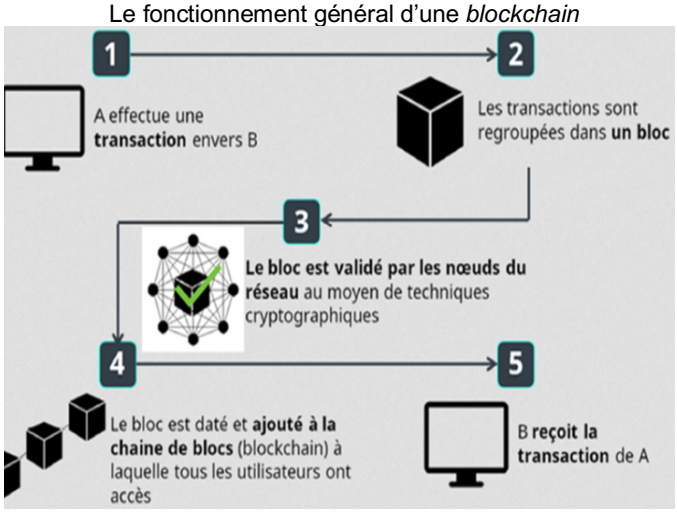
LES NOTES SCIENTIFIQUES DE L'OFFICE
OFFICE PARLEMENTAIRE D'ÉVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES

Note n° 4 — Comprendre les *blockchains* (chaînes de blocs) — Avril 2018

Le fonctionnement général d'une *blockchain*



Source : Blockchain France

Résumé

- *Apparues récemment comme combinaison de technologies plus anciennes formant le protocole sous-jacent au bitcoin, les blockchains permettent des échanges décentralisés et sécurisés, sans qu'il soit besoin d'un tiers de confiance.*
- *Leurs applications dépassent le cadre strict des cryptomonnaies et sont potentiellement nombreuses, mais peu conjuguent, à ce jour, maturité technologique suffisante et pertinence de l'usage.*
- *La recherche doit relever le défi de la capacité des blockchains à monter en charge, ainsi que celui de leur consommation énergétique.*

Contexte de la note

La présente note répond à une demande de la mission d'information commune sur « les usages des *blockchains* et autres technologies de certification de registres » mise en place à l'Assemblée nationale. Elle sera suivie d'une note plus développée. Les chaînes de blocs ou *blockchains* sont des **technologies de stockage et de transmission d'informations, qui reposent sur des registres distribués, sans organe central de contrôle, sécurisées grâce à la cryptographie, et structurées par des blocs liés les uns aux autres, à intervalles de temps réguliers**. Pour comprendre ces registres informatiques, utilisés dans des réseaux décentralisés de pair à pair (*peer to peer*), et qui forment les technologies sous-jacentes aux cryptomonnaies, type particulier de monnaies virtuelles[1], il est nécessaire de revenir à leurs origines[2].

Aux origines des *blockchains*

L'émergence des cryptomonnaies a partie liée avec le **mouvement pour le logiciel libre**, initié dans les années 1980 par Richard Stallman, ainsi qu'avec la communauté « **cypherpunk** »[3], désireuse d'utiliser les technologies de chiffrement pour créer un outil de paiement électronique et garantir des transactions anonymes. Les premières tentatives (en 1990 David Chaum avec digicash, puis en 1998 Wei Dai avec b-money et, surtout, Nick Szabo avec bitgold) sont des échecs. L'invention de hashcash par Adam Back en 1997, avait pourtant marqué un progrès avec l'idée de valider les transactions par la résolution de fonctions de hachage cryptographiques, appelée « preuve de travail ». L'objectif de ces technologies est de rendre inutile l'existence d'un « tiers de confiance », en recourant à un système de confiance distribuée.

L'obstacle à lever résidait dans le problème de la double dépense (risque qu'une même somme soit dépensée deux fois) et, plus généralement, dans celui de la tolérance aux pannes, qu'elles soient accidentelles ou malveillantes[4].

La réponse à ces difficultés est apportée en 2008 dans un **article de Satoshi Nakamoto**[5]. Ce dernier y décrit le fonctionnement d'un protocole infalsifiable utilisant un réseau pair à pair - la *blockchain* – comme couche technologique d'une nouvelle cryptomonnaie – le bitcoin.

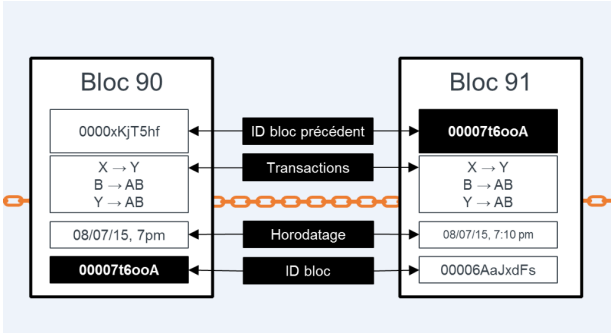
Le bitcoin premier cas d'usage de la *blockchain*

Le bitcoin repose sur un protocole sous-jacent appelé *blockchain*. On parle de chaînes de blocs, ou *blockchains,* car les transactions effectuées entre les utilisateurs du réseau sont **regroupées par bloc** « **horodaté** ». Une fois le bloc validé, en moyenne toutes les dix minutes, la transaction devient visible pour l'ensemble des détenteurs du registre, potentiellement tous les utilisateurs, qui vont alors l'ajouter à leur chaîne de blocs.

Chaque transaction a recours à la cryptographie asymétrique, basée sur le protocole Diffie-Hellman de 1976, qui fonctionne avec une paire de clés, l'une privée et l'autre publique, liées entre elles. La clé publique est diffusable et permet de recevoir des transactions, la clé privée est quant à elle gardée secrète. Protéger ses clés privées est le seul moyen de conserver ses bitcoins en sécurité. Dans la mesure où il est possible de retracer toutes les transactions du propriétaire d'une clé publique, il s'agit plus d'un système pseudonyme qu'anonyme. La

datation des transactions au sein des blocs, appelée « **horodatage** », ordonne cette chaîne.
Chaque bloc, outre les transactions et l'horodatage, possède un identifiant (case à fond noir du bloc 90 dans le schéma ci-dessous), qui permet de relier par chiffrement tous les blocs grâce à un « **hash** »[6]. En informatique, le « **hashage** » permet de convertir n'importe quel ensemble de données numériques en un hash, c'est-à-dire en une suite binaire courte et propre à cet ensemble de données. L'algorithme mathématique utilisé à cet effet est appelé « fonction de hashage ». Le hash d'un ensemble de données peut ainsi être comparé à une empreinte digitale, bien moins complexe que l'individu entier, mais l'identifiant de manière précise et unique. Une fonction de hashage est dite « à sens unique » : elle est conçue de telle sorte que le hash produit, à savoir une image ou empreinte de taille fixe créée à partir d'une donnée de taille variable, fournie en entrée, est impossible à inverser[7].Celle utilisée pour le bitcoin est parmi les plus répandues : il s'agit de la fonction *Secure Hash Algorithm-256* (SHA-256), ainsi dénommée car elle produit des hashs d'une taille de 256 bits.

La structure d'une *blockchain*



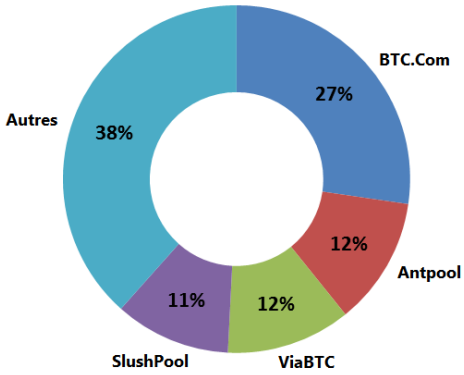
Source : Blockchain France

Nœuds du réseau, « mineurs » et consensus

Chaque bloc est validé par certains utilisateurs baptisés « **mineurs** » (en référence aux chercheurs d'or), et sont transmis aux « nœuds » du réseau, c'est-à-dire aux détenteurs du registre, qui l'actualisent en permanence. La validation des blocs permet de se prémunir du risque d'attaques malveillantes[8]. Aucune autorité centrale ne s'en occupe, puisque les utilisateurs s'en chargent en surveillant le système et en se contrôlant mutuellement. Cette sécurité, source de confiance, est l'un des aspects essentiels de la *blockchain*[9]. Le fait que des centaines de copies du registre soient mises à jour simultanément et régulièrement, au terme d'une compétition cryptographique, rend les *blockchains* quasiment indestructibles. Une « **méthode de consensus** » permettra de décider qui validera le prochain bloc à ajouter à la chaîne. Dans le cas du bitcoin, elle est appelée « **preuve de travail** » (*proof of work*) car elle suppose la réussite à une épreuve cryptographique dénommée « **minage** », qui se répète en moyenne toutes les dix minutes[10]. Elle consiste en la résolution par les mineurs de fonctions de hachage pour obtenir un hash du bloc précédent commençant par un certain nombre de zéros. Cette opération, très coûteuse en puissance de calcul informatique, est motivée par l'obtention d'une récompense en bitcoin par le mineur gagnant. Le bloc validé par ce dernier est transmis de pair à pair à chaque nœud qui ajoute à sa propre chaîne de blocs le bloc ainsi validé.

Si deux blocs sont validés au même moment, les mineurs utilisent l'un ou l'autre et **deux chaînes parallèles se développent**, le protocole prévoit alors que, rapidement, seule **la plus longue subsiste**, c'est-à-dire en pratique celle que la majorité des nœuds aura adopté.
La **rémunération des mineurs** est complétée par des **frais** prélevés sur les transactions qu'ils intègrent à chaque nouveau bloc. Ils sont déterminés librement, mais les mineurs sélectionnant les plus rémunérateurs en priorité, ils augmentent avec le nombre de transactions en attente.
L'**organisation des mineurs en groupement** ou « pool »[11] induit le risque qu'une majorité organisée oriente la validation des blocs. Mais l'intérêt commun des mineurs étant d'éviter la chute des cours, il est censé suffire à garantir le respect des règles, dans une logique de « main invisible » protégeant les intérêts privés. Il faut souligner que quatre pools dont trois chinois, qui s'appuient sur des « fermes de minage », assurent aujourd'hui plus de 60 % de la puissance de calcul nécessaire à la *blockchain* du bitcoin et pourraient utiliser cette position dominante contre l'intérêt des autres utilisateurs.

Les « pools » de mineurs du bitcoin



Source : Blockchain.info (5-9 avril 2018)

D'autres méthodes de consensus que la « preuve de travail » (*proof of work*) existent et sont souvent plus centralisées[12] : la principale alternative, qui présenterait un risque plus grand d'utilisation malveillante[13], est la « preuve d'enjeu », appelée aussi « preuve de participation » *(proof of stake),* basée sur la possession de crypto-monnaies mises en séquestre, et qui se décline à son tour en « preuve de possession » (*proof of hold*), fondée sur la durée de possession, « preuve d'utilisation » (*proof of use*), fonction volume de transactions, ou, encore « preuve d'importance » (*proof of importance*), reposant sur la réputation. D'autres méthodes, moins usitées, peuvent aussi être évoquées : la preuve de capacité, qui consiste à mettre en gage de l'espace disque disponible, ou, encore, la preuve de destruction, qui revient à détruire des cryptos-actifs, pour obtenir la confiance du réseau.

Réformer la *blockchain* : hard et soft forks

Il est possible de modifier les règles régissant une *blockchain*, on parle alors d'embranchement (fork). Cela suppose toutefois qu'une modification du code soit intégrée par l'ensemble du réseau. Toute personne peut proposer une modification toutefois elles émanent le plus souvent de quelques développeurs (un noyau d'une quarantaine dans le cas du bitcoin). On distingue deux types d'évolutions : les « soft forks », lorsque les blocs produits sous la nouvelle version peuvent être ajoutés par des nœuds fonctionnant encore sous l'ancienne version, et les « hard forks », lorsqu'une telle rétrocompatibilité est impossible. Lorsqu'ils ne sont pas adoptés à l'unanimité, les hard forks peuvent donner naissance à des *blockchain*s alternatives et indépendantes de la version originelle. En 2017, bitcoin cash et bitcoin gold sont ainsi nés de hardforks du bitcoin d'origine. Ils peuvent aussi permettre de revenir à un état antérieur de la *blockchain* lorsque celle-ci a été altérée, ce qui suppose d'annuler les transactions ultérieures. Ce fut le cas suite au hacking de l'application « TheDAO » sur la *blockchain* Ethereum.

Le défi de la montée en charge (« scalabilité »)

La **capacité à faire face à une augmentation du nombre de transactions** constitue l'un des principaux défis pour les *blockchain*s, à commencer par celle du bitcoin. Cette dernière ne permettait jusqu'en 2017 la validation que de quatre transactions par seconde en moyenne (plutôt 20 en 2018). Ce défi de la montée en charge (scalabilité) reste entier. Il a conduit à accélérer la naissance d'autres cryptomonnaies, plus de 1500 à ce jour, souvent dites alternatives (« altcoins »). Il a également mené à des innovations encore peu matures d'un point de vue technologique, comme la parallélisation de *blockchain*s collatérales, aux fonctions différentes et complémentaires (« sidechains »), le recours à des bases de données liées à la *blockchain* (« side databases »), ou encore la création d'une nouvelle couche de protocole allégé et rapide sur la *blockchain* (« lightning networks »).

Bien que le rôle de la *blockchain* en tant **technologie sous-jacente des nombreuses cryptomonnaies** soit aujourd'hui dominant, ses protocoles se **déclinent dans de nombreux secteurs** et pourront donner naissance à des applications nouvelles variées dépassant le cadre strict de la finance, même si peu conjuguent, à ce jour, pertinence de l'usage et maturité technologique suffisante. La blockchain Ethereum offre ainsi une infrastructure adaptée à des outils tels que des codes informatiques qui pourraient s'exécuter après avoir été écrits dans une *blockchain* : *smart contracts*, applications décentralisées dites « Dapps »[14] et organisations autonomes décentralisées ou « DAO »[15].

Programmer la *blockchain* : les smart contracts

Les « contrats intelligents » ou *smart contracts* sont des programmes informatiques inscrits dans la *blockchain.* En effet, il est possible d'échanger en son sein des lignes de script, au même titre que des transactions. Ce ne sont pas des contrats au sens juridique. Ces codes informatiques facilitent, vérifient et/ou exécutent un contrat au stade de sa négociation, ou de sa mise en œuvre. Ils peuvent aussi rendre une clause contractuelle inutile, dans le cas où elle serait exécutée par le programme. Par rapport à des programmes classiques, les *smart contracts* présentent l'avantage de bénéficier de la *blockchain*. Ainsi, leur exécution est irrémédiable, dès lors que les conditions spécifiées sont remplies, et leur code est vérifiable librement par les nœuds du réseau. Ils permettent aussi de placer des fonds sous séquestre de manière vérifiable. Leur mise en œuvre suppose toutefois plusieurs préalables, notamment des mécanismes de vérification approfondis – particulièrement utiles en raison de l'immuabilité du registre – ainsi que le développement d'un langage de programmation adapté aux restrictions de volume de données propres à un réseau distribué. Par ailleurs, dans la plupart des cas d'usage annoncés, leur exécution est conditionnée par l'apport et l'export d'informations. Que ce soit pour relever une température, livrer un colis, prouver la réalisation d'un travail, ou donner l'heure d'arrivée d'un avion, un tiers, qualifié d'oracle dans l'écosystème Ethereum, doit faire le lien entre la *blockchain* et le reste du monde physique, ce qui s'apparente au retour d'un « tiers de confiance ».

La distinction entre *blockchain*s ouvertes ou publiques et *blockchain*s fermées ou privées

La distinction *blockchain*s publiques / *blockchain*s privées **ne repose pas sur une distinction entre *blockchain*s de personnes publiques** (États, collectivités…) **et *blockchain*s de personnes privées** (entreprises, ONG…), **mais sur le caractère ouvert ou fermé de la *blockchain***, les protocoles de chaînes de blocs pouvant être distingués selon qu'ils sont ouverts à l'écriture et à la lecture sans restriction (*permissionless*) ou que l'une ou l'autre de ces opérations est soumise à l'acceptation d'un tiers (*permissioned*). En français, on parlera plutôt de *blockchain*s ouvertes ou fermées, ou encore de *blockchain*s publiques ou privées. Les protocoles de *blockchain*s sans restriction d'accès sont les plus connus. Ils soutiennent le bitcoin ou l'ether. Comme il a été vu, n'importe qui peut en devenir un nœud, et ces protocoles nécessitent une méthode de consensus. Il existe aussi une **multitude de protocoles à restriction d'accès**, pour certains particulièrement aboutis et déjà opérationnels. Parmi ces derniers, les *blockchain*s « de consortium »résultent du regroupement de plusieurs organisations indépendantes, voire concurrentes, utilisant la *blockchain* pour réaliser des transactions sécurisées, ou échanger des actes certifiés, sans avoir à financer un intermédiaire de confiance. D'autres protocoles sont utilisés au sein d'une même organisation, pour simplifier

et automatiser des échanges et des certifications. Dans une *blockchain* privée, une autorité régulatrice valide l'introduction de nouveaux membres, et accorde les droits en écriture et en lecture. Cette autorité peut être seule aux commandes, ou gouvernée collégialement par les différents participants. A la différence d'une *blockchain* publique, les *blockchains* privées peuvent exiger une majorité renforcée. De même, il suffit de trois participants pour faire fonctionner une *blockchain* privée, tandis que les *blockchain*s publiques peuvent en compter plusieurs milliers.

Un débat existe pour qualifier les *blockchain*s privées de « vraies » ou de « fausses » *blockchain*s, sachant que créer un produit recourant à ces technologies est aussi un **enjeu de marketing**. Certaines applications fondées sur les *blockchain*s ne semblent pas toujours justifiées, les fonctionnalités offertes par les bases de données partagées et sécurisées existantes apparaissant en effet suffisantes à leur réalisation. Le succès de certaines levées de fond spécifiques à l'écosystème des cryptomonnaies (*Initial Coin Offering* ou ICO) interroge également. Un regard plus distancié paraît nécessaire, en raison des effets de mode propres aux écosystèmes entrepreneuriaux. Ces effets de mode, visibles dans le recours à certains concepts, tels que les technologies disruptives, l'intelligence artificielle, les données massives (*big data*), le *cloud*, l'internet des objets (IoT pour *internet of things*) ou, encore, la *blockchain,* sont parfois le reflet de stratégies marketing séduisantes, mais sans toujours s'accompagner d'innovations aussi majeures que celles annoncées.

Les enjeux énergétiques et environnementaux

Outre les questions de montée en charge, de sécurité, de régime fiscal, ou de cadre juridique, les *blockchain*s posent aussi celle, essentielle, de leurs impacts énergétiques et environnementaux. Les besoins en électricité des *blockchains* fondés sur la preuve de travail sont considérables. Si leur estimation fait l'objet de débats, la consommation pour le seul bitcoin est d'au moins **24 TWh/an**[(16)]. La dépense énergétique étant corrélée à l'intéressement des mineurs, sa croissance est quasi-exponentielle[(17)]. Face à l'explosion des cours, la réduction tous les quatre ans des récompenses de minage (« *halving* »[18]) est insuffisante pour jouer son rôle de régulation de la compétition. De meilleures capacités de calcul ou l'utilisation de surplus électrique ne permettront pas de diminuer la consommation énergétique. En effet, la compétition se jouant sur les coûts, les économies offertes aux mineurs le sont aussi aux attaquants potentiels. L'impact en termes d'émissions de gaz à effet de serre est d'autant plus important que les groupements de mineurs sont surtout établis en Chine, pays qui présente l'intensité carbone la plus élevée au monde[19]. La recherche doit donc **relever ce défi de la consommation énergétique** des *blockchains*, à l'image de l'initiative française BART[20] (« *Blockchain* Advanced Research & Technologies »), qui doit permettre de valider la *blockchain* en consommant moins d'énergie, par des méthodes de consensus robustes aux moyens cryptographiques avancés, tout en développant de nouvelles architectures facilitant la fiabilité et la montée en charge du réseau.

Sites Internet de l'Office :

http://www.assemblee-nationale.fr/commissions/opecst-index.asp

http://www.senat.fr/opecst

M. Gérard Berry, professeur au Collège de France, membre du conseil scientifique de l'OPECST

Mme Emmanuelle Anceaume, chargée de recherche en informatique (CNRS/INRIA/Irisa)

Mme Claire Balva, présidente de *Blockchain* France et de *Blockchain* Partner

M. Jean-Paul Delahaye, professeur émérite en informatique à l'université Lille I

M. Renaud Lifchitz, consultant et chercheur en sécurité informatique et en cryptographie

M. Gérard Memmi, responsable du département d'informatique de Télécom ParisTech

M. Ricardo Perez-Marco, directeur de recherche en mathématiques (CNRS/Université Paris Diderot)

M. Simon Polrot, avocat, fondateur d'Ethereum France et de VariabL

M. Pierre Porthaux, président de *Blockchain* Solutions et d'EmergenceLab

M. Manuel Valente, directeur de la Maison du Bitcoin

M. Daniel Augot, directeur de recherche à l'INRIA

M. Nicolas Courtois, professeur d'informatique au University College London (UCL)

M. Gilles Fedak, chargé de recherche à l'INRIA et président d'iExec

M. Georg Fuchsbauer, chargé de recherche à l'École normale supérieure de Paris et à l'INRIA

M. Fabrice Le Fessant, chargé de recherche à l'INRIA et fondateur de OCamlPro, Move&Play et CleverScale

Références

(1) Les monnaies virtuelles n'ont pas de cours légal, ne sont pas régulées par une banque centrale et ne sont pas délivrées par des établissements financiers. La Banque centrale européenne distingue trois types de monnaie virtuelle : celle fermée utilisée dans les jeux vidéo (son existence est limitée au cadre du jeu), celle utilisant un flux unidirectionnel (elle peut être achetée avec une devise légale, à un taux de change défini, mais ne peut être reconvertie en monnaie légale) et, enfin, celle bénéficiant d'un flux bidirectionnel, comme les cryptomonnaies à l'instar du bitcoin (possibilité de conversion dans les deux sens).

(2) La compréhension de l'histoire et du fonctionnement de ces technologies peut s'appuyer sur les ouvrages suivants : Don et Alex Tapscott « Blockchain Revolution » éditions Penguin Random House ; collectif « La Blockchain décryptée – les clefs d'une révolution » Blockchain France ; Jacques Favier et Adli Takkal-Bataille « Bitcoin » CNRS édition ; Laurent Leloup « Blockchain : La révolution de la confiance » éditions Eyrolles ; Stéphane Loignon « Big Bang Blockchain » éditions Tallandier ; collectif « Bitcoin et Blockchain : vers un nouveau paradigme de la confiance numérique ? » Revue Banque édition ; IEEE Spectrum « Blockchain World », éditions IEEE ; collectif U « Comprendre la blockchain » éditions Uchange ; National Institute of Standards and Technology « Blockchain Technology Overview » U.S Department of Commerce ; Andreas Antonopoulos « Mastering Bitcoin : programming the open blockchain » éditions O'Reilly, disponible en français au lien suivant : https://bitcoin.fr/wp-content/uploads/2016/01/Mastering-Bitcoin.pdf. Les sites suivants peuvent aussi être cités : www.bitcoin.org https://bitcoin.info www.coindesk.com https://cointelegraph.com https://blockchainfrance.net https://blockchainpartner.fr et https://journalducoin.com. TA-SWISS, fondation suisse pour l'évaluation des choix technologiques, membre du réseau EPTA, a lancé en avril 2017 une étude qui évaluera les chances et les risques de la blockchain, avec une remise prévue en juin 2018.

(3) Le mot-valise « cypherpunk », inventé par Jude Milhon, est formé à partir de l'anglais cipher ou chiffrement et « cyberpunk », lui-même issu des mots cybernétique et punk et renvoyant à des œuvres de fiction dystopiques basées sur les technologies. Tim May publie un « Manifeste crypto-anarchiste » en 1992 et Eric Hughes le suit en 1993 avec son « Manifeste d'un Cypherpunk ».

(4) La réponse à ces pannes revient à résoudre, dans le cadre de programmes informatiques, le problème des généraux byzantins, traité dans l'article de Leslie Lamport, Robert Shostak et Marshall Pease « The Byzantine Generals Problem », ACM Transactions on Programming Languages and Systems, vol. 4, no 3, juillet 1982.

(5) Satoshi Nakamoto est le pseudonyme du collectif des fondateurs du bitcoin et de la première blockchain. Il a désigné Gavin Andresen, CTO de la Fondation Bitcoin, comme étant son successeur. Le fonctionnement de cette crypto-monnaie et de la blockchain est décrit dans un article fondateur publié sur internet en 2008 : « Bitcoin: A Peer-to-Peer Electronic Cash System », cf. https://bitcoin.org/bitcoin.pdf Une traduction en langue française est également disponible au lien suivant : https://docs.google.com/document/d/1tEJ4Mtc4o1gGziF37eqHG9OY4OiRyXol5GXSM3pUKy4/

(6) Les arbres de hachage ont été inventés par Ralph Merkle en 1979, d'où l'expression « arbre de Merkle ». Dans le cas du bitcoin ils permettent de réaliser un hash de l'ensemble des transactions d'un bloc, qui est appelé « racine de Merkle » (Merkle Root). L'empreinte de ce bloc résulte alors du hash de cette racine combinée à l'empreinte du bloc précédent.

(7) Alors qu'il est simple de produire un hash à partir d'un ensemble de données, il est considéré comme impossible de remonter à un ensemble de données à partir d'un hash connu, avec les puissances de calcul disponibles aujourd'hui. On dit donc qu'elle est « à sens unique » car l'image d'une donnée par la fonction se calcule facilement mais le calcul inverse d'une donnée d'entrée ayant pour image une certaine valeur est impossible sur le plan pratique.

(8) Les attaques « Sybil » reposent par exemple sur la multiplication de fausses identités, ce qui peut conduire certains acteurs à exercer une influence disproportionnée sur un réseau. Se prémunir de ce type d'attaque suppose soit de contrôler la création de profils (validation d'une identité par courriel, par exemple), ou, en l'absence d'autorité de contrôle, comme c'est le cas pour le Bitcoin la production de calculs informatiques complexes.

(9) C'est pour cette raison que l'on parle à son sujet d'un mécanisme de confiance, « trust machine » comme titrait la revue The Economist en octobre 2015. Ce numéro spécial blockchain permit à cette dernière de « sortir » du milieu des spécialistes, grâce à la réputation de cette revue, et de se voir conférer une crédibilité dans le grand public, notamment auprès des acteurs économiques. Le sous-titre du même numéro de cette revue, « comment la technologie derrière le Bitcoin pourrait changer le monde », évoque quant à lui la révolution potentielle induite par la blockchain.

(10) La « preuve de travail » consiste en un calcul itératif et aléatoire, sa résolution peut donc être plus ou moins longue, mais sa difficulté peut être ajustée de telle sorte à ce que le temps moyen de résolution soit proche d'une durée donnée. Pour le bitcoin, elle est de 10 minutes, sa difficulté étant ajustée tous les 2016 blocs, c'est-à-dire environ tous les 14 jours. La difficulté des fonctions de hashage doit progresser au même rythme que l'évolution des puissances de calcul informatique.

(11) Trois pools de minage français, d'envergure modérée, peuvent être cités : Big Block Data, Wizard Mining et Just Mining.

(12) Ainsi la crypto-monnaie peercoin utilise un mélange entre la « preuve de travail » et la « preuve de participation », c'est-à-dire qu'elle adapte la difficulté du travail de minage en fonction de la « part » de crypto-monnaie possédée par chacun des mineurs. La crypto-monnaie nem a recours à la « preuve d'importance » et l'ether a vocation à reposer sur une « preuve d'enjeu » mais la transition depuis la « preuve de travail » a du mal à se confirmer depuis deux ans : sa blockchain reste en effet fondée sur la preuve de travail. Tezos est un autre projet qui vise aussi l'utilisation de la « preuve d'enjeu ».

(13) Des solutions plus résistantes sont en cours de développement. Silvio Micali, titulaire du prix Turing 2012, propose ainsi le système Algorand dont le fonctionnement correct malgré la présence d'un tiers de nœuds malveillants est prouvé mathématiquement.

(14) Les applications décentralisées, qui sont en réalité distribuées, fonctionnent grâce à des programmes inscrits sur la blockchain. Leur utilisation nécessite toutefois l'intervention d'un tiers.

(15) Les DAO sont des organisations collectives : une association ou une société dont les règles de fonctionnement et les procédures seraient inscrites sur la blockchain.

(16) Parmi les estimations proposées au 2 avril 2018 pour le minage du bitcoin seul, Bloomberg indique 20TWh/an, Digiconomist, 60TWh/an et Morgan Stanley, 140 TWh/an. L'estimation basse de 24 TWh/an est réalisée à partir des performances de la machine la plus efficace du marché, Antminer S9 ($13,5*10^{12}$hashs/s pour une consommation de 1,323W/s) et du nombre global de calculs de hashs au 4 avril 2018 ($28*10^{18}$hashs/s). Le bitcoin nécessiterait donc 2 millions d'appareil environ par seconde ($28*10^{18}/13,5*10^{18}$) pour une consommation de $2*10^{9}$x1,323W/s = 2,7GW/s, ce qui, ramené annuellement, donne 24 TWh.

(17) Le Bitcoin Energy Consumption Index indique ainsi une augmentation de 30% de la consommation énergétique au cours du mois de mars 2018. Karl J. O'Dwyer et David Malone ont montré, dans une étude publiée en 2014, que la consommation du réseau destiné au bitcoin se situait alors dans une fourchette entre 0,1 et 10 GW de puissance électrique et qu'elle serait probablement de l'ordre de grandeur de la consommation d'un pays comme l'Irlande, soit environ 3 GW cf. https://karlodwyer.github.io/publications/pdf/bitcoin_KJOD_2014.pdf Pour suivre l'estimation du Digiconomist au jour le jour : https://digiconomist.net/bitcoin-energy-consumption

[18] *Le protocole de Nakamoto prévoit en effet que la récompense en bitcoin attribuée à chaque mineur validant un bloc soit divisée par deux tous les 210 000 blocs, c'est-à-dire tous les 4 ans. Elle était ainsi de 50 bitcoins jusqu'en 2012, puis de 25 jusqu'en 2016, elle est aujourd'hui de 12,5 et passera à 6,25 en 2020. Elle est versée 100 blocs après validation.*

[19] *La Chine présente, selon les calculs du GIEC, l'intensité carbone la plus élevée du monde, avec 1 050 grammes de CO_2 par kWh d'électricité produite.*

[20] *Cette initiative commune de recherche réunit l'Inria, Telecom ParisSud, Telecom ParisTech et SystemX.*