Qu'est-ce qu'une *blockchain* ?

Jean-Paul Delahaye

Il est assez amusant de voir que la définition proposée de « *blockchain* » par wikipédia en anglais (`https://en.wikipedia.org/wiki/Blockchain`, consultée le 6-10-2017) et la définition du même wikipédia en français (`https://fr.wikipedia.org/wiki/Blockchain`, consultée le 6-10-2017) diffèrent fondamentalement. Il serait facile de trouver des situations où ce qui est considéré comme une *blockchain* par l'un ne l'est pas par l'autre, et réciproquement. La définition anglaise accorde par exemple une importance centrale à l'idée que les blocs sont liés les uns aux autres par des « hash » (résultat de l'application d'une fonction de hachage cryptographique), ce que la définition française ne mentionne pas. La définition française exige en revanche la transparence des données et l'absence de contrôle centralisé, ce que ne fait pas la définition en langue anglaise ! Les textes de ces définitions et quelques autres sont recopiés en annexe à la fin de cet article, et permettent de mesurer la confusion qui règne concernant le concept de *blockchain*.

Sans prétendre mettre tout le monde d'accord, nous allons proposer une définition de *blockchain* à la fois large et précise. Donner une définition trop générale conduirait à dire que les *blockchains* existent depuis bien longtemps, et donc à nier l'invention, en 2008, par Satoshi Nakamoto, et amènerait à refuser l'idée qu'il se met en place une technologie nouvelle des *blockchains*. Donner une définition restrictive, à l'inverse, conduirait à n'accepter comme *blockchain* que celle du *Bitcoin* et ses copies fidèles, ce qui serait absurde et sans intérêt. Il faut viser entre les deux !

Une série de remarques et de commentaires suivra la définition pour expliquer les choix faits et indiquer ce qui peut varier dans la définition en préservant l'objectif de n'être ni excessivement précis, ni démesurément tolérant. Selon sa sensibilité, chacun retiendra telle ou telle variante de la définition, l'essentiel étant qu'elle constitue un outil aidant à comprendre et situer les usages contradictoires faits du mot *blockchain* et de cesser de s'y perdre !

Tentative de définition.

Les points entre crochets sont considérés comme facultatifs. Ces points sont cependant mentionnés ici, car ils permettent de définir des concepts particuliers de *blockchain* : *blockchain ouverte, blockchain fermée (blockchain privée, permisioned blockchain), blockchain support d'un registre de comptes (blockchain support de monnaie cryptographique)*, etc.

Définition.

Un protocole de *blockchain* se définit par les éléments suivants.

•1• Un fichier informatique composé de *pages* (ou blocs) ordonnées, Page 0, Page 1, ..., Page *n*, évoluant par addition de nouvelles *pages*, une à une, sans que ne s'opère jamais aucun retrait, effacement ou modification. Ce fichier, concaténation dans l'ordre de toutes les pages, [Page 0, ..., Page *n*] à l'instant *n*, est le *fichier blockchain*.

[•2• Les pages du *fichier blockchain* sont liées les unes aux autres par des empreintes (« hash ») calculées par l'application d'une certaine *fonction de hachage cryptographique* fixée : l'empreinte de la Page *n*, ou de la concaténation de toutes les *pages* de 0 à *n* est présente dans la Page *n*+1.]

•3• La date et l'heure (approximative) de création de la Page *n* sont inscrites dans la Page *n*, ou au moins son numéro d'ordre, *n*.

•4• L'*état du fichier blockchain* (c'est-à-dire les informations permettant de reconstituer parfaitement le *fichier blockchain*) est présent en chaque point d'un réseau pair à pair associé au *fichier blockchain*, que nous appellerons le *réseau blockchain des nœuds complets*. Dans certains cas (comme pour le *Bitcoin*) au *réseau blockchain des nœuds complets* seront ajoutés des nœuds jouant des rôles plus limités dans le fonctionnement du protocole. Le réseau ainsi complété est le *réseau blockchain*.

[•5• Chaque nœud du *réseau blockchain des nœuds complets* contient une copie à l'identique du *fichier blockchain*. C'est une exigence plus forte que celle exprimée par le point •4• qui ne mentionne que l'*état du fichier blockchain*.]

•6• Chaque page du *fichier blockchain* est en partie constituée de *transactions*, c'est-à-dire de séquences d'informations — des chaînes de caractères — qui ont circulé sur le *réseau blockchain*. Ces transactions respectent un certain format et suivent certaines règles de construction. Le respect du format et des règles est contrôlé par chaque nœud du *réseau blockchain* à chaque fois qu'il reçoit une *transaction*.

•7• Le *réseau blockchain des nœuds complets* est un réseau non centralisé pair à pair (P2P) ; sur ce réseau circulent diverses informations, dont les *transactions* et les *pages* quand celles-ci sont prêtes. Chaque *transaction* et chaque *page* circulent jusqu'à ce que chaque nœud du *réseau blockchain des nœuds complets* en soit informé.

•8• Chaque nœud du *réseau blockchain des nœuds complets* contrôle la Page *n*+1 avant de l'accepter et de l'ajouter à la copie du *fichier blockchain* qu'il détient (soit sous forme exacte, soit sous forme indirecte d'informations permettant de reconstituer exactement le *fichier blockchain*).

•9• Il existe un *protocole de désignation* qui détermine le nœud du *réseau blockchain des nœuds complets* qui compose la Page *n*+1. Le nœud désigné qui compose cette Page *n*+1 à partir des transactions ayant circulé, la fait circuler sur le réseau. Chaque nœud vérifie alors que la page proposée est correcte et que le nœud qui a construit cette Page *n*+1 est bien celui qui a été choisi par le *protocole de désignation*. Si c'est le cas, chaque nœud en déduit l'état suivant du *fichier blockchain* qui est alors constitué de [Page 0, ..., Page *n*, Page *n*+1].

•10• Le *protocole de désignation* donne une certaine chance à chaque nœud du *réseau blockchain des nœuds complets* d'être celui qui compose la nouvelle page.

•11• Quand il y a désaccord sur la page à ajouter entre différents nœuds du réseau et

création de plusieurs *fichiers blockchains* différents (car le protocole de désignation n'a pas fonctionné parfaitement et que, par exemple dû aux temps de latence du réseau, deux nœuds ont construit simultanément une nouvelle *page* et l'ont fait circuler), un *protocole de choix entre blockchains* permet de sortir de la confusion. Il assure le choix d'un *fichier blockchain* parmi ceux en compétition momentanée, et rétablit ainsi un consensus entre tous les nœuds du *réseau blockchain des nœuds complets*.

[•12• Un *système de rémunération* des nœuds est défini. Il constitue une incitation à participer au *réseau blockchain des nœuds complets* et donc à faire circuler les *transactions* et les *pages* en les contrôlant. Il incite aussi à détenir et gérer le *fichier blockchain* ou un fichier équivalent permettant de le reconstituer.]

[•13• De nouveaux nœuds du *réseau blockchain* peuvent se créer à chaque instant ou disparaître sans que le *protocole blockchain* en soi perturbé.]

[•14• Le *fichier blockchain* est lisible et accessible à tous. Toute entité peut créer de nouvelles *pages* à partir du moment où elle est devenue membre du *réseau blockchain des nœuds complets*.]

[•15• Les *transactions* doivent être signées par un *protocole de signature* à clef publique ou par un autre moyen cryptographique.]

[•16• L'ensemble des transactions définit entre autres choses un *registre de comptes*, qui associe des *jetons* ou des fractions de *jetons* à des *numéros de compte*. À chaque instant, l'*état du fichier blockchain* permet de connaître combien de *jetons* se trouvent associés à chaque *numéro de compte*.]

Le vocabulaire

Il est de peu d'intérêt de discuter la question de savoir si on doit dire « une *blockchain* » ou « un *blockchain* » ou même « une chaîne de blocs », ou encore « une chaîne de pages ». L'usage semble s'être imposé, nous dirons donc « une *blockchain* ».

Dans notre définition nous avons utilisé des mots et des groupes de mots en italique. Ils permettent de repérer les éléments centraux de la définition.

Fichier blockchain, page, protocole blockchain, réseau blockchain, réseau blockchain des nœuds complets, nœud complet, état du fichier blockchain, protocole de désignation, protocole de choix entre blockchains, système de rémunération, registre de comptes, jetons, numéro de compte.

On pourra bien évidemment discuter la liste retenue, la raccourcir ou l'allonger. En particulier en augmentant la précision de notre définition, d'autres éléments s'introduiraient naturellement. Notre but est d'obtenir assez de précisions pour permettre une discussion sur ce qu'on peut ou doit appeler *blockchain*, mais nous ne souhaitons pas énumérer tous les détails d'une spécification formelle qui risquerait alors d'être restrictive.

Une base de données comme il en existe depuis longtemps ?

Une question souvent posée est : les *bases de données distribuées*, *réparties* ou *répliquées* sont-elles des *blockchains* ? Si c'était le cas, les *blockchains* existeraient depuis longtemps et Nakamoto n'aurait rien inventé. Il est clair pourtant que les adjectifs *distribué*, *réparti*

et *répliqué* ne sont pas assez restrictifs. Ils peuvent qualifier des bases de données où les données sont éclatées sur plusieurs nœuds d'un réseau (éventuellement centralisé) sans être présentes en totalité sur aucun nœud. Lorsque les données sont toutes présentes en chaque nœud (base de données *répliquées*), elles ne sont pas nécessairement structurées et manipulées comme l'idée de *blockchain* défendue ici l'exige : des pages datées qui s'ajoutent irréversiblement par ordre de création, sans qu'un nœud central en ait seul la maîtrise.

Ces points (page, ordre, date, immutabilité, réseau sans autorité centrale) doivent être exigés pour qu'on puisse parler de *blockchain*. Que les *blockchains* soient une catégorie particulière de *bases de données réparties* est vrai, mais une *blockchain* est une *base de données réparties* très spéciale, dont le fonctionnement est très particulier. Ce type de bases de données est devenu possible récemment grâce aux progrès technologiques permettant, à moindre coût, la multiplication à l'identique des calculs et la recopie à l'identique des données en chaque nœud d'un réseau pair à pair, ce qui autrefois aurait été considéré comme un immense gâchis, ou comme une impossibilité.

Bien sûr, écrire les deux paragraphes précédents constitue un parti pris, mais il est délibéré : il ne faut pas que n'importe quoi puisse être considéré comme une *blockchain*. Il ne faut pas non plus — et c'est pourquoi de nombreux points sont entre crochets — que seule la *blockchain* du *Bitcoin* soit conforme à la définition.

Insistons : les *bases de données répliquées*, peuvent être gérées de manière centralisée : un nœud maître fait les mises à jour et les transmet aux autres nœuds qui les recopient, permettant la synchronisation. Dans le cas d'une *blockchain* la nature pair à pair du réseau (que nous considérons comme faisant partie du concept) interdit une telle mise à jour centralisée.

L'usage du terme DLT, pour *Distributed ledger technology* (*technologie des registres distribués*) doit être mentionné. On l'utilise semble-t-il pour ne pas avoir à parler de *blockchains*, qui évoquent le *Bitcoin* longtemps mal vu dans les milieux des banques et de la finance. Il pourrait servir à désigner une notion un peu plus tolérante de *protocoles blockchain*, plus proche du concept général de *bases de données répliquées*. Comme cet usage n'est pas plus clair que celui de *blockchain*, il ne fait qu'accroître la confusion. Il paraît donc judicieux de l'éviter.

Le chaînage des pages par des empreintes n'est pas essentiel

Le point •2• de la définition doit être considéré comme facultatif. Une concaténation de *pages* peut être rendue infalsifiable simplement parce qu'elle est recopiée à l'identique en divers nœuds indépendants qui se surveillent les uns et autres et veillent à rester cohérents. Les *hash* présents dans les pages (par exemple du *Bitcoin*) qui les lient les unes aux autres sont un moyen possible pour rendre difficile et coûteux la fabrication d'un faux *fichier blockchain*. Cependant cela n'a de sens que lorsqu'on met en œuvre un système d'attribution de l'incitation par une *preuve de travail*, et cela à la condition encore d'exiger qu'il y ait en même temps dans chaque page la solution du problème d'inversion partielle de fonction de hachage (de la preuve de travail) se rapportant au *fichier blockchain* à l'instant *n* (ou quelque chose d'équivalent à un contenu en calcul). Dans un tel système (*Bitcoin Ethereum*, etc.) fabriquer une fausse *blockchain* dont les *k* dernières *pages* sont

différentes des *k* dernières *pages* du *fichier blockchain* exige qu'on calcule autant que le réseau a calculé pour effectuer les *preuves de travail* des *k* dernières *pages*. C'est coûteux, et ce coût de la fabrication d'une *blockchain* de substitution fortifie le *protocole blockchain*. De tels systèmes renforcent la robustesse d'un *protocole blockchain*, mais ce n'est ni un élément central, ni obligatoire de l'idée de *blockchain*. L'accord du *réseau blockchain des nœuds complets* peut se produire sans un tel mécanisme, donc sans que chaque *page* contienne le *hash* d'une ou plusieurs pages précédentes, et sans aucune mise en œuvre d'un algorithme de preuve de travail. Un *fichier blockchain* porté par un nombre fixé de nœuds et fonctionnant par exemple à l'aide un simple consensus majoritaire (la Page *n*, est acceptée par tous si elle est acceptée par plus de la moitié des nœuds) n'a pas besoin de tout cela, qu'elle soit ouverte (tout le monde peut y lire) ou non.

Unicité du fichier *blockchain* et indestructibilité

Nous avons établi une nuance entre *fichier blockchain* et *état du fichier blockchain* car pour opérer un nœud, il est nécessaire de connaître certaines des informations que contient le *fichier blockchain* (pas nécessairement toutes), mais il n'est pas nécessaire que le nœud dispose exactement du *fichier blockchain* dans un format fixé identique en chaque nœud. Un nœud peut par exemple ne garder qu'une partie limitée du *fichier blockchain* ayant une grande probabilité d'être utile pour mener les contrôles, et compresser le reste qui ne serait décompressé qu'en cas de nécessité. On sait très bien aussi que certaines parties d'un *fichier blockchain* deviennent inutiles. L'immutabilité du *fichier blockchain* n'a de sens et n'est importante que pour sa partie active (les UTXO de *Bitcoin* par exemple). Bien évidemment, le plus simple dans la conception d'un *protocole blockchain* est de prévoir que chaque nœud du *réseau blockchain des nœuds complets* détient exactement le même *fichier blockchain* et c'est ce que l'on choisira de faire le plus souvent. Cependant il faut accepter pour disposer d'une définition générale que ce ne soit pas toujours le cas, et que même s'il existe une sorte de fichier de référence unique que nous nommons *fichier blockchain*, il ne soit pas nécessairement présent en chaque *nœud complet*. Un *nœud complet* n'a à garder que la capacité à le reconstituer à partir des informations qu'il stocke, et même, n'a à garder que la capacité à reconstituer la partie susceptible d'être utile pour mener le contrôle des transactions et des pages nouvelles.

Le réseau des nœuds complets et le réseau

Nous avons fait une distinction entre *réseau blockchain des nœuds complets* et *réseau blockchain*, car, comme on le sait bien, tous les nœuds participant à un *réseau blockchain* ne détiennent pas toujours toutes les informations sur l'*état du fichier blockchain*. Les clients légers du *Bitcoin* (« SPV client ») définissent de tels nœuds du réseau *Bitcoin*, qui ne sont pas des *nœuds complets*. Les membres d'un pool de minage dans le cas du *Bitcoin* qu'on doit considérer comme appartenant au réseau de la *blockchain* du *Bitcoin* sont aussi des nœuds du *réseau blockchain* : ils jouent un rôle secondaire, mais pas sans importance puisqu'ils contribuent à rendre les attaques 51 % plus difficiles en augmentant la puissance de calcul de *hash* du réseau.

Apparition et disparition des nœuds

La possibilité de créer des nouveaux nœuds par qui le souhaite et de les faire disparaître sans perturber le *réseau blockchain* est bien évidemment importante pour les *protocoles*

blockchains qu'on veut ouvert (accessible à tous en lecture, ou accessible à tous à la fois en lecture et en écriture). Cependant nous considérons que nous ne devons pas dans la définition du *protocole blockchain* exclure l'idée qu'un nombre fixé d'acteurs constituent les nœuds d'un réseau pair à pair support d'une *blockchain*. De telles *blockchains privées*, à la configuration rigide, sont bien sûr plus faciles à concevoir et à faire fonctionner que les *blockchains ouvertes* comme celle du *Bitcoin*. Elles permettent de créer de la confiance entre acteurs qui n'ont pas de raison d'en avoir entre eux, car par exemple ils sont liés à des entités concurrentes ou ennemies. Quand il y a bien un réseau pair à pair, et un fonctionnement par ajout irréversible de pages une à une, ordonnées et datées, il faut accepter de parler de *protocole blockchain*.

La notion de transactions

Pour disposer d'une définition assez générale, il est naturel de considérer qu'une *transaction* est simplement l'envoi par un nœud d'une information susceptible d'être intégrée dans une page du *fichier blockchain*, sans exiger que cette information détermine un déplacement de *jetons* comme dans le cas d'une *monnaie cryptographique*. Ces *transactions* dans ce sens général, par exemple dans le cas d'un *fichier blockchain* collectant et sécurisant des informations sur des objets de valeurs (objets d'art, diamants, etc.) n'ont pas pour fonction de gérer des *jetons* et de les rendre impossibles à dupliquer, mais simplement de créer des bases sécurisées et indestructibles de données engendrant de la confiance entre ceux qui y accèdent. La manipulation de *jetons* avec un registre de *comptes* est une application possible des *protocoles blockchains*, et c'est évidemment une des plus importantes puisqu'elle crée comme on l'a dit un *internet de la valeur*, mais il serait trop limitatif de ne penser les *protocoles blockchains* que dans cette optique. Partager une vérité, que ce soit celle concernant un *registre de comptes* ou conservant un autre type d'informations, est la fonction des *blockchains* qui ne sont pas seulement des outils pour faire circuler de la valeur. On comprend pourquoi, le point 16 de la définition est facultatif.

Ouverture en écriture et en lecture

Que tout le monde puisse écrire ou lire les informations d'une *blockchain* n'est pas obligatoire. Un *protocole blockchain* utilisé à partager et sécuriser des informations entre un groupe de banques ne sera pas public. Il peut être utile aussi de concevoir des *protocoles blockchain* où seuls quelques acteurs peuvent écrire, mais où tout le monde peut lire ; par exemple une *fichier blockchain* universel de diplômes où seules les écoles et universités peuvent écrire (en signant) les diplômes qu'elles délivrent, mais où tout le monde peut lire.

Signature et anonymat

Ni la signature des transactions, ni l'anonymat de ceux qui détiennent les nœuds et écrivent ou lisent ne sont essentiels à l'idée de *protocole blockchain*. Nul besoin de signer les informations qu'on dépose sur un *fichier blockchain* destiné à recevoir des critiques de livres par exemple. Nul besoin d'anonymat pour un *protocole blockchain* fermé (privé) entre un nombre limité de banques s'échangeant des titres par le biais d'un registre de comptes.

Rémunération et consensus de distribution

Pour créer un *protocole de blockchain ouverte* qui maintient un *registre de comptes* pour des *jetons*, il sera souvent souhaitable de créer un système d'incitation à gérer un *nœud complet*. C'est l'idée de Nakamoto pour le *Bitcoin*. Une façon créer l'incitation est que le *protocole blockchain* engendre de nouveaux *jetons* et les distribue aux nœuds complets. L'éventualité d'attaques Sybil (multiplication des identités de la part d'une seule entité) rend impossible une distribution par un procédé de choix probabiliste équiprobable pour tous les nœuds apparents sur le réseau, car en se créant des identités multiples on multiplierait facilement sa rémunération ce qui fausserait l'équité de la distribution. Un bon protocole de rémunération des nœuds complets doit donc se fonder sur un autre moyen de distribution. On connaît la méthode par les *preuves de travail* adoptée par le *Bitcoin*, *Ethereum* et bien d'autres *blockchains* ouvertes. On sait aussi qu'il existe d'autres protocoles envisagés (preuves d'enjeu, preuves d'espace, preuves « of burn », etc.) mais qu'aujourd'hui les grandes monnaies cryptographiques en terme de capitalisation n'utilisent que le protocole des *preuves de travail*.Y a-t-il une raison profonde à cela ? C'est un problème central de la conception des *blockchains ouvertes à jetons* qu'on ne peut pas considérer comme résolu (voir les hésitations d'*Ethereum* à changer la *preuve de travail* qu'il utilise par une *preuve d'enjeu*).

Gouvernance

Rien dans l'idée générale de *protocole blockchain* ne concerne directement les problèmes de gouvernance, mais bien sûr, c'est une question à considérer dans chaque cas particulier.

Duplication et rétablissement de cohérence

Les inévitables temps de latence des réseaux rendent impossible une synchronisation parfaite des nœuds complets. Il faut donc prévoir dans la conception d'un *protocole blockchain* ce qui doit être fait en cas de duplication du *fichier blockchain* c'est-à-dire en cas d'apparition en deux nœuds différents d'une Page *n* acceptable. La méthode des preuves de travail en inscrivant un contenu en calcul de plus en plus grand dans les pages du *fichier blockchain* offre un moyen naturel de choix entre *fichiers blockchain* présents simultanément sur le réseau : retenir le *fichier blockchain* détenant le plus grand contenu en calcul. D'autres méthodes sont bien sûr possibles, en particulier pour le *blockchains privées* ne concernant qu'un petit nombre de nœuds : ordre de priorité entre les nœuds, votes, choix aléatoire (déterminé par l'utilisation d'une fonction de hachage par exemple), etc.

Les smart-contracts

L'information partagée dans un *fichier blockchain*, peut être celle concernant la gestion d'un *registre de comptes* fixant combien de *jetons* détiennent les différents comptes. Écrire dans le *fichier blockchain* chaque déplacement des *jetons* permet de savoir combien en détient chaque compte. Si personne ne peut falsifier le *registre de compte* (ce que garantit le fonctionnement d'un bon *protocole blockchain*) il en résulte une forme de matérialité des jetons. Chacun existe comme un objet physique : il n'est détenu que par un seul compte à la fois (unicité), il peut circuler — on le retire d'un compte pour le mettre sur un autre (mobilité). Cette quasi-matérialité permet alors d'attribuer aux

jetons une valeur, de les acheter et de les vendre. On connaît cette histoire !

Cependant bien d'autres types d'informations que ces informations sur des comptes de jetons peuvent s'écrire sur un *fichier blockchain*. L'idée d'y déposer des programmes et ce qu'il faut pour les exécuter a donné naissance aux smart-contracts : programmes présents en chaque nœud du *réseau blockchain des nœuds complets* que chaque nœud exécute. De tels programmes sont impossibles à arrêter, ce qui fournit des garanties intéressantes nouvelles pour des programmes de jeu, de pari, ou liés à l'exécution de contrat d'assurance, etc. Ce type d'applications des *protocoles blockchains* est en train de devenir important, comme le succès d'*Ethereum* l'atteste.

L'ancrage des données, l'horodatage

N'oublions pas cependant que l'utilisation la plus simple d'un *protocole blockchain* est le dépôt d'informations datées dans un *fichier blockchain*, même si cette information n'est ni l'indication d'un déplacement de *jeton*, ni celle correspondant à un programme et à son exécution. L'ancrage des données est fondé sur cette idée élémentaire, souvent d'ailleurs en utilisant pour cela le *fichier blockchain* du *Bitcoin* dont le protocole autorise qu'on écrive librement 80 caractères dans chaque transaction. On dépose des données (ou le plus souvent le *hash* de données) sur le *fichier blockchain*. Ces données se trouvent alors fixées de manière définitive et associée à une date (*horodatage*, « timestamping » en anglais), celle de la page où elles ont été déposées. Ce type d'utilisations permet des *preuves d'existence* (tel fichier existait à telle date) et dispense donc par exemple des enveloppes Soleau de l'INPI.

Monnaies programmables et *pseudo-blockchain* ?

Il faut ici évoquer un type d'applications envisagé de plus en plus sérieusement (il semble mis en place à Dubaï) et qui bien que résultant du développement des *blockchains* et des réflexions qui se développent à leur sujet ne doivent pas être considérées comme des *protocoles blockchains*.

Les *jetons* créés sur un *fichier blockchain* en mettant en place un *registre de comptes* sont intéressants, puisque c'est un moyen de disposer comme nous le disions d'objets quasi physiques qu'on pourra faire circuler instantanément d'un point à un autre du globe sans pratiquement aucun coût, de manière anonyme (sous certaines conditions concernant le *protocole blockchain*) et irréversible. Les *jetons* créés pourront être programmables : on choisira par exemple qu'un certain déplacement de *jetons* ne se fera que si trois acteurs parmi 5 signent et qu'une fois la date X est dépassée. Grâce aux smart-contracts si le *protocole blockchain* choisi les permet, on pourra programmer des comportements plus complexes encore, donnant naissance à des contrats d'assurance automatiques (quand un certain événement se produit, un certain nombre de jetons sont déplacés du compte A vers le compte B) et plus généralement à ce qu'on nomme les *organisations autonomes décentralisées* (DAO).

Certaines de ces propriétés des jetons d'un *fichier blockchain* persistent même quand on retire l'exigence du réseau pair à pair. En effet, imaginons une sorte de *fichier blockchain* présent en un point unique et géré de manière centralisée par un acteur unique (par exemple une banque centrale). Cette *pseudo-blockchain* pourrait être accessible en lecture à tous (on pourrait donc surveiller son bon usage par la banque centrale), ne

fonctionner que par ajouts irréversibles de pages numérotées et datées. Cette *pseudo-blockchain* pourrait gérer un *registre de comptes* déterminant qui détient tel ou tel *jeton*. La création de comptes pourrait y être anonyme (comme pour *Bitcoin*) ou non. Le taux de change des jetons émis pourrait être fixé et garanti par la banque centrale détenant de manière centralisée la *pseudo-blockchain*. La banque centrale pourrait émettre de nouveaux jetons selon son bon vouloir, mais pourrait choisir au départ de le faire qu'à la vue de tous si la *pseudo-blockchain* est ouverte en lecture à tous. On pourrait avoir prévu de créer des *pseudo-smart-contracts* sur de telles *pseudo-blockchains* centralisées, régulées, et garanties. On aurait donc à peu près les mêmes fonctions que celles du *protocole blockchain Ethereum*, mais avec un tiers de confiance (la banque centrale) au lieu d'une confiance tirée de la réplication sur un réseau pair à pair du *fichier blockchain*. La possibilité d'accéder en lecture à la *pseudo-blockchain* permettrait le contrôle extérieur de ce que la banque centrale fait, et constituerait pour elle une obligation à respecter la règle d'immutabilité des pages écrites. Une certaine indestructibilité de la *pseudo-blockchain* serait donc aussi acquise.

Ne doutons pas qu'aujourd'hui certains pensent à ce genre de monnaies programmables centralisées fonctionnant sur des *pseudo-blockchain*. Des dollars ou des euros programmables existeront probablement un jour.

L'avenir verra ce type de monnaies naître et peut-être même se substituer à l'argent liquide sous forme de pièces et de billets. Notons aussi que le fonctionnement de telles monnaies n'entraîne aucune dépense excessive d'électricité puisqu'il n'exige pas de minage et de preuve de travail comme le fonctionnement des protocoles du *Bitcoin* et d'*Ethereum*. Des variantes sans anonymat des comptes sont envisageables, avec l'inconvénient alors qu'on ne pourra pas parler d'argent liquide (de « cash »).

L'absence de réseau pair à pair rend impossible de faire entrer ce type de *pseudo-blockchains* dans ce que nous voulons appeler *blockchain*. Utilisons dont un autre mot et parlons par exemple de *monnaies programmables centralisées à pseudo-blockchain*.

Conclusion

Préciser le vocabulaire, permet de mieux comprendre. Si un accord se produit sur le sens des mots on évite la confusion. Aujourd'hui on lit et on entend tout à propos des *blockchains* (voir plus bas les définitions proposées qui se contredisent toutes les unes les autres). Pour mesurer l'importance que prendront les *protocoles blockchain* il faut clairement les distinguer des *bases de données distribuées*, *décentralisées*, *répliquées*. Il faut aussi savoir ne pas confonde les divers usages d'une véritable *blockchain* : ancrage de données, horodatage de données, partage d'informations diverses, gestion d'un registre décentralisé de comptes à jetons, support à smart-contracts. Enfin il faut reconnaître que des concepts voisins mais ne méritant pas le nom de *blockchain* (comme celui que nous proposons de nommer protocole de *monnaies programmables centralisées à pseudo-blockchain*) sont sans aucun doute appelés à avoir leur place.

Exemples divers de définitions de *blockchain*

• Elli **Androulaki**, Christian Cachin, Angelo De Caro, Alessandro Sorniotti and Marko Vukolic, IBM Research, Zurich, 2017. Permissioned Blockchains and Hyperledger Fabric, in « Peter Kunz ed., ERCIM News 110, iBooks, 2017. »

« Blockchains can be defined as immutable decentralised ledgers for recording transactions that - depending on the system - are to various degrees resilient to malicious behaviour. Blockchain peers maintain copies of the ledger that consists of groups of transactions (blocks) linked together into a hash-chain. This effectively establishes total order among blocks and, consequently across transactions. »

• Imran **Bashir**, Mastering Blockchain. iBooks, 2017.

« There are various definitions of blockchain ; it depends on how you look at it. If you look at it from a business perspective it can be defined in that context, if you look at it from a technical perspective one can define it in view of that. Blockchain at its core is a peer-to-peer distributed ledger that is cryptographically secure, append-only, immutable (extremely hard to change), and updateable only via consensus or agreement among peers. Blockchain can be thought of as a layer of a distributed peer-to-peer network running on top of the Internet, as can be seen below in the diagram. It is analogous to SMTP, HTTP, or FTP running on top of TCP/IP. [...] From a business point of view a blockchain can be defined as a platform whereby peers can exchange values using transactions without the need for a central trusted arbitrator. This is a powerful concept and once readers understand it they will realize the tsunamic potential of blockchain technology. This allows blockchain to be a decentralized consensus mechanism where no single authority is in charge of the database. »

• Yves **Caseau**, Serge Soudoplatoff, La blockchain, ou la confiance distribuée, Rapport de *La Fondation pour l'innovation politique* , 2016

« La blockchain est une technologie novatrice qui permet à des utilisateurs d'effectuer des transactions, financières ou non, garanties et auditables par tout le monde, sans avoir besoin d'un tiers de confiance. Après chaque transaction, une nouvelle ligne vient se greffer au bloc, formant une chaîne indéfectible : la blockchain. Elle incarne le livre de compte 2.0, l'historique de chaque transaction étant répertorié dans un registre décentralisé et redistribué. La complexité des algorithmes utilisés rend ces transactions infalsifiables. »

• Tianan **Laurence**, Blockchain for dummies, John Wiley & Sons, 2017

« Originally, *blockchain* was just the computer science term for how to structure and share data. Today blockchains are hailed the " fifth evolution" of computing. Blockchains are a novel approach to the distributed database. The innovation comes from incorporating old technology in new ways. You can think of blockchains as distributed databases that a group of individuals controls and that store and share information. »

• Laurent **Leloup**, *Blockchain, la révolution de la confiance*, Editions Eyrolles, 2017.

« Voici plusieurs définitions qui, crescendo, devraient vous permettre de mieux comprendre ce qu'est la blockchain :

Simpliste : une blockchain est un grand livre de compte ouvert et accessible à tous en écriture et en lecture et qui est partagée sur un grand nombre d'ordinateurs à travers le monde.

Basique : une blockchain est un logiciel qui stocke et transfère de la valeur ou des données via Internet, de façon transparente et sécurisée, et sans organe central de contrôle.

Littérale : une blockchain désigne une chaîne de blocs (conteneurs numériques) dans

lesquelles sont stockées des informations de toute nature : transactions, contrats, titres de propriétés, œuvres d'art, etc.

Généraliste : une blockchain est une technologie pour une nouvelle génération d'applications transactionnelles qui, grâce à un mécanisme de consensus collectif couplé avec l'utilisation d'un grand livre de compte public, décentralisé et partagé, établit la confiance, la responsabilité et la transparence tout en rationalisant les processus d'affaires.

Technique : une blockchain est une nouvelle technologie de base de données s'appuyant en tirant pleinement profit d'internet, du protocole libre, de la puissance de calcul et de la cryptographie. Cette base de données transactionnelle distribuée est comparable à un grand livre comptable (registre ou ledger) dans lequel chaque nouvelle transaction est écrite à la suite des autres, sans avoir la possibilité d'effacer ou de modifier les précédentes. Ce registre est actif, chronologique, distribué, vérifiable et protégé contre la falsification par un système de confiance répartie (consensus) entre les membres ou participants (nœuds).

On peut proposer cette définition qui résume l'ensemble des précédentes : une blockchain est une base de données transactionnelle distribuée, comparable à un grand livre comptable décentralisé et partagé, qui stocke et transfère de la valeur ou des données via Internet, de façon transparente sécurisée et autonome car sans organe central de contrôle. Ce registre est actif, chronologique, distribué, vérifiable et protégé contre la falsification par un système de confiance répartie (consensus) entre les membres ou participants (nœuds). Chaque membre du réseau possède une copie à jour du grand livre (en temps quasi réel) »

• Christopher **Lewis**, Blockchain: Your Comprehensive Guide To Understanding The Decentralized Future, iBooks, 2016.

« The Blockchain is a ledger that helps keep track of all confirmed transactions involved. However, this is not a personal ledger that will track your transactions, but a shared public ledger that automatically includes all the transactions occurred over the whole network. This means that anyone who wants to can have a view of all transactions that have taken place across the network. »

• **MEDEF** et Boston Consulting Group, Livre blanc La blockchain pour les entreprises, 2017.

« Définie comme registre infalsifiable distribué, la blockchain lance la quatrième révolution des facultés de conservation et de partage des informations dont nous souhaitons garder trace. Registre *infalsifiable* parce que la blockchain permet de sécuriser et de garantir un historique de données, une inviolabilité des échanges, c'est-à-dire une source unique de vérité, alors qu'écrits, imprimés ou fichiers se limitent à porter un message sans en assurer la véracité. Registre *distribué* parce que fonctionnant sans organe de contrôle centralisé et pouvant être mis à jour en temps réel par toutes les parties prenantes à un échange. Associée à des méthodes classiques de cryptologie, la blockchain permet aux parties prenantes de contrôler le niveau d'information partagée dans le registre. »

• **Wikipedia** `https://en.wikipedia.org/wiki/Blockchain` (consulté le 6-10-2017)

« A blockchain – originally block chain – is a continuously growing list of records, called *blocks*, which are linked and secured using cryptography. Each block typically contains a

hash pointer as a link to a previous block, a timestamp and transaction data. By design, blockchains are inherently resistant to modification of the data. A blockchain can serve as « an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way. » For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks, which needs a collusion of the network majority. »

• **Wikipédia**, `https://fr.wikipedia.org/wiki/Blockchain` (consulté le 6-10-2017)

« Une blockchain ou chaîne de blocs est une base de données distribuée transparente, sécurisée, et fonctionnant sans organe central de contrôle. Par extension, une chaîne de blocs est une base de données distribuée qui gère une liste d'enregistrements protégés contre la falsification ou la modification par les nœuds de stockage. Une *blockchain* est donc un registre distribué et sécurisé de toutes les transactions effectuées depuis le démarrage du système réparti. Une analogie avec l'Internet (TCP-IP) peut être dressée, car il s'agit dans les deux cas de protocoles informatiques sous-jacents à une infrastructure décentralisée. Internet transfère des paquets de données d'un point A à un point B, alors que la *blockchain* permet à la « confiance » de s'établir entre des agents distincts du système. »