Promesses et (dés)illusions : une introduction technocritique aux blockchains

Pablo Rauzy

Promesses et (dés)illusions : une introduction technocritique aux *blockchains*

Pablo RAUZY[1,2]
pr@up8.edu
[1] LIASD (Laboratoire d'Intelligence Artificielle et Sémantique des Données)
[2] Centre GÉODE (Géopolitique de la Datasphère)
Université Paris 8

Résumé :

« *Une blockchain est un registre distribué et immuable dans lequel sont écrites des informations qui font consensus.* ». Dans cet article, nous commencerons par donner du sens à cette phrase et à l'ensemble des termes qui y sont employés, en nous efforçant quand c'est nécessaire de rendre accessibles les notions informatiques (comme la décentralisation, la distribution, l'immuabilité, ou le consensus) et le fonctionnement technique des outils cryptographiques sous-jacents (comme les condensats, les signatures, ou la preuve de travail ou d'enjeu). L'objectif de cette introduction sera d'atteindre une compréhension réelle de ce qu'est une *blockchain*.
Ainsi équipés, nous discuterons ensuite de ce que les *blockchains* permettent effectivement d'accomplir, et donc surtout ce qu'elles ne permettent pas. Nous questionnerons alors les utilisations qui en sont proposées en nous concentrant sur des cas d'usage typiques des *blockchains* que nous étudierons plus en détails : les « cryptomonnaies » bien sûr, la certification de documents (avec l'exemple des diplômes), et nous mentionnerons également le cas des NFT. Cela nous permettra en conclusion de questionner de manière générale le caractère d'« innovation de rupture » que l'on associe souvent à cette technologie.

1. Introduction

« *Blockchains* : quels enjeux de sécurité, juridiques, économiques, et énergétiques ? », voilà le titre de l'appel à articles en vue de constituer ce numéro spécial de la revue *Terminal*. Les *blockchains* étant depuis quelques années de plus en plus présentes dans de très nombreux secteurs d'activité, la question des enjeux liés à cette technologie sur les quatre axes énumérés ici est en effet capital.

Cependant, avant de s'intéresser à ces enjeux, il semble essentiel de commencer par comprendre ce qu'est concrètement une *blockchain* ainsi que son fonctionnement, afin d'en saisir pleinement les possibilités mais surtout, les limites. Les nombreux usages qui en sont faits sont-ils justifiés ? Ont-ils seulement un sens ? Qu'en est-il dans les faits des promesses de sécurité, de décentralisation, et de désintermédiation presque systématiquement associées aux projets basés sur une *blockchain* ?

C'est notamment à ces questions que nous répondrons dans cet article, qui se veut, dans son ensemble, une sorte d'introduction aux enjeux techniques dont traite ce volume. Dans cette optique,

nous commencerons par définir et expliquer ce qu'est une *blockchain*, ainsi que son fonctionnement, en nous efforçant de ne faire appel à aucun pré-requis technique. Ensuite, nous étudierons plus précisément trois cas d'usage typiques qui nous permettront d'affiner notre compréhension de la nature et des limites des *blockchains*. Enfin, en regard de ce que nous aurons expliqué jusque là, nous questionnerons en conclusion le caractère d'« innovation de rupture » que l'on associe souvent à cette technologie.

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

On peut définir une *blockchain* comme « *un registre **distribué** et **immuable** dans lequel sont écrites des informations qui font **consensus*** » de façon plutôt exacte, mais ça n'aide probablement pas beaucoup ceux et celles qui ne savent pas déjà vraiment ce qu'est une *blockchain*, tant les termes utilisés (en gras) dans cette description sont techniques[1]. Commençons donc par les définir.

« Distribué » veut dire que chaque pair[2] dispose d'une copie complète du registre, de façon à pouvoir le consulter ou le partager sans dépendre de quiconque. Ce terme est souvent confondu avec « décentralisé » ou « pair-à-pair », bien qu'il n'ait pas du tout le même sens.

Dans un réseau complètement *décentralisé* / pair-à-pair, deux pairs peuvent échanger des informations sans qu'aucun autre n'ait même besoin d'être au courant de l'existence de l'échange. C'est le cas lors d'une transaction monétaire en argent liquide. Ce pourrait théoriquement être le cas pour le courrier électronique si chaque personne auto-hébergeait son propre serveur de courriels.

Au contraire, dans un réseau *centralisé*, tout échange d'informations passe par un unique centre qui a donc une connaissance parfaite du réseau et des échanges qui y ont lieu. C'est ce qui se passe pour des transactions monétaires d'un compte PayPal à un autre. C'est aussi comme ça que fonctionnent les échanges de messages sur une plateforme comme Facebook.

Un réseau n'est pas nécessairement complètement centralisé ou décentralisé ; entre les deux, il existe des réseaux dits *fédérés*, qui se comportent comme plusieurs réseaux centralisés dont les centres peuvent communiquer entre eux pour faire le lien entre les pairs qui ne sont pas connectés au même « centre ». Pour ce qui est des transactions monétaires, on peut penser aux virements bancaires SEPA qui peuvent s'effectuer entre deux comptes rattachés à des établissements bancaires distincts. C'est aussi comme ça que fonctionnent en pratique le courrier électronique : l'ensemble des serveurs sont interopérables grâce à l'utilisation de protocoles ouverts, et cela permet aux

1 Notez que le mot « registre » n'est pas en gras : il s'agit ici d'une version numérique du sens commun de ce mot : « livre où l'on inscrit des faits », et non de jargon informatique. Vous pouvez simplement penser à un fichier.

2 On appel « pair » un participant au réseau.

utilisateurs de Gmail d'échanger avec ceux de Yahoo comme avec ceux de n'importe quelle entreprise, université, ou particulier qui choisirait d'auto-héberger ses courriels.

Sur une *blockchain*, une transaction en « cryptomonnaie » consiste en un jeu d'écriture comptable (qui dans le cas le plus simple a pour effet de diminuer le montant associé à un compte sur cette *blockchain* d'autant qu'on augmente le montant associé à un autre compte sur cette même *blockchain*) dans le registre distribué, qui joue du coup le rôle de centre. Il s'agit donc bien d'un réseau de type centralisé[3], mais dont le centre est distribué sur l'ensemble des pairs, qui, comme dans un réseau centralisé classique, disposent de l'ensemble des informations qui passent sur le réseau. La différence est dans la répartition de l'autorité, qui est entièrement détenue par l'acteur central dans un réseau centralisé classique, mais qui dans le cas d'une *blockchain* réside dans les deux notions complexes d'*immuabilité* et de *consensus*.

« Immuable » veut dire que ce qui est écrit dans le registre l'est définitivement, de sorte à pouvoir faire confiance pour toujours à ce qu'on y lit. En pratique, le registre n'existe que sous la forme d'un fichier présent sur les machines des pairs qui participent au réseau, et il est techniquement impossible d'empêcher un pair de modifier sa version locale du fichier. L'immuabilité n'existe donc que virtuellement : il s'agit en fait de rendre impossible une modification *discrète* du registre, au sens où n'importe qui peut facilement vérifier son intégrité. Cette vérification est permise par la structure de chaîne et l'utilisation de *condensats cryptographiques*.

Un *condensat cryptographique* est une empreinte numérique qui doit pouvoir servir à identifier des données. C'est en pratique un grand nombre de taille fixe (par exemple 256 bits) calculé par un algorithme déterministe[4] conçu de façon à ce que le moindre changement dans les données d'entrée (ne serait-ce qu'un bit) provoque une modification importante de la sortie (chaque bit de la sortie a 50 % de chance de changer).

> Par exemple avec l'algorithme SHA-256 (NIST, 2002) le texte « Terminal », encodé en ASCII, a pour condensat le nombre suivant (il est écrit sur 64 chiffres, en hexadécimal[5]) :
> `e0926fdac700b09497b5f0218ea3dd54fa13c0bdeaee6caa7b85e50b852aa05f`.
> Tandis que le texte « terminal » qui, encodé en ASCII également, ne diffère du précédent que d'un seul bit (le « T » majuscule est encodé par l'octet « `01`**`1`**`10100` », tandis que le « t » minuscule l'est par l'octet « `01`**`0`**`10100` »), a pour condensat le nombre suivant :
> `4e686af7bdcc5ae005a247624fd8c7283257c2514f6b3ad2ff5d4cb6d95196e6`.

3 Notamment, il n'est pas possible d'effectuer une transaction d'une *blockchain* à une autre.
4 C'est-à-dire qu'avec les mêmes données en entrée de l'algorithme, on aura toujours le même nombre en sortie.
5 En base 16, où les chiffres de `0` à `9` puis de `a` à `f` représentent les nombres de 0 à 15, c'est-à-dire exactement 4 bits chacun, de `0000` à `1111`.

Il est donc très facile de vérifier, quand on dispose du condensat associé à des données, si celles-ci sont intègres. Dans une chaîne de blocs, chaque bloc est identifié par son condensat, et un ordinateur personnel peut vérifier l'intégrité de plusieurs millions de blocs par seconde. Mais ce qui fait réellement l'immuabilité d'une chaîne de blocs est justement la structure chaînée. L'idée est que chaque bloc contient parmi ses données l'identifiant du bloc précédent dans la chaîne, de sorte à ce que la modification d'un bloc entraîne, en plus de celle de son identifiant, celle de tous les blocs suivants et de leurs identifiants, par réaction en chaîne. La suppression ou l'ajout d'un bloc quelque part dans la chaîne pose le même problème. La seule façon de modifier un bloc de manière discrète, de façon à ce que la nouvelle version de la chaîne soit perçue comme valide pour l'ensemble des pairs, serait de trouver une *collision* dans l'algorithme de calcul de condensat, ce qui est possible en théorie, mais est censé être complètement impossible en pratique.

On appelle « collision » le fait que deux données différentes se retrouvent avec le même condensat. Il y a nécessairement des collisions existantes, puisqu'il y a un nombre fini de condensats possibles (par exemple, sur 256 bits, on ne peut écrire « que » les nombres de 0 à $2^{256} - 1$) qui est bien inférieur à la taille de l'ensemble des données qu'on peut passer en entrée de l'algorithme[6]. Mais trouver une collision sur l'identifiant précis d'un bloc, entre sa version originale et une nouvelle version contenant les modifications qui nous arrangent (faire disparaître une dépense, par exemple), demande des ressources dont il est impossible de disposer en pratique, tant en terme de temps qu'en terme de puissance de calcul : même avec toute la puissance de calcul disponible sur Terre, il faudrait bien plus de temps que l'âge de la planète pour y arriver — à moins de trouver une faille dans l'algorithme bien sûr.

C'est bien l'utilisation de condensats cryptographiques et de la structure de chaîne qui fait l'immuabilité d'une *blockchain*, et rien d'autre (notamment pas la *preuve de travail* comme on peut régulièrement l'entendre). Cette technique d'immuabilité est utilisée dans d'autres technologies et l'était déjà avant l'invention des *blockchains* : il s'agit d'un cas particulier d'utilisation d'*arbres de Merkle* (Merkle, 1987). Cela ne suffit donc pas à caractériser ce qu'est une *blockchain*, et l'ingrédient manquant est la notion de *consensus*.

« Consensus » est ici une notion technique, qui n'a rien à voir avec la définition du mot « consensus » du langage courant, dans lequel sa définition est « accord et le consentement du plus grand nombre, de l'opinion publique »[7]. On atteint le consensus quand l'ensemble des participants

6 C'est le principe mathématique des « tiroirs à chaussettes » : si on range C chaussettes dans T tiroirs avec C > T, alors nécessairement il y aura au moins un tiroir (condensat) qui contiendra plusieurs chaussettes (donnée).

7 Dictionnaire Français en ligne, Larousse https://www.larousse.fr/dictionnaires/francais/consensus/18357 (consulté en juin 2022).

sont d'accord, ou, dans une version plus faible, quand aucun désaccord n'est exprimé. On parle ici d'accords et de désaccords au sens politique, d'une volonté des participants. En informatique, le *problème du consensus* consiste à mettre d'accord un ensemble de machines sur une valeur unique. Il n'est plus question ici de choix politique ou de consentement d'ordre moral. Le consensus est atteint quand toutes les machines (non défaillantes) tombent d'accord sur une valeur, quelle que soit cette valeur, du moment qu'elle a été proposée par au moins une des machines (donc pas forcément par la majorité). Dans le cas d'un système centralisé, une machine faisant autorité peut simplement imposer une valeur aux autres en la leur transmettant. Dans les systèmes distribués, non seulement ceci n'est plus possible, mais en plus certaines machines participant à l'établissement du consensus peuvent être défaillantes (par panne ou par malice). Dans le cas particulier des *blockchains*, cela va même plus loin puisque non seulement l'ensemble des machines n'est pas connu et peut varier, mais en plus chaque machine est considérée comme a priori suspecte[8].

L'objectif dans le cas d'une *blockchain* est de se mettre d'accord sur le prochain bloc à ajouter à la chaîne (c'est-à-dire sur les nouvelles informations à écrire dans le registre), et il est nécessaire que la valeur choisie (le nouveau bloc) soit acceptée par l'ensemble des participants. Une façon d'atteindre ce but pourrait être de récompenser systématiquement tous les participants et d'honorer toutes les demandes d'ajouts légitimes au registre dans le nouveau bloc, mais cela est impossible pour de multiples raisons : on ne connaît pas la liste complète des participants, la taille des blocs est limitée, et récompenser tout le monde systématiquement avantagerait sensiblement les plus anciens participants et donc découragerait l'arrivée de nouveaux. Pour les mêmes raisons, ça ne peut pas être « chacun son tour » non plus. En fait, les contraintes qui s'imposent dans le cas d'une *blockchain* font que la seule façon de trouver une valeur qui ne soit pas contestable est de tirer au sort l'une des propositions. Bien sûr, le tirage au sort ne peut être effectué par une entité particulière (que ce soit une tierce partie ou un participant) : cela nécessiterait de lui faire confiance et elle deviendrait donc une autorité centrale. C'est là que le concept de *preuve de travail* entre en jeu.

La *preuve de travail* est une invention du début des années 90 dont l'objectif était initialement de lutter contre le spam (Dwork et Naor, 1992). L'idée est de rendre prohibitif le coût de l'envoi massif de courriels en demandant à la machine qui envoie les courriels de réaliser du calcul inutile par ailleurs pour chaque message. Dans l'implémentation Hashcash (Back, 1997) de cette idée par exemple (qui est celle reprise avec quelques modifications dans Bitcoin), le protocole demande à l'expéditeur de calculer en boucle le condensat cryptographique de données du message à envoyer (date d'expédition et adresse du destinataire) agrémentées d'un nombre à modifier à chaque fois

8 On verra plus tard que c'est inhérent à la philosophie de la compétition généralisée qui sous-tend les *blockchains*.

(généralement en l'incrémentant) jusqu'à trouver une *collision partielle*, typiquement, que les 20 premiers bits du condensat soient à zéro (ce qui nécessitera donc environ 2^{20} calculs de condensat, c'est-à-dire approximativement une seconde de calcul sur un ordinateur personnel[9]). L'expéditeur doit alors envoyer au destinataire (dans les métadonnées du courriel) le nombre qui a permis de trouver la collision partielle comme *preuve* de son travail de calculs inutiles. Le destinataire peut alors facilement vérifier la preuve, il lui suffit de calculer le condensat avec ce nombre pour voir si les 20 premiers bits sont bien à zéro.

> Si on reprend notre exemple précédent avec le texte « Terminal » et qu'on lui ajoute un nombre, en commençant avec « Terminal0 », il faut aller jusqu'à « Terminal1277191 » pour trouver un condensat (toujours avec SHA-256) qui satisfasse la collision partielle. Cela a donc demandé plus d'un million de tentatives. En revanche, si on nous fournit le nombre 1277191 comme preuve de travail, on peut directement calculer le condensat de « Terminal1277191 », qui se trouve être : `0000061c3401962f21905bec7299328d495d1b10846ac6cf699be03e96497a8f`, pour observer que les 20 premiers bits (et donc les 5 premiers chiffres hexadécimaux) sont bien à zéro, en n'ayant eu à effectuer qu'un seul calcul de condensat.

Dans les *blockchains* qui utilisent ce mécanisme de consensus, la preuve de travail consiste à chercher une collision partielle sur le condensat qui servira d'identité au bloc que l'on souhaite ajouter à la chaîne. C'est cela qu'on appelle le *minage*. En plus de l'identifiant du dernier bloc (pour la structure de chaîne comme on l'a vu plus haut) et des informations que son mineur souhaite ajouter au registre, chaque bloc contient donc un nombre, qu'on appelle un *nonce*[10], qui ne sert qu'à être modifié en boucle jusqu'à tomber sur un condensat valide, c'est-à-dire qui a une collision partielle avec le nombre de zéros voulu au début (nombre qui varie en fonction de la difficulté de minage décidé pour la *blockchain* en question). L'identifiant du dernier bloc est le même pour tout le monde, mais pas forcément[11] les informations que l'on souhaite ajouter sur la chaîne, et c'est ce qui fait que malgré la puissance de calcul (qui joue tout de même un rôle prépondérant), on ne peut pas prédire à l'avance qui va trouver un bloc valide en premier et le transmettre au reste des machines participant au réseau pour vérification, puis ajout à la chaîne (et du coup, abandon de leurs calculs en cours, pour recommencer à zéro à partir de ce nouveau bloc).

> Par exemple, si on avait choisi le texte « terminal » (sans la majuscule) comme donnée initiale dans l'exemple précédent, il aurait suffit d'aller jusqu'à « terminal296762 » pour trouver un condensat valide : `000007085de78efeec7e3e9f120ca34fadfb782f5b386fa63989d5ddbd86269d`, soit près d'un million de calculs de condensat à faire en moins, pour, rappelons-le, un seul bit de différence.

9 Cela peut paraître très peu, voire presque transparent, et ça l'est quand on a un usage légitime du courriel. Mais pour envoyer plusieurs centaines de milliers de courriels comme le font les spammeurs, même une seconde par envoi devient vite prohibitif.

10 Le mot anglais « *nonce* » vient de la contraction de « *number* » et de « *once* ».

11 En fait, ce n'est jamais le cas, comme on le verra plus bas.

C’est ainsi qu’est effectué le tirage au sort non contestable qui sert de mécanisme de consensus pour mettre tout le monde d’accord sur quel sera le prochain bloc dans la chaîne, et donc, les nouvelles informations ajoutées au registre. Il n’est pas impossible que deux blocs valides différents soient trouvés de cette façon presque simultanément[12]. Dans ce cas, chaque mineur choisit, en fonction de ses propres intérêts, à partir duquel il souhaite poursuivre. Si plusieurs versions de la chaîne évoluent ainsi en parallèle, celle qui fait foi est la plus grande (celle qui a le plus de blocs), et les informations contenues uniquement dans les autres n’existent plus dans le registre.

Bien sûr, il est nécessaire qu’il existe une incitation à miner, car le coût de faire ces calculs inutiles par ailleurs se révèle vite très élevé, notamment en terme de consommation d’énergie[13]. Le mineur qui trouve le nouveau bloc doit donc être récompensé. Comme pour le tirage au sort, il n’est pas possible que cette récompense soit distribuée par une entité particulière : cela nécessiterait de lui faire confiance et elle deviendrait alors une autorité centrale. Il est donc impératif que la récompense provienne intrinsèquement de la *blockchain* elle-même. C’est là qu’entrent en jeu les « cryptomonnaies », comme nous le verrons plus bas.

Par souci d’exhaustivité, mentionnons également un autre mécanisme de consensus, la *preuve d’enjeu*. Contrairement à la preuve de travail, la preuve d’enjeu ne nécessite pas de calculs inutiles, elle met en place un tirage au sort pondéré par l’*enjeu* de chaque participant dans la *blockchain*, avec l’idée que plus on a d’enjeu dans une *blockchain*, plus on a envie que celle-ci soit digne de confiance, et donc moins on a intérêt à tricher. L’enjeu est directement lié au montant de « cryptomonnaie » détenu et au temps depuis lequel celui-ci l’est[14]. Ces informations étant détenues par l’ensemble des pairs, le résultat du tirage au sort ne doit pas les surprendre. Ce mécanisme de consensus est moins sûr que la preuve de travail, notamment car il n’impose pas naturellement aux mineurs de ne choisir qu’un seul bloc pour poursuivre la chaîne. Dans le cas de la preuve de travail, faire coexister plusieurs blocs nécessite de diviser sa puissance de calcul entre ceux-ci, et donc de diminuer ses chances de miner le prochain bloc et de recevoir la récompense associée. En revanche, la preuve d’enjeu permet sans surcoût des attaques où l’on fait coexister plusieurs versions du registre en parallèle, par exemple l’une où l’on a bien payé un tiers, et l’autre où l’on dispose encore

12 En tout cas, dans un laps de temps ne permettant pas au premier des deux de s’être propagé à l’ensemble du réseau avant que le second ne soit trouvé et commence à être transmis également.

13 À l’heure où ces lignes sont rédigées, la collision partielle demandée pour la *blockchain* de Bitcoin est de 76 bits à zéro. Pour donner un ordre de grandeur, il faudrait en moyenne de l’ordre du milliard d’années de calcul à un ordinateur personnel pour trouver seul une telle collision. Mais bien sûr ce n’est ni sur une seule ni sur ce type de machine que le minage est fait (les mineurs utilisent aujourd’hui essentiellement du matériel spécifique).

14 Dans la « cryptomonnaie » Peercoin par exemple, les participants ne peuvent miser que la « cryptomonnaie » qu’ils possèdent depuis plus de 30 jours. Sera sélectionné celui dont la mise multipliée par son temps de détention est la plus grande (avec une prise en compte de maximum 90 jours). Le temps de détention est remis à zéro pour la « cryptomonnaie » misée du participant qui l’emporte, et ce dernier ne peut plus être sélectionné pour 30 jours.

des mêmes fonds, pour en payer un autre — c'est ce qu'on appelle la *double dépense*. Plusieurs méthodes pour résoudre ce problème ont été proposées, mais aucune n'arrive au niveau de sécurité de la preuve de travail sans en atteindre le coût. Quoi qu'il en soit, il est aussi nécessaire de récompenser le mineur tiré au sort dans la preuve d'enjeu, sinon il n'y a pas d'incitation à subir l'inconvénient de devoir stocker sa « cryptomonnaie » sans pouvoir y toucher. Comme pour la preuve de travail, et pour les mêmes raisons, cette récompense doit nécessairement provenir intrinsèquement de la *blockchain* elle-même.

Les mécanismes de « consensus » utilisés dans les *blockchains* impliquent donc que chaque mineur propose un bloc différent de ceux des autres, puisque chacun tente de s'auto-attribuer la récompense qui va avec le bloc[15]. On remarque donc que le « consensus » dont il est question ici n'a absolument rien à voir avec celui du langage courant, et ne pourrait d'ailleurs pas en être plus éloigné : ce n'est pas seulement que la valeur de consensus n'était pas voulue par une majorité des participants, mais bien que c'est systématiquement la volonté d'un seul, contre celles de tous les autres, qui est sélectionnée comme valeur de consensus, et qui s'impose à tout le monde.

À présent, la définition que l'on a donnée d'une *blockchain* en début d'article devrait être effectivement compréhensible. Il reste tout de même deux points essentiels à la compréhension non pas de la nature mais du fonctionnement d'une *blockchain* : les aspects réseaux techniques, et la « cryptomonnaie ». Nous mettrons de côté les aspects réseaux techniques (c'est-à-dire le fonctionnement du protocole pair-à-pair utilisé pour la transmission des transactions, des blocs, etc. entre les participants), qui, d'une part, nécessiteraient un article à eux seuls pour réellement expliquer leur fonctionnement sans trop de pré-requis, et, d'autre part, n'ont pas vraiment d'impact sur ce qui nous intéresse ici, à savoir discerner les limites de ce que peut faire et ce que ne peut pas faire une *blockchain*. Ce qu'il faut retenir, c'est : que les usagers de la *blockchain* peuvent envoyer des *transactions* (c'est-à-dire des informations à ajouter dans le registre pour modifier l'état de la *blockchain*) sur le réseau en espérant qu'elles seront ajoutées par des mineurs dans l'un des prochains blocs qui seront ajoutés à la chaîne ; et que les *blocs* valides trouvés par les mineurs sont transmis à l'ensemble des participants pour vérification (de la validité des transactions et de la preuve de travail) puis ajout à la chaîne.

En revanche, comme on l'a vu plus haut, il est impossible de comprendre le fonctionnement d'une *blockchain* sans comprendre celui des « cryptomonnaies ». En effet, les mécanismes de consensus utilisés par les *blockchains* nécessitent de récompenser les mineurs qui trouvent de nouveaux blocs,

15 Un montant de « cryptomonnaie » défini par le protocole, et qui sera vérifié par les autres participants avant l'ajout du bloc à la chaîne. Voir plus bas le paragraphe « Récompense » dans la section sur les « cryptomonnaies ».

et, la récompense devant nécessairement provenir intrinsèquement de la *blockchain*, elle ne peut qu'être un montant de la « cryptomonnaie » associée à la *blockchain*, qui fait donc partie intégrante de son fonctionnement.

3. Étude de quelques cas d'usage typiques

3.1. Les « cryptomonnaies »

On appelle « cryptomonnaie » un actif financier numérique échangeable de pair à pair sans nécessiter d'autorité centrale. Dans ce mot, « crypto » fait référence à la cryptographie, qui est utilisée pour assurer le bon fonctionnement et la sécurité des « cryptomonnaies » ; « monnaie », quant à lui, fait directement référence à leur nature proclamée, mais bien discutable, comme le souligne la Banque de France (2018). Le concept de « cryptomonnaie » existe depuis le début des années 80 (Chaum, 1982), mais c'est vraiment en 2008 que la version actuelle voit le jour avec l'arrivée de *Bitcoin* (Nakamoto, 2008), et c'est d'ailleurs pour Bitcoin que la technologie de la *blockchain* a été mise au point. Depuis, de très nombreuses autres « cryptomonnaies » ont vu le jour, parfois avec certaines différences ou innovations, mais c'est sur l'exemple de Bitcoin, qui reste de loin la plus répandue, que se base cette première étude de cas.

3.1.1. Fonctionnement

Transaction. Pour comprendre le fonctionnement d'une « cryptomonnaie » on peut partir de celui d'une transaction. Chaque transaction a un identifiant (un condensat des données qui la composent), et est composée d'un ensemble d'entrées (les sources) et d'un ensemble de sorties (les cibles). Les sorties sont des paires associant chacune un des destinataires de la transaction et le montant qui lui est destiné. Les entrées sont des paires associant chacune une sortie de transaction passée (identifiée elle-même par une paire composée de l'identifiant de la transaction passée en question et du numéro de la sortie en question dans cette transaction) et une signature cryptographique prouvant l'autorisation de la dépense. Pour être valide, une transaction doit respecter plusieurs contraintes :

1. la somme des montants (qui doivent tous être positifs) dans l'ensemble des sorties doit être inférieure ou égal à celle dans l'ensemble des entrées (si elle est inférieure, le mineur qui permet l'ajout du bloc contenant cette transaction peut récupérer le surplus) ;
2. aucune des sorties de transactions listées en entrée ne doit avoir déjà été dépensée dans un bloc précédent, ni ailleurs dans le même bloc ;
3. et bien sûr, chaque signature cryptographique doit être valide.

Avant d'expliquer ce que veut dire « signature valide » puis de donner un exemple concret de transaction, remarquons que la seconde contrainte impose, pour pouvoir vérifier la validité d'une transaction, de connaître la liste des sorties de transactions non encore dépensées (UTXO, pour « *unspent transaction outputs* »). Cela nécessite de maintenir cette liste à jour, sans quoi il faudrait reparcourir l'ensemble de la chaîne (au mieux, si on a cette information, depuis le bloc contenant la plus ancienne UTXO listée en entrée de la transaction), ce qui serait bien trop long. Nous reviendrons sur ce fait et ce qu'il implique dans le cas d'usage que nous étudierons ensuite (la certification de documents).

Signature. Pour comprendre ce qu'est une signature cryptographique, il nous faut d'abord introduire rapidement le concept de *cryptographie asymétrique*, qui date des années 70. Jusqu'alors, on ne disposait que de la cryptographique qu'on appelle aujourd'hui « symétrique », c'est-à-dire qui utilise la même *clef secrète* pour le chiffrement et le déchiffrement. Cela posait un problème de poule et d'œuf dans la distribution de la clef : deux parties ne peuvent communiquer via un canal sécurisé que si elles possèdent cette information commune, mais ne disposent donc pas avant ça d'un moyen sécurisé de se la transmettre. Sans entrer dans les détails historiques[16], l'invention de la cryptographie asymétrique, qui vient répondre à cette problématique, peut-être attribuée à Diffie et Hellman (1976) pour l'idée, et à Rivest, Shamir, et Adleman (1978) pour la première mise en œuvre pratique. L'idée est que chaque partie dispose d'une paire de clefs : une *clef publique* qui peut être distribuée à tout le monde, et une *clef privée* qui doit être gardée absolument secrète[17]. Ces deux clefs sont mathématiquement liées de sorte qu'une donnée chiffrée avec une clef ne puisse être déchiffrée qu'avec l'autre clef de la même paire. Cela permet d'assurer la confidentialité des messages adressés à un destinataire en ne connaissant que sa clef publique : par exemple, si Alice chiffre un message avec la clef publique de Bob, elle a la garantie que seul Bob pourra le lire puique sa clef privée est nécessaire pour déchiffrer le message[18]. Mais cela permet également (en plus ou par ailleurs) d'assurer l'intégrité et l'authenticité des messages : en calculant un condensat de son message puis en le chiffrant avec sa clef privée, Alice obtient ce qu'on appelle une *signature cryptographique*. En joignant la signature à son message, elle permet à Bob de vérifier que le message n'a pas été altéré (intégrité) et qu'il a bien été envoyé par Alice (authenticité). Il suffit pour cela qu'il calcule le condensat du message qu'il a reçu, et qu'il vérifie qu'en déchiffrant la signature avec la clef publique d'Alice, il obtient bien la même valeur. Si la clef publique d'Alice a bien

16 Cela nécessiterait de nombreuses circonvolutions, impliquant entre autres des militaires états-uniens et le GCHQ, sur les chronologies distinctes des inventions et de leurs publications.
17 C'est-à-dire n'être divulguée à personne, et donc pas même aux tiers avec qui l'on souhaite communiquer.
18 Sauf bien sûr si Bob n'a pas soigneusement protégé sa clef privée et que celle-ci a fuité.

permis le déchiffrement correct de la signature, on a la preuve qu'Alice est l'expéditrice puisque sa clef privée a été nécessaire à la production de la signature.

Voilà ce qu'on appelle une signature valide dans le cas des transactions sur une *blockchain* : une preuve que le détenteur de la « cryptomonnaie » associée à une UTXO autorise sa dépense en ayant signé cryptographiquement cette partie de la transaction avec la clef privée qui correspond à l'identifiant du destinataire de l'UTXO, qui est justement identifié par sa clef publique.

> **Exemple concret de transaction.** Dans le passé, Alice a reçu 10 BTC auxquels elle n'a pas encore touché : il existe une sortie de transaction non dépensée (UTXO) qui associe le montant 10 BTC à la clef publique d'Alice. Alice veut maintenant payer 7 BTC à Bob. Elle va créer une transaction qui a pour entrée son UTXO de 10 BTC signée cryptographiquement par ses soins, et deux sorties : la première associe 7 BTC à la clef publique de Bob, la seconde les 3 BTC restant à sa propre clef publique (son « rendu monnaie »). Alice envoie cette transaction sur le réseau en espérant qu'elle soit prise en compte dans l'un des prochains blocs qui sera miné[19]. Dès que ce sera le cas, Alice disposera d'une UTXO de 3 BTC, et Bob d'une UTXO de 7 BTC. La sortie de transaction qui associait le montant 10 BTC à la clef publique d'Alice a maintenant été dépensée : ce n'est plus une UTXO.
> Si Alice n'avait jamais reçu plus de 7 BTC d'un coup, mais par exemple plusieurs fois 5 BTC, elle aurait pu de façon équivalente utiliser deux UTXO de 5 BTC comme entrées de la transaction.

Récompense. Exception aux règles que nous venons d'énoncer, la première transaction de chaque bloc n'a pas d'entrée, et, s'il n'y a pas d'obligation spécifique concernant ses sorties, elle sert en pratique systématiquement d'auto-récompense pour le mineur qui a trouvé le bloc. Les règles pour cette transaction particulière sont donc différentes. La sommes des montants des sorties de cette transaction ne doit pas dépasser celle de la récompense et des frais de transactions. La récompense provient de la « *coinbase* » : il s'agit de « cryptomonnaie » nouvellement créée, et son montant est défini par le protocole de la *blockchain*. Pour Bitcoin, il a démarré à 50 BTC le 9 janvier 2009 dans le premier bloc miné, et est divisé par deux tous les 210 000 blocs[20], jusqu'à ce qu'il atteigne zéro quand un peu moins de 21 millions de bitcoins auront été distribués de cette façon[21] — il ne restera alors plus que les frais de transaction comme incitation au minage. Les frais de transactions sont récupérés sur les transactions dont la somme des montants associés aux entrées est supérieure à celle des sorties. Soumettre au réseau une transaction qui permet aux mineurs d'espérer récupérer des frais élevés est donc une façon de s'assurer qu'elle sera prise en compte, éventuellement même plus rapidement que les autres. Enfin, dernière règle particulière, les sorties de cette transaction ne

19 Alice peut encourager la prise en compte de sa transaction en se rendant moins de 3 BTC pour offrir le reste en frais de transaction, comme on va le voir dans le paragraphe « Récompense » qui suit immédiatement cet exemple.

20 Soit environ tous les 4 ans, car le protocole de Bitcoin adapte la difficulté du minage — c'est-à-dire la taille de la collision partielle à trouver — à la puissance de calcul disponible sur le réseaux de sorte à ce qu'un bloc soit trouvé approximativement toutes les 10 minutes.

21 Ce qui correspond à une décision arbitraire du ou des créateurs de Bitcoin, et qui est codé en dur dans le protocole.

deviennent des UTXO utilisables que 100 blocs plus tard, pour s'assurer qu'elles ne disparaîtront pas en cas de coexistences temporaires de plusieurs versions parallèles de la *blockchain*[22].

3.1.2. Remarques

Le fonctionnement global d'une « cryptomonnaie » en tête, on peut déjà faire plusieurs remarques.

Usabilité et démocratie. La première concerne l'usabilité de cette technologie. Pour en être réellement maître, il est nécessaire de comprendre et de s'approprier de nombreux concepts du domaine de la cryptographie, ainsi que les bonnes pratiques qui en découlent et ne sont pas du tout évidentes à mettre en œuvre : typiquement, la gestion de ses clefs privées. Si elles ne sont pas correctement sécurisées et qu'un tiers malveillant s'en empare, on peut se faire voler sa « cryptomonnaie ». On peut également perdre définitivement l'accès à sa « cryptomonnaie » simplement en perdant la clef privée associée[23]. Dans les deux cas, il n'existe aucun moyen de récupérer la valeur perdue. En pratique, une grande partie des utilisateurs de « cryptomonnaie » le font via des plateformes qui hébergent leur « portefeuille » (y compris les clefs privées), et ce sont donc en vérité ces plateformes qui détiennent le contrôle de la « cryptomonnaie » associée à ces « portefeuilles ». On se retrouve finalement avec ces tiers de confiance imposés à la majorité des utilisateurs non formés techniquement. Cela remet déjà fortement en question les promesses de désintermédiation régulièrement associées aux *blockchains*.

Ce débat n'est pas sans rappeler celui sur le vote électronique, dont les défenseurs oublient bien souvent la nécessité démocratique de la simplicité et de la transparence de l'urne. Ces deux débats sont d'ailleurs liés puisque le vote électronique est l'une des applications régulièrement proposées des *blockchains* (voir l'analyse de Enguehard (2019) à ce sujet, ou encore la critique par Blanchard et al. (2022) d'un article défendant le vote électronique sur *blockchain*). Il n'est en fait pas étonnant que les défenseurs des *blockchains* ne se préoccupent pas plus que ça des enjeux d'usabilité et de démocratie : Michel Bauwens, qui a fondé et dirige la P2P Fondation[24], qualifie par exemple régulièrement les *blockchains* de « rêve technocratique totalitaire ».

« Portefeuille ». Le mot « portefeuille » tel qu'il est utilisé dans le cadre des « cryptomonnaies » prête à confusion. L'objet qu'on appelle normalement un « portefeuille » contient physiquement de l'argent liquide, et effectuer une transaction dans ce système ne nécessite que les portefeuilles de l'émetteur et du destinataire : il s'agit simplement du déplacement d'objets physiques (l'argent

22 Cf le fonctionnement des mécanismes de consensus, et de la preuve de travail en particulier, expliqué plus haut.
23 Certaines estimations donnent un chiffre autour de 10 % des bitcoins qui seraient ainsi perdus.
24 « La P2P Foundation est une organisation internationale consacrée à l'étude, la recherche, la documentation et la promotion des pratiques pair à pair. » https://wikifr.p2pfoundation.net/

liquide) du premier vers le second. Le système est réellement décentralisé, il est même *acentré* : la transaction s'effectue directement de pair à pair, sans dépendre d'aucun tiers. Dans le cas d'une « cryptomonnaie », comme on l'a expliqué plus haut mais contrairement à ce qui en est le plus souvent dit, ça ne se passe pas du tout de façon décentralisée ou pair-à-pair : le réseau sous-jacent est décentralisé, mais la transaction passe par un centre distribué, le registre. La transaction existe comme une écriture comptable, et correspondrait donc, par analogie avec de la monnaie, à un virement bancaire et non à un paiement en argent liquide. L'utilisation de l'analogie du portefeuille plutôt que de celle du compte en banque (ou d'interface de gestion de son compte en banque) est trompeuse et renforce certaines des illusions qui collent aux *blockchains* (décentralisation, anonymat, etc.). Notons qu'il est possible d'avoir un équivalent numérique de portefeuille avec la technologie Taler (Burdges et al., 2016), un système de transaction numérique respectueux de la vie privée et indépendant des devises utilisées (et ne reposant pas sur une *blockchain*).

Écriture performative. Enfin, une dernière (mais pas des moindres) remarque, qui découle d'une certaine façon de la précédente : il est impératif de comprendre que ce qui fait qu'une « cryptomonnaie » fonctionne, c'est que l'écriture dans le registre est par définition *performative*. La vérité de l'état du monde qu'on cherche à modifier par des transactions de « cryptomonnaie » est l'état de la *blockchain* elle-même : quel est le solde disponible sur chaque compte ? Ce solde se calcule *à partir* des écritures dans le registre : pour chaque compte on part de zéro, et on parcourt la liste des transactions qui le concernent en additionnant les montants des sorties qui lui sont associés et en soustrayant les montants des entrées (ou, de manière équivalente, en additionnant l'ensemble des montants des UTXO associés à ce compte). Cette particularité unique des « cryptomonnaies » doit bien être comprise pour ce qu'elle est, sans quoi le risque d'attribuer aux *blockchains* des vertus qu'elles n'ont pas arrive vite, comme nous allons le voir dans les deux cas d'usage suivants.

3.2. La certification de documents

En dehors des « cryptomonnaies », la certification de documents est, avec la traçabilité qui lui est techniquement tout à fait similaire, l'un des principaux usages proposés et vendus des *blockchains*. Les promoteurs de ces pratiques mettent systématiquement en avant des avantages comme la « sécurité », la « confiance », la « vérifiabilité », la « fiabilité », la « pérennité », etc. de leur produit. Concrètement, il s'agit d'inscrire des certificats, c'est-à-dire des condensats signés cryptographiquement de documents, dans une *blockchain*, de sorte à ce que, théoriquement, n'importe qui puisse vérifier l'existence, l'intégrité, et l'authenticité du document de façon décentralisée. Évidemment, ce n'est pas parce qu'il est écrit sur une *blockchain* qu'Alice est

diplômée de l'Université Paris 42 que c'est vrai[25]. Si l'Université Paris 42 est un établissement reconnu et accrédité à délivrer des diplômes, alors sa signature cryptographique du diplôme permet d'améliorer significativement la confiance dans le diplôme d'Alice… pourvu qu'on dispose à l'avance et de manière certaine de la clef publique de l'Université Paris 42, et bien sûr, qu'on fasse confiance à cet établissement, à ses formations et à sa bonne gestion de sa clef privée. On est donc en présence de tiers de confiance naturels : sans établissements de confiance (étant accrédités eux-mêmes par une autorité externe telle qu'un État), un diplôme n'a pas de valeur. Dans ce type de situation, le recours à une *blockchain* pour stocker les certificats apporterait deux choses. La première, c'est l'aspect décentralisé : si tout le monde peut avoir une copie à jour du registre, il est possible de vérifier dedans la présence d'une certification de diplôme (et l'absence d'une révocation ultérieure de ce diplôme) sans dépendre d'un tiers. Notons que pour être réalistement faisable, cela demande en pratique de maintenir à jour une base de données de l'ensemble des diplômes valides pouvant éventuellement nous intéresser. Tout cela suppose qu'on est sûr de l'intégrité de sa copie du registre. C'est la seconde chose qu'apporterait l'usage d'une *blockchain* : l'immuabilité du registre, que l'on peut vérifier à condition d'en conserver une copie à jour (à moins qu'on n'en récupère une copie au besoin auprès d'un… tiers de confiance).

En plus de la distribution et de l'immuabilité, la troisième propriété d'une *blockchain* est de résoudre le problème du consensus distribué, mais il n'y en a pas besoin ici : seule une liste finie d'acteurs identifiés (les établissements accrédités à délivrer des diplômes) ont la permission d'écrire dans le registre (on parle de « *blockchain permissionnée* », ce qui implique qu'une autorité externe a le pouvoir d'autoriser ou non des acteurs à écrire dans le registre). Dans ce cas, on peut s'économiser toute la partie mécanisme de consensus[26] : il est inutile de recourir à une *blockchain*.

D'autres technologies plus simples et bien moins coûteuses peuvent tout à fait faire l'affaire, et ce même en cas de défiance des acteurs autorisés entre eux et en voulant conserver le type de fonctionnement attendu d'une *blockchain* pour les aspects qui nous intéressent : par exemple il serait possible d'utiliser le logiciel de contrôle de versions Git[27] (Torvalds, 2005) en imposant par dessus un simple protocole à respecter quant au format et à la cadence des écritures dans le registre.

25 L'exemple des diplômes correspond a une utilisation de plus en plus répandue, bien qu'injustifiée techniquement, des *blockchains*. On a pu le voir récemment avec l'exemple de l'Université de Lille qui a choisi d'attester la validité de ses diplômes dans une *blockchain*, voir Dem-Attest-ULille (2022).

26 Il semble même préférable que ce ne soit pas les acteurs disposants de la plus grande puissance de calcul qui puissent décider de qui est diplômé ou non…

27 Git a été créé en avril 2005, et est lui-même inspiré du logiciel BitKeeper, qui a été créé en mai 2000, bien avant l'introduction des *blockchains* en 2008.

Mais en réalité, dans le cas des diplômes typiquement, puisque nous ne sommes absolument pas dans la situation de défiance généralisée supposée par les *blockchains*, il s'agit d'un problème beaucoup plus simple et que l'on sait parfaitement résoudre depuis longtemps. La distribution de diplômes numériques est en effet largement similaire à celle de certificats électroniques, problème résolu au moins depuis l'introduction de la recommandation X.509 (UIT, 1988) à la fin des années 80, que l'on utilise encore quotidiennement dans nos navigateurs web quand on visite un site en HTTPS. Les institutions qui délivrent des diplômes (par exemple les universités) joueraient le rôle d'*autorités de certification*, et celles qui accréditent les premières (par exemple les gouvernements) celui d'*autorités de certification de confiance* disposant de *certificats racines*. Un certificat (ou donc, un diplôme) valide consiste en une chaîne de signatures cryptographiques qui remonte jusqu'à un certificat racine (et dont aucun dans la chaîne n'a été révoqué depuis). En terme de coût, et d'autant plus avec l'usage peu intensif qu'implique le cas de la vérification de diplômes, cela n'a rien à voir avec une *blockchain*. Et cela pourrait encore être optimisé en admettant qu'on n'a pas forcément besoin de faire de la vérification de diplôme de façon décentralisée, en acceptant simplement la mise en place d'une base de données (qui doit exister de toute façon, rappelons-le) étatique interrogeable par quiconque dispose de l'identifiant d'un diplôme.

Il en va de même pour la certification d'actes notariés par exemple, qui perdraient complètement leur sens en l'absence du tiers de confiance représenté par le notaire (c'est-à-dire l'État et la Justice[28]) rendant possible un recours en cas de litige. Comme toutes les *blockchains* dites « privées », la « *blockchain notariale* » n'a d'ailleurs de *blockchain* que le nom puisqu'elle n'implémente pas du tout de mécanisme de consensus (Chaserant et al., 2021). Il ne s'agit finalement que d'une *centralisation* des données des notaires dans une base de données inefficace qui ne peut exister qu'en plus de celle qui sera effectivement utilisée.

En ce qui concerne la traçabilité, typiquement dans l'agroalimentaire, c'est encore pire : le seul rôle des *blockchains* utilisées dans ce cadre est de rendre publics des enregistrements de déclarations faites par les différents intermédiaires sur la chaîne de production jusqu'au consommateur. Il ne peut bien sûr exister aucune garantie technique de la véracité de ces déclarations.

On est ici en plein sur un exemple de confusion sur la performativité de l'écriture, avec la croyance que si c'est écrit dans une *blockchain* c'est forcément vrai, qui est due d'une part à l'incompréhension totale à la fois du fonctionnement de cette technologie et de celui de son usage historique, les « cryptomonnaies », et d'autre part à une idéologie politique libertarienne mêlant

28 En France par exemple, les notaires sont nommés par le garde des Sceaux et à ce titre investis d'une délégation de la puissance publique.

solutionnisme technologique et culte du contrat (ce dernier étant par ailleurs lui aussi mal compris, comme le prouve la croyance de certains en la désintermédiation permise par les *blockchains*).

3.3. Les NFT[29]

Fondamentalement, un NFT (« *non fungible token* », « jeton non fongible » en français) est simplement une « cryptomonnaie » dont il n'existe qu'une seule unité (appelée un « jeton ») qui a la propriété d'être indivisible (elle peut-être transmise mais pas découpée). Un NFT est un morceau d'information (le jeton) uniquement identifiable enregistré sur une *blockchain*, qui lie une identité (son propriétaire) à une donnée représentant un objet numérique ou physique. Il est ainsi censé servir à établir un certificat de propriété transmissible. En tant que certificat de propriété, il souffre de tous les problèmes que l'on a déjà évoqués concernant l'idée d'actes notariés en l'absence de tiers de confiance : l'inscrire dans une *blockchain* n'a aucun effet particulier sur le monde extérieur à celle-ci. En pratique, il ne s'agit donc que d'objets numériques dont la rareté est créée artificiellement de façon coûteuse pour en faire des actifs spéculatifs. À ce niveau, la différence avec les « cryptomonnaies » réside dans le fait que la valeur accordée à chaque NFT suit son propre cours. Les nombreuses promesses qui sont faites autour de cette technologie, notamment à propos d'un « web3 » décentralisé basé sur cette technologie, n'ont donc, sans exception, aucun sens techniquement. Une étude récente (Flick, 2022) de l'éthique des NFT conclue ainsi contre leur implémentation : « il n'y a actuellement aucun cas d'usage ni mise en œuvre possible des NFT qui soit éthique »[30].

4. Conclusion

La technologie de la *blockchain* n'est pas neutre : elle est issue d'une idéologie libertarienne (Golumbia, 2016) qui présuppose un monde de défiance généralisée. Dès qu'on sort du cadre d'un monde sans aucune confiance possible, l'usage d'une *blockchain* ne se justifie plus. On a vu qu'il existe de multiples alternatives moins coûteuses pour arriver au même résultat si on peut se reposer sur la confiance en certains acteurs. On a vu aussi que le coût d'une *blockchain* ne vient souvent pas *à la place* de l'alternative, mais *en plus*, car la base de données représentant l'état courant de la *blockchain* doit exister de toute façon pour des questions d'efficience. Les nombreux projets à base de *blockchains* qui fleurissent partout ne sont jamais le résultat de réflexions sur

29 Au moment de soumettre la proposition de cet article, il semblait impensable de ne pas y faire cas des NFT. Finalement, l'engouement démesuré pour cette technologie est déjà largement retombé au moment de rédiger ces lignes. Une étude plus poussée des NFT est consultable le blog de l'auteur : https://pablockchain.fr/NFT.

30 En anglais dans le texte : "*[NFTs] should not be implemented, as there is currently no ethical use case or means of implementation of NFTs*" (Flick, 2022).

comment résoudre un problème existant, mais plutôt de l'exact inverse : en partant du postulat que la solution est une *blockchain* est ensuite cherché le problème à résoudre.

Pourtant, quand on admet un cadre de défiance généralisée justifiant l'utilisation d'une *blockchain*, la seule chose permise par cette technologie est de modifier, seulement par ajout de nouvelles écritures, l'état d'un registre distribué. Pour ce faire de manière sécurisée, une incitation interne à participer à la *blockchain* doit exister : elle a besoin de sa « cryptomonnaie ». En même temps, il est essentiel de comprendre que la seule vérité garantie par l'écriture d'une information dans une *blockchain* est que l'information en question est écrite dans la *blockchain* en question. N'importe quoi de plus concernerait l'extérieur de la *blockchain* et ne pourrait être garanti que par un tiers de confiance, inexistant dans ce cadre. S'imposent alors les conséquences pratiques de cette réalité : l'usage d'une *blockchain* n'a de sens que si les écritures qu'on y réalise sont directement performatives, sans dépendre d'un tiers pour être « rendues vraies ». Le seul usage valide d'une *blockchain* semble donc être celui des « cryptomonnaies ». Finalement, il ne reste qu'à savoir si cet usage est socialement utile et politiquement désirable…

Bibliographie

(Back, 1997) A. Back, *Hash cash postage implementation*, Cypherpunks mailing-list, mars 1997. http://hashcash.org/

(Banque de France, 2018) Banque de France, *Focus n°16 : L'émergence du bitcoin et autres crypto-actifs : enjeux, risques et perspectives*, mars 2018. https://publications.banque-france.fr/lemergence-du-bitcoin-et-autres-crypto-actifs-enjeux-risques-et-perspectives

(Blanchard et al., 2022) E. Blanchard, F. Li Vigni, P. Rauzy, *Auteur·ices, relecteur·ices : redoublons de prudence face aux effets de modes technologiques*, 2022. https://hal.archives-ouvertes.fr/hal-03741811

(Burdges et al., 2016) J. Burdges, F. Dold, C. Grothoff, M. Stanisci, *Enabling Secure Web Payments with GNU Taler*, 6th International Conference on Security, Privacy and Applied Cryptographic Engineering, SPACE 2016. https://taler.net/papers/taler2016space.pdf

(Chaserant et al., 2021) C. Chaserant, C. Dauchez, S. Harnay, *Du notaire à la blockchain notariale : les tribulations d'un tiers de confiance entre confiance interindividuelle, confiance institutionnelle et méfiance généralisée*, Revue juridique de la Sorbonne, n°3, juin 2021. https://irjs.pantheonsorbonne.fr/sites/default/files/inline-files/Du_notaire_a_la_blockchain_notariale_C_CHASERANT_C_DAUCHEZ_S_HARNAY.pdf

(Chaum, 1982) D. Chaum, *Blind Signatures for Untraceable Payments*, Advances in Cryptology: Proceedings of Crypto '82. https://sci-hub.se/10.1007/978-1-4757-0602-4_18

(Dem-Attest-ULille, 2022) BCDiploma, Université de Lille, *Attestations numériques blockchain de réussite au diplôme de l'Université de Lille*, Livre blanc, 2022. https://www.univ-lille.fr/fileadmin/user_upload/presse/2022/20220114_Livre_blanc_Dem-Attest-ULille_FR.pdf

(Diffie et Hellman, 1976) W. Diffie, M. Hellman, *New directions in cryptography*, IEEE Transactions on Information Theory 22-6, novembre 1976. https://cr.yp.to/bib/1976/diffie.pdf

(Dwork et Naor, 1992) C. Dwork and M. Naor, *Pricing via processing or combatting junk mail*, Advances in Cryptology: Proceedings of Crypto '92. https://link.springer.com/content/pdf/10.1007/3-540-48071-4_10.pdf

(Enguehard, 2019) C. Enguehard, *Blockchain et vote électronique*, Terminal 129, 2019. https://journals.openedition.org/terminal/4190

(Flick, 2022) C. Flick, *A Critical Professional Ethical Analysis of Non-Fungible Tokens (NFTs)*, Journal of Responsible Technology (in press), 2022. https://doi.org/10.1016/j.jrt.2022.100054

(Golumbia, 2016) D. Golumbia, *The Politics of Bitcoin: Software as Right-Wing Extremism*, University of Minnesota Press, 2016. https://www.upress.umn.edu/book-division/books/the-politics-of-bitcoin

(Nakamoto, 2008) S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, novembre 2008. https://bitcoin.org/bitcoin.pdf

(NIST, 2002) NIST, *Secure Hash Standard*, Federal Information Processing Standards Publication 180-2, août 2002. https://csrc.nist.gov/csrc/media/publications/fips/180/2/archive/2002-08-01/documents/fips180-2.pdf

(Merkle, 1987) R. C. Merkle, *A digital signature based on a conventional encryption function*, Advances in Cryptology: Proceedings of Crypto ‘87. https://link.springer.com/content/pdf/10.1007/3-540-48184-2_32.pdf

(Rivest et al., 1978) R. L. Rivest, A. Shamir, L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Communications of the ACM 21-2, février 1978. https://dl.acm.org/doi/pdf/10.1145/359340.359342

(Torvalds, 2005) L. Torvalds, *Initial revision of "git", the information manager from hell*, avril 2005. https://git-scm.com/

(UIT, 1988) Union internationale des télécommunications, Comité consultatif international télégraphique et téléphonique, *série X : réseaux de communications de données : annuaire — Recommandation X.509 : Annuaire – cadre d’authentification*, novembre 1988. https://www.itu.int/rec/T-REC-X.509/recommendation.asp?lang=fr&parent=T-REC-X.509-198811-S