Blockchain : une mauvaise solution à la recherche d'un problème

Pablo Rauzy
Université Paris 8
LIASD / PASTIS (https://informatique.up8.edu/pastis/) et GÉODE (https://geode.science/)
2 rue de la liberté
93 200 Saint-Denis

Résumé

On entend de plus en plus parler de nouvelles technologies telles que les « cryptomonnaies », le « métavers », les « NFT », ou encore le « web3 », et celles-ci sont invariablement présentées comme des innovations incontournables du monde de demain, sans que ne soit jamais vraiment expliqué ni pourquoi ni comment… sauf une chose : c'est grâce à « la blockchain » ! En plus de ces nouvelles technologies, « la blockchain » est censée également révolutionner certaines pratiques existantes : par exemple la certification de documents (notariat, diplômes) ou la traçabilité (supply chain, agro-industrie), et parfois même, la démocratie (vote électronique)…
Après avoir rapidement expliqué les bases du fonctionnement d'une blockchain, nous partirons de cet état de fait technique pour se poser plusieurs questions : concrètement, ça fait quoi, une blockchain ? dans quelles hypothèses ? et du coup, quelles sont les limites de cette technologie ? mais alors, est-ce que ça résout un problème qui existe dans la vraie vie ?
Nous répondrons à ces questions avec un focus sur un des usages que des personnes à la recherche d'un problème à résoudre avec une blockchain poussent énormément dans l'enseignement supérieur et la recherche : la certification de diplômes.
En conclusion, nous reviendrons sur le caractère d'« innovation de rupture » systématiquement associé à cette technologie, et nous nous questionnerons sur son rôle en pratique, non plus techniquement, mais socialement et politiquement.

Mots-clefs

blockchain, chaîne de blocs, enjeux sociétaux, sobriété, identité, diplômes, certification

1 Introduction

Depuis quelques années, la technologie de la blockchain est sujette à un tel buzz qu'elle est mise à toutes les sauces. Les projets utilisant cette technologie se multiplient sans que le choix de l'utiliser ne semble être justifié par la nature des projets en question. La raison à cela semble être le fruit d'un pur effet de mode (lui-même assez directement lié à l'idéologie aveuglée du solutionnisme technologique) et des possibilités de financements qui en découlent.

En règle générale, le principe de ces projets est d'enregistrer des informations dans une blockchain en prétendant que cette technologie apporte une certaine forme de garantie. On voit par exemple régulièrement passer des projets qui consistent à mettre dans une blockchain des informations de traçabilité, des actes notariés, ou encore des diplômes, en promettant par ce biais des garanties de sécurité, de validité, et de pérennité de ces informations tout en permettant une désintermédiation.

Dans cet article, nous commencerons par définir ce qu'est une blockchain avant de revenir sur le fonctionnement de cette technologie. Cela nous permettra de comprendre réellement ce que permet

une blockchain et quelles en sont les limites, que nous discuterons ensuite. Ainsi équipé·es, nous nous concentrerons enfin sur son application principale dans l'enseignement supérieur : la certification de diplômes, et nous verrons que celle-ci n'a aucun sens. En conclusion, nous discuterons le caractère politique des choix techniques, et en particulier de la vision politique qui se cache derrière le choix de recourir à une blockchain.

2 Qu'est-ce qu'une blockchain ?

2.1 Définition

On peut définir une blockchain comme un registre *distribué*, *unique*, et *immuable*, qui ne doit nécessiter aucune confiance pour garantir ces propriétés.

Un *registre* est un document (en l'occurrence, un fichier) où sont consignés des faits. La particularité ici est que l'on veut rendre la participation en lecture et en écriture à ce registre possible pour n'importe qui, tout en garantissant les propriétés évoquées dans la définition, et sans faire confiance à personne.

Le registre doit être *distribué*, c'est-à-dire que chaque participant[1] en possède sa propre copie. Attention à ne le pas confondre « distribué » et « pair-à-pair ». Le réseau sous-jacent, qui va permettre la mise en œuvre du registre, est un réseau pair-à-pair, c'est-à-dire un réseau qui permet à chaque participant de discuter directement avec d'autres sans dépendre d'un centre unique comme ce serait le cas dans un réseau centralisé ; mais notre registre est lui simplement distribué.

Le registre doit aussi être *unique*, c'est-à-dire que les copies qui existent chez chaque participant doivent toutes être identiques : il ne doit exister qu'une seule version du registre.

Le registre doit également être *immuable*, c'est-à-dire qu'il doit être impossible de modifier (ou supprimer) une information qui y a été consignée.

Ces propriétés doivent être garanties en l'absence de confiance envers quiconque (chaque participant ne fait confiance qu'à lui-même) et sans pouvoir connaître l'ensemble des participants.

2.2 Usages

La raison d'être de ces propriétés et de cette contrainte de défiance généralisée tient entièrement à l'application pour laquelle cette technologie a été conçue : une « cryptomonnaie »[2], nommément Bitcoin. Une « cryptomonnaie » est un système de création, stockage, et transaction de jetons numériques ne nécessitant aucun tiers de confiance pour fonctionner.

En effet, il est nécessaire pour la viabilité d'un tel système de s'assurer que n'importe qui ne puisse pas créer de la « monnaie » (des jetons) à l'infini. Pour cette raison, il est nécessaire de rendre impossible la *double-dépense* (dépenser deux fois les mêmes jetons), ce qui n'est pas évident en l'absence de support physique et de tiers de confiance. Ainsi, le registre sert à stocker toutes les transactions qui ont lieu dans le système et doit à lui seul permettre à chaque participant de calculer l'état du système (c'est-à-dire qui possède quels jetons) typiquement pour vérifier qu'une

1 J'écris intentionnellement « participant » et « participants » plutôt que « participant·e » et « participant·es » pour insister sur le fait qu'il s'agit de serveurs, logiciels, etc. et non d'humain·es.

2 Je mettrai systématiquement des guillemets autour de ce terme car la qualification de « monnaie » est tout à fait discutable [2], et il faudrait plutôt parler de *crypto-actifs*.

transaction donnée est possible (c'est-à-dire que l'émetteur était bien en possession des jetons utilisés dans la transaction). La distribution du registre permet aux participants d'effectuer ces vérifications indépendamment. Son unicité permet de garantir l'existence d'une seule version de l'historique des transactions (pour éviter par exemple que le destinataire d'une transaction ne possède une version alternative du registre dans laquelle les jetons qu'il doit recevoir n'ont pas encore été dépensés alors qu'ils le seraient dans une autre version). Enfin, son immuabilité permet de garantir la cohérence du système (empêcher par exemple la disparition de transactions passées qui changeraient de façon incohérente l'état du système, en permettant par exemple à leurs émetteurs de récupérer les jetons dépensés dans ces transactions disparues).

De nombreux autres usages ont été proposés et mis en œuvre : traçabilité (supply chain, agro-industrie), contractualisation automatisée (notariat), certification de documents (actes de propriété, diplômes), et même démocratie (vote électronique). Nous reviendrons sur ces idées et en particulier sur la certification de diplômes après avoir regardé de plus près comment fonctionne une blockchain dans la section suivante.

3 Le fonctionnement d'une blockchain

Nous nous contenterons ici de présenter les aspects du fonctionnement d'une blockchain essentiels à la discussion de leurs limites dans le cadre qui nous intéresse. Pour une présentation plus complète, voir [9].

Pour des raisons d'efficacité, les transactions sont ajoutées en *bloc* plutôt qu'individuellement au registre. Un participant souhaitant effectuer une transaction la diffuse sur le réseau pair-à-pair en espérant que celle-ci sera validée puis prise en compte par des participants spéciaux appelés « mineurs »[3], qui l'ajouteront alors au bloc qu'ils tenteront d'ajouter au registre (nous verrons plus bas comment). À chaque ajout d'un bloc au registre, le système doit garantir les propriétés vues dans la définition, voyons comment.

3.1 Immuabilité

Chaque bloc est identifié par son contenu au moyen d'un *condensat cryptographique*[4] de celui-ci : si le contenu d'un bloc est modifié ne serait-ce que d'un bit, son condensat change et ne sera plus égal à son identifiant. Cela permet de vérifier l'intégrité des blocs individuellement. Dans une blockchain, chaque bloc contient l'identifiant du bloc précédent. Ce chaînage des blocs permet ainsi de vérifier l'intégrité de l'entièreté du registre, la modification d'un bloc entraînant l'invalidité de son identifiant dans le bloc suivant. C'est ainsi qu'est simulé son immuabilité (on parle de « simulation » car en réalité il s'agit d'un fichier sur un ordinateur, qui peut évidemment être modifié, mais les modifications seront du coup détectées et empêcheront la participation au réseau).

3 Ce terme a été choisi par analogie avec l'extraction minière de l'or et est utilisé pour désigner les machines qui jouent ce rôle sur le réseau autant que leurs propriétaires, ce qui en plus d'introduire une confusion entre travail et capital, est révélateur d'une certaine vision politique de la monnaie (nommément le *métallisme*, par opposition à la monnaie-dette) qui se trouve du coup inscrite au fondement même de la technologie.

4 Un condensat cryptographique est un nombre de taille fixe calculé avec une fonction déterministe à sens unique : sur une entrée donnée, elle renverra toujours le même nombre en résultat (le *condensat* des données d'entrée, on parle aussi d'*empreinte* ou de *hash*), mais il est pas possible d'inverser la fonction pour retrouver les données d'entrée correspondantes à un condensat donné.

3.2 Distribution

Lorsqu'un bloc doit être ajouté au registre, il est transmis sur le réseau pair-à-pair à l'ensemble des participants, et chacun peut vérifier indépendamment la validité du bloc (il contient bien le condensat du précédent, son identifiant est bien le condensat de son contenu) et des transactions qu'il contient (étant donné l'historique des transactions dans le registre, les transactions contenues dans le nouveau bloc sont bien valides), puis l'ajouter à sa copie locale du registre, si tout va bien.

3.3 Unicité

On sait garantir l'unicité d'un registre quand celui-ci est centralisé (il existe une autorité qui fait référence), ou, dans le cas d'un registre distribué, quand les participants coopèrent pour tenir à jour leur version du registre[5]. Dans le cas d'une blockchain, on ne fait confiance à personne par hypothèse, donc la coopération n'est pas une option. La seule solution est donc de simuler la centralisation du registre[6], ce qui nécessite de résoudre le problème du *consensus distribué*.

3.4 Consensus distribué

Le principe du consensus distribué est de mettre l'ensemble des participants « d'accord » sur une valeur. Pour une blockchain, ce sera le prochain bloc à ajouter au registre. Dans le contexte de défiance généralisée, il est impossible de satisfaire tout le monde : la taille d'un bloc est limitée et les participants ont des intérêts divergents, et on ne peut pas organiser un vote ni faire « chacun son tour » puisqu'on ne connaît pas l'ensemble des participants. La seule solution est donc de recourir à un *tirage au sort non contestable*. Il y a essentiellement deux façons de faire un tel tirage au sort dans un contexte distribué et de défiance généralisée : le « minage » par *preuve de travail*, et le « minage » par *preuve d'enjeu*.

3.4.1 Preuve de travail

Le principe de la preuve de travail [1][8] est de faire un paquet de calculs inutiles, jusqu'à trouver *par hasard* la solution x d'une inéquation de la forme $H(bloc, x) < seuil$, où H est une fonction de calcul de condensat cryptographique pour empêcher la possibilité de calculer x directement à partir du $bloc$ et du $seuil$. Le $seuil$ est le même pour tout le monde, mais comme le $bloc$ de chaque mineur est différent, le plus petit x satisfaisant l'inéquation ne sera pas le même pour tout le monde. Il est donc impossible de prédire qui trouvera une solution en premier[7]. Mais une fois une solution trouvée, elle est facilement vérifiable par n'importe qui.

Le premier « mineur » qui trouve une solution pour son bloc le diffuse accompagné de la valeur de la solution x qui sert donc de preuve de travail, en permettant de vérifier l'inéquation. À sa réception, les autres participants vérifient la validité du bloc, et, si c'est bon, l'ajoutent à leur copie du registre. Les « mineurs » abandonnent alors leurs calculs en cours, fabriquent un nouveau bloc avec les transactions qu'ils souhaitent encore ajouter au registre, puis se relancent immédiatement dans des calculs inutiles pour espérer remporter le prochain tirage au sort.

5 On voit ça tous les jours par exemple chez les développeur·euses qui collaborent autour d'un dépôt Git.

6 On remarquera que les transactions d'une « cryptomonnaie » sont centralisées sur un registre distribué, et donc pas pair-à-pair. Une transaction en « cryptomonnaie » ressemble beaucoup plus à un virement interne qu'à un paiement en liquide. Tout comme le titre de l'article « *Bitcoin: A Peer-to-Peer Electronic Cash System* » [10] est trompeur, le terme « portefeuille » (« *wallet* ») devrait être remplacé par « compte ».

7 Bien sûr, disposer de plus de puissance de calcul reste un avantage conséquent.

Le fait que les calculs soient inutiles pour s'assurer qu'il soit coûteux (matériel spécifique, électricité) fait partie du modèle de sécurité : il ne faut pas qu'un participant puisse avoir intérêt à diviser sa puissance de calcul pour faire exister plusieurs versions du registre en parallèle (ce qui lui permettrait des doubles dépenses). Malgré ce coût, il serait dangereux qu'un trop petit nombre de participants soient des « mineurs », car leur pouvoir de décision sur l'ensemble du système serait alors trop important, et le rapprocherait inéluctablement d'un système centralisé. Il est donc nécessaire d'inciter au minage à l'aide d'une récompense lors du « minage » réussi d'un bloc. Bien sûr, il ne peut y avoir d'autorité extérieure ou de tiers de confiance qui distribue les récompenses dans le contexte de défiance généralisée qui est supposé. Les récompenses doivent donc nécessairement être distribuées en « cryptomonnaie » (nouvellement créée ou issue de frais de transaction) que les « mineurs » s'attribuent via une transaction spéciale du bloc qu'ils « minent »[8].

3.4.2 La preuve d'enjeu

La preuve de travail étant une catastrophe écologique, le principe de la preuve d'enjeu est de se passer des calculs inutiles en permettant à des participants spéciaux de procéder directement à un tirage au sort classique. Pour s'assurer que ceux-ci ne trichent pas (puisqu'on est toujours dans un contexte de défiance généralisée), le tirage au sort est cette fois-ci pondéré par une *mise*. La mise est un montant de « cryptomonnaie » bloqué pour participer au tirage, sachant que plus on a misé gros et depuis longtemps, plus on a de chance d'être tiré au sort. Les mises sont publiques et donc le résultat du tirage ne doit pas surprendre, de sorte qu'il ne soit pas contesté par les participants.

En termes de sécurité, l'idée est que plus on peut miser gros, plus on a intérêt à ce que le système soit de confiance et donc moins on a intérêt à tricher d'une façon ou d'une autre. Cela reste tout de même moins solide que la preuve de travail et n'est jamais tout à fait auto-suffisant.

Comme pour la preuve de travail, une récompense est nécessaire comme incitation à participer au « minage », qui exige l'immobilisation de montants importants de « cryptomonnaie », pour éviter un effet de contraction du pouvoir de décision. Pour les mêmes raisons, cette récompense doit également être distribuée en « cryptomonnaie ».

3.4.3 Nécessité fonctionnelle de la « cryptomonnaie » et de lui donner une valeur

Que ce soit avec la preuve de travail (pour la récompense) ou avec la preuve d'enjeu (pour la mise comme pour la récompense), une blockchain ne peut pas fonctionner sans sa « cryptomonnaie ».

Pour que la « cryptomonnaie » puisse jouer son rôle d'incitation à la participation dans le mécanisme de consensus, il est nécessaire qu'elle ait une valeur marchande, y compris hors du système fermé qu'est la blockchain dont il est question. Or, il ne s'agit que de jeux d'écritures sur un registre, liées à rien dans la vraie vie. Le seul moyen d'attribuer une valeur aux jetons de la « cryptomonnaie » est d'en limiter la quantité, de mettre en place un marché, et de tenir un discours les rendant désirables. La valeur d'un jeton d'une « cryptomonnaie » correspond à ce que le prochain pigeon est prêt à payer pour. C'est ce qu'on appelle la *théorie du plus grand fou* [13] en économie, et c'est à rapprocher des *pyramides de Ponzi* ou de la pratique du *pump'n'dump*.

8 On remarquera ici que la notion de « consensus » des blockchains est très éloignée de celle du langage courant puisque le « consensus » se fait sur le bloc proposé par un mineur contre l'avis de tous les autres, puisque chacun propose un bloc différent au moins en ce qui concerne l'attribution de la récompense, qu'il se destine forcément.

4 Les limites des blockchains

Les éléments de fonctionnement des blockchains vus dans la section précédente nous permettent maintenant de discuter des limites de cette technologie.

4.1 La solution du problème de la solution

S'il existe une autorité extérieure ou un tiers de confiance, on a pas besoin de résoudre le problème du consensus distribué, et donc on a pas besoin de blockchain : on peut fournir le même service de manière plus simple et moins coûteuse, en s'appuyant sur la confiance existante.

Dans une situation de défiance généralisée, aucun tiers ne peut assurer la correspondance entre l'écriture dans le registre et la vraie vie. Une blockchain ne peut donc garantir par elle-même que ce qui est vraie *parce que* c'est écrit dans son registre. De ce fait, la seule application qui fait sens est donc la mise en œuvre d'une « cryptomonnaie ».

Une blockchain a besoin de sa « cryptomonnaie » pour fonctionner, et la mise en œuvre d'une « cryptomonnaie » est la seule chose que peut vraiment faire une blockchain : blockchain et « cryptomonnaie » sont des solutions qui sont leur propre problème.

4.2 Catastrophe écologique : une structure de donnée inefficace et intrinsèquement coûteuse

Pour s'assurer de la validité d'une transaction, il faut entre autre vérifier que l'émetteur dispose bien de la « cryptomonnaie » dépensée. Une blockchain ne liste que les modifications du système (les transactions) : le montant de « cryptomonnaie » disponible sur un compte[4] correspond à ce qui y a déjà été encaissé et qui n'a pas encore été dépensé. Si on ne dispose que du registre, il faut donc le relire en entier pour chaque vérification, ce qui est évidemment impensable.

En pratique, on est obligé de maintenir une vraie base de données de l'état du système, comme le ferait un système centralisé, pour y accéder directement plutôt que de le recalculer à chaque fois. Le maintien de cette base de données doit être fait indépendamment par chaque participant.

En comparaison, le coût d'une blockchain n'est donc jamais à la place mais toujours en plus du coût de la base de données centralisée équivalente démultiplié par le nombre de participants. Et cela reste vrai même en cas d'usage de la preuve d'enjeu comme mécanisme de consensus distribué.

Évidemment, la preuve de travail reste une catastrophe bien supérieure. Exemple avec la consommation annuelle de Bitcoin[9] : ~80 Mt de CO_2, ~140 TWh d'énergie électrique, ~30 kt de déchets électroniques, ~2 000 GL d'eau. En normalisant ces chiffres pour avoir des données par transaction, on peut comparer avec le système VISA par exemple : 1 transaction Bitcoin consomme autant d'énergie que ~560 k transactions VISA, et émet autant de CO_2 que ~1M transactions VISA.

9 Source : https://digiconomist.net/bitcoin-energy-consumption (accès début 2024).

4.3 « Tragédie des communs »[10]

Par définition, l'arrivée de nouveaux participants doit être possible à tout moment (sinon, on connaît l'ensemble des participants et on a plus besoin d'une blockchain). Bien sûr, les nouveaux participants doivent pouvoir récupérer l'historique du registre. Sauf qu'avec le temps, le registre ne fait que grossir et son stockage comme son partage, deviennent de plus en plus coûteux.

Comme on fait l'hypothèse d'une situation de défiance généralisée et de concurrence entre les participants (pour les récompenses), on se retrouve face à un dilemme du prisonnier : puisque chaque participant doit de toutes façons maintenir pour son usage une base de données avec l'état du système au fur et à mesure de l'ajout de blocs au registre, il n'a pas besoin de conserver l'historique pour lui-même, et peut donc décider de laisser les charges du stockage et du partage aux autres dès qu'elles lui semblent trop coûteuses. Évidemment, l'arrêt de la participation de certains augmente le coût pour les autres qui sont moins nombreux à partager l'historique sur le réseau pair-à-pair… jusqu'à ce qu'il n'y ait (presque) plus personne d'assez altruiste et que l'arrivée de nouveaux participants ne soit donc plus possible, ou qu'elle dépende d'un trop petit nombre d'altruiste en qui il faudra alors faire confiance, ce qui casse le modèle de défiance généralisée pris comme hypothèse et justifiant le recours à une blockchain en premier lieu.

Les hypothèses qui justifient le recours à une blockchain empêchent sa pérennité.

4.4 Un élitisme aveuglé et ultra-individualiste

La cryptographie asymétrique vraiment décentralisée ne peut pas être conviviale : les notions en jeu ne sont pas simples à appréhender, et il est notoirement difficile de conserver ses clefs privées de façon sécurisée et fiable, même pour des professionnel·les averti·es… Cela pose également des problèmes techniques et politiques : les erreurs (fuites, fausses manipulations, pertes, etc.) sont définitives et irrémédiables, et il est impossible d'imposer des décisions collectives. L'alternative à la décentralisation absolue n'est pas forcément la centralisation : en termes d'architecture réseau, la fédération est une approche pragmatique beaucoup plus réaliste et qui, bien qu'elle nécessite de la confiance et donc sorte du cadre justifiant le recours à une blockchain, est en fait utilisée en pratique même pour les « cryptomonnaies » : *exchanges* centralisés, *hosted wallets*.

En plus d'être politiquement et techniquement indésirable, la décentralisation totale est un mythe.

4.5 La vérité sur la blockchain

Dans le cas des « cryptomonnaies », on a affaire à de l'*écriture performative* : les transactions ne sont qu'un jeu d'écriture, sans aucun lien avec le monde réel, elles ont lieu *parce qu*'elles sont écrites, du fait même d'être écrites.

Ça ne fonctionne pour rien d'autre ! Une certification ne peut être issue que d'une autorité de confiance. La valeur d'un contrat provient de l'existence d'une autorité tierce (la justice) pour contraindre à son application. La traçabilité de l'origine d'un produit implique de faire confiance aux déclarations des différents acteurs qui inscrivent les étapes dans le registre. Quant au vote

10 Je n'aime pas le terme de « *tragédie* » qui sous-entend une forme d'inéluctabilité à la disparition des communs alors qu'un commun dispose normalement d'une gouvernance pour s'assurer de sa pérennité, mais dans le cas des blockchains et de la défiance généralisée, il faut reconnaître que la mise en place de toute organisation/structure humaine nécessitant une forme de confiance sociale est censée être impossible…

électronique… je n'ai toujours vu nulle part à quelle problématique du vote électronique une blockchain répondrait, j'ai par contre vu énormément de soucis avec l'idée d'en utiliser [3][6].

La seule vérité garantie par l'écriture d'une information sur une blockchain est que cette information est écrite sur cette blockchain.

5 La certification de diplômes

Un diplôme universitaire est nécessairement délivré par un établissement d'enseignement supérieur habilité à le faire, typiquement par un état. C'est d'ailleurs de là que provient sa valeur.
Vouloir mettre des certifications de diplômes dans une blockchain n'a donc aucun sens, car seul l'établissement qui a délivré le diplôme est réellement en mesure de certifier son authenticité : il s'agit d'une autorité centrale indispensable à la certification du diplôme, quelle que soit la façon dont celui-ci existe, sur papier ou numériquement. On est donc par nature en dehors du cadre qui justifie le recours à une blockchain : il y a un nombre fini d'acteurs identifiés qui peuvent écrire dans le registre, il n'y a donc pas besoin de résoudre le problème du consensus distribué (comme d'ailleurs dans tous les cas de blockchains « de consortium » ou « permissionnée », que l'on peut systématiquement remplacer par l'équivalent d'un dépôt Git [11] ou d'une base de données).

Pourtant, plusieurs initiatives de ce type ont vu le jour, et la pratique existe bel et bien dans certains établissements de l'ESR [4]. Concrètement, il s'agit d'enregistrer dans une blockchain des condensats d'attestations de diplômes signées cryptographiquement avec la clef privée de l'établissement diplômant. Cela permet théoriquement à n'importe qui disposant d'une copie de la blockchain de vérifier l'authenticité d'un diplôme, pourvu qu'il dispose de manière certaine de la clef publique de l'établissement diplômant, et bien sûr, qu'il fasse confiance à cet établissement, à ses formations, et à sa bonne gestion de sa clef privée… finalement la blockchain utilisée ne sert que de support de distribution des attestations.

La question se pose aussi de la possibilité de révocation des diplômes. Comme pour vérifier la validité d'une transaction d'une « cryptomonnaie », si on ne maintient pas une base de données à jour de qui a quel diplôme, pour vérifier qu'une personne a bien un diplôme il est nécessaire de parcourir la blockchain pour vérifier qu'il lui a bien été décerné puis qu'il n'a pas été révoqué. En pratique, aucune entreprise ou administration ne va payer pour elle seule le coût de la maintenance de la base de données de *tous* les diplômes pour les quelques-uns qu'elle doit vérifier de temps en temps, et la vérification va donc se faire auprès de tiers de confiance, comme l'établissement qui a délivré le diplôme, ou tristement, mais plus réalistement, auprès de la start-up qui a réussi à vendre ce service à des établissements naïfs.

Enfin, *si* certifier numériquement des diplômes est utile, alors c'est faisable de manière plus efficace et moins coûteuse sans blockchain. 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 à la fin des années 1980 [12], 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 de 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, les listes de révocations étant publiques). En matière 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, d'autant que cette infrastructure reste en fait nécessaire avec une blockchain. On pourrait également admettre qu'on n'a pas forcément besoin de faire de la vérification de diplôme de façon décentralisée, et accepter simplement la mise en place d'une base de données étatique interrogeable par quiconque qui dispose de l'identifiant d'un diplôme.

6 Conclusion

L'incompréhension de la nature performative de l'écriture dans le cas des « cryptomonnaies » pour lequel les blockchains ont été conçues a permis la propagation de la croyance en des propriétés presque magiques de garantie de véracité ou d'authenticité qu'une blockchain n'est en réalité aucunement capable de fournir. Cette incompréhension, couplée à la propagande venant autant des marchés spéculatifs de « cryptomonnaies » que des entreprises cherchant à vendre leurs « solutions » à base de blockchains, explique l'effet de mode et l'omniprésence de cette technologie (qui semble heureusement sur le déclin actuellement[11]).

Les projets ayant recours à une blockchain sont systématiquement le fruit du questionnement « j'ai une blockchain, que faire avec ? », car une blockchain ne sera jamais la réponse à « j'ai tel problème à résoudre, comment faire ? ».

Comme on l'a vu dans le cas des diplômes, il y a systématiquement une solution alternative plus simple et moins coûteuse sans blockchain. De façon générale, une blockchain est une mauvaise solution à la recherche d'un problème. C'est un serpent qui se mord la queue : elle nécessite sa « cryptomonnaie » pour fonctionner et les « cryptomonnaies » en sont le seul cas d'usage qui soit techniquement justifié, mais dont la pertinence reste à questionner politiquement [8].

En effet, blockchain et « cryptomonnaie » sont des technologies non neutres, d'idéologie libertarienne [7]. Elles pré-supposent une défiance généralisée et des comportements ultra-individualistes. Finalement, l'usage concret principal des blockchains est celui de véhicule de propagation et de normalisation de la pensée libertarienne : individualisme contre le bien commun ; refus de la régulation au profit de la loi du plus fort ; vision *métalliste* de la monnaie contre la notion de *monnaie-dette*, rejetée, car elle nécessite de la confiance sociale mais qui correspond à la réalité de notre système monétaire ; déplacement de la confiance depuis les personnes et structures organisationnelles vers la technologie, sans en voir ou admettre les limites ; et enfin, la volonté, typiquement avec le « web3 », de la généralisation de la concurrence et de l'économie de marché à toute interaction, informatique comme humaine.

Dans l'enseignement supérieur, combattre la mise en œuvre de certification de diplômes par blockchain est nécessaire, non seulement parce que c'est inutilement coûteux dans un contexte budgétaire toujours très compliqué, mais aussi parce que ça participe d'une idéologie qui tend à détruire les valeurs des services publics de l'éducation et de la recherche.

11 Heureusement (ou pas), la hype autour des LLM fait qu'une bonne partie des « expert·es » blockchain sont devenu·es des « expert·es » IA…

Bibliographie

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

[2] 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

[3] 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

[4] 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

[5] 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

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

[7] 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

[8] N. Hadjadji, *No Crypto. Comment Bitcoin a envoûté la planète.* Éditions Divergences. https://www.editionsdivergences.com/livre/no-crypto-ideologie-et-populisme-au-royaume-des-cryptomonnaies

[9] P. Rauzy, *Promesses et (dés)illusions : une introduction technocritique aux blockchains*, Terminal 136, 2023. https://journals.openedition.org/terminal/9059

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

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

[12] 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

[13] Wikipédia, *Théorie du plus grand fou*. Accès 2024. https://fr.wikipedia.org/wiki/Th%C3%A9orie_du_plus_grand_fou