CHAPITRE 1

Qu'est-ce que la *blockchain* ?

1. DANS QUEL CONTEXTE LA *BLOCKCHAIN* A-T-ELLE ÉMERGÉ ?

La technologie *blockchain* suscite beaucoup d'intérêt et d'espoirs dans nombre de secteurs de l'économie [1]. Elle est apparue dans un contexte de défiance envers le monde de la finance et la capacité des États à en encadrer les dérives. Après la crise financière de 2008, et la mise en cause des gouvernements et des institutions financières, s'est développée l'idée d'une nouvelle forme de confiance qui reposerait sur la technologie et les échanges pair à pair [2], sans intermédiaire. Cette idée a donné naissance à l'application la plus connue de la *blockchain*, à laquelle on la réduit parfois abusivement, la monnaie virtuelle *bitcoin*. Avec le *bitcoin,* c'est en effet une alternative au système financier institutionnel accusé de parasitisme et d'immobilisme qui est proposée. La fiabilité de cette alternative ne dépend pas du bon vouloir ou des décisions, contestées, des gouvernants, mais d'une « froide » technologie qui ne peut être accusée de partialité. Pour les partisans du *bitcoin* et plus généralement des crypto-monnaies, la monnaie est chose bien trop sensible (c'est depuis 2008 prouvé) pour être confiée aux bons soins des États [3].

À cette défiance envers le système financier et les États s'est ajoutée une méfiance accrue envers le petit nombre d'acteurs du *Web* devenus incontournables, les GAFA (Google, Amazon, Facebook, Apple) et BATX (Baidu, Alibaba, Tencent, Xiaomi), chacun majoritaire sur son marché (trafic vers les publicités, *e*-commerce, réseau social ou smartphones) [4]. Certains en appellent donc à une « re-décentralisation » du *Web* [5], mouvement que permettrait la technologie *blockchain*.

---

1. Par ex. Paris Europlace, rapport du groupe *FinTech sur* « *Les impacts des réseaux distribués et de la technologie blockchain dans les activités de marché* », 23 octobre 2017. *A contrario*, V. par ex. A. Hankin, « Can blockchain technology live up to the hype? Barclays analysts say no », *MarketWatch*, 16 avril 2018.
2. V. Glossaire.
3. Institut Sapiens, *Bitcoin, totem & tabou – Que présage l'essor des cryptomonnaies ?*, février 2018, p. 7.
4. C. Jeanneau, *L'âge du web décentralisé*, Digital New Deal Foundation, avril 2018, p. 5-8.
5. *Ibid.*, p. 8.

2. QUELLES SONT LES CARACTÉRISTIQUES DE LA *BLOCKCHAIN* ?

2.1 Décentralisation et partage

De façon approximative, la *blockchain* peut être appréhendée comme une base de données sécurisée, dont la sauvegarde est partagée et les informations validées par des règles de consensus. Plus techniquement, elle sert de support à la tenue de registres partagés, distribués auprès des membres d'un réseau qui en sont les gardiens, registres portant sur des informations ou opérations vérifiées et gravées indéfiniment et de façon intangible dans une « chaîne de blocs ».

La première caractéristique de la *blockchain* est d'être « décentralisée » puisque les opérations qui y sont enregistrées ne sont pas validées par un acteur spécifique, mais par un consensus [6] dont les modalités sont définies par le protocole [7] de la chaîne.

Sa seconde caractéristique est d'être « partagée » : le registre qu'elle constitue est en effet reproduit dans la mémoire d'un certain nombre d'ordinateurs indépendants les uns des autres, les nœuds [8] du réseau, qui ensemble assurent la pérennité et la cohérence du système.

2.2 Architecture de la *blockchain*

En termes techniques, la *blockchain* est une « méta-technologie » [9], dans la mesure où elle combine plusieurs technologies : en premier lieu Internet, mais aussi « une base de données, une application logicielle, un certain nombre d'ordinateurs connectés, des clients pour y accéder, un environnement logiciel autour [et] des outils pour la contrôler » [10].

On parle en général de « la » *blockchain*. Toutefois, il en existe plusieurs, certaines partageant un même protocole, notamment les plus usités, *Bitcoin* et *Ethereum*.

---

6. V. Glossaire.
7. V. Glossaire.
8. V. Glossaire.
9. W. Mougayar, *Business blockchain – pratiques et applications professionnelles*, Dicoland, avril 2017, p. 37.
10. *Ibid*.

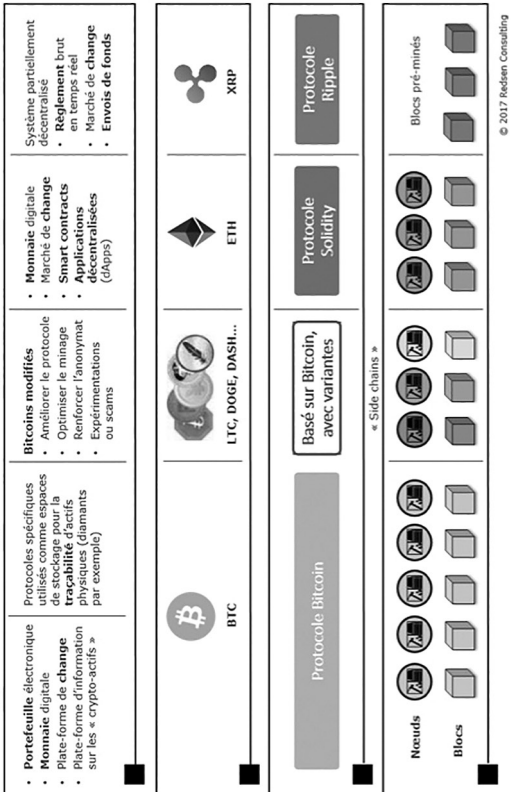
Toute *blockchain* comporte plusieurs niveaux :

– le premier est celui du réseau décentralisé composé de « nœuds », participants actifs reliés entre eux qui se partagent un registre et mettent leur capacité de calcul à disposition du réseau, dont certains, les mineurs [11], vont valider des blocs [12] ou ensembles de transactions ou d'informations. Le nombre de nœuds actifs du *bitcoin* est estimé à environ 6 000 ;
– le deuxième est celui du protocole créé et amélioré par des développeurs et mis à la disposition du réseau, qui va définir les règles de fonctionnement de la chaîne et permettre l'exécution des applications du quatrième niveau ;
– le troisième est celui des crypto-actifs, les jetons (*tokens*) [13], dont l'objectif est de transférer de la valeur entre membres du réseau. Dans le cas particulier des crypto-monnaies, le jeton est à la fois la valeur et le support numérique de cette valeur ;
– le quatrième et dernier niveau est celui des applications développées pour fournir des services et informations à la *blockchain*. Dans le cas du *bitcoin*, ces applications peuvent être des plateformes d'échange de *bitcoins* en monnaie *fiat* ou de conservation des *bitcoins* (portefeuilles électroniques ou *wallet* [14]). Les *smart contracts* [15] sont des applications.

Chaque niveau se repose sur le niveau inférieur pour fonctionner. Plus le niveau est bas, plus la sécurité offerte est importante.

11. V. Glossaire.
12. V. Glossaire.
13. V. Glossaire.
14. V. Glossaire.
15. V. Glossaire.

Ce mode de fonctionnement peut être schématisé comme suit :



Source : « La technologie *Bitcoin* et ses variantes ». Christophe Vriet. Redsen Consulting, 2017. Extrait de l'article https://www.redsen-consulting.com/fr/inspired/finance/adopte-une-blockchain.

La *blockchain* se fonde sur un transfert de la confiance à un réseau décentralisé dont les membres, ou une partie de ceux-ci, valident des informations ou opérations, constituant ainsi des blocs qui viennent alimenter une chaîne qui se développe au fur et à mesure de la validation des blocs. La chaîne est enregistrée et mise à jour par chaque nœud du réseau. Bien évidemment, cette démultiplication des enregistrements engendre un « gaspillage » des capacités de stockage mises à la disposition du réseau, par opposition au stockage chez un intermédiaire de confiance unique ; mais ce « gaspillage » est aussi la condition du partage et de la sécurité des informations enregistrées sur la chaîne.

2.3 Création des blocs et minage

La création d'une chaîne de blocs suit schématiquement la logique suivante. Un ensemble de transactions est regroupé au sein d'un même bloc qui, pour être validé et ainsi confirmer les transactions qu'il contient, suppose la résolution d'un problème de calcul complexe. Cette validation est dénommée minage, par référence à l'exploitation de métaux précieux. Dans le cas particulier du *bitcoin*, il s'agit de résoudre une équation de la fonction de « hachage » [16] SHA-256 dont la particularité est l'imprédictibilité de ses résultats. Si le résultat d'une donnée d'entrée se calcule aisément, en revanche l'opération inverse, qui consiste à retrouver cette donnée à partir du résultat, est très longue : le nombre de combinaisons possibles s'élève à 10^{77} et la seule façon de résoudre le problème consiste à tester chaque combinaison, l'une après l'autre. Par conséquent, la probabilité de résolution de cette équation est proportionnelle à la capacité de calcul de chaque mineur. La dépense nécessaire pour résoudre ce problème rendu « artificiellement » [17] complexe est la garantie du maintien au sein de la chaîne d'acteurs honnêtes et motivés. Le premier mineur à résoudre l'équation communique son résultat aux autres mineurs qui cessent de travailler sur leur bloc. Le bloc est ensuite approuvé par consensus, c'est-à-dire, dans le cas du *bitcoin*, par plus de la moitié des nœuds [18]. Ce type de minage est généralement dénommé minage par « preuve de travail » (*proof of work*) [19], preuve qui consiste en la diffusion de la solution par le mineur le plus rapide aux autres mineurs. L'identité alphanumérique du bloc, dénommée « hach », qui faisait l'objet du problème de calcul, est ensuite reportée dans le bloc suivant, assurant ainsi la continuité de la chaîne.

16. V. Glossaire.
17. J. Gossa, « Les *blockchains* et *smart contracts* pour les juristes », *Dalloz IP/IT*, 2018, p. 393.
18. Institut Sapiens, étude préc., p. 27.
19. V. Glossaire.

D'autres variantes de minage sont envisageables dans les *blockchains* : minage par consensus d'un certain nombre de « nœuds » clés ou de nœuds constitués en « sous-réseau » (*sharding*) ou minage par « preuve d'enjeu » (*proof of stake*) [20], où le mineur est tiré au sort, mais où chaque membre de la chaîne a une chance d'être désigné proportionnelle à son intérêt dans la chaîne [21]. On ne parle parfois plus dans ce cas de minage mais de *forging*.

Il peut également être envisagé de ne soumettre à la validation de la chaîne de blocs principale qu'une partie des transactions effectuées entre membres, celles supérieures à un certain montant par exemple, les autres étant orientées sur une chaîne latérale (*sidechain*) soumise à des règles de validation moins exigeantes [22] : la chaîne *Lightning network*, qui compte environ 1 000 nœuds actifs se superpose ainsi au réseau *bitcoin*, les opérations effectuées entre membres n'étant pas immédiatement inscrites sur la chaîne *bitcoin* mais seulement après une période donnée. Ainsi, seul le solde des opérations de cette période sera présenté à la chaîne principale [23].

L'avenir est probablement à ces nouveaux modes de validation qui permettront aux chaînes de valider les transactions plus rapidement, sans toutefois compromettre le niveau de sécurité, qui constitue l'une des caractéristiques fondamentales de la *blockchain*.

Dans le cas des *blockchains* « privées » [24], les règles de validation des blocs peuvent être différentes de celles exposées ci-dessus (qui caractérisent seulement les *blockchains* publiques) et même prévoir un contrôle total de l'organisateur ou du sponsor de la chaîne. On s'écarte alors du modèle classique de la *blockchain* puisqu'on y réintroduit un tiers de confiance.

Le mineur qui a validé le bloc perçoit généralement une rémunération. Pour le *bitcoin*, la rémunération obtenue pour la validation d'un bloc décroît d'environ 50 % tous les quatre ans. Elle était ainsi de 50 *bitcoins* à la création de cette « monnaie » et n'est aujourd'hui plus que de 12,5 *bitcoins*. Les mineurs sont rémunérés par la création *ex nihilo* de *bitcoins* qui semble ne « coûte[r] rien à personne, même pas aux bénéficiaires du service » [25]. On notera que la baisse régulière de la rémunération des mineurs ainsi que le plafonnement et la

20. V. Glossaire.
21. Ou proportionnelle à la participation qu'il accepte de mettre en dépôt. V. J.-P. Landau, *Les crypto-monnaies*, rapport au ministre de l'Économie et des Finances, 4 juillet 2018, p. 21.
22. Medef et Boston Consulting Group, *Livre blanc : La blockchain pour les entreprises*, juin 2017, p. 28.
23. V. définition du minage « lightning » dans le rapport Landau préc., p. 21.
24. V. *infra*, typologie des *blockchains*.
25. C. Chouard, « L'ironie du bitcoin », *La Tribune*, 20 mars 2018, p. 93.

décélération de la création de *bitcoins* – 99,8 % des *bitcoins* auront été émis en 2040 [26] – risquent de faire perdre toute attractivité au minage. Il faudra alors trouver un mode de rémunération alternatif pour les mineurs afin d'assurer le fonctionnement de la chaîne [27].

Les mineurs peuvent par ailleurs être rémunérés par les membres d'une chaîne qui souhaitent que leur transaction soit prioritairement incluse dans un bloc (en raison, par exemple, de son montant) [28]. Ces frais ne sont pas totalement négligeables [29]. Le minage aurait généré un chiffre d'affaires de 2 milliards de dollars en 2017 [30].

On pourrait résumer l'économie du minage comme suit [31] : plus une crypto-monnaie est utilisée, plus sa valeur augmente et plus elle attire des mineurs qui perçoivent une rémunération significative en échange de la mise à disposition de leur capacité de calcul. À l'inverse, moins la crypto-monnaie est utilisée, moins elle attire des mineurs, qui préféreront consacrer leurs ressources à d'autres monnaies.

En pratique, les mineurs constituent souvent des *pools* de minage [32]. En effet, afin d'augmenter leur puissance de calcul et donc la rapidité avec laquelle ils résolvent les problèmes mathématiques qui conditionnent la validation d'un bloc, les mineurs regroupent leur capacité informatique.

À l'heure où la responsabilité sociétale et environnementale des entreprises prend une importance considérable, il paraît utile d'évoquer la dimension environnementale du minage. L'utilisation de fortes puissances de calcul pour la validation des blocs implique une consommation d'énergie gigantesque [33].

---

26. AMF, *Risques et Tendances* n° 15, juillet 2014, p. 63.
27. C. Bondard, G. Chenu, S. Dufournaud, F. Guiader, H. de Vauplane, « Blockchain – Quelques utilisations actuelles de cet outil en droit des affaires – Monnaies virtuelles, transmission des instruments de paiement, outils de financement, smart contracts, etc. », *JCP E*, n° 36, 7 septembre 2017, n° 11.
28. Cela aurait été le cas pour 97 % des transactions en 2014. V. Rapport Landau préc., p. 23.
29. Ils dépendent du volume de transactions et se seraient élevés à un montant compris entre 3 et 30 euros par transaction sur la période octobre 2017-janvier 2018. V. Rapport Landau préc., p. 23.
30. Rapport Landau préc., p. 32.
31. C. Catalini et J. Gans, « Some Simple Economics of the Blockchain », *MIT Sloan Research Paper* N° 5191-16, 21 septembre 2017, p. 9.
32. Le minage se fait désormais essentiellement avec du matériel spécialisé, plus rapide que les processeurs d'ordinateurs, composé de puces *Application Specific Integrated Circuits* (ASIC).
33. Pour un avis plus nuancé, V. « Bitcoin, une révolution monétaire ? », *Tikehau Capital CIO Letter*, mars 2018.

Quelques chiffres suffisent à illustrer ce propos : la validation d'une unique transaction en *bitcoins* implique une consommation en kilowattheures équivalente à celle d'un ménage américain pendant une semaine ; une même opération en *bitcoins* est aussi énergivore que 500 000 transactions effectuées avec une carte Visa [34]. Par ailleurs, l'énergie électrique consommée provient essentiellement de centrales au charbon localisées en Chine [35], pays qui, paradoxalement, a interdit les plateformes d'échange de *bitcoins* sur son territoire et envisagerait de prohiber également les activités de minage [36]. Les modes alternatifs de minage sont moins énergivores et exigent un investissement en matériel informatique et, partant, une rémunération des mineurs moins importants. La contrepartie sera bien évidemment un niveau de sécurité moins élevé dont il faudra vérifier s'il satisfait aux exigences des utilisateurs de crypto-monnaies, puisque le haut niveau de sécurité et l'immuabilité des opérations sont avancés comme les arguments principaux en faveur du *bitcoin*.

En Europe, l'encadrement des activités de minage n'a été envisagé que sous l'angle de sa compatibilité avec la réglementation européenne sur l'énergie. Dans une réponse au Parlement européen, la Commissaire chargée du numérique a précisé que si l'énergie consommée pour le minage était produite conformément à la réglementation, il n'y avait aucune raison de l'interdire ou même de l'encadrer [37]. Toutefois, reconnaissant l'impact des crypto-monnaies sur la consommation d'énergie, elle a indiqué que la Commission avait décidé de suivre ce sujet, ajoutant que de nouvelles applications de la *blockchain* – peut-être avait-elle à l'esprit le minage par *proof of stake* – semblent moins énergivores. De son côté, l'écosystème français de la *blockchain*, constatant que le coût de l'électricité en France est prohibitif pour le minage, plaide pour des mesures fiscales permettant d'y développer cette activité [38].

34. R. Bloch, « La phénoménale consommation d'énergie du bitcoin », *Les Échos.fr*, 11 novembre 2017.
35. *Ibid*.
36. V. par ex. F. Schaefer, « La Chine veut débrancher les « mines » à bitcoins », *Les Échos.fr*, 11 janvier 2018.
37. http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=P-2018-000559&language=EN.
38. France Digitale et Chaintech, *Toward a regulatory framework for crypto-assets*, juin 2018.

3. QUELLES SONT LES DIFFÉRENTES VARIÉTÉS DE *BLOCKCHAIN*[39] ?

Il est vraisemblable que de multiples *blockchains* se développeront dans les années à venir. Certaines seront **publiques**, c'est-à-dire ouvertes à tous, comme les *blockchains Bitcoin* ou *Ethereum*. D'autres seront **privées** ou « permissionnées » (*permissioned*), c'est-à-dire que leur accès sera réservé à certains utilisateurs pour un usage plus ou moins précis ; les règles d'accès ou de validation des opérations ou informations qui y sont enregistrées étant fixées par des règles de consensus. Certaines chaînes dites de « **consortium** » sont en fait des chaînes privées, contrôlées par quelques nœuds, même si le terme peut recouvrir des réalités variables, s'agissant notamment de l'accès aux informations de la *blockchain*[40].

L'intérêt de la chaîne privée peut consister à rendre chacun des membres responsable de son contenu, sauf si cette responsabilité est confiée à un ou plusieurs de ces membres, voire à un tiers, et d'en répartir les coûts et la propriété entre eux[41]. Dans le secteur financier, fortement réglementé, l'identification d'un responsable de la chaîne et de son contenu paraît souhaitable et le choix de chaînes privées ou de consortium s'imposera. Mais nombre de spécialistes considèrent que les véritables innovations et apports sont à attendre des chaînes publiques[42].

Pour les puristes, la réintégration dans les *blockchains* privées ou de consortium d'un tiers de confiance leur fait perdre leur raison d'être initiale. On relèvera toutefois que ces chaînes privées conservent les avantages d'authenticité, d'infalsifiabilité et de traçabilité offertes par la technologie *blockchain*.

---

39. Sur la notion de *blockchain* « privée » ou « publique », V. notamment G. Canivet, « Blockchain et régulation », *JCP E*, 7 septembre 2017, p. 1469, n° 6-7 ; rapport Landau préc., p. 80. Sur les avantages et inconvénients d'une *blockchain* privée, V. dans un cas spécifique, S. Leboucher, « Blockchain, la Banque de France entre en production », *Banque*, 30 août 2017.
40. V. par ex. la définition qui en est donnée par N. Devillier, « Jouer dans le "bac à sable" réglementaire pour réguler l'innovation disruptive : le cas de la technologie de la chaîne de blocs », *RTD Com*. 2017, p. 1037 et rapport Landau préc. Pour le rapport Landau, les *blockchains* de consortium sont « des formes hybrides de *blockchain*, entre publique et privée », p. 80.
41. V. C. Jeanneau, *op. cit*., p. 17.
42. *Ibid.*, p. 18.

4. QUELS PRINCIPES ÉCONOMIQUES SOUS-TENDENT LA *BLOCKCHAIN* ?

La théorie économique qui sous-tend la *blockchain* a été présentée dans un article remarquable de deux économistes nord-américains[43]. La *blockchain* présente l'avantage de réduire les coûts d'intermédiation ainsi que ceux d'acquisition d'un réseau.

***Blockchain* et intermédiation**. Un intermédiaire apporte de la valeur à un marché en réduisant l'asymétrie d'information entre deux parties et le risque d'aléa moral (*moral hazard*) grâce aux vérifications auxquelles il procède. Plus les marchés sont distants – ce qui implique souvent que les parties n'aient pas de relations préexistantes ou de connaissance mutuelle – et plus l'enjeu économique de la transaction considérée est important, plus le service proposé par l'intermédiaire a de la valeur pour l'une ou l'autre des parties. Pour ce qui est du prix de ce service, plus un intermédiaire est prédominant sur un marché, plus il est libre de fixer, et donc d'augmenter ce prix. Par ailleurs, les vérifications faites par l'intermédiaire impliquent que l'une ou l'autre des parties, voire les deux, ainsi que des tiers, lui communiquent des informations confidentielles, et qu'il les conserve.

Sur la *blockchain*, les intermédiaires sont remplacés par la confiance que placent les membres d'un réseau dans la chaîne de blocs et les règles de consensus qui la régissent. Le recours à un intermédiaire peut parfois rester nécessaire, mais en ce cas l'avantage reste acquis puisqu'au lieu de recourir à plusieurs intermédiaires (banque, courtier, expert, notaire, par exemple), on limitera le nombre d'intermédiaires requis. Comme l'indiquent les deux économistes, les gains en coût d'intermédiation sont importants lorsque la transaction porte sur un bien totalement dématérialisé ; ils le seront moins lorsque, au contraire, la transaction porte sur un bien physique (immeubles, métaux précieux, etc.) pour lequel l'intervention d'un intermédiaire sera toujours requise pour faire le lien entre le bien et son enregistrement sur la chaîne. Par ailleurs, le fait pour les parties de ne pas transmettre d'informations à un ou plusieurs intermédiaires permet de limiter les risques de diffusion ou d'utilisation, volontaire ou involontaire (piratage par exemple), de ces informations.

***Blockchain* et acquisition de réseau**. La *blockchain* offre aux développeurs de plateformes et de services la possibilité de se constituer un réseau ou de créer une communauté à moindre coût. Le financement de leur projet se fait souvent sous forme d'ICO, à laquelle souscrivent des investisseurs et des utilisateurs experts convaincus par l'intérêt du projet avant son lancement (*early*

43. C. Catalini et J. Gans, art. préc.

adopters). L'adoption progressive du projet par un réseau qui se développe, de plus en plus rapidement [44], est facilitée par l'absence de position dominante des acteurs qui ne sont pas en capacité de restreindre l'accès à leurs services par les utilisateurs, voire de l'interdire ou simplement même de le rendre plus difficile ou lent.

5. QUELLES SONT LES PRINCIPALES FONCTIONS DE LA *BLOCKCHAIN* ?

Bien que relativement ancienne [45], la *blockchain* n'est pas une technologie mature et ses applications pouvant avoir un réel impact sur l'économie restent pour partie inconnues à ce jour. Elle serait aujourd'hui dans une phase d'« exubérance irrationnelle », la plupart des usages qui en sont faits n'étant pas réellement disruptifs et sa maturation économique ne devant pas intervenir avant 2025 [46].

Un grand nombre de projets liés à la *blockchain* ne voient jamais le jour. Par ailleurs, une part significative d'entre eux masquent des escroqueries. On peut toutefois tenter d'identifier ce que la *blockchain* pourrait apporter à l'économie.

5.1 Transmission désintermédiée d'informations ou de valeurs

Les opérations sont réalisées de pair à pair (égal à égal ou *peer to peer*), sans généralement faire intervenir d'intermédiaire. Certaines opérations peuvent impliquer des intermédiaires [47], notamment lorsque la valeur transmise porte sur un bien corporel, mais l'esprit de la *blockchain* est de mettre utilisateurs ou consommateurs en lien les uns avec les autres. La faculté d'effectuer des opérations pair à pair n'est pas nouvelle. Toutefois, la fiabilité dans les échanges entre pairs n'est désormais plus assurée par un tiers de confiance, mais repose sur le réseau et le protocole : selon la formule célèbre de L. Lessig, « *Code is law* » [48]. Ce qui ne signifie pas, dans l'esprit de L. Lessig, qu'Internet,

---

44. Les auteurs citent le cas du *bitcoin* qui a atteint une valeur de marché d'un milliard de dollars en 4 ans, alors qu'il n'a fallu que deux ans à *l'ether* pour atteindre la même valeur. C. Catalini et J. Gans, art. préc., p. 13.
45. Institut Sapiens, étude préc., p. 25.
46. Gartner, « The irrational exuberance that is blockchain », 21 février 2018.
47. Sur l'intermédiation des tiers de confiance, V. T. Douville et T. Verbiest, « Blockchain et tiers de confiance : incompatibilité ou complémentarité ? », *D.* 2018, p. 1144.
48. L. Lessig, « Code is law – on Liberty in Cyberspace », *Harvard Magazine*, 1er janvier 2000.

ou la *blockchain*, soit une zone de non-droit, mais un espace régi par la loi du code informatique.

On peut penser que la *blockchain* facilitera certaines démarches ou opérations pour lesquelles des intermédiaires sont indispensables aujourd'hui, tels le greffe des tribunaux de commerce dans le cas de la création d'une société, l'INPI dans le cas du dépôt d'une marque ou le notaire pour une transaction immobilière par exemple.

5.2 Conservation et partage des informations

La *blockchain* permet la conservation décentralisée, et donc partagée, de données ou documents immuables, dont l'accès peut être libre ou réservé à certains usagers.

Le partage de l'information permet un gain substantiel en coûts de gestion d'un contrat ou d'une transaction : « Une opération financière est en général saisie dans 10 à 15 bases de données distinctes durant sa vie, avec les coûts d'interface, de réconciliation ou de disparité que cela implique. Une saisie unique dans un registre commun partagé entre toutes les parties prenantes d'une opération induirait immédiatement une énorme économie de temps et d'argent »[49].

5.3 Sécurisation de données ou de valeurs

Sécurité de la *blockchain*. La sécurité du dispositif, et particulièrement celle des échanges entre membres du réseau, est assurée par des outils cryptographiques offrant un chiffrement asymétrique[50] qui permet à deux parties d'échanger des données sans avoir préalablement défini entre elles les méthodes de cryptage et décryptage de leurs échanges. Par ailleurs, la vérification des opérations de la chaîne s'opère par le biais de messages encryptés assurant la fiabilité de la chaîne. L'incitation des mineurs à investir des moyens informatiques importants pour résoudre des problèmes mathématiques et ainsi garantir l'authenticité et la validité des opérations est également déterminante, apportant une réponse au problème du consensus dans les réseaux décentralisés (parfois appelé « problème des généraux byzantins »)[51].

---

49. D. Tourre, « 2017, l'année 1994 des blockchains pour la finance ? », *La Tribune*, 27 novembre 2017.
50. V. Glossaire.
51. Paris Europlace, rapport préc., p. 21 et s. ; rapport Landau préc., p. 16-17.

Le risque de défaillance du système est considérablement limité car la *blockchain* ne repose pas sur une unique infrastructure, mais sur un réseau d'infrastructures (ordinateurs connectés entre eux)[52]. La défaillance d'un ou plusieurs membres ou nœuds du réseau n'entraînera pas celle du réseau.

Jusqu'à ce jour, les seuls cas avérés d'attaques réussies contre la *blockchain* concernent des plateformes d'échange de crypto-monnaies ou des applications, et non les protocoles *blockchain* eux-mêmes. Les failles ont donc touché l'environnement de la *blockchain* et non la *blockchain* elle-même.

Authentification de la propriété d'un bien ou d'un droit[53]. La *blockchain* permet d'authentifier la propriété d'un bien ou d'un droit, rendant impossible son transfert simultané, et donc frauduleux, à deux cessionnaires (« propriété intelligente » ou *smart property*[54]) grâce à la « continuité virtuelle »[55] de la chaîne de propriété transparente et sécurisée. Elle permet de surmonter le problème de la « double dépense » dans les échanges dématérialisés : « Lorsqu'un internaute A envoie un fichier à un internaute B (…) B ne reçoit en réalité pas le fichier lui-même mais une copie. L'internaute A de son côté conserve son fichier (…). Ce problème fondamental est résolu par la *blockchain* (…). Lorsque A envoie [son bien] à B (…) A ne le possède plus »[56].

Pour certains auteurs, il est préférable de parler de certification plutôt que d'authentification, qui supposerait la vérification de la validité et de l'efficacité d'un acte. Il s'agit en particulier de préserver le rôle et les attributs du notaire, en raison de la délégation de puissance publique qui lui est conférée et des vérifications auxquelles il peut procéder et qui sont absentes des protocoles *blockchain*[57]. Un exemple des limites de l'authentification permise par la *blockchain* : conformément à l'article 712 du Code civil, la propriété d'un bien peut, dans certaines hypothèses, s'acquérir par prescription. Seule une vérification de l'absence de possession effective du bien par un tiers pendant une certaine durée permettra de confirmer qu'un titre opère bien transfert de propriété. On notera enfin que l'effet rétroactif de la prescription acquisitive – le possesseur sera considéré comme propriétaire à compter du premier jour de possession – paraît peu compatible avec l'immuabilité de la *blockchain*[58]. Dans ce cas précis, le recours à un tiers de confiance sera toujours nécessaire.

---

52. W. Mougayar, *op. cit.*, p. 71 ; C. Jeanneau, *op. cit.*, p. 15-16.
53. Dans le cas d'un diplôme par ex., V. T. Coeffé, « Le MIT utilise la blockchain pour certifier les diplômes obtenus par les étudiants », www.blogdumoderateur.com, 12 mars 2018.
54. W. Mougayar, *op. cit.*, p. 64-65.
55. V. Medef et Boston Consulting Group, étude préc., p. 21.
56. V. C. Jeanneau, *op. cit.*, p. 12.
57. Open Law, Coala, Ecan, *Smart contracts : études de cas et réflexions juridiques*, p. 27-28, https://ecan.fr/Smart-Contracts-Etudes.pdf.
58. *Ibid.*

En matière d'authenticité ou de propriété d'un bien, l'assurance offerte par la *blockchain* sera maximale si le bien est immatériel (et donc « numérisable ») et plus faible s'il est matériel puisque les services d'un ou plusieurs tiers de confiance seront requis pour vérifier que le titre ou l'empreinte numérique est effectivement celle du bien considéré [59].

5.4 Automatisation de certaines tâches : les *smart contracts*

La *blockchain* permet la mise en place de programmes informatiques dénommés « contrats intelligents » (*smart contracts*) ou « contrats déterministes », dont les éléments s'exécutent automatiquement si certaines conditions objectivement constatées sont remplies.

59. Sur cette problématique du « last mile », V. C. Tucker et C. Catalini, « What blockchain can't do », *HBR*, 28 juin 2018 ; J. Gossa, art. préc.