La chaîne de blocs est une technologie réactionnaire

Pablo Rauzy — pr@up8.edu
Université Paris 8
Laboratoire LIASD / équipe PASTIS (https://informatique.up8.edu/pastis/)
Centre GÉODE (https://geode.science/)

Résumé < 500 signes :
Une technologie est toujours située politiquement, ne serait-ce que par qui la contrôle, mais parfois même par conception. La chaîne de blocs, ou *blockchain*, a été conçue pour la mise en œuvre de la première « cryptomonnaie », Bitcoin. Loin d'être neutre, elle sert de véhicule de propagande à l'idéologie libertarienne. Dans cet article nous expliquons le fonctionnement de cette technologie pour en démontrer les limites techniques et révéler son idéologie intrinsèquement réactionnaire.

Résumé :
Une technologie, quelle qu'elle soit, n'est jamais neutre. Ne serait-ce que parce qu'elle existe dans un système qui ne l'est pas, et que ses effets sont en partie dictés par qui la contrôle. Mais cela va parfois plus loin, certaines technologies embarquent une idéologie de par leur conception même. Dans cet article, nous allons montrer que c'est notamment le cas de la chaîne de blocs, ou *blockchain*, une technologie initialement conçue pour la mise en œuvre de la première « cryptomonnaie », Bitcoin. Nous verrons que cette technologie sert de véhicule de propagande à ses partis pris idéologiques, typiquement par son application partout sans que cela ne soit techniquement justifiable. Pour ce faire, nous commencerons par expliquer le fonctionnement d'une chaîne de blocs, cela nous permettra de démontrer ses limites techniques et de révéler l'idéologie intrinsèquement réactionnaire voire fascisante de cette technologie.

Mots-clés : chaîne de blocs, blockchain, politique

The Blockchain is a Reactionary Technology

Abstract < 500 characters:
Technologies are always politically situated, if only by who controls them, but sometimes even by design. Blockchains were invented and designed for the implementation of the first "cryptocurrency", namely Bitcoin. Far from being neutral, they actually serve as a vehicle for libertarian ideology. In this paper, we explain how blockchains work to demonstrate their technical limitations and to reveal their inherently reactionary ideology.

Keywords: blockchain, politics

Introduction

Depuis une quinzaine d'années, la technologie des chaînes de blocs, ou *blockchains*, est à la mode. Cette mode est savamment entretenue de deux façons simultanées : d'un côté par une bulle spéculative gigantesque autour des « cryptomonnaies », ce pourquoi cette technologie a été conçue, et de l'autre par le financement de très nombreux projets recourant à une chaîne de blocs par pure idéologie du solutionnisme technologique, sans que cela ne soit techniquement justifiable.

L'effet concret de l'omniprésence des chaînes de blocs, au-delà de son coût écologique délirant, est la propagation et la normalisation de l'idéologie libertarienne. La conception-même des chaînes de blocs prend comme postulat un monde ultra-individualiste où la confiance sociale est supposée impossible et où la notion de propriété privée est érigée en dieu.

Dans cet article, nous allons expliquer le fonctionnement technique d'une chaîne de blocs. Cela permettra de mettre en évidence les limites de cette technologie et ainsi de démontrer en quoi son usage pourtant très répandu n'est pas justifiable d'un point de vue technique, mais peut s'expliquer par la recherche d'une hégémonie politique et culturelle libertarienne, c'est-à-dire d'extrême droite[1], tout à fait compatible avec le techno-fascisme de la Silicon Valley[2].

Qu'est-ce qu'une chaîne de blocs ?

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

Un *registre* est un document (en l'occurrence, un fichier informatique) où sont consignés des faits. La particularité ici est que l'on veut rendre la participation à ce registre, consultation ou ajout de nouveau contenu, possible pour n'importe qui, tout en garantissant les trois propriétés susmentionnées, mais sans faire confiance à personne.

Le registre doit être *distribué*, c'est-à-dire que chaque participant en possède sa propre copie. Attention à ne pas confondre « distribué » et « décentralisé ». Le réseau sous-jacent, qui permet la mise en œuvre du registre, est un réseau décentralisé 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 ; mais le 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.

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 »[3], nommément

---

1 David Golumbia, *The Politics of Bitcoin: Software as Right-Wing Extremism*, Minneapolis, University of Minnesota Press, 2016.

2 Nastasia Hadjadji et Olivier Tesquet, *Apocalypse Nerds, comment les techno-fascistes ont pris le pouvoir*, Quimperlé, Ed. Divergences, 2025.

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 transaction donnée est valide (c'est-à-dire que l'émetteur était bien en possession des jetons utilisés dans la transaction au moment de celle-ci). La *distribution* du registre permet aux participants d'effectuer ces vérifications indépendamment, sans devoir faire confiance à quiconque. Son *unicité* garantit 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 par ailleurs dans une autre version. Enfin, son *immuabilité* garantit la cohérence du système, en empêchant par exemple la disparition d'une transaction passée dans laquelle des jetons que l'on cherche à dépenser l'auraient déjà été.

Comme expliqué en introduction, de nombreux autres usages des chaînes de blocs que des « cryptomonnaies » ont été proposés et mis en œuvre : registre de traçabilité (supply chain, agro-industrie), contractualisation automatisée (notariat), certification de documents (actes de propriété, diplômes), et même démocratie (vote électronique). Nous ne nous attarderons pas dessus si ce n'est pour expliquer en quoi la technologie est parfaitement inappropriée à ces usages, laissant ainsi paraître des choix de conceptions idéologiques et non techniques dans l'ensemble de ces projets.

Le fonctionnement d'une chaîne de blocs

Afin de rester accessible, nous n'entrerons pas ici trop précisément dans le détail de la technique, sans pour autant sacrifier la rigueur scientifique requise pour réellement penser les enjeux politiques. Nous nous limiterons donc à développer les grandes lignes des aspects techniques pertinents à la compréhension des limites de la technologie et à la mise en exergue des choix politiques de sa conception[4].

Le concept de chaîne de blocs a donc été inventé pour la mise en œuvre d'une « cryptomonnaie », Bitcoin[5]. Comme on l'a vu, la chaîne de blocs est le registre dans lequel sont stockées les transactions. Pour des raisons d'efficacité, les transactions y sont ajoutées en bloc plutôt qu'individuellement. Un participant souhaitant effectuer une transaction diffuse celle-ci sur le réseau pair-à-pair en espérant qu'elle sera validée puis prise en compte par des participants spéciaux appelés « mineurs » (nous reviendrons plus loin sur le choix, tout à fait politique, de ce terme), qui l'ajouteront alors au bloc qu'ils tenteront d'ajouter au registre (nous verrons comment). À chaque ajout d'un bloc au registre, le système doit garantir les propriétés vues plus haut : immuabilité, distribution, unicité.

---

3 Le terme « cryptomonnaie » est désormais consacré, mais « crypto-actifs » serait plus juste, cf Banque de France, « Focus n°16 : L'émergence du bitcoin et autres crypto-actifs : enjeux, risques et perspectives », 2018.

4 Pour aller plus loin sur la technique en restant relativement accessible à un lectorat non scientifique, cf Pablo Rauzy, « Promesses et (dés)illusions : une introduction technocritique aux blockchains », Terminal, n°136, 2023.

5 Satoshi Nakamoto, « Bitcoin: A Peer-to-Peer Electronic Cash System », bitcoin.org, 2008.

Immuabilité

Dans le registre, chaque bloc est identifié par son contenu au moyen d'un *condensat cryptographique* de celui-ci.

Un *condensat cryptographique* est un nombre qui joue le rôle d'empreinte digitale d'une donnée numérique : une même donnée aura toujours le même condensat, mais une modification même minime de la donnée changera complètement son condensat. Un condensat cryptographique a aussi la propriété d'être très facile à calculer à partir d'une donnée, mais d'être impossible à calculer en sens inverse (retrouver la donnée à partir de son condensat).

Si le contenu d'un bloc est modifié ne serait-ce que d'un bit, son condensat change. Cela permet de vérifier l'intégrité d'un bloc donné. Dans une chaîne de blocs, chaque bloc contient entre autres 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. Corriger le bloc suivant pour rétablir la cohérence du registre nécessite de modifier son contenu et donc son identifiant, qui se retrouve alors invalide dans le bloc d'après, et ainsi de suite par réaction *en chaîne*. C'est ainsi qu'est simulé (on parle de « simulation » car en réalité il s'agit d'un fichier sur un ordinateur, qui est donc modifiable, mais le mécanisme mis en œuvre permet de détecter les modifications et d'empêcher alors la participation au réseau) l'immuabilité d'une chaîne de bloc.

Distribution

Lorsqu'un bloc doit être ajouté au registre, il est transmis à l'ensemble des participants, et chacun peut vérifier indépendamment la validité du bloc (s'il contient bien le condensat du précédent, si son identifiant est bien le condensat de son contenu) et des transactions qu'il contient (vu l'historique des transactions dans le registre), puis l'ajouter à sa copie locale du registre, si tout va bien.

Unicité

On sait garantir l'unicité d'un registre quand il est centralisé (il y a une autorité qui fait référence), ou, dans le cas distribué, quand les participants coopèrent pour tenir à jour leur copie du registre. Dans le cas d'une chaîne de blocs, 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, ce qui nécessite de résoudre le problème du *consensus distribué*.

Le principe du *consensus distribué* est de mettre l'ensemble des participants « d'accord » sur une valeur. Pour une chaîne de blocs, 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 techniquement deux *mécanismes de consensus* permettant de mettre en œuvre 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*.

Le principe de la *preuve de travail* est de réaliser un paquet de calculs inutiles de condensats cryptographiques du bloc que l'on souhaite ajouter au registre, en modifiant à chaque fois une des données qu'il contient qu'on appelle *nonce* et qui ne sert qu'à ça, jusqu'à tomber *par hasard* sur un condensat plus petit qu'un certain seuil qui détermine la difficulté de travail attendue.

Pour visualiser l'exercice, on peut imaginer 100 dés à six faces numérotés de 1 à 100 et disposés dans un seau d'une façon parfaitement et entièrement déterminée par les données du bloc, de sorte que renverser plusieurs fois le seau pour un même bloc donne chaque fois l'exact même résultat. Le « minage » consiste alors à renverser le seau de dés en boucle en redisposant chaque fois précisément les dés en fonction du bloc, dont seul le *nonce* est modifié pour chaque lancer, jusqu'à tomber sur un résultat où les dés 1 à 30 (le seuil de difficulté de la preuve de travail) sont des 1.

Le premier « mineur » qui y parvient gagne le tirage au sort, il peut diffuser son bloc avec la valeur du *nonce* qui lui a permis de réussir le challenge et qui sert de preuve de travail (les autres participants peuvent disposer les dés de l'exacte même façon dans leur seau identique et constater sur le résultat du lancer qu'au moins les 30 premiers dés donnent 1). À la réception du bloc, les autres participants vérifient sa validité et l'ajoute alors à leur copie du registre. Les « mineurs » abandonnent leurs calculs en cours, construisent un nouveau bloc avec les transactions qu'ils souhaitent ajouter au registre et l'identifiant du bloc qui vient d'être validé, puis se relancent immédiatement dans des calculs inutiles pour espérer remporter le prochain tirage au sort.

Le fait que les calculs soient inutiles pour s'assurer qu'il soit coûteux (matériel spécifique, électricité) fait partie du modèle de sécurité : par exemple, 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 (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 trop important, et le rapprocherait inéluctablement d'un système centralisé. Il est donc nécessaire d'inciter à la participation *via* une récompense lors du « minage » réussi d'un bloc. Bien sûr, il ne peut y avoir de tiers de confiance qui distribue les récompenses dans le contexte de défiance généralisée qui est pris comme hypothèse. 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 ».

La preuve de travail étant une catastrophe écologique, le principe de la *preuve d'enjeu* est de se passer au maximum 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 enregistrées sur le registre, 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 insuffisamment solide et nécessite d'être complété par exemple par une preuve de travail affaiblie.

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 », et cette récompense doit également être distribuée en « cryptomonnaie » pour les mêmes raisons.

Quel que soit le mécanisme de consensus utilisé, une chaîne de bloc nécessite donc une « cryptomonnaie » pour fonctionner.

Nécessité fonctionnelle de la spéculation

Pour que la « cryptomonnaie » puisse jouer son rôle d'incitation à la participation, il est nécessaire qu'elle ait une valeur marchande, y compris hors du système fermé qu'est une chaîne de blocs (pour payer le matériel, l'énergie, etc.). Or, il ne s'agit que de jeux d'écritures sur un registre, liés à rien dans la vraie vie. Le seul moyen d'attribuer une valeur aux jetons de la « cryptomonnaie » sans introduire de tiers de confiance est d'en limiter la quantité, de mettre en place un marché spéculatif, et de tenir un discours les rendant désirables. La valeur d'un jeton d'une « cryptomonnaie » correspond alors à ce que le prochain pigeon est prêt à payer. C'est ce qu'on appelle la *théorie du plus grand fou* en économie, et c'est à rapprocher des *pyramides de Ponzi* ou de la pratique du *pump and dump*.

Vocabulaire et politique des chaînes de blocs

Monnaie ?

Les jetons de « cryptomonnaie » sont donc des actifs numériques purement spéculatifs. Difficile de les qualifier sincèrement de monnaie si on s'en tient à la définition la plus courante en économie, qui demande qu'une monnaie puisse servir de réserve de valeur (l'aspect purement spéculatif rend la valeur de ces jetons extrêmement volatile), d'unité de compte (idem, et on remarque d'ailleurs que même les cours des différentes cryptomonnaies entre elles est toujours exprimé en dollars ou en euros), et d'intermédiaire d'échange (propriété triviale mais qui reste fausse concernant les « cryptomonnaies » qui ne sont acceptées presque nulle part comme moyen de paiement).

Malgré tout, il existe différentes définitions de ce que doit être une monnaie, et il est intéressant de se pencher sur la nature monétaire qu'aurait une « cryptomonnaie » considérée comme telle. Dès l'introduction du concept, Bitcoin est défini par son concepteur d'« espèce » (« *cash* ») échangeable de « pair-à-pair » (« *peer-to-peer* ») dès le titre de son article[6]. Il s'ensuit l'usage de termes comme « portefeuille » (« *wallet* ») pour parler des dispositifs de gestion (émission, réception, conservation) de « cryptomonnaies ». Pourtant, comme on l'a vu, une « cryptomonnaie » ne correspond à rien d'autre qu'un jeu d'écritures dans un registre, et il n'est donc pas possible de l'utiliser de manière directement pair-à-pair comme on pourrait le faire avec de l'argent liquide. Pour avoir lieu, une transaction en « cryptomonnaie » doit nécessairement passer par une écriture dans son registre unique et distribué, à la vue de tous. S'il s'agit de monnaie, celle-ci est donc clairement scripturale et non fiduciaire. La bonne analogie devrait donc être de parler de « compte » et non de « portefeuille ». Mais le choix du vocabulaire employé n'est pas technique, il est politique. Ce choix techniquement erroné vient d'une part de la défiance envers les banques, l'article introduisant Bitcoin est publié au sortir de la crise bancaire et financière de 2008, et d'autre part du cadre idéologique ultra-individualiste dans lequel est pensée cette technologie. Bien que la dette soit la nature profonde de la monnaie[7], il n'est en effet pas question pour les concepteurs de Bitcoin et des chaînes de bloc d'accepter l'idée de *monnaie-dette* : la valeur que l'on peut accorder à une dette repose entièrement sur la confiance portée à son débiteur, et la notion même de confiance est réfutée dans le cadre de pensée libertarien qui base toute sa construction sur la naturalisation de la notion de propriété privée. Cela explique la volonté de créer l'équivalent numérique d'une *monnaie-métal*, physiquement constituée d'une marchandise précieuse donnant ainsi une valeur intrinsèque à la monnaie fiduciaire, et dont la possession est le seul moyen de

6 Cf. note 5.
7 David Graeber, *Dette : 5 000 ans d'histoire*, Arles, Actes Sud, 2011.

contrôle possible. Cette intention affichée de créer un « or numérique » se retrouve également dans le choix de l'analogie avec l'extraction minière.

Minage ?

Contrairement à ce que l'on pourrait penser, l'analogie avec l'extraction minière de l'or n'est pas issu d'une tentative de vulgarisation du fonctionnement des chaînes de blocs. Il s'agit en vérité d'un choix de politique monétaire qui a précédé et orienté la conception de la technologie. On retrouve en effet cette analogie comme justification de multiples décisions techniques arbitraires dans l'article qui introduit Bitcoin. Par exemple, le protocole prévoit de récompenser la participation au mécanisme de consensus (qui permet d'ajouter un bloc de transactions au registre) par un montant fixe (et même qui diminue dans le temps) malgré le coût de participation augmentant à mesure que plus de puissance de calcul est ajoutée au réseau. Cette décision est justifiée par une analogie directe avec l'extraction minière : « *L'ajout régulier de nouvelles pièces est analogue aux mineurs d'or qui dépensent de plus en plus de ressources pour trouver de l'or et le mettre en circulation.* »[8]. De même, le fait que cette récompense soit divisée par deux tous les 4 ans est justifié par l'idée que plus on a extrait d'or dans les mines moins il en reste, et donc plus il est difficile d'en trouver de nouveau même avec une augmentation significative de l'effort d'extraction.

On retrouve encore cette analogie dans le choix d'avoir limité à un maximum (21 millions) le nombre total de bitcoins qui pourront être en circulation, tout comme il y a une quantité d'or finie sur Terre. Le choix de concevoir une monnaie basée sur un métal précieux révèle encore la famille de pensée politique et économique dans laquelle s'inscrit la conception de Bitcoin. On peut en effet lire dans l'article « *Une fois qu'un nombre déterminé de pièces aura été mis en circulation, la récompense ne sera plus constituée que des frais de transaction, ce qui évitera alors toute inflation.* »[9]. On retrouve ici l'idée selon laquelle la valeur de chaque chose est nécessairement marchande, serait le fruit d'un équilibre entre offre et demande pour cette chose, et donc dépendrait directement de sa rareté. Il suit naturellement de ce raisonnement que l'inflation, c'est-à-dire la dévaluation du pouvoir d'achat d'un montant donné de monnaie, ne peut être dû qu'à une augmentation de la quantité de monnaie, rendant celle-ci moins rare. Ce lien de cause à effet mécanique entre création monétaire et inflation est évidemment faux, mais il persiste dans les théories économiques classiques, les plus à droite politiquement[10].

Enfin, on notera à propos du minage que quand on parle de chaînes de blocs, le terme de « mineurs » se réfère aux personnes qui possèdent les machines et perçoivent la valeur générée par le « minage », ce qui introduit une confusion entre travailleurs et capitalistes. Ce n'est d'ailleurs pas le seul terme qui introduit de la confusion.

Consensus ?

Comme on l'a vu dans la section sur l'unicité du registre, la notion de « consensus » des chaînes de blocs est très éloignée de celle du langage courant, le « consensus » se faisant 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. Ce qui est appelé

---

8 En anglais dans le texte (cf note 5) : « *The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation.* ».

9 En anglais dans le texte (cf note 5) : « *Once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free.* ».

10 Voir également cet entretien avec les économistes Marlène Benquet et Théo Bourgeron : « *Chez Eric Zemmour, on retrouve la connexion entre l'extrême droite et les cryptomonnaies* », Alternatives économiques, 2022.

« atteindre le consensus » dans le contexte des chaînes de blocs est donc en réalité une mise en concurrence généralisée.

La confusion introduite par le terme de « consensus » est largement utilisée dans les discours de propagande favorable aux cryptomonnaies et aux chaînes de blocs, et participe à légitimer le recours à cette technologie pour des usages pour lesquels elle est pourtant inadaptée, comme le vote électronique.

Technique et politique des chaînes de blocs

Au niveau technique, deux aspects indépassables du fonctionnement d'une chaîne de blocs participent au caractère réactionnaire de cette technologie : l'un sur la question écologique, et l'autre sur la question démocratique. Avant de nous pencher sur ces deux questions, il est important d'expliquer pourquoi, à l'exception des « cryptomonnaies » pour lesquelles la technologie a été conçue, l'intégralité des projets basés sur des chaînes de blocs ne peuvent justifier techniquement le choix de recourir à cette technologie.

Inutilité technique

En effet, contrairement à ce qui est systématiquement prétendu, une chaîne de blocs ne peut apporter aucune garantie de sécurité, et ce pour une raison simple : en règle générale, ce qui est écrit sur une chaîne de blocs n'a aucune valeur de vérité dans le monde réel, si ce n'est pas appliqué/imposé par une autorité tierce. Exactement de la même manière que le contenu d'un contrat n'a de valeur que tant que l'ensemble des parties l'ayant signé restent d'accord avec, ou qu'il existe une autorité tierce qui a la capacité de contraindre les parties récalcitrantes à l'honorer. Cette pensée magique s'explique par une confusion sur la nature de l'écriture dans une chaîne de blocs. Effectivement, dans son usage premier, qui concerne les transactions d'une « cryptomonnaie », elle est *performative* : puisqu'il ne s'agit que de jeux d'écriture, lié à rien dans la vraie vie, une transaction existe et a bien eu lieu *parce qu*'elle est consignée dans le registre. La chaîne de blocs servant donc dans ce cas de définition de la réalité, on peut considérer qu'elle « garantit » ce qui y est consigné. Mais dès qu'il s'agit d'apporter la moindre garantie sur des phénomènes extérieurs à la chaîne de blocs, cela ne fonctionne plus. Pour tous les autres usages, des tiers de confiance sont donc nécessaires, ce qui brise immédiatement l'hypothèse de défiance généralisée qui est un présupposé essentiel à l'utilité d'une chaîne de blocs. Sauf, bien sûr, quand l'objectif réel est de dénigrer politiquement les tiers de confiance en question, comme c'est le cas avec les nombreux projets de diplômes sur chaîne de blocs dont l'objectif politique est de saper la confiance dans les universités publiques (qui donne pourtant leur valeur aux diplômes)[11].

Surcoût écocide

Écologiquement, recourir à une chaîne de blocs alors qu'on peut techniquement s'en passer est irresponsable, et cela indépendamment de si le « minage » utilise la preuve de travail (bien que ce soit évidemment bien pire quand c'est le cas). En effet, par nature, une chaîne de blocs ne stocke que les opérations de modification du système qu'elle représente, et non son état. Par exemple pour une « cryptomonnaie », on y écrit seulement les transactions, et non qui possède quels jetons ou encore les soldes des comptes. L'état du système peut être recalculé à partir du registre, mais il serait tellement coûteux et inefficace de le recalculer à chaque fois qu'il doit en réalité être

11 Voir par exemple Arnaud Levy, « Pour les solutions low tech, contre les blockchains inutiles », 2023.

maintenu par ailleurs. Pour vérifier qu'une transaction est valide il faut entre autres s'assurer que son émetteur est bien en possession des jetons concernés, et cela nécessite d'avoir quelque part la liste à jour des jetons possédés par l'émetteur, dans un format rapide et facile à interroger, c'est-à-dire une base de données « classique ». Évidemment, cette base de données doit exister et être tenue à jour chez chaque participant indépendamment (sinon on se retrouve avec une autorité centrale qui nécessite de la confiance). En fait, quand on fait le choix d'utiliser une chaîne de blocs, ce n'est jamais *en remplacement*, mais toujours *en supplément* (et démultiplié par le nombre de participants) de l'alternative qui pourrait avoir été choisie directement à la place.

Élitisme antidémocratique

Il est extrêmement courant de voir les chaînes de blocs défendues comme alternative à des systèmes centralisés perçus comme autoritaires. Il faut d'abord remarquer que, si l'on sort de l'état d'esprit ultra-individualiste et qu'on accepte la possibilité de confiance sociale, même un système centralisé peut être démocratiquement contrôlé. Ensuite, il est à noter que la présentation de cette alternative est une fausse dichotomie : il est tout à fait possible de concevoir des systèmes entre les deux extrêmes que sont le pur centralisé et le pur pair-à-pair, comme les systèmes fédérés par exemple[12].

La décentralisation totale promue dans les discours favorables aux chaînes de blocs porte en elle un élitisme forcené et antidémocratique : pour être mise en place, elle nécessite que chaque participant non seulement appréhende des notions complexes de cryptographie asymétrique mais aussi qu'il soit en mesure de conserver et protéger ses clés cryptographiques de manière parfaitement sécurisée (ce qui est notoirement difficile), et qu'il les utilise sans aucune erreur de manipulation, celles-ci étant définitives et irréparables par conception (puisque la chaîne de bloc est immuable). Ces inconvénients sont acceptés voire présentés comme désirables par les défenseurs des chaînes de blocs, car c'est aussi ce qui permet d'empêcher techniquement toute possibilité de régulation ou de mises en œuvre de décisions collectives (typiquement, pour se soustraire à l'impôt), perçues comme des enfreintes à une liberté individuelle qui se veut absolue.

Cette exigence démocratiquement indésirable est en effet techniquement nécessaire pour bénéficier des avantages que sont censés procurer les chaînes de blocs (notamment en ce qui concerne l'absence de confiance). Pourtant, cette même exigence est en pratique parfaitement irréaliste : même dans le cas des « cryptomonnaies », seul cas d'usage où l'écriture dans le registre est performative et qui permettrait en théorie de se passer de tiers de confiance, ce n'est dans les faits pas comme ça que les chaînes de blocs sont utilisées. Au contraire, la quasi-intégralité des transactions en « cryptomonnaies » sont effectuées depuis des plateformes d'échanges, ces places de marché des « cryptomonnaies » plus-ou-moins régulées mais en tout cas centralisées, qui peuvent offrir une interface simplifiée à leurs utilisateurs en hébergeant et en contrôlant à leur place leur « portefeuille », c'est-à-dire leurs clés cryptographiques censément privées… Ces plateformes jouent un rôle de tiers de confiance indispensable en pratique, alors que la technologie est justifiée par l'idée de s'en passer. Cette contradiction technique n'empêche pas les défenseurs des chaînes de blocs et des « cryptomonnaies » de revendiquer les aspects théoriques pourtant inexistants dans la pratique, ce qui montre que la pseudo-technicité de leurs discours n'est qu'une façade pour leur propagande idéologique.

---

12 Par exemple, le protocole SMTP permet l'échange de courrier électronique entre n'importe quels serveurs : on n'est pas obligé d'avoir un compte chez Google pour échanger avec un utilisateur de Gmail, sans pour autant qu'il soit nécessaire que chacun soit capable de gérer son propre serveur de courrier électronique. De même, le protocole SEPA permet d'effectuer des transferts bancaires entre comptes hébergés chez différentes banques.

Conclusion

Dans cet article, nous avons vu que la technologie de la chaîne de blocs est ancrée très à droite politiquement, autant dans les présupposés qui ont guidé sa conception (ultra-individualisme, défiance généralisée, métallisme) que dans le fonctionnement technique qui en découle (nécessité fonctionnelle de la spéculation, surcoût systématique écocide, élitisme antidémocratique). Nous avons également démontré l'inutilité de cette technologie en dehors de ce pourquoi elle a été initialement conçue, les « cryptomonnaies », qui ne sont rien d'autre que des actifs numériques purement spéculatifs dont on peut également contester l'utilité sociale[13]. Son utilisation pourtant répandue en dehors de cet usage s'explique alors en partie par un effet de mode technosolutionniste auquel s'ajoute une confusion, entretenue entre autres par le vocabulaire employé, sur les réelles capacités techniques offertes par cette technologie. Finalement, sa raison d'être semble surtout tenir de son utilisation comme véhicule de banalisation et de propagation des idéaux libertariens qu'elle prend comme hypothèse de fonctionnement et qu'elle impose donc comme cadre de pensée. L'extrême droite ne s'y trompe d'ailleurs pas, et se saisit déjà pleinement de cette opportunité comme l'ont montré plusieurs enquêtes récentes[14,15,16,17,18]. Bref, la chaîne de blocs est une technologie réactionnaire.

13 À ce sujet, lire Nastasia Hadjadji, *No crypto, comment Bitcoin a envoûté la planète*, Quimperlé, Ed. Divergences, 2023 (en particulier les chapitres 3 et 5).

14 Nastasia Hadjadji, « Libertariens et plus si affinités ? Chez les patrons français de la crypto, la tentation de l'extrême droite », Observatoire des multinationales, 2025.

15 Nastasia Hadjadji, « « La France est un Socialistan » : sur YouTube, la sphère crypto française ouvre grand les portes à l'extrême droite », Observatoire des multinationales, 2025.

16 Olivier Petitjean, « Molly White : « Le secteur des cryptomonnaies est une composante majeure du mouvement techno-fasciste » », Observatoire des multinationales, 2025.

17 Alexandre Berteau et Youmni Kezzouf, « Cryptomonnaies : l'extrême droite française laisse libre cours à sa nouvelle manie », Mediapart, 2025.

18 Nastasia Hadjadji, « Comment Sarah Knafo s'appuie sur la crypto pour « trumpiser » l'extrême droite française », Observatoire des multinationales, 2026.