Alyra - Consultant Blockchain

LES "CINQ PILIERS DE LA BLOCKCHAIN", UNE EXTRAPOLATION ÉCLAIRANTE

Bastien Ebalard

Introduction

Nous allons dans cette partie tenter, à partir de la présentation que fait Andreas Antonopoulos des 5 piliers de la blockchain, de vous proposer une extrapolation libre réalisée par nos soins, dont nous avons l'espoir qu'elle soit aussi structurante qu'éclairante pour vous, nos apprenantes et apprenants.

Lorsque l'on parle des 5 piliers de la blockchain, entendez bien qu'il s'agit ici d'une tentative de cadrage de la part de cette éminence et non d'une définition figée : c'est un travail d'exploration et de théorisation scientifique majeure, mais ce n'est pas une qualification juridique.

Voici donc ces fameux cinq piliers :

1. **Open**
2. **public**
3. **neutral**
4. **borderless**
5. **censorship resistant**

Andreas Antonopoulos reste avant tout un chercheur et ne se prend pas pour un prophète, contrairement à certains comme Roger Ver ou Dr. Craig S. Wright, que vous pouvez aller chercher sur le net et qui s'apparentent plus à des gurus qu'à des éclaireurs. Il n'est en aucun cas dogmatique et si pour lui une blockchain est par essence publique, il conçoit bien entendu qu'il puisse y avoir une gradation du degré de (dé)centralisation, mais sans que cela ne vienne remettre en cause l'existence des 5 piliers.

Une dernière chose en forme de pointe d'humour : sachez que pour Andreas Antonopoulos, toute blockchain qui ne répondrait pas favorablement aux cinq critères qu'il cite comme piliers de la blockchain, ne représente qu'une seule chose : du « bullshit » et rien d'autre ! Nous vous laissons le soin de traduire, et d'en tirer vos propres conclusions…

Pour une présentation détaillée de cette qualification peu valorisante, voir ici la passionante conférence « Blockchain vs. Bullshit: Thoughts on the Future of Money » : https://www.youtube.com/watch?v=SMEOKDVXlUo

A. Être ouverte (le pilier « open »)

- **L'ouverture aux utilisateurs**

Cela signifie que tout le monde peut accéder à la Blockchain, sans aucune forme de vérification de qualification (niveau d'études, compétences particulières), de statut (économique, social) d'origine (sociale, ethnique) ou d'identité (ethnique, culturelle, genrée). Il n'y a donc personne qui vérifie les informations vous concernant, personne qui puisse vous « filtrer », que ce soit à l'entrée ou à la sortie du « ledger », le nom générique que l'on donne à un réseau blockchain particulier.

Osons une analogie musicologique éclairante : Nous sommes en 2019 et vous êtes à BitStock, le Woodstock de la Blockchain. C'est un lieu aux règles « hors-norme » et ce, dans tous les sens du terme : hors norme dans le sens de « hors des normes établies » et hors norme dans le sens de « avec peu ou pas de norme », un peu comme un Woodstock qui posait de nouvelles règles morales en opposition avec les valeurs conservatrices de la société américaine d'alors (le « hors des normes établies ») et qui en même temps se proposait d'abolir le maximum de normes, quelle que soit leur nature ou leur objet (le « avec peu ou pas de normes »). Vous êtes donc en cet endroit aux règles différentes et vous vous y sentez bien, car vous êtes libres. Vous n'êtes pas dans la file d'attente d'une sombre boîte de nuit sous-dimensionnée à attendre qu'un homme en noir vous autorise ou non à pénétrer le

temple noctambule, vous êtes au cœur d'un Woodstock éternel, au sein duquel vous pouvez évoluer en toute liberté tant que vous respectez autrui et les règles de la vie en communauté. Le consensus moral rejoint ici le consensus informatique : pas de chef, pas de structure pyramidale, mais un ordre public à maintenir et des règles de vie en communauté que tout le monde doit respecter. Si elles ne sont pas respectées, c'est la division qui guette : les « chain splits » que l'on nomme soft et hard forks en fonction de leur nature et qui cassent le pacte moral qui liaient tous les festivaliers entre eux. Nous étudierons tout cela prochainement.

Pour le moment, retenez simplement deux choses :

- À tout moment, vous êtes libre de quitter le festival, mais vous pouvez y revenir quand vous voulez, sans jamais avoir à présenter de ticket. D'ailleurs, il n'y a pas de police ni de portiques, mais vous êtes en totale sécurité. C'est cette sécurité totale qui aux profanes de la blockchain semble « magique » et qui n'en a rien

- Au sein du festival Bitstock, Bitcoin ne s'est jamais arrêté, il dure depuis maintenant plus de 10 ans et sa scène ne s'est jamais tue :il a su faire face aux orages et autres intempéries ainsi qu'à la concurrence des autres festivals. Bien sûr, certains artistes n'étaient plus d'accord avec la programmation (oui, c'est un jeu de mots) et ont fini par créer leur propre dérivé en reprenant ce qui avait fait le succès de Bitcoin. On a vu fleurir des « Bitcoin cash », des « Bitcoin SV » ou des « Bitcoin ABC » mais aucun n'a jamais réussi à supplanter ou même atteindre le niveau du célèbre Bitcoin. Souvent copié, jamais égalé, voilà pourquoi Bitcoin est si important à évoquer lorsque l'on discute de blockchain, au-delà même du fait qu'il fut le premier représentant d'une espèce désormais en pleine expansion.

Cette analogie festivalière n'a pas pour but de pousser à la consommation de psychotropes mais de vous faire comprendre que vous êtes tout à la fois libre de participer ou de ne pas participer à un réseau blockchain. Plus étonnant encore, vous êtes également libre de le quitter et d'y revenir quand bon vous semble. Pourquoi ? parce que Bitcoin et les autres blockchains publiques ont éradiqué un élément devenu fondamental à toute procédure d'inscription à un service en ligne : le KYC (pour Know Your Customer), qui est d'ailleurs souvent accompagné de son comparse AML (Anti Money Laundering).

- **Le KYC/AML, qu'est-ce que c'est ?**

De manière schématique et assez basique, le KYC, pour « Know Your Customer » soit « connaissez votre client », et l'AML, pour « Anti Money Laundering » soit « politique anti-blanchiment », c'est à peu près la combinaison des questions qui suivent :

Qui êtes-vous ?
Où habitez-vous ?
Que faites-vous avec votre argent ?
D'où vient votre argent ?
Et toute autre question que votre banque, votre FAI, votre administration, et n'importe quel service en ligne peut vous demander, sans que l'on ne sache vraiment comment ni pourquoi.

- **L’ouverture aux participants**

Ce qui est particulièrement intéressant avec le caractère « ouvert » de la blockchain, c’est qu’il revêt une autre dimension que la seule **libre entrée et sortie** du réseau en tant que **participant**. Il offre cette même possibilité en tant que **programmeur** ou **développeur**. Quand on vous disait que ce festival était extraordinaire et hors-norme au sens propre, on ne vous mentait pas. « Bienvenue à Bitstock, le seul endroit au monde où les festivaliers prennent le contrôle de la programmation ! Ici, le festival, c’est vous ! » pourrait être le slogan de cette grande fête cryptographique.

Nous dépassons en effet ici le seul cadre de l’utilisateur du réseau pour celui, plus large, du participant au réseau. Comme leurs noms respectifs l’indiquent, **un utilisateur utilise et un participant participe**. Ce n’est pas exactement la même chose, vous en conviendrez, et la différence tient au degré d’engagement (et en aucun cas d’adhésion, précision importante) de l’individu ou entité dont il est question. Cette possibilité laissée à tout utilisateur du réseau (tout « nœud » connecté au réseau donc vous, moi, elle et lui) est absolument **révolutionnaire et méritocratique (voir explications ci-après)**, car elle abolie une constante dans l’histoire de l’organisation sociale des sociétés humaines en même temps qu’elle ouvre des perspectives d’un monde tout simplement plus intelligent, plus juste et plus efficace.

L’heureux festivalier de Bitstock est donc non seulement autorisé à **ACCEDER** à la plateforme mais aussi autorisé à **MODIFIER** la plateforme. C’est la première fois dans l’histoire de l’humanité que nous nous trouvons en présence d’un mode organisationnel du travail qui puisse réellement faire émerger l’intelligence collective, ce graal que tous les passionnés de la connaissance ou presque souhaitent, du plus profond de leur être.

C’est une véritable révolution, en ce qu’il est aujourd’hui impossible de prendre une application ou un service internet aussi répandu et utilisé que Bitcoin et d’y proposer des modifications (du code, du protocole, des règles en général) qui pourront ou non être acceptées par les utilisateurs dudit service ou de ladite application selon des règles préétablies (consensus) et contre lesquelles les initiateurs du projet ne peuvent rien. Cela n’existe tout simplement pas encore, mais la blockchain permet de le concevoir. C’est un véritable renversement de la logique d’innovation, qui passe d’une émanation interne (les modifications/améliorations du service, de l’application ou de la plateforme sont le fait des ingénieurs et développeurs salariés de l’entreprise) à une émulation globale passant par l’ouverture à l’innovation venant de l’extérieur. Vous savez comment cela s’appelle ? L’intelligence collective.

- **Un mode d'organisation du travail révolutionnaire et abolitionniste**

Pourquoi ? Parce que la blockchain met fin à la verticalité et à la centralisation de nos organisations. Que ce soit concernant la société dans son ensemble avec le système de votation représentatif (élections d'intermédiaires ou délégués démocratiques) ou au sein des entreprises avec la pyramide des « N+ » (nomination d'intermédiaires professionnels), la plupart de nos processus organisationnels sont basés sur l'idée qu'il doit y avoir hiérarchie entre personnes pour que l'ensemble (composé de ces personnes) fonctionne de manière cohérente et efficace.

Le mode d'organisation que propose la blockchain nous apprend que non, que tout ceci est fondé sur -une fois n'est pas coutume- une croyance. Cette croyance est le fruit de siècle voire de millénaires d'Histoire et nous ne pouvons en détailler les rouages et le développement, mais sachez simplement que, tout comme la valeur que l'on finit par croire attachée à un bout de papier appelé arbitrairement billet de banque, on finit par penser que seule un mode d'organisation précisément et méthodiquement hiérarchisé est valable pour faire progresser notre espèce. Or, organiser et structurer ne signifient pas invariablement hiérarchiser.

- **La promotion d'un processus méritocratique et démocratique**

Pourquoi ? Parce que la blockchain n'est pas qu'une « simple » remise en cause de la verticalité et ne fait pas la promotion d'un mode d'organisation horizontal dans la seule perspective d'un monde plus juste ou plus fraternel, mais qu'elle promeut les meilleurs d'entre nous. En d'autres termes, elle est un outil de la méritocratie, voire, pour certains, l'expression de la méritocratie elle-même. Ceci est loin d'être une formule incantatoire : au festival de la blockchain, on peut être à la fois chanteur, musicien, producteur, ingénieur du son ou simple spectateur. Il n'y a aucune limite si ce n'est celle conjuguée de la compétence et de la démocratie.

- **La méritocratie**

La compétence car pour pouvoir travailler à l'amélioration du protocole Bitcoin par exemple, il faut pouvoir être reconnu pour la qualité de son travail par ses pairs, les développeurs. Pour ce faire, il faut apporter des preuves tangibles de son savoir-faire, comme par exemple la publication du code (ou de briques de code) d'un logiciel en open source sur Github (https://github.com), la plateforme préférée des développeurs, ou en démontrant sa connaissance informatique sur le forum préféré de la communauté geek, Reddit (https://www.reddit.com).

- **La démocratie**

La démocratie car la seule compétence ne suffit pas et qu'il faut pouvoir remporter l'adhésion non seulement de ses pairs (les développeurs) mais également de la communauté toute entière (les utilisateurs du réseau, particuliers comme entreprises). Dans la blockchain, on appelle ces groupes de développeurs des « clients ». L'un des groupes de développeurs les plus reconnus et les plus plébiscités pour son travail sur le protocole Bitcoin est celui de **Bitcoin Core** (https://bitcoin.org/fr/wallets/desktop/windows/bitcoincore/) qui est de loin le plus apprécié et le plus reconnu par la communauté pour la qualité de son travail.

Il n'est cependant pas le seul puisque d'autres groupes proposent d'autres fonctionnalités spécifiques, tels que :

- **Armory** (https://bitcoin.org/fr/wallets/desktop/windows/armory/), qui propose un wallet connecté à un noeuds complet (donc un client "complet") construit en langage Python permettant de stocker des bitcoins "à froid" sans avoir besoin d'être connecté au réseau
- **Electrum** (https://bitcoin.org/fr/wallets/desktop/windows/electrum/), qui propose un wallet en tant que client "léger", c'est à dire qu'il ne télécharge pas une copie intégrale de la blockchain mais une version allégée (voir le chapitre de ce bloc intitulé *" Un mode d'organisation décentralisé : des nœuds (nodes) pour remplacer les serveurs centralisés").*

N'oubliez jamais que le code source d'une blockchain publique, telle que Bitcoin ou Ethereum, est et sera toujours public. En quelques sortes, on pourrait assimiler ces blockchains à des logiciels, ou disons du software (par opposition au hardware) open source, car toute contribution, quelle qu'elle soit et de quelque développeur que ce soit, sera toujours la bienvenue. Elle devra simplement être acceptée par la « communauté » en fonction des règles de consensus qui ont été établies….par la communauté….dans le code source. La boucle est bouclée.

- **La méthode de consensus ou le mode de scrutin de la blockchain**

L'aspect démocratique réside dans le fait que tout changement, toute modification au protocole proposée par un des clients doit être acceptée par la majorité des **nœuds du réseau** avant d'être implémentée et, dans le cas de Bitcoin, obtenir en sa faveur un certain pourcentage de la puissance de calcul totale des ordinateurs connectés au réseau. Mais pour d'autres blockchains, d'autres principes de calcul peuvent être appliqués, il n'y a aucune vérité absolue dans ce domaine, simplement des tentatives de concilier au mieux deux aspects absolument essentiels de la blockchain : la décentralisation et la sécurité. Toute la difficulté pour les concepteurs d'une blockchain réside dans le fait que ces deux aspects sont généralement inversement corrélés Ces règles de vote et de gouvernance sont matérialisées par ce qu'on appelle « la méthode de consensus », qui n'est autre que le plus petit dénominateur commun de normes à respecter pour faire partie du réseau. Suivant le type de blockchain considéré, la méthode de consensus ne sera pas la même et la méthode de gouvernance sera donc différente d'une blockchain à l'autre. Deux exemples de consensus emblématiques dont nous détaillons plus loin le fonctionnement :

- **Le consensus Proof of Work (PoW)** majoritairement utilisé dans les blockchains publiques. Ces dernières sont qualifiées de **« permissionless »,** soit « sans permission », ce qui signifie qu'il n'y a aucune permission à demander pour faire partie du réseau. Elles sont donc **ouvertes à tous.**

- **Le consensus Proof of Stake (PoS)** largement popularisé chez les blockchains privées. Ces dernières sont qualifiées de **« permissionned »,** soit « avec permission », ce qui

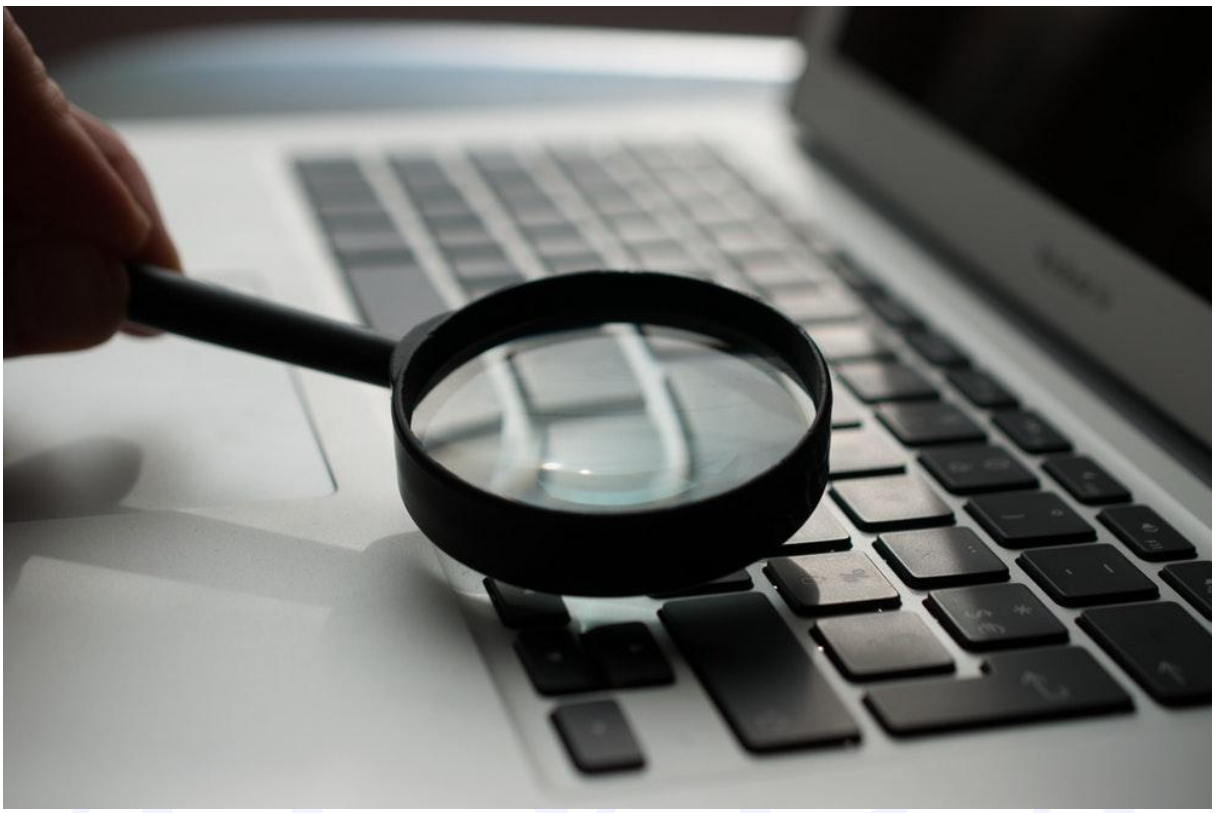
signifie qu'il y a des critères à remplir pour être être autorisé à rejoindre le réseau. Elles ne sont donc **pas ouvertes à tous.**

Voici un article un peu technique mais fort intéressant sur le sujet et…en français et libre accès :
https://medium.com/@godefroy.galas/analyse-et-comparaison-des-mécanismes-de-consensus-dans-la-blockchain-f91aee511ea3

Pour le moment, retenez simplement que la méthode de consensus choisie révèlera des choix de gouvernance tels que le degré d'ouverture, de transparence ou de décentralisation souhaité par ses créateurs. Cela équivaut peu ou prou au mode de scrutin dans le champ politique, qui a lui aussi des incidences majeures sur la manière de comptabiliser les voix et la méthode de gouvernance qui en découle. En Allemagne par exemple, le scrutin proportionnel est privilégié autant que possible, tandis qu'en France, on privilégie le suffrage universel uninominal majoritaire à un tour, c'est-à-dire que celui ou celle qui obtient 51% des votes remporte l'ensemble de suffrages, ce qu'on appelle la « prime » majoritaire.

Comparaison n'est pas raison…mais aide souvent à la compréhension ! Nous pourrions ainsi nous amuser à rapprocher la méthode allemande du consensus PoW et la méthode française du consensus PoS. Voir à cet effet ici https://fr.wikipedia.org/wiki/Scrutin_uninominal_majoritaire_à_un_tour et ici http://www.lemondepolitique.fr/cours/droit/droit-constitutionnel/droit-constitutionnel-general/peuple-souverain/scrutins pour le mode de scrutin uninominal majoritaire à un tour et ici pour son équivalent dans la blockchain bitcoin https://bitcoinmagazine.com/articles/why-some-changes-to-bitcoin-require-consensus-bitcoin-s-layers-1456512578.

B. Être publique (le pilier « public »)



- **Une information exhaustive, vérifiable par tous**

Il s'agit d'un caractère essentiel de la blockchain : celui de pouvoir **VERIFIER** ou, autrement dit, le pouvoir d'**AUDITER**. L'un des aspects principaux de cette technologie réside effectivement dans le fait que toute information ayant circulé au travers de la blockchain et/ou étant stockée dans cette dernière (une transaction au sein d'un bloc, un bloc au sein d'une chaîne de blocs, pensez aux poupées russes comme mode de représentation mental) est vérifiable.

Qu'est ce qui est vérifiable et par qui ? **TOUT et PAR TOUS**. Vous commencez à vous y habituer, mais il y a effectivement un caractère absolu à la transparence et à la sécurité, qui peut parfois nous dérouter de prime abord, tant cela est rare aujourd'hui : tous nos systèmes d'information (SI) sont en effet modifiables, attaquables, hackables, corruptibles. Tout cela à la fois. Et tous sans exception…sauf à évoquer la blockchain.

Imaginez à quel point cela est révolutionnaire : la possibilité laissée à chacun de chercher, trouver et vérifier l'existence et la véracité de telle ou telle information de manière systématique, certaine et absolue. Sans jamais et nulle part la possibilité de se tromper ou que cette information puisse avoir été corrompue. C'est la première fois dans l'histoire de l'humanité que cela est possible. C'est pour cela que nous, membres de la communauté blockchain, n'avons aucun doute quant à son potentiel copernicien ou disruptif (nous ne sommes pas sectaires).

Nous insistons réellement sur ce point : aucune organisation, aucune entreprise, aucun État n'est jamais parvenu à établir un protocole de communication et de stockage informationnel qui soit incorruptible par essence. Et encore, nous n'évoquons même pas le fait que tout cela se fasse de manière…automatique. Vous commencez peut-être mieux à comprendre pourquoi les banques, les assurances et autres actuaires, bref, tous les métiers d'intermédiation en général, hurlent au scandale. En réalité, ils ont compris que le loup était dans la bergerie, et ils tentent par tous les moyens de retenir leurs moutons qui, comme chacun le sait, ont tendance à être à la fois peureux et mimétiques…

Ne vous méprenez pas, en blockchain, lorsque l'on part **de valeur, de données et de transactions,** nous ne limitons pas à son acception financière. Il est indéniable que la blockchain Bitcoin est de loin la plus importante (en termes de valorisation capitalistique, la communauté privilégiant le terme de « market cap », Bitcoin oscillant entre 40 et 80% environ, voirt graphique ci-après) et la plus utilisée (en termes de nombre de nœuds connectés comme de nombre de transactions traitées), mais la technologie blockchain va bien au-delà de Bitcoin et permet d'échanger de la valeur sous toutes ses formes. En témoigne l'existence d'Ethereum, deuxième blockchain par market cap (voir graph ci-après) et qui permet d'éditer des « smart contracts » (« contrats intelligents » en français), assimilables à des programmes informatiques contractuels auto-exécutants sur blockchain et se déclenchant à la manière d'une fonction « SI ». Nous étudierons le fonctionnement plus en détail au cours de la semaine 6).

Aujourd'hui, une transaction blockchain n'est plus limitée à un échange financier, mais peut prendre la forme d'un document notarié, d'une fiche médicamenteuse ou d'un diplôme d'université. A terme, tout, ou presque, devrait pouvoir s'échanger sur la blockchain. Vraiment tout ? Oui, vraiment tout, à compter du moment où cette valeur est de nature numérique ET/OU peut être traduit/illustrée/représentée de manière numérique. Il n'est en effet pas nécessaire de détenir l'objet en lui-même sur la blockchain, une simple traduction ou preuve cryptographique suffisant.

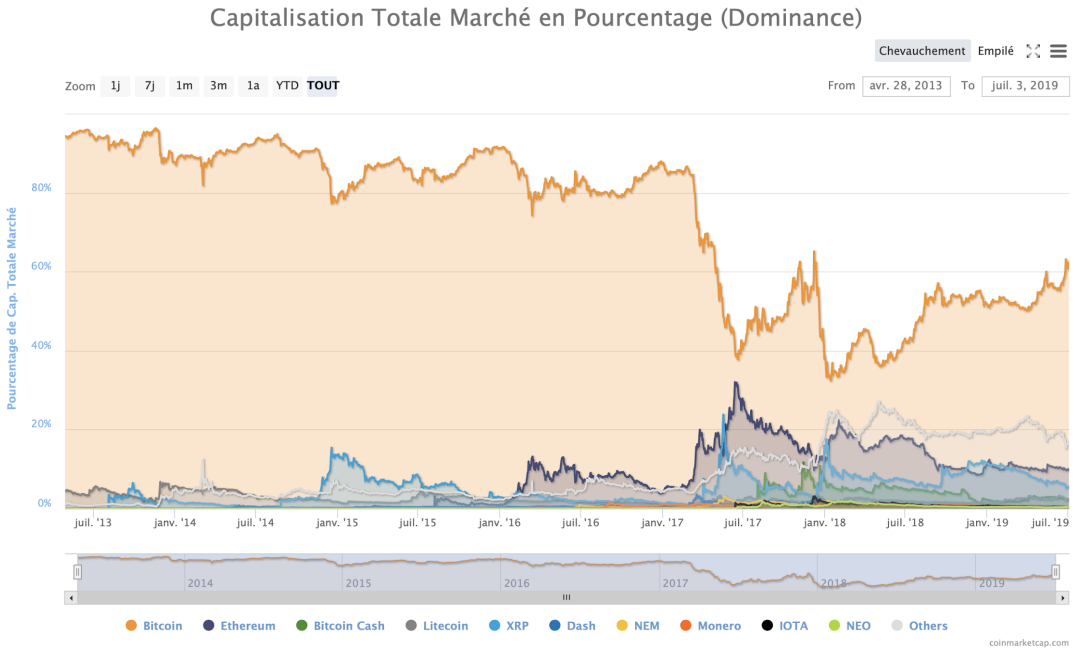
Enfin, sachez que ce **mode de lecture et d'écriture en accès libre et totalement transparent** laisse entrevoir de fantastiques possibilités organisationnelles, qui passeraient presque pour incongrus tant elles sont inédites en leur contours. Il s'agit **d'organisations de travail collaboratives** pensées sur un **mode décentralisé**. Ce qui sera peut-être une réalité demain est encore difficilement pensable aujourd'hui en termes business, car cela n'a tout simplement pas d'équivalent dans l'histoire du monde marchand. Autant il existe des structures associatives fonctionnant (plus ou moins) bien sur une base décentralisée, autant il n'y a pas d'exemple de structures profitables (au sens marchand) qui n'ait pas une forme de direction centralisée, que ce soit sous forme physique (headquarters ou siège) ou symbolique (cf les startups dites « nomades » mais qui sont en réalités régies par des principes pyramidaux). Ces formes d'organisation du travail répondent à l'acronyme barbare de **DAO**, pour **Decentralized Autonomous Organizations**, ou Organisations Autonomes Décentralisées, en français (cf. https://fr.wikipedia.org/wiki/Organisation_autonome_décentralisée et https://blockchainfrance.net/2016/05/12/qu-est-ce-qu-une-dao/).

Nous n'en sommes qu'aux prémices, mais avant même de penser à des entreprises passant à un modèle DAO, ce qui nécessiterait un travail d'adaptation et d'harmonisation des

législations nationales, nous pouvons d'ores et déjà imaginer des projets de recherche et/ou d'enseignement sur ce mode. Retenez cependant qu'à ce jour, le projet de DAO ayant le plus fait parler de lui l'a été pour de mauvaises raisons, puisque "*The DAO*" a tout simplement floué une grande partie de ses investisseurs, en raison d'une faille de sécurité dans le code source du projet ayant abouti au vol d'un tiers des fonds collectés...

- Pour le site de la fondation Ethereum, c'est par ici : https://www.ethereum.org

- Pour le site d'information en français sur la technologie Ethereum, c'est par là : https://www.ethereum-france.com



Pour les autres données concernant le market cap et toute autre agrégat de nature financière, un site particulièrement est à privilégier, dont est tiré le graphique sur la répartition de la capitalisation totale par pourcentage, ***CoinMarketCap***, que vous trouverez au lien suivant et qui est désormais également disponible en français : https://coinmarketcap.com/fr/

- ## L'intégrité de la donnée face au risque de manipulation humaine

Nous attirons votre attention sur un point particulier : lorsque nous écrivons que toute information, de quelque nature qu'elle soit, est vérifiable, nous entendons par là que l'information disponible dans la blockchain apporte la garantie absolue que c'est bien exactement, parfaitement et totalement cette information qui a été intégrée à la blockchain. Elle n'a donc pas pu être altérée et l'auditeur ou le vérificateur à l'assurance absolue que ce qu'il consulte est bien ce qu'il cherche. En revanche, et c'est là toute la subtilité, cela ne signifie en aucun cas que l'information elle-même soit juste, vraie ou véridique.

Pour l'écrire dans des termes plus familiers, **aucun doute ne peut subsister quant à la forme** de la donnée stockée, mais **le doute reste permis quant au fond** de ce qui est stocké. Prenons une analogie usuelle, pour plus de praticité : imaginons une blockchain non plus numérique mais transposée au monde physique, en l'occurrence, une blockchain de sacs à main. Un beau jour d'été 2011, un riche industriel chinois de la province de Schenzen fait l'acquisition d'un sac à main Louis Vuitton, non pas auprès de la marque elle-même ou d'un distributeur certifié, mais auprès d'un revendeur d'une boutique de luxe à Hong-Kong. Sept ans plus tard, par une pluvieuse nuit d'automne, ruiné, il souhaite vendre une partie des nombreux biens de luxe qu'il a accumulé au cours de ces 6 années.

Ne se rappelant pas de la totalité des montants, dates d'achat et autres variables du prix (la valeur d'échange longuement étudiée au cours de la première semaine du programme), il va donc aller vérifier ces éléments dans la….blockchain ! En rentrant sa clef publique et en en ouvrant l'accès grâce à sa clef privée (système de double clef vu précédemment), il va pouvoir accéder à l'historique de ses achats avec les fiches produit correspondantes. Il va donc trouver le sac LVMH dont il avait fait l'acquisition pour sa sœur ainsi que toutes les informations liées qui sont stockées dans la blockchain : taille, matière, prix, poids, couleur et bien d'autres choses encore. Il a, comme vous le savez maintenant, la certitude absolue que ces informations sont bien celles qui ont été intégrées à l'époque lorsqu'il a fait cet achat : une fois que la transaction a été « settled » via les mécanismes de consensus, les informations produit ont été automatiquement intégrés au sein de la transaction elle-même (principe de l'empreinte cryptographique, notamment), elle-même intégré à un bloc particulier, lui-même intégré à la chaîne correspondante.

Et c'est là qu'intervient le drame : notre (plus si) jeune entrepreneur ruiné voit apparaître un point d'exclamation cerné d'un triangle rouge et, lorsqu'il met son curseur en surbrillance, il laisse échapper un cri : l'autorité locale hongkongaise de lutte contre la fraude et la contrefaçon s'est aperçu que ce revendeur non certifié écoulait des articles de très bonne facture mais néanmoins contrefaits.

Cette petite histoire est là pour que vous reteniez que si la blockchain dispense bien d'avoir recours tiers pour établir la confiance dans la transaction et dans l'inaltérabilité des données stockées, elle ne résout pas tous les problèmes liés à la confiance. Il reste donc encore beaucoup de chemin à parcourir pour aboutir à un système économique où la confiance est établie de manière automatique et absolue en tout lieu et tout le temps.

Néanmoins, nous disposions d'ores et déjà de pistes pour parer aux défaillances humaines du système. Car c'est une autre précision importante : dans l'exemple que nous venons d'étudier, en aucun cas il ne s'agit d'une défaillance de la blockchain elle-même, mais bien d'une manipulation humaine intentionnelle, qui aurait de toute manière porté préjudice, blockchain ou pas.

Une des possibilités à l'étude aujourd'hui est celle des blockchains par secteur ou par filière. L'intérêt, c'est qu'il existe généralement des structures de gouvernance préexistantes sur lesquelles s'appuyer pour limiter les comportements frauduleux. Dans le cas de notre histoire, nous pourrions ainsi imaginer une blockchain de la filière du luxe, avec une blockchain qui se calerait sur la chaîne d'approvisionnement elle-même, retraçant toutes les étapes de la fabrication du cuir dans les tanneries jusqu'à la vente en boutique. Un

organisme de contrôle pourrait par ailleurs être chargé de vérifier régulièrement le respect des standards par les acteurs de la chaîne.

Plus simplement encore, si nous imaginons une blockchain, non plus du luxe, mais des grandes maisons du luxe, le problème de la contrefaçon est quasiment résolu, car cette fois, l'acheteur a la certitude absolue que non seulement les informations liées au sac et contenues dans la blockchain sont bien celles qui ont été entrées par les acteurs de la filière, mais il a également la garantie que son sac n'est pas un faux, puisque LVMH elle-même l'a certifié sur blockchain.

C. Être neutre (« le pilier neutral »)

Selon Andreas Antonopoulos, une blockchain digne de ce nom se doit d'être neutre. Mais neutre à l'égard de quoi et de qui exactement ? La réponse a le mérite d'être aussi limpide qu'incisive : **à l'égard de tout et de tous**. Dans la conception française de l'échange économique, de l'organisation sociale et des relations humaines en général, il est assez hardi d'imaginer cette neutralité, qui correspond plus à la conception anglo-saxonne du terme.

Il faut en fait partir du concept de la **liberté d'expression** et de sa déclinaison dans sa version latine comme dans sa version anglo-saxonne, car elles diffèrent largement. Disons que dans le premier cas (la version latine), il y a certaines exceptions à la liberté de parole ou de réunion, qui font dire à certains commentateurs outre-manche que nous avons une liberté d'expression conditionnée, et que ce que nous appelons exceptions sont en fait des

restrictions pures et simples à la liberté. Dans le deuxième cas en revanche (la version anglo-saxonne), nous sommes en présence d'une conception extensive de la liberté sous toutes ces formes dont, évidemment, la liberté d'expression. La thématique du « free speech » ou de la liberté de parole en français, est extrêmement importante : c'est bien pour cela que regroupements néo-nazis ou des rassemblements salafistes sont possibles au Royaume-Uni alors qu'ils ne le seraient jamais en France.

C'est de cette **neutralité extensive** dont il est question ici, lorsque Andreas Antonopoulos en fait mention en tant que l'un des « cinq piliers » de la blockchain. Bitcoin, ou toute autre blockchain publique, ne peut et ne doit avoir de goût, de préférence, d'appétence pour qui que ce soit ou quoi que ce soit. C'est d'ailleurs ce qui est au cœur des critiques de nombreux académiques lorsqu'ils s'emparent du sujet blockchain : Bitcoin serait la monnaie, pêle-mêle, du crime organisé et du terrorisme sous toutes leurs formes, ainsi que du blanchiment d'argent et des autres joyeusetés de ce type. Tout cela est évidemment faux, à la fois sur un plan théorique mais également pratique.

Il faut effectivement intégrer une bonne fois pour toutes que Bitcoin est un protocole et non un État ou une banque. Que voulons-nous vous dire par là ? Nous souhaitons simplement que vous compreniez que Bitcoin ne suit aucun agenda politique. Il a un but, certes, celui de remplacer le système financier actuel, délétère, corrompu et inefficace. Mais il est ironique de constater que nombre d'académiques imputent justement à Bitcoin un agenda *de facto*, puisqu'il serait la monnaie de tout ce qui se rapporte de près ou de loin au mal. Pourtant, c'est tout le contraire, Bitcoin n'a aucune préférence, mais aucune aversion non plus : il ne filtre pas, contrairement aux banques et aux États, via l'édiction de listes noires.

- **Bitcoin, une monnaie traçable et non anonyme**

Venons-en aux faits. Sur un plan théorique, vous devez assimiler que Bitcoin est une **cryptomonnaie pseudonyme et non anonyme**. Cette distinction est absolument fondamentale et ne semble pas être intégrée par les défenseurs du système bancaire, financier et monétaire actuel, qu'il s'agisse de banquiers d'affaires, de banquiers centraux, de hauts fonctionnaires du trésor ou de Bercy, et de toutes sortes de partisans de la

mondialisation heureuse. Il existe bien des **cryptomonnaies anonymes**, par défaut ou par fonctionnalité additionnelle (**Monéro par défaut** ou **Zcash par fonctionnalité** par exemple), dont on peut questionner le bien-fondé, mais ce n'est simplement pas le cas de Bitcoin. Nous sommes ici dans un programme d'apprentissage et non un meeting politique, il faut donc être honnête avec nos apprenants : il existe bien des moyens détournés pour tenter d'anonymiser une transaction Bitcoin, même si cela demeure expérimental et confidentiel. Pour preuve, une des méthodes utilisées à cet effet, CoinJoin, est détaillée ici : https://cryptoast.fr/coinjoin-melanger-bitcoins/. Cependant, vous devez garder en tête, comme nous vous l'avons expliqué, que pour pouvoir être implémentée au protocole, cette fonctionnalité doit être acceptée par consensus.

Soyons encore plus complets, et osons vous transmettre ce passionnant article publié sur Medium et donnant des moyens détournés, ou hors protocole, d'anonymiser au mieux son utilisation du réseau Bitcoin : https://medium.com/@rickytheghost1981/bitcoin-anonymity-guide-2019-how-to-use-btc-like-a-straight-up-g-e3bf55f680fa

En français, vous trouverez des informations pertinentes sur le sujet ici https://bitcoin.org/fr/proteger-votre-vie-privee et ici https://journalducoin.com/guides/anonymat/comment-acheter-bitcoin-anonyme/

Dans le cas de cryptomonnaies anonymes, le protocole sous-jacent fait en sorte qu'on ne puisse retracer la transaction en brouillant les pistes, à l'image de ce qui se fait avec l'utilisation d'un VPN sur le réseau Thor si l'on transpose le cas à internet. Une transaction Bitcoin, elle, est absolument et totalement traçable, c'est-à-dire que l'on peut connaître l'identifiant (soit la clef publique, qui n'est autre qu'une suite de caractères) de l'initiateur

comme du receveur de la transaction. Un individu ou une personne morale peut posséder plusieurs clefs publiques, certes, mais une clef publique, soit un identifiant, ne peut appartenir qu'à une seule personne et non à plusieurs. Bravo, vous venez de comprendre en quelques mots la différence entre une monnaie anonyme et une monnaie pseudonyme, vous venez donc de dépasser la vision (réelle, feinte ?) qu'en ont nombre d'académiques.

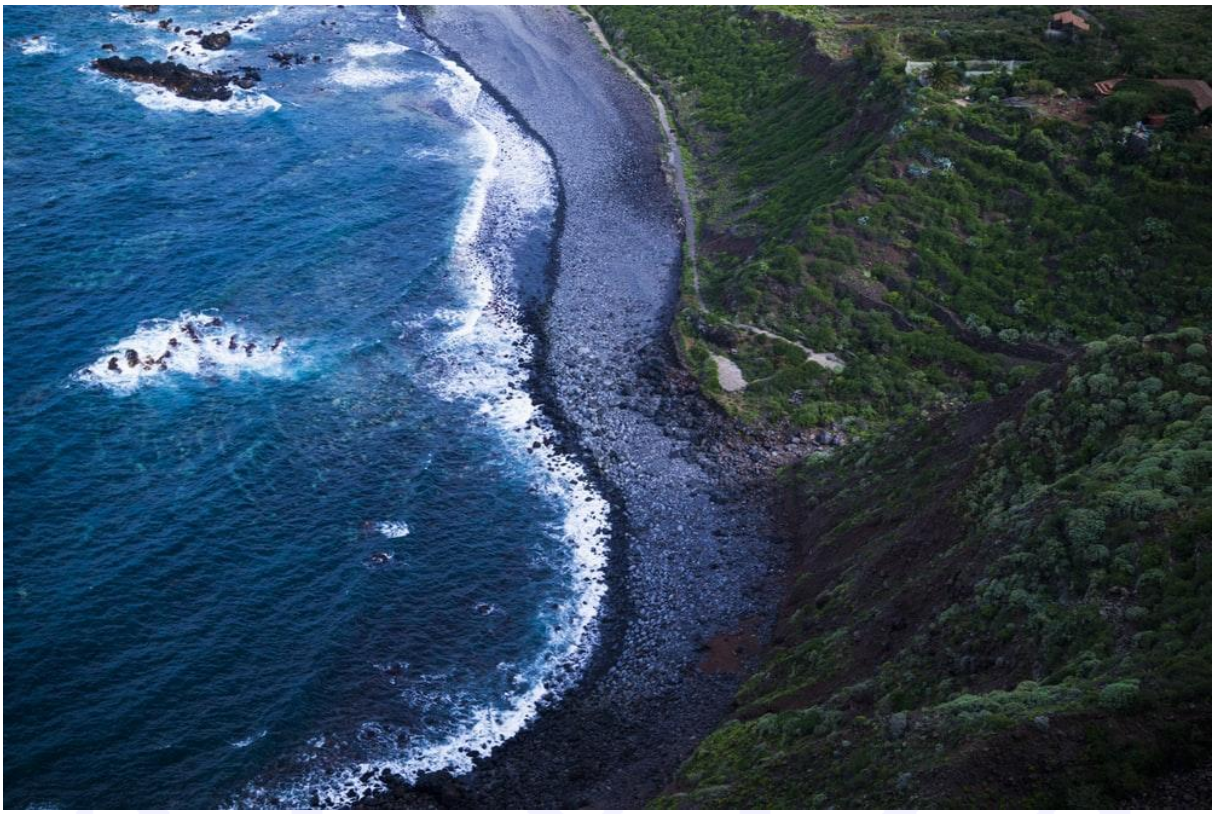
Sur le plan pratique, il est évidemment clair que ni Bitcoin ni aucune autre cryptomonnaie n'arrive à la cheville ni même à l'orteil des monnaies FIAT pour ce qui est du financement ou du blanchiment des activités illégales (voir le BLOC 1 pour la définition, l'historique et la critique de ces monnaies, celles que nous utilisons aujourd'hui). A cet effet, vous pouvez lire (en anglais) l'étude publiée conjointement par la Fondation pour la Défense de la Démocratie (FDD) et Elliptic et qui aboutit à la conclusion que moins d'1% du total des transactions Bitcoin sont liées au blanchiment d'argent, contrairement à une idée largement répandue et qui voudrait que ce soit la monnaie privilégiée des organisations criminelles transnationales. Vous trouverez cette étude dans son intégralité ici : https://www.fdd.org/analysis/2018/01/10/bitcoin-laundering-an-analysis-of-illicit-flows-into-digital-currency-services/

A titre de comparaison, prenons l'exemple d'une grande bande internationale respectable et largement présentes dans les aéroports du monde entier. Si nous savons depuis longtemps qu'HSBC a été créée à Hongkong, il y a un siècle et demi, par des commerçants écossais liés au trafic d'opium, nous savons peut-être moins qu'elle est aujourd'hui l'un des principaux financeurs du crime organisé. Si vous en avez le temps, nous vous conseillons très vivement de visionner le film documentaire *Les gangsters de la finance*, réalisé par les excellents Jérôme Fritel et Marc Roche et qui retrace l'histoire trouble de la banque. Au passage, ces deux réalisateurs de brio avaient également été à l'initiative du film *Goldman Sachs, la banque qui dirige le monde,* extraordinaire réquisitoire contre l'affairisme coupable de banquiers d'affaires déconnectés de l'économie réelle.

- Pour le premier, c'est par ici : https://www.arte.tv/fr/videos/069080-000-A/les-gangsters-de-la-finance/

- Pour le second, c'est par là : https://vimeo.com/134308032

D. Être sans frontière (le pilier « borderless »)



C’est peut-être le caractère le plus évident et le plus essentiel. La blockchain est une technologie « sans frontières », exactement comme Internet. La différence majeure avec Internet, c’est que ce caractère n’est pas aménageable, il n’est pas modifiable à la carte, selon les désidératas de telle ou telle entité. Nous en revenons, comme souvent avec la blockchain, à son caractère décentralisé. Car si Internet est aménageable, c’est parce qu’il est centralisé. Il n’y a pas d’autre explication. Si Internet fonctionnait sur une base décentralisée, comme cela avait été imaginé au départ, il ne serait pas aménageable dans son accès ou son contenu.

Le problème ici, c’est le principe de territorialité : un fournisseur d’accès, un moteur de recherche, un diffuseur de contenu etc. répondent tous positivement au principe de territorialité, car leurs serveurs sont localisés. Bien sûr, dans le cas de Google et d’autres services comparables, les serveurs ne sont pas tous regroupés au même endroit mais installés dans plusieurs endroits de la planète. Cela diminue les risques associés à la territorialité, mais ne les exclue pas. Il est bien entendu plus difficile pour un attaquant de mener une attaque par déni de service (https://fr.wikipedia.org/wiki/Attaque_par_déni_de_service) si les serveurs ne se trouvent pas tous exactement au même endroit, mais cela n’est pas impossible lorsque l’on dispose de moyens (financiers, techniques et humains) importants.

Une infrastructure blockchain, elle, est par nature décentralisée, et ne peut donc être mise en échec par une telle attaque. Tant qu’il restera un nœud connecté au réseau, elle ne cessera pas de fonctionner et ses données ne seront pas corrompues : bref, son intégrité

profonde ne sera pas affectée. Les nœuds du réseau recevant tous la même copie actualisée en temps réel de l'état de la blockchain, cibler une partie, même une grande partie des nœuds de manière coordonnée n'empêchera pas la blockchain de continuer à fonctionner. Vous savez comment cela s'appelle ? Une **technologie résiliente**. Et là aussi, il s'agit de quelque chose de totalement nouveau, pour vous comme pour vos organisations.
Il n'y a donc aucune frontière dans le monde décentralisé de la blockchain : elle (la blockchain) est partout et tout le temps à la fois, et sans que l'on s'en rende compte. Un peu comme l'air que l'on respire ? N'exagérons rien ☺. Ce que nous voulons dire par là, c'est que vous n'avez pas besoin d'emmener avec vous tout un matériel ou même le moindre support physique pour être en permanence connecté à la blockchain. A compter du moment où vous vous êtes identifié au moins une fois sur le réseau, vous y êtes connecté par défaut et en permanence. Pour cela, il suffit que vous disposiez d'un couple clef publique/clef privée, et que vous n'oubliez JAMAIS la clef privée qui associée à la clef publique, bien sûr, car elle n'est connue que de vous seul. En cas de perte, l'accès au compte est définitivement perdu. En revanche, il est possible de retrouver sa clef publique à partir de sa clef privée, et voici comment : https://journalducoin.com/bitcoin/comment-obtenir-adresse-cle-privee-bitcoin/

Pensez au couple clef publique/clef privée de la manière suivante : la clef publique est l'identifiant, la clef privée le mot de passe. Retenez-le. Sur Internet, votre identifiant peut être rendu publique sans que cela ne vous nuise, mais si vous faites de même avec votre mot de passe, bien chanceux serez-vous si les informations associées à votre identifiant (photos, emails, données bancaires…) ne sont pas dérobées dans l'heure. Soit ces données seront vendues sans que vous ne le sachiez, soit vous aurez le déplaisir de recevoir un email de chantage vous incitant, pour récupérer l'accès à votre compte, à payer une rançon…en cryptomonnaie. Voir à cet effet l'aventure qui est advenue à la mairie de Baltimore au début de l'année 2019 et le dénouement qui l'a conclu :
https://www.developpez.com/actu/264413/Baltimore-le-retour-a-la-normale-apres-l-attaque-par-ransomware-va-couter-plus-de-18-millions-de-dollars-l-addition-pourrait-etre-plus-salee/

Puisque n'importe qui dans le monde peut créer sa propre clef publique à partir de n'importe quel appareil (ou « device » en anglais) connecté au réseau blockchain de son choix, l'abolition des frontières est totale. Elle se manifeste à la fois :

- Géographiquement : Toute personne sur terre peut accéder au réseau de la bloclchain de son choix. Précision importante, nous parlons évidemment ici des blockchains dites publiques, ou permissionless. Ce n'est pas le cas des blockchains privées ou de consortium, dont l'accès est par essence réservé à certains acteurs. Nous qualifions dans ce cas cet accès de « conditionné », ou « permissionné », si l'on reprend la terminologie anglosaxonne. Rien ni personne ne peut empêcher :
    - La blockchain de fonctionner partout et tout le temps
    - Un individu de s'y connecter sur un critère géographique
    - Un individu d'y opérer des transactions sur un critère géographique
    - Deux individus vivant à un bout et l'autre de la planète d'échanger de la valeur via blockchain

- Techniquement : Aucune qualification technique particulière n'est requise pour pouvoir accéder, connecter à ou transacter sur une blockchain. Il suffit, comme on l'a

vu, de créer un couple clef publique/clef privée (soi-même via des tutoriels disponibles sur Github ou via un générateur de clef comme celui-ci https://www.bitaddress.org). Il faut également savoir qu'il n'y a pas besoin de disposer d'un important débit internet pour utiliser la blockchain bitcoin par exemple, un simple téléphone captant quelques ko de débit étant largement suffisant. Pour l'anecdote, il y a même récemment eu une transaction bitcoin réalisée en dehors de tout usage d'Internet, via des ondes radios, le 12 février 2019. Vous trouverez des informations sur ce sujet ici : https://blockblog.fr/vous-pouvez-envoyer-des-bitcoins-via-radio-sans-internet-ni-satellite/ Évidemment, nous pouvons en rester à l'anecdote, mais il est à la fois intéressant, impressionnant et enthousiasmant de constater qu'une telle technologie puisse se passer d'Internet, sur lequel tous nos réseaux de communication, qu'ils soient informatiques ou non, sont aujourd'hui basés.

- Économiquement et socialement : Quel que soit son statut économique, que l'on soit riche ou pauvre, bancarisé ou non, homme ou femme, vivant en démocratie ou en dictature, et bien d'autres choses encore, il n'est pas possible de contraindre la blockchain à éviter ou empêcher quiconque d'y accéder. Nous en revenons, comme souvent, à la liberté et à son corolaire technologique, la décentralisation, pour exprimer et expliquer le refus par essence d'ancrer territorialement la blockchain, de quelque manière que ce soit.

Voici, à toute fin utile, une liste non exhaustive de solutions (sites/logiciels/tutos) permettant de générer un couple clef publique/clef privée :

- Adresses classiques : www.bitaddress.org (et sur Github : https://github.com/pointbiz/bitaddress.org)
- Adresses Segwit : www.segwitaddress.org (et sur Github : https://github.com/coinables/segwitaddress/releases)
- Logiciel Vanitygen (Windows, Linux et OsX)
- Site internet bitcoinpaperwallet.com : https://bitcoinpaperwallet.com/bitcoinpaperwallet/generate-wallet.html
- Site internet mircoin.com (« brainwallets ») : https://mircoin.com (et sur Github : https://github.com/ibtci/mircoin)
- Site internet bitcoinvanitygen.com : http://bitcoinvanitygen.com

Les implications de cette a-territorialité de la blockchain sur les questions de propriété, de copyright, d'ancrage géographique ou d'accession sociale vont être absolument immenses. Il est impossible de les prévoir aujourd'hui, pas plus qu'il n'était possible de prévoir la trajectoire que prendrait Internet il y a 40 ans. Dans le monde tel que nous l'avons conçu est

dirigé par la pensée économique libérale, elle est une remise à plat complète et totale des modèles économiques et des modes de coopération à l'échelle internationale.

E. Être résistante à la censure (le pilier « censorship resistant »)

- **La blockchain comme rempart à la censure d'Etat**

La censure est un concept large qui peut prendre de nombreuses formes et qui n'est en rien limité à la censure d'État, la plus connue comme la plus évidente, parce que les exemples historiques ou actuels sont légion, notamment. Sans éprouver la nécessité de se plonger dans les archives de la Stasi ou de la propagande soviétique, nous savons néanmoins qu'un régime tel que celui qui est en vigueur en Chine depuis le 1er octobre 1949 a très bien su adapter la forme comme les moyens de sa censure à la modernisation du monde. Loin d'être resté empêtrée dans les méandres de l'Histoire, la Chine continentale a parfaitement négocié le virage du capitalisme international, tout en l'adaptant à un contexte politique intérieur structuré autour de la volonté d'un contrôle étroit de la population.

Activement ancrée dans le XXIème siècle, la Chine dispose évidemment d'Internet, et n'en prive pas sa population par défaut comme le ferait le voisin Coréen du Nord, mais elle en **contrôle les moyens d'accès comme le contenu**, qu'elle peut modeler selon les desiderata

du comité central. Il y a bien sûr des sites et contenus dont l'accès est interdit, mais plutôt qu'une censure d'État grossière, c'est un une approche plus subtile qui est privilégiée : le contrôle de l'opinion. Les autorités chinoises ont compris qu'elles ne pourraient pas empêcher 1,5 milliards d'habitants d'être au courant des affaires du monde, certes, mais elles ont surtout compris qu'Internet pouvait être un formidable outil de fabrique de l'opinion.

Ce que nous avons jugé, en Occident, comme un moyen d'émancipation et de promotion de la liberté (de penser, de communiquer, d'informer) a été renversé pour en faire un véritable KGB numérique. Tout est tracé, pisté, surveillé, il n'y a pas d'exceptions à cela ou elles sont généralement payées très cher par leurs instigateurs. Pour ce faire, les autorités chinoises ont fait en sorte de promouvoir un équivalent national à chaque service/plateforme/application d'envergure lié à Internet. Ainsi, des équivalents de Google, de Youtube et de Facebook sont en vigueur dans le pays, qui permettent de faire exactement la même chose mais qui disposent de backdoors très efficaces pour surveiller ce que la population va chercher sur Internet.
Nous vous conseillons à cet effet un article détaillé de Wikipedia sur le sujet :
https://fr.wikipedia.org/wiki/Censure_d%27Internet_en_république_populaire_de_Chine

Les autorités ne cachent d'ailleurs pas leurs intentions aux éventuels étrangers de passage, en témoigne l'enquête conjointement menée par le New York Times, Motherboard, The Guardian, Süddeutsche Zeitung et NDR et qui a révélé le 3 juillet 2019 l'implémentation systématique d'un malware sur les téléphones d'étrangers à la frontière avec la province du Xinjiang, d'où sont originaires les Ouïgours et qui est particulièrement surveillée par les autorités, d'ailleurs soumise à un statut administratif spécial
https://www.phonandroid.com/chine-installe-malware-android-espion-smartphone-certains-touristes.html.

Cela nous pousse à faire une remarque d'ordre général : il est impératif que vous compreniez que la blockchain est, comme Internet, une technologie NEUTRE. Il est absolument inopportun de lui attribuer par essence tel comportement ou telle dérive, tout simplement parce qu'elle est un SUPPORT technologique et non une simple technologie d'application. Exactement comme Internet. Pourtant, c'est encore aujourd'hui l'angle d'attaque favori des détracteurs de la blockchain que de lui attribuer toutes sortes de méfaits (voir par exemple l'affaire silkroad, qui a défrayé la chronique et qui permit au *Monde* de distiller quelques inepties lors de sa fermeture en 2013, notamment à qualifier Bitcoin de monnaie « virtuelle » et « anonyme » permettant à ce supermarché Internet de la drogue de prospérer
https://www.lemonde.fr/technologies/article/2013/10/03/silk-road-ferme-et-alors_3488971_651865.html).

Il ne viendrait pourtant à l'idée de personne de condamner le téléphone en tant qu'invention parce qu'il sert aux dealers (bien plus que Bitcoin !) pour être contacter par leurs clients. Plus révélatrice encore est l'absence de charge contre le fonctionnement d'Internet, puisque c'est bien ce dernier qui a permis à un site comme silkroad de voir le jour puis de prospérer, et non la blockchain. Le plus étonnant, c'est que l'incongruité de la situation ne semble pas émouvoir les journalistes du *Monde* ou et leurs confrères décrivant Bitcoin comme la monnaie de la drogue, des réseaux criminels et du terrorisme.

- ## La blockchain contre toute forme de censure

Au-delà de la censure « classique » de nature étatique, il est indéniable qu'il existe aujourd'hui une multitude d'autres formes de censure sévissant sur Internet, du simple fait de sa centralisation. Oui, là-aussi, la réponse passe par la décentralisation, qui garantit qu'aucun individu, groupe d'individus ou corporation n'ait suffisamment de pouvoir donc de contrôle sur le réseau pour en modeler l'usage.

Les plateformes populaires telles que Facebook, Instagram ou Youtube ont toutes des politiques actives de censure de contenus, selon des critères qui leur sont propres. Certes, d'aucun peut arguer que ces politiques sont motivées par un souci louable de lutte contre la haine, la violence, les contenus offensants ou explicites, mais rien ne nous garantit que ces critères soient justes et, surtout, nous n'avons absolument aucun pouvoir dessus. Ils sont édictés de manière arbitraire et parfois stupide (voir l'exemple de la censure du tableau de Gustave Courbet *L'origine du monde* et la suppression du compte associé par Facebook en 2011 https://www.lemonde.fr/pixels/article/2018/02/01/censure-de-l-origine-du-monde-sur-facebook-une-attaque-contre-la-democratie_5250611_4408996.html). Par ailleurs, étant une traduction numérique de principes moraux, ils sont de nature contestable, car ce qui apparaitra comme un standard moral dans un certain pays ne le sera pas dans un autre : il s'agit donc bien d'une censure discrétionnaire et non de l'application de principes universels.

La blockchain, au contraire de l'Internet centralisé que nous connaissons aujourd'hui, c'est le monde de la liberté absolue : aucun gouvernement, aucune entreprise, aucun individu ne peut vous censurer. Encore une fois, il faut voir la censure au sens large, et nous avons parfois oublié, nous, occidentaux, que nous en faisons tous les jours l'expérience. Si vous tentez d'envoyer de l'argent à un proche à l'étranger et que votre banque s'est mise en tête de placer son pays de résidence sur une quelconque liste de surveillance, il est fort probable que votre virement ne lui parvienne pas, ou en tout cas pas facilement, pas avant d'avoir procéder à un KYC/AML renforcé (voir précédemment). Cela s'appelle de la censure et elle est de nature bancaire.

Il est une dernière chose dont nous souhaitons vous parler concernant les risques de censure liées à la centralisation des services (il s'agit d'une relation dialectique) : si cela n'est pas (encore ?) le cas aujourd'hui, où Internet demeure malgré tout un espace de communication, à défaut d'être un espace de liberté, une menace pourrait à l'avenir émerger sur les décombres de la société industrielle : les coupures intentionnelles de service globaux de la part d'entreprises privées et/ou de structures étatiques. Malgré le discours ambiant sur le dépassement de l'État-nation (forme hybride de gouvernance inventée au XVIIIème siècle) par des multinationales surpuissantes, nous ne vivons pas dans un monde où le totalitarisme technologique a pris le pas sur la tyrannie politique.

Il est certain, pourtant, qu'à avoir trop délaissé les questions éthiques et morales liées au numérique et à l'informatique, le grand public (occidental) court un grand risque, celui de voir accaparer toute dimension autre que simplement technique par des institutions suivant un agenda politique, qu'elles soient d'ordre gouvernemental ou privé. Un évènement passé totalement inaperçu devrait pourtant faire retentir l'alarme de nos esprits : le 2 juillet 2019,

l'espace de quelques dizaines de minutes, des millions de sites internet à travers le monde furent rendus totalement inaccessibles, affichant tous le même message d'erreur : « 502 bad gateway ».

Pourquoi ? Parce que le service Cloudflare, qui gère l'hébergement (et d'autres fonctionnalités) d'une grande partie des sites internet populaires à l'échelle mondiale (Discord, Soundcloud, Medium, Pinterest, Dropbox…) a été mis en défaut, non par une attaque de type Ddoss ou autre, mais par une « erreur de manipulation d'origine humaine » lors de la mise un jour d'un logiciel interne. Il n'y avait donc pas d'intention manifeste de nuisance, mais cela en dit long sur l'apparente facilité à fermer totalement ou à restreindre l'accès aux services Internet que nous utilisons tous les jours. S'apercevoir qu'il « suffit » de mettre la main sur un hébergeur tel que Cloudflare pour stopper le cours normal du fonctionnement d'Internet est au mieux déconcertant, au pire alarmant.

Vous trouverez plus d'informations sur cette entreprise qui possède environ 35% des parts du marché des réseaux de diffusions de contenu (CDN), ainsi que sur cette panne, via le lien suivant : https://www.zdnet.fr/actualites/quand-cloudflare-begaie-internet-trebuche-39887031.htm. Pour l'anecdote, sachez que deux des principales places de change (echanges) de cryptomonnaies, Coinbase et Bitfinex, étaient rendues inaccessibles durant cet épisode. Il est ironique de constater que la plupart des « bugs » attribués à la technologie blockchain sont en réalité le fait d'autres technologies, comme ici Internet. Conclusion de cet évènement : Internet peut être arrêté, stoppé, censuré, en tout ou partie. La blockchain, elle, n'est ni arrêtable, ni stoppable, ni censurable. Et tous ceux qui vous diront le contraire sont dans le faux, qu'ils soient militants ou simplement mal informés.