comme industriels. On peut penser que, si la blockchain venait à réellement s'imposer comme un système d'importance majeur, les universités et écoles françaises puissent développer des cours autour du sujet et faire émerger, par la recherche, des spécialistes du sujet reconnus à l'international. Au-delà de la blockchain elle-même, il peut être intéressant d'investir de manière plus générale dans les problématiques de cryptographie, qui sont absolument fondamentales dans le fonctionnement des blockchains.

Ces quelques pistes ne doivent pas nécessairement être considérées comme des recommandations mûrement réfléchis. En particulier, la blockchain est une technologie peu mature

et qui devrait évoluer à bien des égards. A ce titre, il est sans doute trop tôt pour définir de grandes orientations mais ces quelques réflexions permettent d'ouvrir le sujet et, surtout, ont pour vocation de susciter le débat et l'échange quant à la vision que l'État doit avoir par rapport aux blockchains, mais également de manière plus générale, par rapport à cette « révolution numérique » dont on parle beaucoup actuellement et qui pose en effet de vraies questions, parfois même sur nos modèles de société.

4.3.4 Synthèse

Nous avons, dans cette section, présenté deux grands axes qui devraient selon nous présider à toute réflexion réglementaire sur les blockchains. Il nous semble d'une part que la réglementation doit suivre un principe de neutralité technologique et encadrer les applications sans pour autant fixer des règles sur les technologies sous-jacentes. En revanche, il est important de mener une réflexion globale sur les multiples enjeux que posent les nouvelles technologies, et notamment certaines questions soulevées par les blockchains. D'autre part, il nous semble qu'il faut considérer les blockchains avec une certaine prudence, celles-ci n'étant encore pas une technologie mature.

Bien des questions se posent en matière de réglementation, auxquelles nous ne prétendons pas avoir de réponses fermes et définitives. Comment réglementer des technologies par nature internationalisées, sans contrôle, et pour le moment peu standardisées ? Quel rôle l'État doit-il avoir vis-à-vis de ces technologies, comment peut-il favoriser le développement des blockchains en France ? Les blockchains n'en sont finalement qu'à leurs prémices et ces questions trouveront sans doute des réponses plus précises dans les années à venir.

4.4 Quel avenir pour les blockchains ?

Nous en convenons, le titre peut paraître accrocheur. Aussi, nous nous devons de prévenir que cette partie ne saurait en aucun cas prédire avec exactitude ce que sera l'avenir exact de cette technologie. Mais nous chercherons à réunir quelques éléments de réponse, certains ayant d'ailleurs déjà été largement abordés, afin d'exprimer une opinion qui nous paraît sensée et pragmatique sur ce que nous pouvons attendre de cette (ces ?) technologie(s). Loin du *buzz* médiatique, mais sans pour autant vouer les blockchains aux gémonies, nous présentons un point de vue assez nuancé et quelque peu sceptique sur l'avenir des blockchains, ou *a minima* sur leur avenir immédiat.

4.4.1 Quelques remarques générales

En résumé

Blockchains publiques et privées

- Blockchains publiques : trop de limites, esprit incompatible avec une économie réaliste
- Blockchains privées : réintroduction de garde-fous, mais technologie moins révolutionnaire que les blockchains publiques
- Une opposition entre idéalisme (blockchains publiques) et pragmatisme (blockchains privées) ?

Un effet de mode

- bitcoin a fait l'objet d'un véritable emballement médiatique
- Emballement exploité par de multiples entreprises
- Beaucoup de communication mais peu de projets concrets et matures

De véritables intérêts

- Décentralisation, mécanismes de consensus
- Le développement de projets doit partir d'un besoin réel et identifié

Il nous paraît important d'insister une fois de plus sur la distinction majeure entre blockchains publiques et blockchains privées. Cette distinction est absolument fondamentale tant ces deux familles de technologies sont différentes et sont applicables dans des univers assez distincts. Les blockchains publiques sont nées de la volonté de créer un système sans contrôle, presque anarchiste. Elles font émerger des formes de société, où se côtoient mineurs et utilisateurs, et ce sans chef ni confiance, mais avec des mécanismes de vote qui ressusciteraient presque l'idéal de la démocratie athénienne. Certains y voient l'émergence d'un système apte à réhabiliter l'idéal d'un internet libertarien, sans contrôle ni influence de quiconque. Pourtant, cette liberté est en forme de trompe-l'œil. Il n'en demeure pas moins que le système nécessite une forme de confiance. Ce n'est plus une confiance placée en un ou des organismes de contrôle, mais une confiance placée dans l'honnêteté de la majorité. C'est certes un bel idéalisme mais, dans les faits, sur bitcoin, l'identité des mineurs (des consortiums chinois), leur nombre qui diminue, ainsi que la relative opacité du système semblent nous ramener à des intérêts privés, qui plus est pas forcément bien définis. Surtout, cette liberté (fût-elle de façade) se fait au détriment d'une forme de sécurité. Nous avons déjà évoqué nombre de limites en termes de protection des utilisateurs, notamment l'absence de garantie d'état, l'irréversibilité des transactions, la volatilité des crypto-monnaies, … Les blockchains privées résultent donc d'une volonté de réintroduire un certain nombre de garde-fous pour utiliser cette technologie dans le cadre d'une économie plus réaliste et respectueuse d'un certain nombre de principes. La fermeture du système entre un certain nombre d'acteurs agréés ou encore la possibilité de revenir sur des transactions favorisent la protection des consommateurs. Pour autant, ces évolutions peuvent apparaître comme une dénaturation de la technologie initiale, qui perd ainsi certaines de ses caractéristiques principales, si bien que certaines blockchains privées s'apparentent désormais plus à des bases de données partagées, avec certes des mécanismes de vote et une certaine robustesse. L'opposition blockchains publiques contre blockchains privées serait-elle alors une forme de débat entre idéalisme et pragmatisme ?

On voit se développer un véritable effet de bulle, autour du terme « blockchain », qui est devenu un vrai *buzz word*. Cet effet d'annonce vient plutôt des blockchains publiques, et de la communication qui a été faite autour de bitcoin. Mais il semblerait que de multiples entreprises ou start-ups se soient emparées de cet effet de mode pour à leur tour développer des projets blockchains, avec cependant des réticences bien compréhensibles à utiliser des systèmes comme bitcoin, d'où l'émergence de systèmes privées. Cet effet de bulle se traduit à notre sens par beaucoup d'excès, à commencer par une communication intempestive autour des blockchains

comme la nouvelle révolution numérique, alors même que très peu de projets concrets émergent et qu'aucun ne s'impose comme une véritable *killer app*, à savoir une application qui, sur un cas d'usage précis, se positionne comme l'acteur majeur et incontournable. Pourtant, de nombreuses entreprises affichent aujourd'hui leurs ambitions et les fonds de *venture capital* ont levé des centaines de millions de dollars sur des projets blockchains, sans que cela n'ait, à notre sens, été couronné de résultats tangibles jusqu'à maintenant. Cela est, à notre sens, lié à deux problèmes. Tout d'abord, cette technologie n'est pas mature et cela prendra sans doute encore plusieurs années avant que les blockchains aient atteint un degré de maturation suffisant, malgré l'effervescence et l'agitation qui existent autour d'elles. De plus, les blockchains semblent pâtir de projets qui se veulent simplement dans l'air du temps, sans pour autant que n'émerge un cas d'usage réel et un véritable besoin.

A notre sens, l'avenir de cette technologie (blockchains publiques comme privées) ne peut être envisagé que sous l'angle d'un certain pragmatisme, à l'écart d'une agitation finalement contre-productive qui dessert l'émergence de projets pertinents. Il nous semble pertinent de ne pas chercher à utiliser la blockchain comme une fin en soi, mais plutôt d'étudier au cas par cas l'intérêt d'un tel système, en termes de réduction de coûts, de délais ou d'intermédiations. Par l'aspect décentralisé et pair-à-pair, ainsi que par l'idée d'un consensus, les blockchains peuvent avoir un réel intérêt. FundsDLT en est une illustration, par le développement d'un système plus rapide ayant favorisé une forme de désintermédiation. Il peut également y avoir de véritables intérêts en termes de traçabilité des données, par exemple. Mais, comme pour tout projet de développement, le déploiement d'une blockchain devrait partir d'un besoin réel, identifié, sur lequel la blockchain est réellement pertinente et non de la simple volonté de s'intéresser à une technologie dans l'air du temps, en cédant aux sirènes de l'enthousiasme et de la précipitation.

4.4.2 L'avenir des blockchains publiques

En résumé

Trop de limites au développement des blockchains publiques

- Pas d'autorité
- Pas de protection des utilisateurs

Crypto-monnaies

- Trop risquées, actif essentiellement spéculatif
- Peu attractives par rapport à des monnaies d'État

Comment faire émerger des applications larges pour les blockchains publiques ?

- Revenir sur certains principes « anarchistes »
- Faire émerger une *killer app*

Smart contracts

- Idéal du code is law
- Risque de bogues, contrôle difficile de l'exécution
- Automatisation qui requiert malgré tout qu'un homme rédige le contrat !
- Inapplicables dans la réglementation
- Peu attractifs pour le grand public

Une fois énoncé ce principe de pragmatisme, nous nous proposons de revenir sur certaines limites actuelles des blockchains publiques qui, à notre sens, empêcheront cette technologie de se développer de manière massive, tout du moins dans un avenir proche. La première idée est qu'aujourd'hui, les blockchains publiques nous semble fondées sur des principes en totale inadéquation avec « l'économie réelle » : absence d'autorité centrale, de protection, rôle opaque des mineurs, … Comme évoqué précédemment, cela nous semble être une frein majeur au

développement de systèmes blockchains publics, tout du moins en ce qui concerne les deux cas d'usage principaux aujourd'hui : les crypto-monnaies et les *smart contracts*.

Les crypto-monnaies demeureront à notre sens un actif de spéculation et de blanchiment, tant qu'aucune autorité ne pourra contrôler les transactions. Un utilisateur privilégiera toujours une monnaie d'État (et les mécanismes de protection qui l'accompagnent) qu'un système opaque implémentant un moyen de paiement assez instable. Tout du moins tant que demeurera un système bancaire fonctionnel, en l'absence de crise systémique extrême. Mais parier sur l'effondrement du système bancaire nous paraît quelque peu malsain et les conséquences seraient autrement plus graves que de savoir si la blockchain pourrait alors offrir une alternative crédible, ce qui n'apparaît pas comme une évidence. Quant à l'idée que les crypto-monnaies elles-mêmes puissent provoquer la chute du système bancaire en offrant une alternative libertarienne, elle nous semble illusoire tant le consommateur a de bonnes raisons de privilégier une monnaie traditionnelle.

En ce qui concerne les *smart contracts*, il existe aujourd'hui sur les blockchains privées une forme d'extrémisme, qui s'exprime par la théorie du *« code is law »*. Le code informatique ferait donc loi sur les *smart contracts*, sans qu'intervienne une quelconque forme d'intervention humaine. D'une part, cela est dangereux car ne laissant aucune place à la contestation : si le contrat s'est exécuté, même à tort, aucun recours n'est possible. Or, un programme informatique, aussi fiable soit-il, est toujours exposé à l'existence d'un bogue, ou d'une faille, comme en a témoigné l'affaire *The DAO*. D'autre part, dire que le code fait loi sans intervention humaine est un vœu pieu : il faudra bien que quelqu'un rédige le code informatique lui-même ! L'assureur serait donc remplacé par un codeur informatique, mais il n'en demeurerait pas moins que le contrat serait rédigé par une personne physique. Par ailleurs, affirmer que le code fait loi consiste à oublier un peu vite que les États disposent d'une autorité et que le cadre réglementaire ne peut être dépassé au nom de principes libertariens. Utiliser un *smart contract* sans garde-fou sera donc une prise de risque mais restera possible sur le marché de niche que représentent les blockchains publiques, sans possibilité d'être utilisés en tant que tel par des acteurs contrôlés par l'État. Enfin, on peut douter de la volonté du grand public de souscrire à des contrats rédigés dans du langage informatique, que la majorité sera bien incapable de comprendre. Malgré l'avantage que représente une exécution automatisée, les risques et les limites en termes de compréhension des clauses nous semble un frein à la volonté du plus grand nombre d'utiliser un tel système.

A ce titre, il nous semble que les blockchains publiques ne pourront trouver d'application grand public dans leur format actuel. A notre sens, une blockchain publique ne pourra émerger que si l'une deux conditions suivantes est atteinte : soit faire tomber un certain nombre des limites évoquées, soit faire émerger une *killer app*, à savoir un cas d'usage sur lequel les propriétés quelque peu anarchistes des blockchains publiques ne sont pas des limites mais une force. La première condition nous semble difficile à atteindre, tant elle va à l'encontre de ce qui fait l'essence même d'une blockchain publique. Faire tomber des limites a déjà été fait, et a débouché sur l'émergence des blockchains privées, qui finalement apparaissent comme des systèmes bien différents. Mais il paraît difficile à croire que, techniquement, l'État parvienne à mettre en place des mécanismes sur une blockchain publique permettant de garantir les fonds, de lutter efficacement contre le blanchiment, de saisir les fonds d'un acteur illégal ou encore de s'assurer que le système ne soit pas trop influencé par des acteurs dominants. La deuxième condition est en revanche possible, mais toutefois nous pensons qu'une telle *killer app* n'émergera pas dans l'immédiat. La gestion de l'identité nous semblerait à ce titre un cas d'usage intéressant, en offrant aux utilisateurs la possibilité de reprendre le contrôle de leurs données, sur un système qui ne serait détenu par aucun acteur, public comme privé. Bien entendu, se poseraient des questions de sécurité numérique et de propagation à grande échelle de la technologie. En particulier, comment inciter malgré tout le grand public à faire confiance à un système contrôlé par des inconnus, bien que ceux-ci aient un pouvoir de nuisance limité ? De nombreuses barrières existent encore, et il est bien hasardeux de parier sur l'avenir des blockchains publiques. Si nous devions nous y risquer, nous dirions donc que celles-ci

prendront du temps à se développer. Par ailleurs, si une *killer app* devait émerger, nous mettrions une petite pièce sur la gestion de l'identité, mais la réflexion sur le sujet (du moins de la part du W3C) nous semble encore en être à ses prémices.

4.4.3 L'avenir des blockchains privées

En résumé

L'intérêt des blockchains privées

- Réintroduction de principes pragmatiques
- Vrai intérêt de la technologie : décentralisation, consensus, partage des données

Mais technologie victime d'un effet de mode

- La crainte de la révolution numérique
- Une technologie qui nécessite de vraies compétences
- Trop de précipitation

Au risque de faire hurler les puristes, l'avenir immédiat des blockchains pourraient passer par le développement de systèmes privés, ou DLT. Comme évoqué précédemment, ces blockchains semblent nettement plus adaptées à des développement au sein d'une économie répondant à un certain nombre de règles. Ces systèmes nécessitent une forme de confiance, de contrôle, mais apportent des mécanismes de protection et de sécurité nécessaires. L'aspect décentralisé, par le réseau pair-à-pair, peut avoir de vrais intérêts, en interconnectant directement certains acteurs, favorisant ainsi la désintermédiation et l'accélération de processus longs. Le partage des données, bien que non spécifique à la blockchain, peut présenter des intérêts, par exemple en termes de traçabilité et de difficulté à falsifier des données. L'idée de consensus présente aussi un intérêt assez novateur, en créant un système sur lequel un acteur n'aurait pas la possibilité d'écrire une transaction de manière unilatérale, sans accord de ses pairs. Enfin, l'aspect distribué du système présente également un intérêt en termes de transparence, chaque acteur ayant un accès aux données, et ne pouvant les falsifier de manière simple. Les *smart contracts* présentent également des intérêts, par exemple dans le cadre de processus de désintermédiation. L'exemple de FundsDLT illustre une situation où un intermédiaire de confiance, chargé de collecter l'argent de l'acheteur et le titre du vendeur, est remplacé par un *smart contract* bloquant l'argent et le titre tant que la transaction n'est pas complète, avant de réaliser l'échange. Malgré quelques limites, notamment techniques (par exemple, l'aspect distribué n'est pas toujours conciliable avec des bases de données de grande taille et la nécessité du consensus ne permet pas la mise en oeuvre de systèmes en temps réel), les blockchains privées présentent donc un certain nombre de caractéristiques tout à fait pertinentes sur certains cas d'usage.

Nous regrettons à ce titre que cette technologie soit quelque peu victime d'un effet de mode. On parle tellement de révolution numérique (et non digitale !) aujourd'hui que certaines entreprises semblent totalement pétrifiées à l'idée de rater le train en marche et se précipitent sur chaque nouvelle technologie à la mode de manière pas toujours pertinente. Développer un projet numérique nécessite à la fois une compétence et un intérêt réel. Or, cela ne semble pas toujours le cas. L'enjeu de la numérisation ne doit pas faire oublier à certaines entreprises que ce n'est pas leur coeur de métier et qu'il n'y a pas nécessairement d'urgence absolue, surtout au risque de développer des projets non réfléchis et finalement totalement contre-productifs. La blockchain a ses intérêts, certes, mais elle ne doit pas être une fin en soi mais plutôt un moyen, celui de mettre en place un système qui répond à des besoins bien spécifiques. En l'état actuel, et en ayant discuté avec des acteurs partageant notre constat, il nous semble que beaucoup d'entreprises développent des projets blockchains parce qu'elles ont la crainte que leur concurrent n'en fasse de même, mais sans nécessairement savoir pour quel usage. On voit donc se développer beaucoup de preuves de

concept mais sans que n'émergent aujourd'hui réellement des projets concrets particulièrement révolutionnaires (nous nous refusons d'utiliser l'adjectif « disruptif », tout autant à la mode que le terme de blockchain). Prenons l'exemple du consortium R3, créé pour réfléchir à la possibilité d'utiliser des blockchains pour remplacer le système Swift de gestion des transactions bancaires. Cela nous semble être une application possible (bitcoin est bien un registre de transactions monétaires !) mais il nous semble que l'initiative a été précipitée et que certains acteurs s'y sont insérés sans volonté réelle de développer un tel système, mais plutôt comme une contrainte pour éviter d'être dépassés par leurs concurrents. Les conclusions actuelles du consortium ne vont pas vraiment dans le sens d'un tel système, et celui-ci prendrait beaucoup de temps à être mis en place, loin de l'agitation permanente que suscitent les blockchains.

En conclusion, il nous apparaît que les blockchains privées peuvent véritablement faire émerger des applications pertinentes. Si nous devions parier, il nous semble que les premières applications seraient plutôt en interne à certaines entreprises, ou partagées entre des acteurs économiques, sans que ces applications n'aient nécessairement de visibilité auprès du grand public. Les blockchains pourraient être utilisées pour améliorer le *back office* de certaines entreprises, peut-être est-ce même une opportunité pour moderniser certains systèmes, en particulier des systèmes de registres (registres de transactions bancaires, registres notariaux, cadastres, …). On peut également penser qu'elles favoriseront la désintermédiation sur certains secteurs, ainsi que la traçabilité (par exemple dans des chaînes d'approvisionnement complexes, à condition que les acteurs aient une volonté commune de mettre en place un tel système). Mais la maturité technologique est encore insuffisante et l'émergence de projets complexes et réellement novateurs ne nous semble pas imminente.

4.4.4 Synthèse

Si les blockchains publiques ont été une vraie révolution, notamment en termes de gouvernance, elles nous semblent présenter aujourd'hui trop de limites pour prétendre être utilisées à large échelle auprès du grand public ou dans des secteurs régulés. A ce titre, les blockchains privées réintroduisent bon nombre de garde-fous afin de réinscrire la technologie dans une économie plus pragmatique, abandonnant au passage nombre de principes novateurs des blockchains publiques. Si ces systèmes présentent un véritable intérêt, ils nous semblent être victimes d'un effet de mode qui pousse trop d'acteurs à développer des projets sans avoir identifié un besoin réel.

L'avenir des blockchains publiques nous semble, du moins à court terme, être finalement proche de ce que sont ces technologies aujourd'hui : des systèmes sur des marchés de niche, pour lesquels le grand public n'a qu'un intérêt très limité. Afin de développer des systèmes capables de toucher un large public, les blockchains publiques devront sans doute soit abandonner quelques principes trop libertariens, soit parvenir à faire émerger une *killer app*.

Les blockchains privées, quant à elle, présentent de vrais intérêts mais font avant tout l'objet de déclarations d'intention plus que de développements concrets. Il paraît parfois difficile de séparer le bon grain de l'ivraie, bien que certains systèmes, tel que *FundsDLT*, émergent avec un intérêt réel et une utilisation justifiée d'un DLT.

Ce qu'il faut retenir

14. Si bitcoin fut avant tout une révolution en termes de gouvernance, l'esprit insufflé par cette technologie présente trop de limites pour pouvoir l'utiliser dans des applications grand public ou des secteurs régulés.

- Crypto-monnaies : nécessaires au bon fonctionnement des blockchains publiques / peu attractives auprès du grand public
- Trop de limites en termes de gouvernance : incompatible avec certaines réglementations / pas de protection des utilisateurs / confiance difficile en un système opaque

15. La régulation et la réglementation s'intéressent à l'émergence de la blockchain. Si le régulateur financier interdit l'utilisation de blockchains publiques, il n'exclut pas la possibilité d'utiliser des DLT. La réglementation cherche également à s'adapter pour favoriser l'émergence de projets blockchains.

- Principes de régulation financière : protection des consommateurs, lutte anti-blanchiment, stabilité financière
- Utilisations possibles des blockchains sur le secteur financier : en interne (optimisation du *back office*), entre des acteurs (désintermédiation), auprès du grand public
- État des projets sur le secteur financier : beaucoup de déclarations d'intention / peu de projets matures et concrets
- Le point de vue de l'ACPR : interdiction d'utiliser des blockchains publics dans les secteurs bancaires et assurantiels / pas d'interdiction d'utiliser des DLT mais contrôle des risques
- Réglementation : exemple du marché des titres non cotés / consultation auprès du secteur / volonté d'adapter la réglementation pour favoriser le développement de projets

16. Nous recommandons une réglementation qui suive un principe de neutralité technologique, et qui sache garder une flexibilité par rapport à une technologie aujourd'hui peu mature.

- Neutralité technologique : pas de réglementation ciblée sur la blockchain / réflexion globale sur les enjeux du numérique
- Nécessité de ne pas se précipiter : blockchains encore peu matures / peu de risques majeurs avec la réglementation actuelle / possibilités d'alléger le cadre réglementaire pour favoriser le développement de la technologie
- Ouvertures : sur la réglementation et la régulation (quels secteurs, quelle dimension internationale, quelle standardisation ?) / sur le rôle de l'État (développement de projets blockchains, contrôle des blockchains publiques, accompagnement du développement technologique ?)

17. L'avenir des blockchains nous semble devoir s'écrire sur le long terme, loin de l'agitation médiatique actuelle. En l'état, nous doutons du potentiel des blockchains publiques. Les blockchains privées nous semblent présenter des intérêts certains mais être victimes d'un effet de mode.

- Véritable effet de mode autour du terme blockchain / débat entre idéalisme des blockchains publiques et pragmatisme des blockchains privées
- Avenir des blockchains publiques : trop de limites actuellement / nécessité de revenir sur certains principes ou de faire émerger une *killer app*
- Avenir des blockchains privées : intérêt réel / trop de communication / nécessité d'identifier des besoins réels

5 Bibliographie

1. *Blind signatures for untraceable payments.* **Chaum, D.** s.l. : Springer, 1983. In Advances in cryptology.

2. *Bitcoin: A peer-to-peer electronic cash system.* **Nakamoto, S.** 2008.

3. **Satoshi Nakamoto. *bitcoin.fr.* [En ligne] https://bitcoin.fr/satoshi-nakamoto/.**

4. SULLEYMAN, AATIF. Man who 'threw away' bitcoin haul now worth over $80m wants to dig up landfill site. *The independent.* [En ligne] https://www.independent.co.uk/life-style/gadgets-and-tech/news/bitcoin-value-james-howells-newport-landfill-hard-drive-campbell-simpson-laszlo-hanyecz-a8091371.html.

5. Namecoin. *Wikipedia.* [En ligne] https://en.wikipedia.org/wiki/Namecoin.

6. *Ppcoin: Peer-to-peer crypto-currency with proof-of-stake.* King, S., & Nadal, S. s.l. : self-published, 2012.

7. Collomb, A., Sok, K. *Blockchain et autres registres distribués : quel avenir pour les marchés financiers ?* s.l. : OPINIONS.

8. *A next-generation smart contract and decentralized application platform.* Buterin, V. s.l. : Ethereum, 2014.

9. *A survey of attacks on Ethereum smart contracts.* Atzei, N., Bartoletti, M., & Cimoli, T. s.l. : IACR Cryptology, 2016.

10. *Automatic conflict detection on contracts.* Fenech, S., Pace, G. J., & Schneider, G. Berlin : International Colloquium on Theoretical Aspects of Computing, 2009.

11. Leloup, L. *Blockchain: La révolution de la confiance.* 2017 : s.n.

12. Terzuri, David. les consensus proof of work vs proof of stake. *Blogchaincafe.* [En ligne] http://blogchaincafe.com/les-consensus-proof-of-work-vs-proof-of-stake.

13. *Coinfox.* [En ligne] http://www.coinfox.info/news/reviews/6417-proof-of-work-vs-proof-of-stake-merits-and-disadvantages .

14. Consommation electrique du réseau Bitcoin. *Bitcoin.fr.* [En ligne] https://bitcoin.fr/quelle-est-la-consommation-electrique-du-reseau-bitcoin/ .

15. Total Electricity Net Consumption. *U.S. Energy Information Administration (EIA).* [En ligne] https://www.eia.gov/beta/international/data/browser/#/?pa=0000002&c=ruvvvvvfvtvnvv1urvvvvfvvvvvvfvvvou20evvvvvvvvvvnvvuvo&ct=0&tl_id=2-A&vs=INTL.2-2-AFG-BKWH.A&vo=0&v=H&start=2013&end=2014 .

16. Hash Rate. *Blockchain.info.* [En ligne] https://blockchain.info/fr/charts/hash-rate .

17. Ledger. *lamaisondubitcoin.* [En ligne] https://lamaisondubitcoin.fr/2016/08/18/ledger-nano-s-un-coffre-fort-pour-vos-bitcoins-et-ethers/ .

18. Blockchain et Sidechains. *Bitcoin.fr.* [En ligne] https://bitcoin.fr/blockchain-et-sidechains/ .

19. *Sex, Drugs, and Bitcoin: How Much Illegal Activity is Financed Through Cryptocurrencies?* Foley, S., Karlsen, J., & Putniņš, T. J.

20. *Les Echos.* [En ligne] https://www.lesechos.fr/20/01/2018/lesechos.fr/0301142691303_en-plein-coeur-de-paris--un---bitcoin-boulevard---pour-les-commercants.htm.

21. *Bitcoin-asset or currency? revealing users' hidden intentions.* Glaser, F., Zimmermann, K., Haferkorn, M., Weber, M., & Siering, M. 2014.

22. ***Is Bitcoin a decentralized currency?. I.*** **Gervais, A., Karame, G., Capkun, S., & Capkun, V. 2014, EEE security & privacy.**

23. Livre Blanc. ***dock.io.*** **[En ligne] https://dock.io/whitepaper.**

24. ***openpds: Protecting the privacy of metadata through safeanswers.*** **de Montjoye, Y. A., Shmueli, E., Wang, S. S., & Pentland, A. S. 2014, PLOS ONE.**

25. W3C, Community Group. [En ligne] https://w3c-ccg.github.io/did-spec/.

26. ACPR. Blockchain et Enjeux de supervision. [En ligne] http://www.strategie.gouv.fr/sites/strategie.gouv.fr/files/atoms/files/blockchain_et_enjeux_de_supervision_4_mai.pdf.

27. Trésor, DG. Consultation publique sur le projet de réformes législative et réglementaire relatif à la Blockchin. ***https://www.tresor.economie.gouv.fr/Ressources/File/434688.*** **[En ligne]**

28. Europlace, Paris. [En ligne] https://www.agefi.fr/fintech/actualites/quotidien/20170529/place-reclame-a-bercy-blockchain-efficace-219349.

29. A 25% attack. ***BitcoinMagazine.*** **[En ligne] https://bitcoinmagazine.com/articles/selfish-mining-a-25-attack-against-the-bitcoin-network-1383578440/ .**

30. ***Majority is not Enough: Bitcoin Mining is Vulnerable.*** **Gün, Ittay Eyal and Emin.**

31. Prix de l'électricité. ***Commission Européenne.*** **[En ligne] http://ec.europa.eu/eurostat/statistics-explained/index.php/Electricity_price_statistics .**

32. ***Blogchaincafe.com.*** **[En ligne] http://blogchaincafe.com/combien-ca-couterait-une-attaque-51 .**