Blockchain : quelle confiance, pour quels usages ?

Par **Clément JEANNEAU**
Cofondateur de Blockchain Partner, *leader* français du conseil sur les *blockchains* et actifs numériques

En octobre 2015, la revue *The Economist* consacra sa une à une technologie encore inconnue du grand public, la *blockchain*, alors désignée comme une « machine à créer de la confiance ». Cette couverture sonna le top départ d'une frénésie autour d'une innovation dont les possibilités et les limites ont, depuis, souvent été mal perçues. Vue comme complexe, voire obscure, la *blockchain* est devenue l'archétype du "*buzzword*", suscitant emballement chez les uns, agacement chez les autres.

L'économiste Nouriel Roubini, qui se range dans la deuxième catégorie, parle même d'une « escroquerie » et de « la technologie la plus surfaite et la moins utile de toute l'histoire humaine » (1) – rien que ça ! Cet avis très tranché symbolise les réactions disproportionnées, les plus laudatives comme les plus sévères, autour de la *blockchain*. Plus de dix ans après sa création et cinq ans après son entrée sur le terrain médiatique, cette technologie mérite des analyses plus dépassionnées. Peut-on avoir confiance en la *blockchain*, elle qui permettrait justement, dit-on, de se passer de tiers de confiance ? Et si oui, pour quels usages concrets ? C'est tout l'objet de cet article.

Un malentendu originel

Si la *blockchain* a suscité autant de controverses, c'est notamment parce que le ver était dans le fruit dès le départ : aucune définition de la *blockchain* ne fait *consensus*. L'enjeu n'est pas seulement le choix des termes pour décrire cette technologie, mais bien le périmètre qui entoure celle-ci. Ainsi, si une *blockchain* est une base de données décentralisée (partagée entre tous ses utilisateurs, et fonctionnant sans organe central de contrôle), toute base de données décentralisée n'est pas une *blockchain* : il lui faudrait pour cela des caractéristiques supplémentaires, dont la liste peut faire débat.

Exemple typique : si les droits d'écriture et de lecture des données qui y sont inscrites sont réservés à certains acteurs spécifiques, une base de données décentralisée peut-elle être une *blockchain* ? Oui, potentiellement, répondront la plupart des acteurs du secteur, pour qui il faut alors parler de « *blockchain* privée ». Non, répondront certains puristes, pour qui une *blockchain* n'a de sens qu'en version publique, lorsque ces droits sont ouverts à tous.

Au cœur de la confiance, le protocole de *consensus*

L'enjeu n'est pas anecdotique. La confiance envers une *blockchain* tient à la façon dont les informations y sont inscrites et gérées. C'est toute la question de ce qui est appelé « le protocole de *consensus* » : la façon dont les acteurs d'une *blockchain* se mettent d'accord sur l'inscription et la gestion des données, et notamment leur authenticité. On touche là au cœur de la *blockchain* comme « machine à générer (ou non) de la confiance ». Pour schématiser : si le protocole de *consensus* est jugé faible, la confiance générée envers les données ne peut qu'être fragile ; s'il est robuste, la confiance est alors (plus) forte.

(1) « La grande escroquerie de la blockchain », tribune dans Les Échos, 30/10/2018

La *blockchain* dont le protocole de *consensus* est jugé généralement le plus robuste est la première *blockchain* à avoir vu le jour : celle de Bitcoin, née en 2009, justement en écho à la crise de confiance engendrée par la crise financière. Son protocole de *consensus* repose sur un algorithme, appelé le *Proof of Work* (preuve de travail), qui, en quelques mots, repose sur le travail d'acteurs, d'entités et d'individus, appelés « mineurs » : ceux-ci sont en compétition pour résoudre le plus rapidement possible un problème mathématique complexe dans l'objectif de confirmer une transaction sur le réseau, ce qui leur permet alors de toucher une récompense financière. La transaction vient ensuite valider l'inscription d'une donnée sur la chaîne, c'est-à-dire sur le registre : à chaque transaction peut en effet être associé un (petit) ensemble de données.

Pourquoi l'invention de la *blockchain* Bitcoin était inédite

La confiance envers la *blockchain* Bitcoin tient à un assemblage inédit, qui mêle une couche technologique (algorithme de *consensus*, cryptographie asymétrique, réseau pair à pair et registre distribué) avec une deuxième couche, composée d'incitations économiques. En très bref : il est plus rentable, pour un acteur qui dispose d'une forte puissance de calcul, de participer à l'activité du réseau (en tentant de valider des transactions) que de l'attaquer (en tentant de le pirater, ce qui n'est de toute façon à la portée de quasiment aucune entité). En effet, plus l'on dispose d'une forte puissance de calcul, plus l'on a de chances de résoudre en premier le problème mathématique en question et ainsi de remporter la récompense qui vient avec la validation d'une transaction.

Si le terme – assez galvaudé – de « révolution » devait être appliqué aux *blockchains*, ce serait pour qualifier cet assemblage qu'il serait le moins illégitime. La *blockchain* Bitcoin n'est pas infaillible : aucun système informatique ne l'est. Cependant, pour reprendre les mots du grand informaticien français Gérard Berry, « un système est sûr non pas quand il est inattaquable – ce qui est théoriquement impossible –, mais quand cela coûte trop cher de l'attaquer » [(2)]. Or ce principe est au cœur de la *blockchain* Bitcoin, aujourd'hui la plus sûre de toutes les *blockchains* publiques.

Cela ne signifie pas pour autant que la *blockchain* Bitcoin est idéale en tout point : sa forte consommation énergétique est fréquemment désignée comme l'un de ses grands inconvénients, de même que sa vitesse pour valider des données, plus limitée que sur d'autres *blockchains* par mesure de sécurité. En réalité, il n'existe pas de « meilleure » *blockchain* dans l'absolu : tout dépend des critères qui comptent le plus pour les utilisateurs d'un protocole par rapport à leurs besoins.

Cela ne signifie pas non plus que la *blockchain* Bitcoin est totalement novatrice : son inventeur anonyme, se cachant derrière le pseudonyme Satoshi Nakamoto, est venu piocher dans des décennies de recherche académique. La quasi-totalité des composants techniques de Bitcoin proviennent en effet de travaux de recherche publiés dans les années 1980 et 1990.

La première application ouverte par la *blockchain* : la rareté numérique

En réalité, l'originalité de la *blockchain* Bitcoin tient à la combinaison d'éléments qui n'avaient jamais été imbriqués les uns avec les autres. Ainsi, si Bitcoin ne fut pas la première monnaie digitale, elle fut la première à incorporer l'idée d'un algorithme de *consensus* empêchant le problème de la double dépense (le fait d'émettre deux transactions dépensant le même avoir) – ce sans quoi il ne peut y avoir de confiance envers une monnaie.

Ce faisant, la *blockchain* Bitcoin, qui s'appuie sur un croisement inédit d'innovations en théorie

(2) Entretien publié par Rue89 le 21/11/2016

des jeux, en cryptographie, en informatique, entre autres domaines, a permis ce qui n'avait jamais été possible jusqu'à présent : envoyer en ligne une unité de valeur d'un acteur A à un acteur B sans duplication ni passage par un tiers de confiance. En d'autres termes, la *blockchain* Bitcoin a rendu possible la rareté numérique. Lorsqu'un internaute A envoie un fichier (document texte, image, son, vidéo…) à un internaute B, il envoie en réalité une copie, et conserve le premier fichier sur son terminal ; avec Bitcoin, il est devenu possible de s'envoyer de la rareté numérique de pair à pair, c'est-à-dire sans passer par une autorité centrale comme une banque.

La *blockchain* est à la valeur ce qu'Internet a été à l'information

Pourquoi est-ce important ? Parce que ce qui est valable pour le Bitcoin l'est également pour de multiples autres actifs numériques échangeables *via* une *blockchain* (qu'il s'agisse de celle de la *blockchain* Bitcoin ou d'une autre, la principale alternative s'appelant Ethereum). Ces actifs, pouvant être créés par tout internaute, sont appelés « jetons », ou *tokens* en anglais – de là la notion de « tokenisation », qui consiste à créer sur une *blockchain* la représentation numérique d'actifs existants (actions, obligations, actifs immobiliers, etc.).

En définitive, la *blockchain* est à la valeur ce qu'Internet a été à l'information. Internet a permis de décentraliser l'information, en donnant à chaque internaute un pouvoir inédit : celui de publier et d'échanger toute information qui soit, instantanément, auprès du monde entier, sans devoir en demander la permission. La *blockchain* permet de décentraliser la valeur. Avec la *blockchain*, tout internaute s'empare d'un nouveau pouvoir : créer et échanger tout actif de valeur qui soit, avec l'internaute de son choix, (quasi) instantanément, sans nécessiter la permission d'un quelconque tiers.

Une confiance pour quels usages ?

L'intérêt que l'on peut porter aux *blockchains* comme génératrices de confiance dépend étroitement de l'intérêt que l'on porte à ses usages. Comme nous venons de l'expliquer, le premier usage historique des *blockchains* est la création et l'échange d'actifs numériques sans intermédiaire. C'est ce que le grand public connaît sous le terme de « cryptomonnaies », et ce que les entreprises expérimentent depuis quelques années pour des applications financières et immobilières, notamment sous le terme de « tokenisation » présenté plus haut. La banque Santander et la Société générale ont ainsi commencé à expérimenter en 2019 la « tokenisation » d'obligations sur la *blockchain* Ethereum.

Gérer des actifs numériques sur une *blockchain* peut permettre, en particulier, de se passer d'intermédiaires lors des échanges, avec l'automatisation des processus d'émission et d'échange d'actifs. Ce faisant, les entreprises peuvent bénéficier de réductions de coûts, de contraintes et de temps, et limiter le risque de contrepartie pour certaines opérations. Ces applications relèvent d'une logique d'optimisation pour les acteurs financiers existants, mais peuvent également ouvrir de nouvelles possibilités, par exemple l'accès facilité aux marchés de capitaux à des structures plus petites, ou l'apparition de nouveaux produits et services financiers.

Au-delà de la finance

La finance et l'immobilier ne sont pas les seuls secteurs concernés. Le concept de « rareté numérique », qui rend possible la propriété, la portabilité et la traçabilité d'actifs nativement numériques, ouvre de nouveaux champs que commencent à explorer un nombre croissant d'acteurs du sport (autour de l'idée de cartes de collection numériques liées à des sportifs professionnels, comme le propose la prometteuse *start-up* française SoRare, qui a signé des accords avec les plus grands clubs de

football européens), du luxe (autour du concept de « vêtements digitaux »), de l'art ou encore du jeu vidéo.

De façon plus traditionnelle, loin des questions d'actifs numériques, une *blockchain* peut également être utilisée en tant que registre. Elle peut alors servir à prouver l'existence à un temps T d'une donnée ou d'un document numérique (ce qui a des applications en propriété intellectuelle au travers de l'« enveloppe Soleau numérique », comme le propose la solution Datatrust), ou à prouver l'intégrité de données ou documents numériques. C'est ce qui explique, entre autres usages, pourquoi la *blockchain* est aujourd'hui utilisée pour lutter contre les faux documents.

Exemples d'applications réelles

Les exemples d'applications dans le tissu économique, bien que méconnus, sont variés. Rien qu'en France, pensons aux différents établissements d'enseignement supérieur français qui l'utilisent pour certifier leurs diplômes (par exemple, l'ESCP et l'EM Lyon *via* la *start-up* BCDiploma) ; aux nombreux groupes du CAC 40 qui se servent de la *blockchain* Ethereum pour garantir l'authenticité de leurs communiqués de presse et lutter ainsi contre les *fake news* en communication financière (dont Renault, Natixis, Bouygues, Crédit agricole, *via* la plateforme Wiztrust qui s'appuie sur Datatrust) ; au groupe Kering qui utilise depuis l'an dernier la *blockchain* Bitcoin pour enregistrer les certificats d'authenticité numériques des montres de sa marque Ulysse Nardin ; ou encore aux bailleurs sociaux comme Immobilière 3F et acteurs du BTP comme Léon Grosse qui ont recours à la *blockchain* Bitcoin (*via* la plateforme ContractChain), pour garantir la bonne conformité des documents des contrats.

La *blockchain* peut également s'avérer intéressante en version privée, pour s'organiser collectivement entre acteurs qui ne se font pas confiance *a priori* et/ou qui rencontrent des difficultés à collaborer : entreprises concurrentes ou (lointaines) partenaires, entreprises d'une même chaîne de valeur, entités d'un même groupe, etc. Grâce à la décentralisation du registre, le problème politique de la propriété de ce registre est réglé, puisque celui-ci devient techniquement réparti entre tous ses acteurs.

Le cas de la Banque de France

Ce dernier usage correspond par exemple au projet « Madre » développé par la Banque de France, dont la *blockchain* privée a été mise en production en 2018. Jusqu'alors, la Banque de France collectait elle-même les requêtes d'identifiants créanciers SEPA – envoyées par les banques commerciales pour le compte de leurs clients – et gérait elle-même l'attribution de ces identifiants. La Banque de France a choisi de décentraliser le registre : celui-ci est aujourd'hui une *blockchain* répartie entre les banques commerciales et la Banque de France. Chaque acteur dispose ainsi d'une transparence sur la base de données, sans qu'aucun ne la contrôle plus qu'un autre.

En outre, la Banque de France a utilisé des *smart contracts* – des programmes autonomes qui s'appuient sur la *blockchain* et sur des référentiels de confiance (liste des SIREN à jour, etc.) – pour automatiser le processus d'attribution des identifiants et l'inscription de ceux-ci sur le registre. Ce nouveau système a permis de réduire les délais de traitement, de plusieurs jours à quelques minutes.

Une nouvelle économie numérique… en devenir

Dans l'immense majorité des cas cependant, une *blockchain* a peu d'intérêt par rapport à une base de données traditionnelle : cette technologie n'a pas vocation à devenir la règle pour gérer des

données. Son usage ne correspond qu'à certains besoins très spécifiques, cités ci-dessus. Au-delà, il faut bien percevoir que l'essentiel ne se joue pas dans les blockchains privées, ou fermées : bien que celles-ci puissent être parfois intéressantes pour les organisations, elles sont l'équivalent des intranets par rapport au réseau ouvert qu'est Internet. À partir des concepts de « rareté numérique » et de « tokenisation », la *blockchain* ouvre la voie à une nouvelle économie numérique, dont les applications n'ont de sens que sur des *blockchains* ouvertes.

Malgré des avancées réelles ces dernières années, les besoins de facilité d'utilisation, de confidentialité et de rapidité restent encore à satisfaire pour que cette économie numérique prenne son essor massivement. Ce chemin prendra encore plusieurs années et ne doit pas être précipité au détriment des impératifs de fiabilité ; ce sera à ce prix que les utilisateurs grand public pourront accorder véritablement leur confiance aux *blockchains*.