ACADÉMIE DES TECHNOLOGIES

POUR UN PROGRÈS RAISONNÉ, CHOISI ET PARTAGÉ

La *Blockchain* : une technologie disruptive avec des enjeux de sûreté, résilience et impact environnemental

Rapport de l'Académie

Académie des technologies
Le Ponant — Bâtiment A
19, rue Leblanc
75015 PARIS
+33(0)1 53 85 44 44

secretariat@academie-technologies.fr
www.academie-technologies.fr

ISBN : 979-10-97579-53-1
couverture : Hessyz - Adobe stock

ACADÉMIE
DES TECHNOLOGIES
POUR UN PROGRÈS RAISONNÉ, CHOISI ET PARTAGÉ

LA *BLOCKCHAIN* : UNE TECHNOLOGIE DISRUPTIVE AVEC DES ENJEUX DE SÛRETÉ, RÉSILIENCE ET IMPACT ENVIRONNEMENTAL

Rapport de l'Académie

Avril 2024

Sommaire

Résumé 6

Chapitre 1
Pourquoi un rapport sur la *blockchain* ? 8

Chapitre 2
La *blockchain* : explications introductives 10

2.1. Quatre piliers fondamentaux 11
- Sceau cryptographique pour assurer l'immuabilité 12
- Communications pair à pair pour assurer flexibilité et résilience 12
- Algorithmique distribuée et décentralisée 12
- Système ouvert (sans tiers de confiance) 13

2.2. Des difficultés scientifiques fondamentales 16
- Limites fondamentales pour les systèmes distribués 16
- Quand les systèmes distribués sont ouverts 17

2.3. Une révolution donnant naissance à des extensions et variantes 19
- Smart contracts 19
- *Non-Fungible Tokens* (NFT) 20

Chapitre 3
Quelques cas d'usage représentatifs 21

3.1. Les cryptoactifs privés (de type *bitcoin*) 22
- Taxonomie : attention aux termes « public » et « privé » 22
- Leur raison d'être 23
- Ce que c'est 24
- Le cahier des charges 25
- Développements récents 25

3.2. Les monnaies numériques de banque centrale 26
- CBDC (*Central Bank Digital Currency*) : ce que c'est 27
- Leur raison d'être 27
- Le cahier des charges 29

3.3. Catena-X : écosystème de données collaboratif pour filière industrielle 30
- Contexte et raison d'être 30
- Le passeport-batterie, un cas d'usage d'une *blockchain* 32
- Cahier des charges 33

3.4. L'organisation autonome décentralisée (DAO) 33
- Le contexte : Metavers et Web3 33
- DAO (*Decentralized Autonomous Organizations*) : ce que c'est 34
- Difficultés et perspectives 35

Chapitre 4
Une infrastructure coûteuse en énergie 37
4.1. Coût énergétique de la *blockchain* 37
4.2. Quelques pistes pour réduire la consommation 41
- Ajuster la *blockchain* permissionnée au cahier des charges du cas d'usage considéré 42
- Des architectures plus complexes pour être moins coûteuses 43
- Mécanismes d'incitation : du PoW vers le PoS ? 44

Chapitre 5
Conclusion et messages 46
5.1. État des lieux et constatations 46
- La *blockchain* : une révolution dans la conduite sûre de transactions à l'échelle mondiale 46
- État général de la recherche 46
- De nouvelles directions : des registres (*ledger*) aux graphes (DAG) 47
- Les *blockchains* les plus visibles 47
- Le cas de l'Estonie 48
- *Hyperledger*, plateforme et écosystème pour *blockchain* B2B 48
- Une résilience à toute épreuve, avec quelles conséquences ? 49

5.2. Recommandations 50
- Combattre le coût énergétique excessif en développant des solutions nouvelles 50
- La recherche reste vivante et il convient de l'encourager 51
- B2B : mieux fonder les boîtes à outils de *blockchain* permissionnées et les *smart contracts* 51
- Favoriser le développement de boîtes à outils bien fondées pour tout type de *blockchain* 52
- Progresser sur l'établissement d'un cahier des charges pour un usage donné 52
- Organismes gouvernementaux ou de régulation : évaluer et intervenir 53
- Vers une démarche de certification 55

Résumé

La *blockchain* (chaîne de blocs) est une technologie disruptive qui apporte une solution logicielle, élégante, mais présentant de sérieuses difficultés, à nombre des problèmes posés par la conduite sûre de transactions à l'échelle mondiale et en univers ouvert. Parmi les technologies construites au-dessus de la *blockchain* figurent les *smart contracts* (destinés à asseoir les transactions) et les NFT (*Non-Fungible Tokens*) permettant de définir des objets numériques. L'intérêt de la technologie *blockchain* réside dans les applications qu'elle permet, lesquelles se sont considérablement élargies au-delà des cryptomonnaies pour quoi elle a été initialement proposée. Pour des raisons de performance, la *blockchain* n'est pas une technologie de stockage de données, et ce bien qu'elle conserve de manière sûre la mémoire des données qui lui sont confiées.

La *blockchain* est une technologie essentielle pour l'Europe et la France, en quête d'une réindustrialisation sous condition de souveraineté. Il en existe de nombreuses réalisations, avec une grande variabilité dont ce rapport donnera une idée.

Solution distribuée et décentralisée, résiliente aux agressions inhérentes aux mondes ouverts (où les acteurs peuvent ne pas être connus), la *blockchain* est une infrastructure reposant sur des acquis fondamentaux de la recherche (mécanismes de consensus dans des mondes distribués ouverts, et cryptographie). La résilience des *blockchains* est essentiellement assurée par la preuve de possession d'une ressource rare (monnaie, puissance de calcul, etc.) par chaque acteur candidat à ajouter un bloc.

Ce sont les mécanismes mêmes qui assurent la résilience d'une *blockchain*, qui sont à l'origine d'une consommation énergétique souvent jugée excessive : c'est le vice sérieux qui est la contrepartie du service offert.

Ces caractéristiques quelque peu hors du commun motivent les recommandations qui suivent.

1. Il faut combattre le **coût énergétique excessif** en favorisant l'émergence de solutions nouvelles (adaptations d'architectures, propositions d'algorithmes de consensus)

2. Dans un écosystème dominé par un mode de publication par réseaux sociaux, il faut promouvoir la publication de résultats et produits dans des publications soumises à l'évaluation par les pairs, tout en favorisant la recherche dans un esprit d'ouverture.

3. À côté des cryptoactifs à l'origine du concept (le *bitcoin*) se développent des *blockchains* s'adressant à des filières B2B (chaîne logistique par exemple). Ces évolutions appellent le développement de l'open source et de boîtes à outils reposant sur des **validations scientifiques précises** des composants proposés et de leurs interactions.

4. La variété des usages de cette technologie milite en faveur d'un corpus de savoir-faire pour **l'établissement de cahiers des charges pertinents** (portant sur les points essentiels) assurant le bon dimensionnement de la *blockchain* envisagée. Ce corpus doit s'appuyer sur les études scientifiques mentionnées au point précédent.

5. Les organismes gouvernementaux doivent pouvoir mesurer une *blockchain* et intervenir dessus, ce qui appelle l'établissement d'un **nutriscore énergétique** et l'identification précise de l**eviers d'intervention** par les concepteurs d'une *blockchain*. Ceci suppose que les acteurs gouvernementaux soient bien **formés** aux technologies *blockchain*.

6. Enfin, nous pensons que la résilience même des *blockchains* pose un problème à nos sociétés et à leurs organes gouvernementaux, et que cela appelle le développement d'une démarche de **certification**, s'inspirant pour partie de l'expérience acquise dans des secteurs critiques tels que les transports et l'aéronautique en particulier.

Chapitre 1

Pourquoi un rapport sur la *blockchain* ?

La *blockchain* est un buzz, mais c'est aussi une technologie qui secoue notre société. À l'origine de la *blockchain* est le *bitcoin*, premier cryptoactif[1] ; son importance ne cesse de croître, même si elle demeure une part négligeable de la finance globale dans le monde.

Figure 1 : source : https://www.wavestone.com/fr/insight/radar-2021-startups-blockchain-crypto-france/.
Le paysage des secteurs concernés et des startups créées autour de la *blockchain*.

1. CoinMarketCap (en date du rapport) : *The global crypto market cap is $2.56T* (1T$ = 1 Trillion$ = $10^{12}$$). Comparé à la masse monétaire mondiale en 2021 (banque mondiale), évaluée à 143,5 % du PIB mondial, soit 138,52T$, le marché global des cryptoactifs est à 1,8 % environ.

Au-delà ces cryptoactifs, la *blockchain* a envahi de larges secteurs d'activité de nos sociétés, comme l'illustre la Figure 1. Nous reviendrons plus en détail sur ces usages de la *blockchain*.

À titre indicatif, la *blockchain* a drainé, pour 2022, un montant total de financement dans le monde estimé à $26.8B[2], dont environ la moitié pour des compagnies situées aux USA, le reste étant réparti à parts égales entre Europe et Asie.

La *blockchain* a déjà donné lieu à des rapports, dont nous retenons en particulier celui publié en 2021, sous la houlette de la DGE du gouvernement français[3]. Ce rapport DGE contient des développements techniques plus précis que le nôtre, et identifie 18 verrous et 14 recommandations, listées sans priorité. En référence à ce rapport, le présent travail a cherché à dégager une architecture conceptuelle (introduite à la Figure 2), dont nous espérons qu'elle aidera à la fois les pouvoirs publics et les consortiums désireux d'examiner le recours à une *blockchain*. Et nous avons dégagé un ensemble bien plus resserré de 7 recommandations.

2. https://www.cbinsights.com/research/report/blockchain-trends-2022/
3. https://www.entreprises.gouv.fr/files/files/etudes-et-statistiques/rapport-final-blockchain.pdf, long rapport (107 pages) publié en 2021 sous la houlette de la DGE ; il est très bien documenté sur le plan technique et comporte des cartographies précieuses, tant en France qu'au niveau mondial.

Chapitre 2

La *blockchain* : explications introductives

Une *blockchain* est une structure de données qui permet la construction d'un registre d'informations public et immuable[4]. Par *public* nous entendons le fait que chacun d'entre nous peut lire l'entièreté de ce registre et peut y inscrire de nouvelles informations sans aucun recours à un tiers de confiance (banques, institutions étatiques, entreprises…). Immuable signifie que, à l'exception des derniers blocs du registre non encore validés, son contenu ne peut être modifié ultérieurement. La structure de données en question est une suite temporelle de blocs, chaque bloc incluant du contenu et faisant référence au bloc précédent, d'où l'appellation « chaîne de blocs », *blockchain* en anglais.

4. https://www.senat.fr/rap/r17-584/r17-584.html Comprendre les *blockchains* : fonctionnement et enjeux de ces technologies. Rapports d'office parlementaire. Rapport n° 584 (2017-2018), déposé le 20 juin 2018.

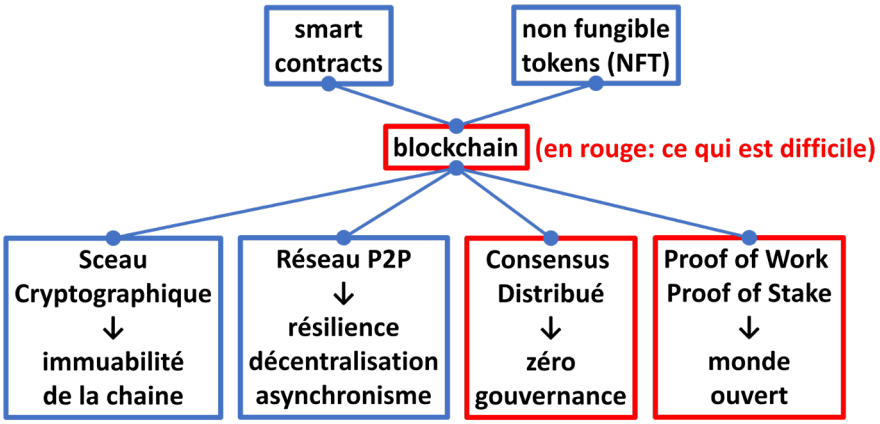


Figure 2 : La *blockchain* : quatre piliers fondamentaux et deux concepts dérivés importants. Les éléments encadrés en rouge soulignent les difficultés clés. Dans chaque boîte décrivant un pilier, on indique en haut la technologie, et, sous la flèche, le service qu'elle vise à rendre. Cette figure sera déclinée pour illustrer les divers points du rapport.

La Figure 2 illustre les quatre piliers fondamentaux sur lesquels repose la *blockchain*. Nous les développons maintenant.

2.1. Quatre piliers fondamentaux

La *blockchain* est maintenue et mise à jour sur un réseau de nœuds (en gros des ordinateurs, que nous appellerons « acteurs » dans la suite). Chacun de ces nœuds est capable de réaliser des transactions qui ont pour effet de modifier la *blockchain* en ajoutant un bloc à sa tête (sans modification de la queue de *blockchain* ni des blocs déjà enregistrés). Lors de chaque transaction, chaque nœud du réseau met à jour sa version de la *blockchain* — et/ou celles qui lui sont communiquées par les autres nœuds du réseau. Il est donc essentiel que ces versions soient cohérentes entre elles.

La construction, délicate, de ce registre distribué repose sur quatre piliers.

Sceau cryptographique pour assurer l'immuabilité

Un **sceau cryptographique** (aussi appelé « *hash* ») assure l'immuabilité de la chaîne de blocs. Ce sceau est la sortie d'une procédure qui prend en entrée un document quelconque et renvoie une chaîne de caractères très courte, qui permet de certifier l'intégrité du document. Chaque bloc porte un tel sceau qui garantit ainsi l'immuabilité de son contenu. Il est impossible de le modifier sans invalider ce sceau. Comme chaque bloc inclut aussi le sceau du bloc précédent, l'intégrité de toute la *blockchain* est garantie par le dernier sceau.

Communications pair à pair pour assurer flexibilité et résilience

Ces communications pair à pair (P2P) permettent à un ensemble d'acteurs de communiquer efficacement sans avoir recours, ni à une horloge globale, ni à un système de routage centralisé, ni même à de la mémoire partagée. Les communications reposent sur un processus aléatoire : chaque acteur maintient une connexion avec un petit nombre d'autres acteurs, et modifie ces connexions très régulièrement pour tenir compte de l'arrivée et du départ d'acteurs dans le système. La propagation de rumeurs constitue une image intuitive de la diffusion d'informations dans un tel réseau pair à pair. Les délais de communication sont donc très variables.

Algorithmique distribuée et décentralisée

L'algorithmique distribuée désigne la famille des algorithmes qui sont exécutés par un ensemble d'acteurs (ordinateurs) pour exécuter collectivement une fonction sur la seule base de connaissances locales ou acquises par communication. Ces entités communiquent entre elles via un réseau de communication dont les délais de communication sont variables (c'est le cas pour un réseau pair à pair). Elles peuvent effectuer des actions concomitantes sur la base de leurs connaissances locales ou acquises par communications. En raison de la variabilité des délais de communication, les connaissances locales ne sont pas nécessairement cohérentes. Le mode opératoire ainsi créé est appelé *concurrence* par la communauté scientifique. La reconstitution d'une vision cohérente des informations connues par chaque site nécessite des protocoles délicats.

Ces systèmes distribués doivent en outre faire face à la présence de comportements indésirables, voire hostiles, de la part de certaines entités.

Pour résumer, ces comportements indésirables, ainsi que les délais de communication variables, causent de l'incertitude et ont pour conséquence l'impossibilité de résoudre, en toute généralité, le problème dit du ***consensus***[5]. De nombreux algorithmes de consensus existent, ils diffèrent selon les hypothèses portant sur l'infrastructure de communication et le comportement des acteurs.

Système ouvert (sans tiers de confiance)

Lorsqu'elles sont développées en l'absence de tiers de confiance, les *blockchains* sont appelées *permissionless* (pour exprimer que l'accès est ouvert et qu'aucun tiers de confiance n'est utilisé). Les *blockchains* qui ne sont pas ouvertes sont souvent qualifiées de *permissioned*, ou *privées*. Pour la suite, nous nous autoriserons les néologismes suivants adaptés au Français : ***permissionné*** (pour *permissioned*) et ***non permissionné*** (pour *permissionless*).

Nous nous focalisons maintenant sur le cas non permissionné. En raison de l'absence de tiers de confiance et de contrôle d'accès, on fait face à la présence inévitable et éventuellement massive d'entités exhibant un comportement indésirable. À cet état de fait, il faut rajouter le caractère fondamentalement asynchrone et autonome du comportement des agents du système. Tout ceci requiert la conception de mécanismes d'incitation poussant à un comportement globalement vertueux. L'objectif de tels mécanismes est de convaincre chaque entité qu'il est dans son propre intérêt de respecter scrupuleusement les règles du jeu[6].

5. Attention, le mot « consensus » ne fait pas référence à un concept moral ou sociétal, il est ici à prendre au sens de l'informatique des systèmes distribués : c'est le fait que toutes les entités s'accordent sur une information, une donnée, une décision, etc. L'impossibilité du consensus se traduit par le fait que les tentatives de résolution vont, par exemple, diverger et ne pas terminer.
6. La plupart des mécanismes d'incitation utilisés dans une *blockchain* sont de nature économique ou monétaire. Mais il existe des contextes où la rétribution monétaire n'est pas nécessairement la ressource appropriée : il faut alors identifier la bonne ressource et proposer le mécanisme de rétribution qui va avec. Dans tous les cas il faut une ressource qui soit accessible à tout acteur de la *blockchain* et cependant difficile à acquérir.

Les entités entrent dans le système et en sortent *ad libitum*. Néanmoins il faut s'accorder sur ce qu'est l'état courant de la chaîne de blocs, pour que toutes les entités en aient une vue identique. Il va donc falloir sélectionner un sous-ensemble d'entités parmi l'ensemble des entités (dont nous rappelons qu'elles sont inconnues), pour limiter le nombre de candidats qui concourent à la création d'un bloc, lesquels sont appelés *mineurs*. Les deux grands mécanismes de sélection actuels sont *Proof-of-Work* et *Proof-of-Stake*, sur lesquels nous reviendrons plus en détail en Section 2.2.

Le ou les élus créent chacun un bloc, candidat à continuer la chaîne de blocs en cours. L'unicité de l'élu est assurée avec une très forte probabilité. Toutefois, des cas de non-unicité sont possibles, qui donnent alors lieu à des bifurcations de la *blockchain*, appelées *fork*[7] (bifurcation en français).

Une vue simplifiée du scénario de fonctionnement est donnée à la Figure 3.

7. Un *fork* est le plus souvent *soft* (attaque par l'insertion d'un bloc), mais peut aussi être *hard,* c'est-à-dire correspondre à un changement de version du protocole (comme pour *Ethereum* lors du passage à la PoS).

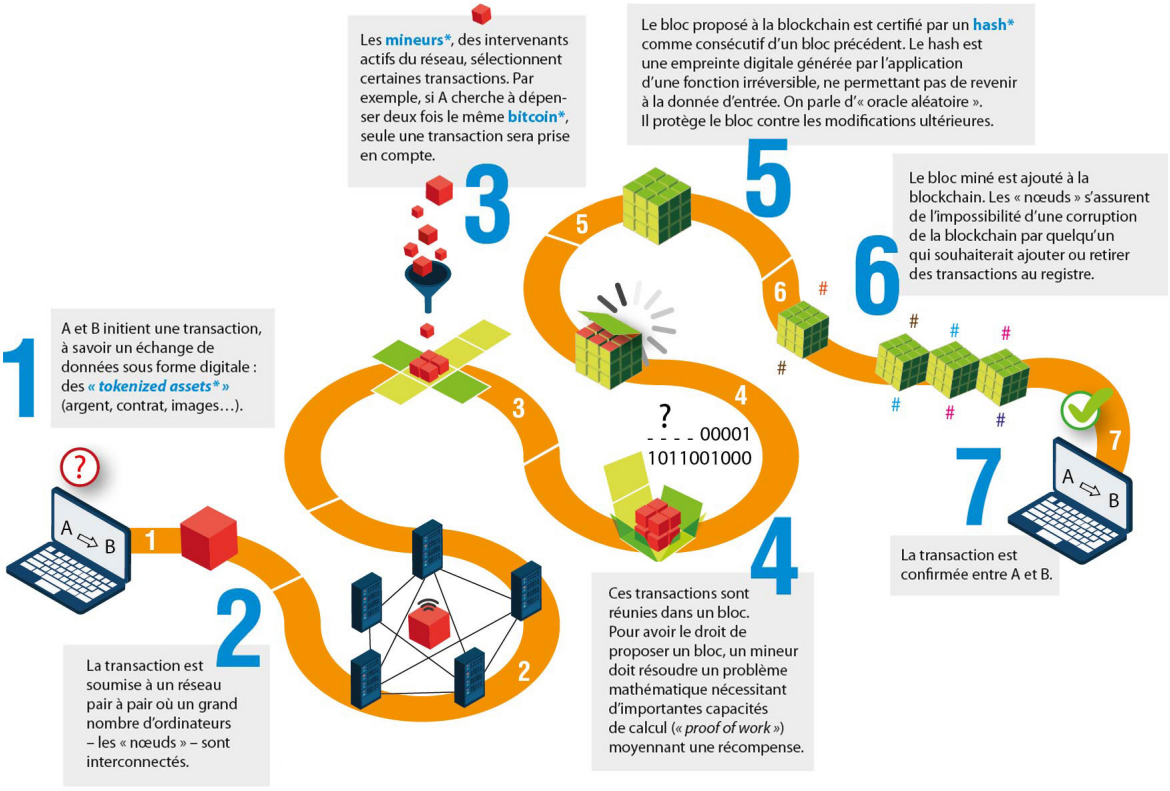


Figure 3 : source https://www.institutdesactuaires.com/magazine/article/schema-de-fonctionnement-de-la-blockchain/2371.
Il y manque toutefois la mention de l'étape de *consensus*, qui se cache derrière l'étape 3.

2.2. Des difficultés scientifiques fondamentales

→ *Pour une première lecture, cette section peut être omise.*

Parmi les quatre piliers développés ci-dessus, certains présentent des difficultés fondamentales, sur lesquelles il est bon de revenir.

Limites fondamentales pour les systèmes distribués

Nous avons déjà introduit la notion de ***système distribué***, consistant en un ensemble de composants s'exécutant sur des ordinateurs en réseau et ceci de manière totalement asynchrone (pas d'horloge commune), et qui communiquent par envoi de messages. Les messages mettent un temps fini, mais non nécessairement connu, pour parvenir à leur destinataire ; le nombre de composants peut être connu ou non connu ; chaque composant est supposé pouvoir communiquer avec tous les autres. Mais il peut y avoir des pannes (arrêts involontaires de composants ou de communications, ou perversion de messages ou de composants). Sur de tels systèmes, seuls des algorithmes particuliers peuvent être exécutés : les *algorithmes distribués*[8]. Il existe un théorème célèbre et fondateur : le résultat d'impossibilité de Fischer, Lynch et Paterson (1985) établit qu'il est impossible de résoudre le problème du consensus binaire[9] dans une infrastructure de communication asynchrone de façon déterministe même si on se limite à l'existence d'une seule panne franche. Les systèmes distribués dont il est fait usage dans certains de nos cas d'usage n'échappent pas à cet oukase, et c'est donc une satisfaction *probabiliste* de ces propriétés de cohérence que l'on peut espérer (ce qui suffit en pratique si cette probabilité est suffisamment proche de 1)[10]. L'identification précise des propriétés qu'on peut avoir selon les hypothèses faites sur

8. Voir à ce sujet l'excellent cours introductif au Collège de France par Rachid Guerraoui.
9. Le consensus binaire est une tâche élémentaire qui permet aux participants de proposer « 0 » ou « 1 » et doivent décider de façon irrévocable une des valeurs proposées. Cette tâche élémentaire se retrouve comme composant d'un grand nombre d'algorithmes distribués. Elle est difficile à réaliser car, si l'on prend la métaphore du vote, on ne connait pas le nombre de participants (et donc pas ce qu'est la majorité), et décider de ce nombre est à son tour un problème de consensus.
10. Le résultat d'impossibilité de FLP ne concerne qu'une résolution déterministe du consensus. Ce résultat ne s'applique pas lorsque l'on souhaite que les propriétés soient satisfaites avec une certaine probabilité.

l'infrastructure qui porte l'échange des données, a été la question centrale de toute une communauté de recherche depuis 1980 et jusqu'à nos jours. De nombreux algorithmes de ***consensus***[11] existent aujourd'hui. Pour la plupart, ils supposent connu l'ensemble des acteurs.

Quand les systèmes distribués sont ouverts

Dans les systèmes ouverts et à l'opposé des systèmes fermés, il est très facile pour un adversaire de se « faire passer » pour un grand nombre d'entités. Il n'a qu'à se forger un grand nombre d'adresses et le tour est joué. Par exemple, il peut utiliser toutes ces adresses dans une procédure de vote qui consisterait à compter le nombre de votes pour décider. Ce type d'attaque est connu sous le nom d'*attaque Sybil*[12]. On contre ce type d'attaque en demandant à un nœud de ***prouver la possession d'une certaine ressource, qui ne puisse pas être dupliquée, qui puisse être possédée par chacun (même en très petite quantité) et qui ait de la valeur (qui soit difficile à obtenir).***

Dans le cas de la *blockchain*, ce problème d'attaque Sybil prend la forme suivante. Chaque entité, élue ou non, conserve la chaîne contenant le plus de blocs. À cause de la concurrence, le consensus sur le résultat de cette règle n'est pas garanti ; et le *fork* est précisément un cas de non consensus. Il est rare, mais doit être résolu rapidement pour éviter la formation de chaînes parallèles (registres concurrents incohérents entre eux, mais partageant un historique commun) — et donc, pour prendre l'exemple du *bitcoin*, pour éviter la présence d'attaques de type « double dépense » lancée par des utilisateurs mal intentionnés. On rend très faible la probabilité de non-consensus en utilisant un algorithme approprié, relatif à la ressource mentionnée plus haut. Aujourd'hui les plus appropriées que l'on ait trouvées sont la ressource de calcul (à la base du *Proof of Work*, PoW) et l'argent (à la base du *Proof of Stake*, PoS). Ces deux approches

11. Au-delà du problème de consensus originel, le terme générique de « consensus » est utilisé pour toute cette famille d'algorithmes qui visent à synchroniser des décisions prises collectivement de manière décentralisée, par un ensemble d'acteurs. Il y a autant (et même plus) d'algorithmes de consensus que de jeux d'hypothèses sur l'infrastructure de communication et le comportement des acteurs.
12. Voir Douceur, J.R. (2002). The Sybil Attack. In : Druschel, P., Kaashoek, F., Rowstron, A, IPTPS 2002.

(PoW ou PoS) possèdent des caractéristiques bien différentes, et, pour les deux, les calculs (éventuellement considérables) qu'elles induisent n'ont pas d'autre but que de réaliser le consensus.

Pour le *bitcoin*, c'est le mécanisme dit de preuve de travail[13] (***Proof of Work, PoW***) qui a été proposé. Dans le cas de consensus à base de PoW, la règle « on ne garde que la chaîne de blocs ayant nécessité le plus de calcul » permet de résoudre les *fork*s. En pratique, les conflits de *fork* sont résolus en moins d'une heure dans le cas de *bitcoin* (une heure correspond à une bifurcation dont les branches contiennent en moyenne 6 blocs). **Un point fort de la PoW est la simplicité de son protocole et des hypothèses sur lesquelles il repose, ce qui en a permis la validation formelle. La PoW a, en revanche, le défaut quasi-rédhibitoire d'une consommation énergétique excessive**, voir la Section 4.1.

Dans le cas de consensus à base de preuve de ***PoS***[14] utilisé maintenant par le système *Ethereum*, la présence de *fork*s dépend de la procédure de sélection des participants qui seront impliqués dans la création des blocs. Cette procédure de sélection peut par exemple s'appuyer sur la mise sous séquestre d'une certaine quantité d'actifs, ou sur une élection randomisée des participants pondérée par la quantité d'actifs de tous les participants. Les participants sont donc sollicités dynamiquement (*online*) pour valider tel ou tel bloc, d'où la difficulté suivante : si un participant ne

13. La Preuve de Travail (*Proof-of-Work*, PoW) repose sur la résolution d'un problème cryptographique (dont la résolution est coûteuse en ressource de calcul), appelé *minage*. Chaque entité, élue ou non, conserve la chaîne contenant le plus de blocs. À cause de la concurrence, le consensus sur le résultat de cette règle n'est pas garanti. On rend très faible la probabilité de non-unicité en jouant sur les échelles de temps : l'intervalle de temps entre deux créations de blocs est long relativement à l'incertitude sur le timing des communications (d'où le faible nombre de transactions par seconde). Voir aussi https://www.fool.com/terms/p/proof-of-work/ : *Why do miners compete to update the blockchain? The winner receives awards in the form of newly minted crypto coins and transaction fees. Which miner wins? With PoW cryptocurrencies, each new block of transactions has a specific hash. For the block to be confirmed, a crypto miner must generate a matching target hash. The miner's aim is to be the first miner with the target hash. Finding the target hash is like using trial and error to solve a hard puzzle. Therefore, mining capacity depends largely on a miner's computational power.*

14. La Preuve de Possession (*Proof-of-Stake*, PoS) repose sur la possession d'actifs (monnaie numérique dans le cas d'*Ethereum*). Dans les deux solutions, la probabilité d'être sélectionné est proportionnelle à la quantité de ressource détenue. À ce stade, cette élection ne garantit pas l'unicité de l'entité élue (avec la PoS, cette unicité a lieu avec une très forte probabilité).

répond pas, est-ce une défaillance ou une attaque délibérée ? Pour lever cette inconnue, les protocoles de PoS se complexifient considérablement, tant du côté des mécanismes d'incitation/pénalisation que du côté des hypothèses de synchronicité et disponibilité ; et tout ceci avec une forte variabilité selon les *blockchains* utilisant la PoS. **Cette complexité explique les difficultés à prouver que ces solutions fondées sur la PoS font ce qu'on en attend, et ce sous des hypothèses réalistes.**

2.3. Une révolution donnant naissance à des extensions et variantes

L'invention de la *blockchain* associée au *bitcoin* est bien une révolution : un nouveau paradigme de système transactionnel « distribué-ouvert-immuable » a été identifié, pour lequel une solution a été proposée alors que la communauté scientifique ne croyait pas cela possible. Ce paradigme a trouvé son application immédiate dans le *bitcoin*, appelée cryptoactif et qui est une monnaie numérique virtuelle. Cette monnaie est privée au sens de la théorie de la monnaie c'est-à-dire sans banque centrale[15]. L'utilisation d'une *blockchain* a ensuite été élargie, comme nous allons le voir, à d'autres cas d'usage. Mais surtout, la *blockchain* a servi de support au développement de quelques autres infrastructures notables, intéressantes en tant que telles.

Smart contracts

Souvent, les systèmes collaboratifs impliquent que les transactions elles-mêmes soient immuables ainsi que leur séquencement. La *blockchain* peut contenir du code exécutable, on parle alors de *smart contract*[16].

15. Mais, attention, le *bitcoin* est déployé sur une *blockchain* publique selon la classification utilisée pour les *blockchains*, voir à ce sujet l'introduction de la section 3.1 sur une question de taxonomie.
16. Selon https://www.ibm.com/topics/smart-contracts : *Smart contracts are typically used to automate the execution of an agreement so that all participants can be immediately certain of the outcome, without any intermediary's involvement or time loss. They can also automate a workflow, triggering the next action when predetermined conditions are met.* Attention : l'usage du mot « contract » est un abus de langage (mais il est consacré) ; un *smart contract* n'est pas un contrat au sens juridique du terme. Si cela peut être vu comme un accord implicite entre deux parties, on dispose d'assez peu de jurisprudence sur ce sujet et la loi n'apporte pas de vraie reconnaissance aux *smart contracts*.

Ces *smart contracts* sont des programmes qui peuvent être invoqués par les utilisateurs du système. Ils peuvent ainsi fournir des entrées et déclencher des opérations, dont les résultats sont en retour inscrits dans la *blockchain* sous-jacente. Comme le code et les traces d'exécution sont disponibles dans la *blockchain*, on peut vérifier que l'exécution s'est bien passée en accord avec le code. Attention, cela ne garantit en rien que le code en question soit « sain » (exempt de bug) ni « correct » au regard d'un effet attendu ni que le séquencement de tels codes ne crée pas, en soi, de problème. Ces propriétés fondamentales sont laissées à la responsabilité du développeur du code et sont hors du champ des services rendus par les infrastructures que nous étudions dans ce rapport. La référence[17] montre une liste de pertes subies du fait de failles dans des *smart contracts*.

Non-Fungible Tokens (NFT)

Un NFT (de l'anglais *non-fungible token*) ou jeton non fongible, est un objet informatique (un jeton) suivi, stocké et authentifié grâce à un protocole de *blockchain*, auquel est rattaché un identifiant numérique, ce qui le rend unique et non fongible[18]. Ce jeton accorde des droits, de propriété ou autre, sur un objet réel ou virtuel comme une œuvre d'art (souvent numérique), un contrat, un diplôme etc., et est associé à un propriétaire comme tout jeton de *blockchain*. En général, le NFT n'est pas enregistré tel quel dans la *blockchain*, et le système enregistrera plutôt une référence vers l'objet numérique, par exemple un lien vers le système (externe) qui contient l'objet numérique. Il est aussi possible que ce système soit lui-même distribué sans pour autant être une *blockchain*. Le jeton étant non fongible, le propriétaire est garanti unique, ce qui donne la valeur au jeton.

17. https://rekt.news/fr/leaderboard/
18. Nous recommandons particulièrement la lecture de l'ouvrage suivant d'Étienne Ghys : *Le b.a.-ba des NFT*, Odile Jacob, à paraitre en 2024. La lecture en est intéressante pour le caractère pédagogique de ce texte, au-delà même des NFT, mais aussi pour la *blockchain* en général.

Chapitre 3

Quelques cas d'usage représentatifs

Si la première *blockchain* proposée, celle du *bitcoin*, combine tous les éléments ci-dessus, des variantes ont été, depuis lors, proposées qui les modifient ou les adaptent selon le contexte applicatif visé. Nous conformant en cela aux coutumes des utilisateurs industriels, nous parlerons encore de *blockchain* (ou « *blockchain* » quand des pincettes s'imposent), bien que toutes les caractéristiques énoncées précédemment n'en soient pas forcément réunies. Commençons par examiner quelques cas d'usage.

Nous pouvons classer les cas d'usage de la *blockchain* en deux grandes catégories :

a) Cas d'utilisation de la *blockchain* centrée sur les cryptoactifs (ou actifs numériques). Ces actifs représentent des actifs à but de commercialisation ou de financiarisation

b) Les cas d'utilisation de la *blockchain* pour les entreprises, axés sur le partage de données d'un écosystème.

En tout état de cause, il faut garder en tête que, pour des raisons de performance, la *blockchain* n'est pas une technologie de stockage de données (ce pour quoi IPFS est une solution appropriée[19]).

19. IPFS (*Interplanetary file system*) est un système de stockage de fichiers fréquemment utilisé dans le monde des *blockchains*, car il donne des garanties renforcées d'intégrité, en utilisant des sceaux numériques. Mais il n'est pas une *blockchain*.

Comme illustré par la Figure 1, la *blockchain* impacte un nombre important de secteurs. Outre la finance et les cryptoactifs, sont également concernés les services de type IT, le secteur notarial, et la logistique en complément de l'IoT. La *blockchain* s'avère d'ores et déjà précieuse pour les assurances, pour les industries du luxe et la lutte contre la contrefaçon, pour l'agroalimentaire et la traçabilité, pour la santé (traçabilité des lots de médicaments, pour un retrait plus facile en cas de défaut constaté), pour en citer quelques-uns. Plus généralement, le déploiement de l'économie circulaire appelle des solutions de traçabilité non répudiable, précisément apportées par la *blockchain*.

Le but de cette section n'est pas de faire un panorama de ces usages, mais plutôt d'en passer en revue un nombre restreint de cas, choisis pour leur caractère illustratif.

3.1. Les cryptoactifs privés (de type *bitcoin*)

Taxonomie : attention aux termes « public » et « privé »
Attention ! Nous avons une difficulté avec l'acception de l'opposition **public/privé** pour les deux premiers cas d'usage, relevant de la monnaie.

– Dans la communauté « *blockchain* », le terme « public » (*non permissionnée*) indique que l'infrastructure est accessible à toute entité sans enregistrement préalable ni contrôle d'accès ; par opposition, le terme « privé » (*permissionnée*) indique que les utilisateurs constituent un consortium de membres identifiés. Selon cette taxonomie, le *bitcoin* est une monnaie publique.

– Dans la communauté des économistes, le terme « public » fait référence à une monnaie de banque centrale, tandis que le terme « privé » fait référence à une monnaie échappant à tout contrôle de banque centrale. Dans cette taxonomie, le *bitcoin* devient privé, tandis que le dollar ou l'euro sont des monnaies publiques.

Dans notre présentation des deux cas d'usage relatifs à la monnaie, nous nous sommes appuyés sur des textes émanant de la sphère économiste.

Nous avons choisi d'en conserver la taxonomie. Pour les autres cas d'usage, nous suivons la taxonomie de la communauté *blockchain*.

Leur raison d'être

Selon le papier fondateur de Satoshi Nakamoto (2008)[20] dont nous reproduisons l'introduction en note de bas de page[21], la motivation première pour le *bitcoin* est d'offrir un système de paiement électronique basé sur une preuve cryptographique permettant à des utilisateurs de réaliser entre eux des transactions sans le besoin d'un tiers de confiance (e.g. une banque, un organisme étatique). Pour cela, il faut : 1/ un mécanisme de transactions impossibles à défaire pour protéger de la fraude ; 2/ une solution au problème de la double-dépense en utilisant un serveur d'horodatage distribué pair à pair afin de garantir la correction de la chronologie et l'intégrité des transactions ; 3/ un système qui demeure sûr tant que les nœuds honnêtes contrôlent collectivement plus de puissance CPU que celle de chacun des groupes de nœuds d'attaquants coopérants éventuels. Tous ces mécanismes visant à établir la confiance sans tiers reposent sur le coût, et donc la cherté, de la puissance de calcul.

20. *Bitcoin* : A Peer-to-Peer Electronic Cash System, Satoshi Nakamoto. https://bitcoin.org/bitcoin.pdf

21. *Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust-based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for nonreversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party. What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.*

Ce que c'est

Depuis cet article fondateur, qui a introduit en même temps la technologie *blockchain* et le *bitcoin*, les cryptoactifs se sont rapidement développés. Il s'agit d'actifs monétaires numériques et décentralisés, car nés d'initiatives venant non pas des autorités monétaires, mais d'agents privés. C'est pourquoi on peut parler de monnaies privées en contraste avec les monnaies publiques ou officielles.

Mais, avec les cryptoactifs, s'agit-il de monnaies au sens plein du terme ? Pour répondre à cette question, la distinction faite il y a longtemps par John Hicks, Prix Nobel d'économie, entre monnaie complète et monnaie partielle est éclairante. Une monnaie est complète si elle remplit les trois fonctions traditionnelles de la monnaie : unité de compte, intermédiaire entre les échanges (ou fonction transactionnelle de la monnaie), réserve de valeur. Une monnaie partielle ne satisfait au plus que deux des trois fonctions habituelles de la monnaie.

Jusqu'à présent, le *bitcoin* et les autres cryptoactifs demeurent des monnaies partielles. Car ils ne remplissent que de façon très marginale la fonction spécifique de la monnaie : la fonction transactionnelle. Seuls deux pays ont conféré jusqu'à maintenant un cours légal au *bitcoin* : le Salvador depuis décembre 2021 (où il circule à côté du dollar américain), et la République centrafricaine qui accepte la circulation parallèle du *bitcoin* et du franc CFA (valide en date de 2022). La volatilité empirique des cryptoactifs en fait de mauvaises unités de comptes, de très médiocres étalons des valeurs. C'est cette volatilité empirique qui a concrètement conduit les Salvadoriens à bouder jusqu'à présent le *bitcoin* au profit du dollar pour leurs règlements courants. L'excès de volatilité est susceptible de s'infléchir lorsqu'il est question de « *stablecoins* » ancrés sur une monnaie publique avec une parité en principe fixe. Mais, même-là, certains « *stablecoins* » se sont révélés depuis deux-trois ans être éminemment instables, avec des plateformes de négociation qui n'ont pas été en mesure de faire face à des retraits impromptus et massifs de liquidités de la part des investisseurs.

Malgré les critiques, nombreuses et importantes, que l'on peut formuler à l'égard de ces cryptoactifs, on se doit malgré tout de constater qu'elles sont installées, sans doute durablement, dans le monde monétaire.

Le cahier des charges

C'est celui résumé dans la Section 1 où le concept de *blockchain* (sous sa forme utilisée pour le *bitcoin*) est dessiné. Tous les éléments développés dans cette section interviennent dans le *bitcoin*, et plus généralement dans toute monnaie privée électronique. Les mécanismes incitatifs sont, vu le contexte, eux-mêmes économiques : la rétribution est monétaire (en *bitcoin*s par exemple).

Développements récents

La SEC, le régulateur financier américain, a autorisé en janvier 2024 la commercialisation de fonds indiciels cotés (ETF) sur le *bitcoin*. Elle l'a fait malgré elle, sous la contrainte de décisions de justice qui avaient été initiées par les porteurs de tels projets.

Cela veut dire concrètement que le lancement d'ETF en *bitcoin* par de grands opérateurs (*BlackRock*, *Fidelity*…) comme par des start-ups va donner une impulsion à l'essor du premier cryptoactif (le *bitcoin* fait près de 50 % du total). Désormais, le grand public, via les ETF, dispose d'un accès plus facile, moins coûteux, plus « démocratique » au *bitcoin*. Pour tout le monde, mais, fait nouveau, également pour la clientèle de détail (« retail market »), l'investissement en *bitcoin* devient plus flexible, car le seuil de l'investissement requis chute drastiquement, et plus liquide, car les ETF bénéficient d'une cotation quotidienne. On s'attend à ce que l'*Ethereum*, second cryptoactif du point de vue de la taille, bénéficie rapidement du même élargissement que le *bitcoin*. Et on imagine mal que, compte tenu du phénomène de globalisation financière, du poids des marchés financiers américains et d'interconnexion des marchés, les régulateurs financiers d'Europe et d'ailleurs puissent durablement rester à l'écart du mouvement…

Le régulateur financier, qui n'est pas, rappelons-le, la banque centrale, consacre ainsi le leader des monnaies privées qu'est le *bitcoin*. Paradoxe, ou désir de surveiller un peu ce qui, au départ, vous échappe ? On y verra plus clair à l'usage. Reste prévisible ce que pressentait la SEC elle-même : l'impulsion ainsi donnée au marché des cryptoactifs va rendre plus compliqué le respect des réglementations applicables, qu'il s'agisse

des textes anti-blanchiment ou anti-financement du terrorisme[22], ou des autres règlements relatifs aux cryptoactifs.

3.2. Les monnaies numériques de banque centrale

Attention, nous continuons à utiliser la taxonomie « publique/privée » telle qu'introduite à la section précédente pour le *bitcoin*.

Dans la mesure où les cryptoactifs sont privés et décentralisés, ils représentent un défi, voire une menace, pour les banques centrales et pour la politique monétaire qu'elles mènent. Car elles viennent empiéter sur le pouvoir monétaire des États, sur la régulation des paiements et de la masse monétaire par les banques centrales, et sur des prérogatives des régulateurs bancaires et financiers. Par exemple, sur ce dernier point, elles peuvent dans certains cas servir à contourner les réglementations relatives à la lutte contre le blanchiment de l'argent sale et contre le financement du terrorisme.

Plus récemment, l'initiative de Facebook/Meta de mettre sur le marché un cryptoactif, d'abord baptisée Libra puis ensuite dénommée Diem, a déclenché une réaction des banques centrales et des pouvoirs publics. Variété de « *stablecoin* » ancrée sur le dollar, le Diem, s'il avait vu le jour, aurait potentiellement concerné près de deux milliards et demi d'individus, tous les utilisateurs de Facebook. Cette affaire a donné lieu à un bras de fer entre Facebook et les pouvoirs publics américains, européens. Ce fut un vrai test de la capacité de ces derniers à s'opposer à une initiative monétaire majeure de l'un des GAFAM (Google, Apple, Facebook, Amazon, Microsoft). Tout le monde s'y est mis, la Fed, la BCE, le G20, pour bloquer dans l'œuf le Diem. La riposte des autorités a consisté en un blocage réglementaire du projet de Facebook.

22. Selon https://www.chainalysis.com/, 0,34 % de l'activité des cryptoactifs est considérée comme criminelle, ce qui paraît comme un taux somme toute acceptable au regard d'autres actifs financiers. En revanche, si l'on regarde les choses plus qualitativement et du point de vue sociétal, le fait que les cryptoactifs soient un support qui rende possible la cybercriminalité (penser aux *ransomwares* qui attaquent nos services publics et des entreprises) peut constituer un point fortement négatif.

Le secteur des cryptoactifs sera, dans un futur proche, l'objet d'initiatives publiques[23] : les *monnaies numériques de banque centrale* (CBDC suivant l'acronyme anglais). Même si elles sont moins populaires que les monnaies de type *bitcoin*, nous pensons que les CBDC ont peut-être plus d'avenir.

CBDC (*Central Bank Digital Currency*) : ce que c'est

Face à l'essor et à la multiplication des cryptoactifs, les banques centrales, avec la bénédiction des gouvernements, ont réagi en annonçant le lancement de **monnaies numériques de banques centrales (*Central Bank Digital Currency*, CBDC)**. Puisque la technologie *blockchain* est là, pourquoi ne pas l'appliquer au pivot de tout système monétaire et financier, la monnaie de banque centrale ? Cette dernière est constituée des billets et des pièces en circulation ainsi que des réserves des banques auprès de la banque centrale, à laquelle s'adosse la monnaie créée par les banques via les crédits qu'elles accordent et les dépôts qu'elles collectent, selon la formule canonique, « les crédits font les dépôts ».

Leur raison d'être

Les banques privées sont vent debout contre les CBDC, car elles craignent de voir les dépôts fuir vers la banque centrale. Néanmoins, de nombreux arguments sont avancés en faveur des CBDC (la liste des avantages ne doit pas faire oublier certains coûts de l'opération, nous y reviendrons) :

– **introduire les nouvelles technologies dans les banques centrales et la politique monétaire.** Cette demande des agents non financiers pour l'innovation technologique dernier cri existe partout, même dans les pays en développement ainsi que le suggère l'essor de la monnaie digitale en Afrique subsaharienne ;

23. La préparation d'une CBDC est très avancée en Chine (pour qui c'est sans doute une des voies pour contrer la prédominance du dollar), assez avancée aux USA. Le déploiement se fait plus lentement en Europe (échéance repoussée à 2025-2026), surtout en raison de l'opposition des banques privées pour les raisons mentionnées plus haut.

- **conserver à la monnaie banque centrale sa fonction de pivot du système monétaire.** La CBDC satisfait la demande du public et des entreprises pour des espèces dématérialisées. Ce cryptoactif sera échangé à la parité 1/1 entre les différentes formes (cash, dépôts, version digitale…) qu'elle est susceptible de revêtir ;

- **renforcer la transparence, la traçabilité et la sécurité des paiements.** Pour que les CBDC s'acclimatent, les banques centrales devront rassurer les futurs utilisateurs sur le fait que ces monnaies digitales ne seront pas une intrusion de style « Big Brother » dans la vie de chacun, et qu'il n'y aura pas de recoupements entre les différentes sources de données, sauf manquement réglementaire ou fiscal supposé ou avéré ;

- **élargir l'inclusion financière.** Sur le continent africain où le taux de bancarisation est souvent faible (40 %), la monnaie digitale privée, malgré sa dimension « technocratique », n'a pas accru la fracture sociale ; elle aurait plutôt favorisé l'inclusion financière y compris en milieu rural ; la CBDC en fera de même, jouant un rôle complémentaire à celui des néo-banques et de la monétique ;

- **réduire les coûts et les temps de transaction.** Sur ce terrain-là, monnaies digitales privées et publiques se rejoignent. Car les unes et les autres, grâce aux protocoles impliqués, aux volumes échangés et au jeu des économies d'échelle, diminuent drastiquement le coût unitaire des transactions, particulièrement lorsque celles-ci impliquent des pays ayant des monnaies différentes. Dans une économie ouverte, la réduction des coûts de transfert de la monnaie a des avantages microéconomiques évidents. Elle a l'inconvénient de rendre moins coûteuses les sorties de capitaux en cas de spéculation contre la monnaie nationale ;

- **promouvoir le rôle international de la monnaie domestique.** Que se passerait-il concrètement si par exemple l'Eurosystème renonçait à l'euro numérique, alors que le dollar numérique et le yuan numérique étaient mis en œuvre ?

Le cahier des charges

– La CBDC, tout comme les cryptoactifs, n'a pas d'existence physique. Elle doit être enregistrée dans un registre (« *ledger* »), constitutif de la *blockchain* (« ***distributed ledger technology*** »). Cette exigence est donc commune à toutes les formes de cryptoactif. La propriété d'immuabilité reste donc essentielle.

– S'agissant du caractère distribué et ouvert, les besoins sont plus subtils. S'adossant à une banque centrale, la CBDC pourrait se satisfaire d'une vision centralisée, approche qui offre de nombreux avantages sur le plan de l'efficacité[24]. Toutefois, parmi les avantages attendus d'une CBDC (cf ci-dessus), **les deux derniers (transactions, international) impliquent une pluralité d'acteurs bancaires**. Il faut donc que l'approche retenue pour les CBDC résolve les problèmes de gouvernance posés par cette pluralité. Si ceci exclut une approche pleinement centralisée, cela n'implique pas nécessairement de déployer tous les mécanismes des cryptoactifs privés offrant décentralisation et ouverture. Il y là un champ permettant de travailler sur le compromis décentralisation/efficacité. Plus précisément :

  – si l'on considère que les acteurs du secteur des CBDC sont officiellement enregistrés, alors le système support n'est plus ouvert (et ce, quel que soit le nombre de ces acteurs) ;
  – enregistrer les acteurs du secteur des CBDC est une forme de gouvernance. Si l'on considère que, au vu de la population des acteurs des CBDC, cette forme de gouvernance est difficile à construire par des moyens juridiques, alors on peut vouloir se tourner vers une approche de système ouvert.

24. Des sociétés comme Visa sont capables de traiter plus de 20 000 transactions par seconde à l'échelle mondiale, contre 7 transactions par seconde pour le *bitcoin*, en raison du nombre important de messages à échanger pour assurer la cohérence des livres de compte. Toutefois les choses évoluent vite pour les cryptoactifs, puisque les projections pour *Ethereum* sont de plusieurs dizaines de milliers par seconde (source : https://fr.cointelegraph.com/news/bitcoin-lightning-network-vs-visa-and-mastercard-how-do-they-stack-up). Par ailleurs, les systèmes centralisés disposent de protocoles qui font que toute transaction est entièrement réalisée ou non, et ne laissent pas le livre de compte dans un état intermédiaire incohérent en cas de panne. Dans les systèmes décentralisés, en cas de panne et de façon exceptionnelle, il peut se produire des écarts entre les copies des livres de compte.

3.3. CATENA-X : ÉCOSYSTÈME DE DONNÉES COLLABORATIF POUR FILIÈRE INDUSTRIELLE

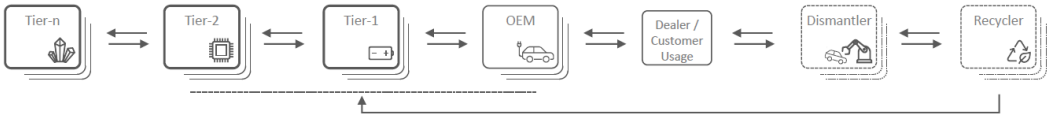
La *blockchain* s'avère particulièrement pertinente pour les usages industriels, en particulier dans le contexte de la *supply chain* et du concept d'entreprise étendue. Un besoin central est de pouvoir y partager des données non répudiables. Dans le cas où cette extension est multinationale, l'établissement d'un entrepôt de données classique pose la question du choix du pays où l'établir et des législations qui seront alors applicables ; ceci peut s'avérer un casse-tête, que le recours à une *blockchain* permet de contourner. Heureusement, l'établissement d'un tiers de confiance est le plus souvent possible, auquel cas les *blockchains* privées (ou *permissionnées*), de type *Hyperledger* (voir Section 5.1 et la page 48), conviennent. Comparées aux *blockchains non permissionnées*, ces solutions plus légères deviennent incontournables lorsque certaines des données à partager sont collectées via de l'IoT. Le cas d'usage que nous présentons ici relève de cette catégorie.

Catena-X est une plateforme qui vise à créer un écosystème d'échange de données collaboratif à l'échelle de l'industrie dans toute la chaîne de valeur mondiale de l'automobile, en commençant par la R&D et en s'étendant à la chaîne d'approvisionnement, à la fabrication, et à la mise au rebut et au recyclage des véhicules.

CONTEXTE ET RAISON D'ÊTRE

Contexte : une filière industrielle

L'objectif général de Catena-X est de couvrir toute la filière comme l'indique le schéma ci-dessous, et d'y servir de support à tous les échanges d'information :



Dans ce contexte, Catena-X offre un *espace de données partagé* avec, entre autres, les caractéristiques suivantes :

– un modèle opératif uniforme pour tout l'espace de données et

– une gouvernance neutre,

le tout en assurant la *souveraineté* de chaque participant :

– pour les données : il garde le contrôle de ses propres données ; plus précisément, chaque membre de l'espace de données conserve ses données dans sa propre infrastructure et échange ses données à travers les mécanismes de connecteurs après identification du receveur ;

– pour les services : il choisit son fournisseur dans un marché ouvert ;

– pour les opérations (partage de données spécifiques, suivant des règles établies de durée, fréquence, etc.) : il garde le contrôle de la localisation de ses données puisque les données restent dans sa propre infrastructure ;

– pour les questions d'identité : la plateforme lui offre toutes les garanties.

L'ambition est de mettre en place un écosystème de données ouvert où les données sont échangées entre toutes les entreprises de chaque chaîne de valeur. Pour cela, le projet s'appuie sur des composants OpenSource s'appuyant sur des standards d'échange de données définis par IDSA — International DataSpace Association.

De nombreux cas d'usage sont déjà identifiés parmi lesquels : la traçabilité des composants, la protection de l'environnement (avec la mesure de l'empreinte carbone tout au long de la chaîne de valeur), l'amélioration de la qualité (avec la résolution collaborative des motifs d'erreur), la gestion de la demande et de la capacité, la fabrication *as-a-service* (basée sur un équilibrage flexible des capacités entre les usines intelligentes intégrées sur la plate-forme) et le passeport de batterie qui nous développons maintenant.

LE PASSEPORT-BATTERIE, UN CAS D'USAGE D'UNE *BLOCKCHAIN*

Le cas d'usage spécifique « **passeport-batterie** » est intéressant. Ce passeport permet le partage des données relatives aux batteries afin de satisfaire les réglementations à venir (janvier 2027) sur le recyclage/la remise à neuf de ces batteries. Les passeports-batterie sont gérés comme des NFT[25], stockés dans une *blockchain* utilisée pour créer une couche de vérification dans l'espace de données.

L'objectif du partage de données et de rester sélectif dans ce que l'on partage ; par exemple, on peut indiquer qu'il y a eu des changements sur les procédés mis en œuvre pour la fabrication de la batterie, sans partager ces procédés. On a donc coexistence des deux notions de partage et de secret. Les différents acteurs de la chaîne de valeur bénéficient donc du partage de données :

- les constructeurs de batteries gardent leur secret de composition et fabrication, tout en assurant leur conformité ESG[26] ;

- les constructeurs automobiles sont les principaux acheteurs et utilisateurs des batteries de voiture, et vont donc être en mesure de prouver leur conformité aux régulations ;

- les ateliers de réparation et les clubs automobiles lisent les informations relatives aux performances et à l'historique des réparations afin de pouvoir travailler correctement sur les batteries. Ils ajoutent de nouveaux détails de réparation une fois leur travail terminé ;

- les ateliers de recyclage et de remise à neuf lisent les données relatives à la production et au cycle de vie afin de pouvoir recycler correctement les batteries.

25. Non-Fungible Token https://fr.wikipedia.org/wiki/NFT, voir aussi le paragraphe sur les NFT à la Section 1.3.
26. https://www.opendatasoft.com/fr/glossaire/les-criteres-environnementaux-sociaux-et-de-gouvernance-esg/ Critères Environnementaux Sociaux et de Gouvernance

Cahier des charges
La *blockchain* utilisée dans le cas d'usage « passeport de batterie » de Catena-X est en cours d'implémentation et sert d'illustration à l'utilisation de la technologie *blockchain* dans les espaces de données. Au-delà de ce cas d'usage précis, voici les éléments principaux du cahier des charges :

– l'infrastructure est distribuée (réseau pair à pair ou autre) ;

– l'immuabilité est, là encore, requise ;

– orientation vers un système d'enregistrement (fermé, qui ne nécessite donc pas de PoW ni de mécanisme d'incitation) ;

– le cahier des charges fait apparaître le besoin d'inclure des actions (réparations, réutilisation d'une batterie dans un autre véhicule…) qui doivent être synchronisées avec certaines données. Dans certains cas, cela peut nécessiter le recours à du code exécutable, qui est alors inscrit dans la *blockchain* (par exemple par le recours aux *smart contracts*).

Il faut trouver le moyen de rétribution des participants en dehors des mécanismes liés à la *blockchain*, puisque cette dernière n'est pas intimement liée à des transactions monétaires. Un mécanisme de réputation paraît approprié.

3.4. L'organisation autonome décentralisée (DAO)

Le contexte : Metavers et Web3
L'engouement d'une part de la population mondiale pour s'auto-organiser autour de moyens de paiement comme les cryptoactifs, amène à de nombreuses réflexions autour du concept d'organisation autonome décentralisée. À ce stade, ce concept qui comporte des aspects politiques, sociologiques et économiques, n'a pas encore donné lieu à des réalisations concrètes d'ampleur qui permettraient de le valider. Cependant le numérique favorise le fonctionnement de communautés même à grande échelle (comme Wikipédia) avec des échanges moins hiérarchiques, plus horizontaux. Dans certains domaines, il permet d'envisager, avec les

blockchains, des pistes nouvelles pour résoudre des problèmes plus ou moins bien identifiés. C'est le cas pour :

– **les métavers**, le futur d'Internet ? En s'appuyant sur les technologies de réalité virtuelle et augmentée, les métavers proposent des réseaux de mondes virtuels. Une difficulté qu'ils soulèvent est de permettre à un individu de garder, entre plusieurs de ces mondes, son identité, ses objets numériques (par exemple, des avatars) et ses droits. Les métavers pourraient utiliser des *blockchains* comme système d'interopérabilité ;

– **le Web3**, une prochaine étape du web ? La *blockchain* est utilisée à la base d'une infrastructure pair à pair, sécurisée pour que les utilisateurs du réseau puissent publier sur le web de l'information, tout en gardant un contrôle direct sur leurs données. Ils n'ont plus à les confier à des serveurs, comme c'est le cas dans le web actuel.

Nous présentons ici une application plus modeste, mais d'une certaine façon aussi plus précise, les *decentralized autonomous organizations*, DAO pour faire court.

DAO (*Decentralized Autonomous Organizations*) : ce que c'est

Les DAO proposent des organisations typiquement numériques de communautés sans qu'il soit nécessaire d'avoir d'autorité centrale. Une DAO s'appuie sur une *blockchain* et des *smart contracts*. La *blockchain* sert au partage de ressources par les membres de la communauté (peut-être même anonymement). Les *smart contracts* permettent de définir et renforcer les règles de fonctionnement et la gouvernance de la communauté. La transparence du fonctionnement de la communauté est garantie par la *blockchain* et par l'accès au code des *smart contracts* ; chacun peut voir ce qui se passe. Une fois enregistrées, les transactions sont immuables.

Le projet « The DAO » était un premier exemple d'une DAO. Son but était d'organiser une importante campagne de levée de fonds de capital-risque en 2016. Le système était basé sur la *blockchain Ethereum*. Peu de temps après son lancement, un tiers des fonds (en cryptoactif) a été détourné par des hackers mal intentionnés, ce qui a conduit à une partition de la

blockchain Ethereum (un *fork*). Quelques mois plus tard, la valeur du fonds était retirée des places d'échanges de cryptoactifs, signant de fait la fin de l'aventure.

Cette DAO permettait à des investisseurs de s'organiser pour lever des fonds en partageant les risques et les profits, sans avoir besoin de faire confiance à l'un d'entre eux pour gérer le tout. Le système était supposé fonctionner sans qu'il y ait besoin d'une autorité particulière au-delà de celle du code enregistré dans la *blockchain* (sous forme de *smart contract*). Ce modèle a été repris par la suite dans des cadres différents comme le financement collectif de logiciels ou la gestion d'organisations caritatives. On peut aujourd'hui trouver des systèmes pour déployer facilement des DAO comme la plateforme Aragon.

Comme indiqué précédemment, les DAO permettent des formes de coopération et de partage sophistiqués sans nécessiter le contrôle d'un acteur prépondérant. D'un point de vue économique, elles pourraient contribuer à éviter de fortes concentrations capitalistiques, comme celles des grandes entreprises du web. Les DAO offrent également des pistes pour expérimenter de nouvelles formes de gouvernance de communautés. Certains y voient des routes pour encourager des formes de démocraties participatives.

Difficultés et perspectives

Les DAO soulèvent différentes difficultés :

– leur fonctionnement est gravé dans leur code. Les évolutions qui n'ont pas été prévues dans la DAO posent problème. Elles demandent l'évolution du *smart contract*, ce qui est lourd et lent. Un imprévu peut avoir des conséquences dramatiques, car la communauté n'a pas le moyen de réagir rapidement. Les membres peuvent être amenés à voter pour faire évoluer les règles de la communauté, de l'admission de nouveaux membres, à la gestion des conflits, au partage des profits comme des pertes. Des aspects de la gouvernance peuvent également être délégués à un groupe d'experts ;

– les participants à une DAO peuvent être vus comme des partenaires économiques dont les interactions sont régies par le *smart contract* enregistré dans la *blockchain*. Le *smart contract* joue alors le rôle d'une forme de contrat entre les partenaires. Par la nouveauté des DAO, la valeur juridique d'un tel contrat est discutable, et d'ailleurs les DAO elles-mêmes n'ont pas aujourd'hui véritablement d'existence juridique.

On peut voir les métavers et le Web3 comme essentiellement des bulles spéculatives. Les DAO sont relativement récentes. Pour ces différents services, l'encre n'est pas sèche et l'avenir n'est pas clair. Pourtant, ils intéressent de nombreuses entreprises. Ce qui manque encore aujourd'hui dans cette direction, c'est peut-être une *success story* véritablement socialement positive pour être convaincante.

Chapitre 4

Une infrastructure coûteuse en énergie

La *blockchain* vise à assurer, sans tiers de confiance, l'ensemble des services dont a besoin un système collaboratif distribué et ouvert, avec les garanties d'immuabilité et de sécurité : ce sont ces objectifs mêmes qui sont source de complexité et, partant, de coût énergétique.

4.1. Coût énergétique de la *blockchain*

Plusieurs études permettent de chiffrer la consommation d'énergie et l'impact environnemental du *bitcoin*[27] [28] et de nombreux sites web donnent des visualisations graphiques et des comparaisons pour cette consommation, par exemple le CCAF (*Cambridge Centre for Alternative Finance*[29]), le *Digiconomist*[30] et la *Columbia Climate School*[31].

Les méthodes d'estimation varient entre ces articles. Les plus fines prennent en compte le mix énergétique dans les pays des différents mineurs, mais toutes donnent des ordres de grandeur comparables : **le réseau *bitcoin* a une consommation électrique de 125±30 TWh par an, soit le quart de la consommation annuelle électrique de la France,**

27. H. Vranken, "Sustainability of bitcoin and blockchains", *Current Opinion in Environmental Sustainability,* vol. 28, pp. 1–9, Oct. 2017, doi : 10.1016/j.cosust.2017.04.011.
28. S. Köhler and M. Pizzol, "Life Cycle Assessment of Bitcoin Mining, " *Environ. Sci. Technol*., Nov. 2019, doi : 10.1021/acs.est.9b05687.
29. https://ccaf.io/
30. https://digiconomist.net/bitcoin-energy-consumption
31. https://news.climate.columbia.edu/2022/05/04/cryptocurrency-energy/#:~:text=How

consommation largement due au mécanisme de consensus utilisé (PoW)[32], voir également Figure 6 ci-après.

Les quatre propriétés fondamentales assurées par la *blockchain* du *bitcoin* ont des coûts énergétiques qui peuvent être classés comme indiqué à la Figure 4.

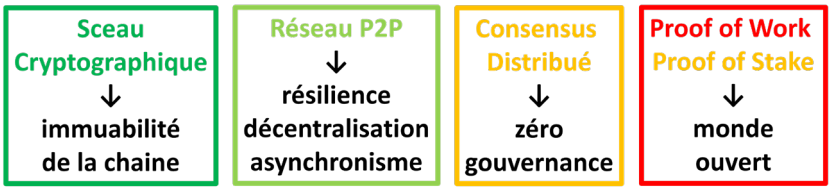


Figure 4 : la comparaison entre les coûts énergétiques des divers composants de la *blockchain* est rendue par un code couleur allant du vert franc au rouge vif.

Il est intéressant de noter que la consommation peut fluctuer assez fortement, par exemple en réponse à une variation du cours du *bitcoin* (cf. les fortes fluctuations au cours de l'année 2021 sur la Figure 5 ci-dessous). Au-delà de ces fluctuations, une tendance générale est perceptible avec un rythme de consommation annuelle qui a pratiquement doublé en 4 ans, entre le début 2020 et le dernier trimestre 2023.

32. Voir https://ccaf.io/cbnsi/cbeci University of Cambridge, Cambridge Centre for Alternative Finance.

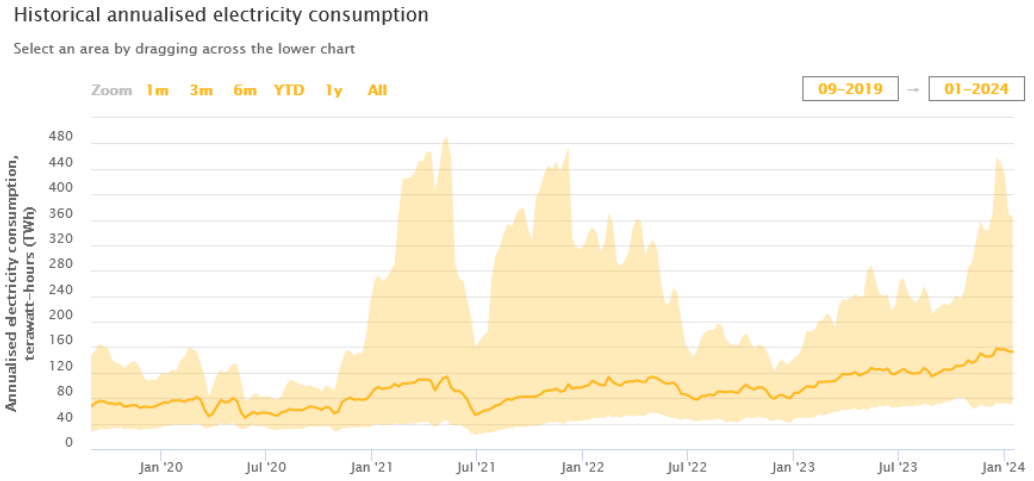


Figure 5 : Rythme annualisé de la consommation énergétique consacrée au minage du *bitcoin*. La plage colorée indique l'incertitude entre estimations basse et haute, et la courbe continue représente la « meilleure estimation » (best estimate) [source : https://ccaf.io/cbnsi/cbeci]

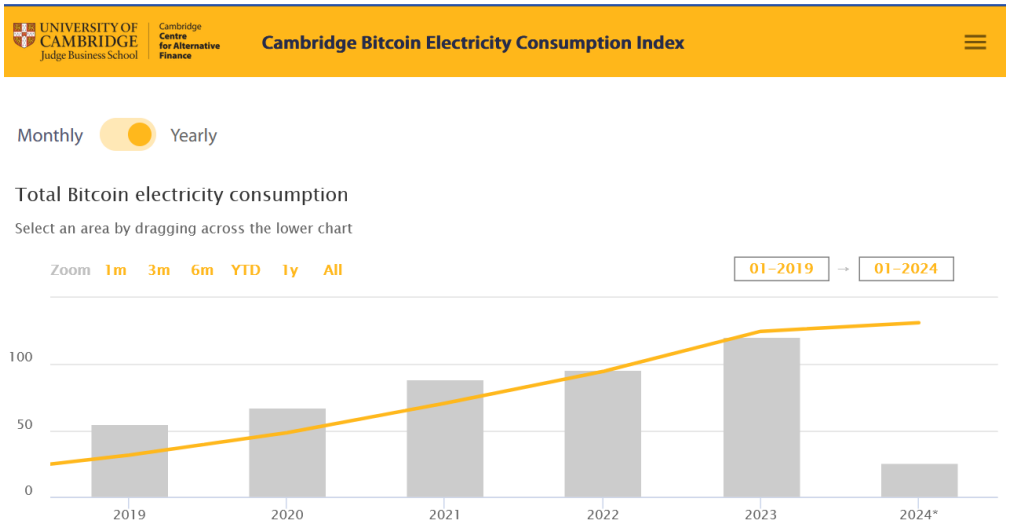


Figure 6 : Source : https://ccaf.io/cbnsi/cbeci

Cette consommation électrique représente une part substantielle de celle de l'ensemble des centres de données[33], ou encore 25 % de la consommation électrique de la France ou la totalité de celle des Pays-Bas ; mais elle ne concerne qu'un nombre beaucoup plus limité de personnes (quelques centaines de milliers) au niveau mondial. Par ailleurs les cartes ASIC dédiées utilisées pour le minage n'étant généralement pas recyclées car rendues obsolètes par l'arrivée des générations suivantes, c'est, en termes de terres rares, l'équivalent de deux iPhone 12 qui se trouve consommé pour le minage de chaque *bitcoin*[34].

L'exemple du *bitcoin* est caractéristique des systèmes de *blockchains* fondés sur la preuve de travail (PoW). C'est cet algorithme qui constitue (pour plus de 99 %) la part très largement responsable de l'impact environnemental du *bitcoin*.

Les tenants de ce minage de *bitcoin*s soutiennent que l'empreinte carbone de la méthode reste limitée, puisque les mineurs travaillent sur des centres de données alimentés par une électricité verte et que, de plus, ils peuvent facilement s'ajuster à l'intermittence des énergies renouvelables[35]. Même si ceci est vrai, au moins en partie, l'argument paraît court, car l'électricité renouvelable consommée par la méthodologie PoW n'est bien sûr plus disponible pour d'autres usages sociétaux prioritaires, à un moment où la plupart de ces derniers sont l'objet d'un effort intense de numérisation (industries et services, transports…). La même objection peut être opposée à l'argument utilisé *mutatis mutandis* pour expliquer que les consommations PoW encouragent à long terme la décarbonation massive de l'électricité, par exemple en favorisant les investissements dans la récupération du méthane (fuites, torchères, déchets…). Enfin la comparaison avec l'exploitation des mines d'or (130 TWh/an), ou la consommation électrique des sèche-linge américains (70 TWh/an, en diminution, et tout en rappelant qu'il y a 100 millions de foyers aux États-

33. A. D. Vries, "Cryptocurrencies on the road to sustainability: Ethereum paving the way for *Bitcoin*", *PATTER*, vol. 4, no. 1, Jan. 2023, doi : 10.1016/j.patter.2022.100633.
34. https://digiconomist.net/bitcoin-energy-consumption
35. Voir par exemple Bitcoin : une solution contre-intuitive au changement climatique | by Alexandre Stachtchenko | Apr, 2023 | Medium

Unis) n'est pas non plus convaincante, car leurs rôles industriels et sociaux sont très différents. Tous ces arguments font l'impasse sur le fait que le calendrier de l'urgence climatique est extrêmement serré et que, au-delà des nécessaires investissements massifs dans les énergies décarbonées, il ne peut être respecté que par des usages beaucoup plus sobres, d'autant plus sobres que l'usage est plus crucial pour la société.

4.2. Quelques pistes pour réduire la consommation

Il est souvent rapporté que les *blockchains non permissionnées* (pour les systèmes ouverts) ont une faible bande passante[36]. Ceci résulte de la taille des blocs, du temps de résolution du consensus et des mécanismes d'élection. Le ratio « coût énergétique/efficacité » reste donc insatisfaisant et son amélioration reste un sujet constant de recherches. Dans cette section nous passons en revue quelques propositions pour améliorer ce ratio. Comme on va le voir, elles sont de natures variées. À partir du moment où les utilisateurs se considèrent comme étant dans un contexte de système ouvert, ils préfèrent s'appuyer sur une infrastructure *blockchain* existante, vu la complexité d'un développement de ce type. Au plus quelques dizaines de telles *blockchains* sont proposées et beaucoup moins sont largement utilisées.

Nous illustrons ces approches par quelques figures qui déclinent la Figure 2.

36. *Bitcoin* insère dans la *blockchain* quelques transactions par seconde. Des améliorations à la marge permettent d'augmenter un peu ce chiffre. Quelques *blockchains* prétendent atteindre des dizaines de milliers de transactions natives par seconde (en laboratoire, en pratique il y a des instabilités).

AJUSTER LA *BLOCKCHAIN* PERMISSIONNÉE AU CAHIER DES CHARGES DU CAS D'USAGE CONSIDÉRÉ

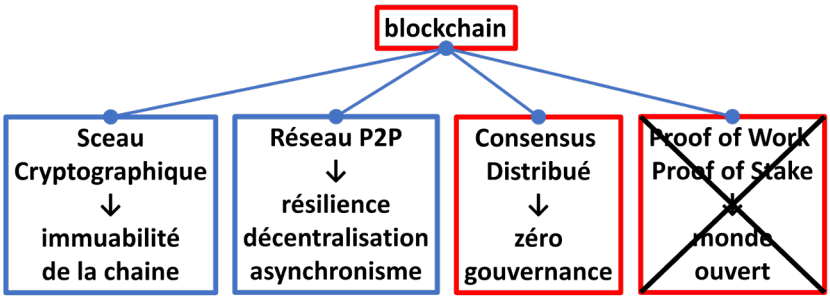


Figure 7 : simplification lorsqu'on peut se satisfaire d'une *blockchain* permissionnée.

Lorsqu'une gouvernance peut être mise en place, qui écarte le besoin de *blockchain* non permissionnée, alors l'ajustement de la *blockchain* au cahier des charges devient le moyen le plus efficace de réduire les coûts d'exploitation. Ceci suppose deux conditions :

– produire un cahier des charges qui apporte les bonnes informations ;

– pouvoir configurer une « *blockchain* » au plus juste en fonction du cahier des charges.

DES ARCHITECTURES PLUS COMPLEXES POUR ÊTRE MOINS COÛTEUSES

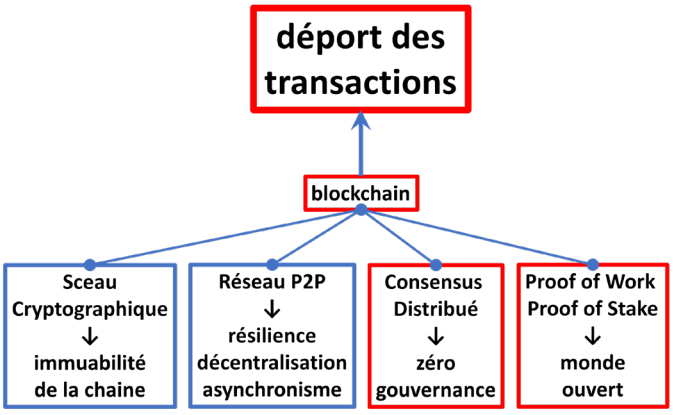


Figure 8 : réarchitecturer en déportant les transactions proprement dites hors de la *blockchain*, n'y conservant que la trace de leur référence (la *blockchain* est figurée à dessein comme étant rapetissée).

Une famille d'approches intéressante pour augmenter l'utilité et la bande passante consiste à déporter des transactions hors de la chaîne (ces transactions pouvant éventuellement être une *blockchain* parallèle), et à enregistrer une trace de ces transactions (en réalité un sceau cryptographique) en une seule transaction sur la chaîne principale. Cela recouvre des mécanismes très différents, dont voici quelques exemples :

– le réseau ***Lightning*** permet aux utilisateurs d'échanger des fonds et de les faire circuler, sans toutefois exprimer ces transferts sur la couche principale. Au niveau de la *blockchain* sont seulement enregistrées les *créations et fermetures de canaux* d'échange de valeurs, ainsi que les parties qui y sont impliquées. Les canaux permettent librement et plus efficacement des transactions privées au sein du réseau virtuel ainsi temporairement créé. À la fermeture du canal, une certaine trace des transactions effectuées est alors publiée dans la *blockchain*. Cela entraîne un gain substantiel en bande passante ;

– une autre mesure possible est de proposer une couche de transactions (***rollup***), dite de niveau 2, déportée hors de la *blockchain* principale, dite de niveau 1, et se construisant au-dessus de la technologie des *smart contracts*. Un opérateur[37] exécute les transactions initiées hors chaîne par les utilisateurs, et soumet le sceau de l'état induit par ces transactions à la *blockchain* de niveau 1. Selon la technologie utilisée, divers mécanismes de contrôle permettent d'assurer la validité des transactions hors chaîne ainsi que celle de ce sceau[38]. Ainsi, seul l'opérateur se charge de l'exécution, et la chaîne principale est réduite à une chambre d'enregistrement, ce qui allège le travail des validateurs. Une seule transaction de niveau 1 encapsule ainsi de nombreuses transactions de niveau 2, et il est espéré que la bande passante gagne ainsi plusieurs ordres de grandeurs. *Ethereum* a ainsi annoncé son évolution vers une architecture reposant sur le *rollup*.

MÉCANISMES D'INCITATION : DU POW VERS LE POS ?

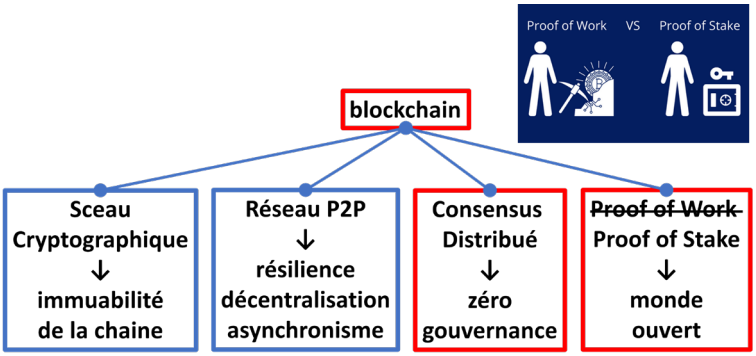


Figure 9 : migrer du PoW vers le PoS.

37. Cet opérateur est une notion laissée volontairement abstraite : cela peut être une entité centrale, un consortium ouvert, avec du consensus et des propriétés diverses, voire une *blockchain*.
38. On distingue des mécanismes de dénonciation vérifiable de fraudes, et des mécanismes de publication continue de la validité des transactions. Le premier cas, *optimistic rollup*, est relativement *low tech*, le deuxième, *validity rollup*, fait appel à de la cryptographie récente non standard et très avancée (*zero knowledge*).

Une autre piste pour améliorer les performances énergétiques du mécanisme de consensus dans les *blockchains* ouvertes consiste **en l'abandon du PoW, *Proof of Work*** (trop gourmand en énergie) au profit d'autres techniques, dont la plus connue est ***le PoS, Proof of Stake*** (preuve d'enjeu). Ces techniques sont réputées réduire cet impact de plusieurs ordres de grandeur : une réduction d'au moins un facteur 1000 est citée pour l'utilisation par *Ethereum* d'un algorithme PoS (algorithme toutefois non formellement validé à ce jour). Des billets (blogs) et rapports récents[39] [40] [41] [42] [43] estiment que les *blockchains* publiques n'utilisant pas la PoW consomment entre 4 et 6 ordres de grandeur de moins d'électricité que le réseau *bitcoin*, et que le gain par transaction peut même atteindre 8 ordres de grandeur pour devenir négligeable, par exemple de l'ordre de la consommation du chargement d'une page web ou de l'envoi d'un mail. Cette évolution exige que ces solutions alternatives soient *spécifiées formellement et prouvées* correctes, ce qui reste, à notre connaissance, ouvert[44].

39. L. Cocco, R. Tonelli, and M. Marchesi, "An Agent Based Model to Analyze the Bitcoin Mining Activity and a Comparison with the Gold Mining Industry, " *Future Internet*, vol. 11, no. 1, p. 8, Jan. 2019, doi : 10.3390/fi11010008
40. T. Q. Tezos, "Proof of Work vs. Proof of Stake : The Ecological Footprint, " Mar. 16, 2021. https://medium.com/tqtezos/proof-of-work-vs-proof-of-stake-the-ecological-footprint-c58029faee44 (accessed Mar. 24, 2021).
41. "Sustainable Blockchain : Estimating the Carbon Footprint of Algorand's Pure Proof-of-Stake." https://www.algorand.com/resources/blog/sustainable-blockchain-calculating-the-carbon-footprint (accessed Jan. 11, 2023).
42. Crypto Carbon Ratings Institute (CCRI), "Energy Efficiency and Carbon Footprint of PoS Blockchain Protocols, " Jan. 2022. https://carbon-ratings.com/dl/whitepaper-pos-methods-2022 (accessed Jan. 24, 2023).
43. Bitcoin, une solution contre-intuitive au changement climatique, Alexandre Stachtchenko, Apr 2023, Medium.
44. Le rapport commandité par la DGE (cf. note de bas de page 3) contient beaucoup plus de précisions techniques accompagnées de références sur ces sujets, nous y renvoyons le lecteur désireux d'en savoir plus.

Chapitre 5

Conclusion et messages

5.1. État des lieux et constatations

La *blockchain* : une révolution dans la conduite sûre de transactions à l'échelle mondiale

La technologie *blockchain* est une révolution qui apporte une solution élégante à bien des problèmes posés par la conduite sûre de transactions à l'échelle mondiale et en univers ouvert. Il faut se rappeler que, pour des raisons de performance, la *blockchain* n'est pas une technologie de stockage de données. Cependant, **cette vertu s'accompagne d'un vice très sérieux concernant la consommation énergétique.**

État général de la recherche

S'agissant des coutumes de travail de cette filière, on peut formuler les quelques remarques suivantes. Le domaine fait preuve d'une créativité débordante. Les annonces et documents se font principalement en dehors des vecteurs académiques (réseaux sociaux, messagerie). Beaucoup de protocoles sont proposés, sans que pour autant leur justification par une étude formelle soit fournie (contrairement au domaine de la cryptographie, par exemple). C'est sans doute pourquoi, en France tout du moins, le monde académique et en son sein les communautés qui auraient vocation à s'y intéresser, portent un intérêt insuffisant au domaine ; et on peut le regretter.

De nouvelles directions : des registres (*ledger*) aux graphes (DAG)

S'agissant de nouvelles directions de recherche, il est intéressant de voir apparaître un nouveau paradigme (voir par exemple[45]) où, au lieu de viser à produire un registre (*ledger*), l'on cherche à construire, par consensus distribué et ouvert, un DAG (*Directed Acyclic Graph*) organisant les blocs selon un lien de causalité. Les points de croissance de la structure sont ainsi plus nombreux et peuvent être traités en parallèle. Les auteurs prétendent ainsi à une meilleure efficacité de leur nouveau consensus. Les analyses fournies pour valider formellement l'approche sont de nature probabiliste. S'il devient difficile de rattacher cette nouvelle direction au domaine de la *blockchain* (puisque de chaîne il n'est plus question), tous les objectifs fondamentaux restent néanmoins les mêmes.

Les *blockchains* les plus visibles

Nous l'avons vu, le concept de *blockchain* est une révolution sur le plan scientifique et technologique. Il a résolu le problème de l'établissement d'un monde transactionnel ouvert, mais sûr, sans le recours à un tiers de confiance : un problème que la communauté s'accordait à considérer comme insoluble. La notion de registre distribué fiable et ouvert a apporté une réponse. Attention, le qualificatif « sûr » n'est pas à prendre au pied de la lettre : cette sûreté est garantie avec une forte probabilité, ce qui suffit en pratique.

Parmi les infrastructures ayant pignon sur rue, à côté de *bitcoin* qui est dédié à la monnaie, *Ethereum* ressort comme étant largement utilisée et assez flexible pour être reprise comme base pour des usages divers. Les trois grandes propriétés de la *blockchain* (distribuée, ouverte, immuable)

45. E. Anceaume, A. Guellier, R. Ludinard and B. Sericola, "Sycomore, a Directed acyclic graph of blocks that securely self-adapts to transactions demand", Proceedings of the 16th IEEE International Symposium on Network Computing and Applications (NCA), 2018. Abstract : We propose a new way to organize both transactions and blocks in a distributed ledger to address the performance issues of permissionless ledgers. In contrast to most of the existing solutions in which the ledger is a chain of blocks extracted from a tree or a graph of chains, we present a distributed ledger whose structure is a balanced directed acyclic graph of blocks. We call this specific graph a SYC-DAG. We show that a SYC-DAG allows us to keep all the remarkable properties of the Bitcoin blockchain in terms of security, immutability, and transparency, while enjoying higher throughput and self-adaptivity to transactions demand.

sont intéressantes à combiner, en tout ou partie, selon les besoins. Faire au plus juste permet, le cas échéant, de faire l'économie de mécanismes coûteux.

Le cas de l'Estonie

L'Estonie est pionnière de l'utilisation du numérique dans l'administration[46]. Dans les éléments développés pour ce faire on en trouve deux intéressants (open source comme la plupart des blocs) :

Keyless Signature Infrastructure (KSI Blockchain) : une *blockchain* spécialisée dans la gestion de *timestamps* pour préserver l'intégrité des documents numériques au sein de plusieurs registres publics au cours du temps (ceci a été développé par une entreprise estonienne, Guardtime, et aussi utilisée par l'Otan, US DoD, Lockheed Martin, Ericsson…) [lien GitHub, papiers techniques]. KSI est utilisé comme chambre d'enregistrement de signatures d'intégrité, mais pas pour le stockage lui-même ni pour les échanges qui utilisent XRoads (infrastructure centralisée d'échange de donnée).

e-Democracy qui comprend le système d'élection i-Voting, utilisé depuis 2005 pour les élections en Estonie, et s'appuyant sur la *blockchain* Stellar. Ce système de vote électronique permet aux électeurs de participer aux élections de n'importe où dans le monde [lien GitHub, détails techniques].

Hyperledger, plateforme et écosystème pour *blockchain* B2B

Les messages que nous avons reçus des industriels lors de nos interviews indiquent qu'ils semblent préférer une plateforme *blockchain* existante, plutôt qu'un assemblage fait maison de composants à façon. Concevoir une plateforme collaborative B2B se résume alors à coder, au-dessus d'une plateforme *blockchain* existante, un *smart contract* et une application qui interagit avec lui. La *blockchain* utilisée est alors de type permissionné. La fondation Hyperledger suit cette approche. Elle se présente comme un

46. voir le site e-Estonia et une présentation.

écosystème global[47] pour *blockchain* B2B (ou plus généralement *blockchain* pour les entreprises). La base en est une *blockchain* permissionnée, dont l'algorithme de consensus peut être configuré et sélectionné, dans une bibliothèque prédéfinie, selon les besoins de l'application[48]. En tout état de cause, point besoin n'est de PoW.

Une résilience à toute épreuve, avec quelles conséquences ?

La résilience des *blockchains* (non permissionnées) est leur point fort principal, comme on l'a vu. Elles ont été précisément conçues pour résister à toute forme d'agression, à commencer par les modifications hostiles[49]. Mais cette résilience est aussi source de problèmes en raison de la quasi impossibilité technique de stopper ou même de contrôler une *blockchain*. De fait, comme le montre la sous-section « développements récents » de la Section 2.1 concernant le *bitcoin* (il y est souligné que le changement de position récent de la SEC à propos du *bitcoin* s'est fait sous pression), cette résilience constitue une pression sur les autorités de régulation et manifeste le fait que, lorsqu'elle est doublée d'une popularité due au nombre de ses utilisateurs, la *blockchain* échappe au contrôle politique des États. Les moyens d'arrêter de telles infrastructures semblent peu nombreux : le contrôle des entrées et sorties de la *blockchain* (lors de la conversion en monnaie publique), l'incitation externe à la perte de confiance, voire le recours à un *hard fork*, un *fork* volontaire et malveillant destiné à créer un futur alternatif au *bitcoin*[50]. Ces moyens sont tous délicats à utiliser. De ce point de vue, la résilience des *blockchains* peut donc être perçue comme une menace sur nos sociétés.

47. Selon le site de la fondation, Hyperledger est "*The open source, global ecosystem for enterprise-grade blockchain technologies that are at the core of critical developments and implementations around the world.*"
48. Voir l'article suivant de présentation de Hyperledger https://8112310.fs1.hubspotusercontent-na1.net/hubfs/8112310/Hyperledger/Offers/Hyperledger_Arch_WG_Paper_1_Consensus.pdf
49. L'Ether est protégé par une réserve de l'ordre de 50 milliards d'euros. La protection du *bitcoin* est par le biais de la PoW, dont la violation demande une possession d'au moins 50 % des ressources totales.
50. Par exemple, sous le contrôle d'un ETF, voir https://viresinnumeris.fr/etf-bitcoin-blackfork/.

5.2. Recommandations

Commençons d'abord par un avertissement. Le lecteur pourrait s'attendre à ce que ce rapport formule une opinion forte sur le ratio inconvénients/bénéfices associé à la *blockchain*, pour nos sociétés. Le présent rapport a égrené plusieurs observations à ce sujet. Toutefois, de telles appréciations sont souvent entachées d'*a priori* moraux ou idéologiques[51]. Pour notre appréciation globale, nous avons donc choisi de nous placer d'un point de vue différent. **Laissant aux entités dont c'est le rôle le soin de formuler des appréciations morales ou de société, nous concentrons nos recommandations sur les moyens, pour nos sociétés, d'observer, évaluer et mesurer, et sur les leviers pour agir en conséquence.** Nous y avons ajouté quelques recommandations d'ordre plus général.

Notre étude nous conduit donc à formuler les recommandations suivantes.

Combattre le coût énergétique excessif en développant des solutions nouvelles

Il est essentiel de progresser sur l'efficacité (en particulier énergétique) de chacun des mécanismes de la *blockchain*, tout en en préservant les vertus.

Parmi les approches qui semblent intéressantes, figurent les **adaptations d'architectures** (qui déportent hors de la *blockchain* la partie « lourde » des données ou transactions considérées).

Un axe de progrès essentiel réside dans les approches autres que la PoW (*Proof of Work*) pour assurer la résilience en mode ouvert. En particulier, les diverses et nombreuses variantes de la PoS (*Proof of Stake*) réclament des travaux qui en assureraient la validité formellement. Plus généralement :

Toute nouvelle proposition assurant la sûreté en mode ouvert doit être étayée par des études formelles prouvant les propriétés affichées.

51. Voir par exemple un discours ministériel récent : https://www.vie-publique.fr/discours/270363-bruno-le-maire-15042019-blockchain-stockage-transmission-informations

LA RECHERCHE RESTE VIVANTE ET IL CONVIENT DE L'ENCOURAGER

De nombreuses variantes continuent à être proposées à partir des techniques utilisées dans le *bitcoin* et, surtout, autour de *Ethereum*. Il faut encourager les travaux visant à valider formellement (ou invalider) ces propositions : ces résultats sont nécessaires pour étayer ces diverses propositions dont la raison d'être principale est, tout de même, la sécurité et la résilience.

Par ailleurs, il convient de porter attention aux nouvelles explorations de la recherche, en particulier celles qui concernent le passage d'une chaîne (*ledger*) à un graphe (DAG, *Directed Acyclic Graph*). Ces nouvelles approches, qui ouvrent des possibilités nouvelles de parallélisme, pourraient être porteuses d'améliorations de performance, en particulier en matière de débit de traitement des transactions.

Face à une communauté qui opère en publiant largement hors des circuits validés par les pairs, il convient de soutenir les activités de recherche avec une vision ouverte laissant la place aux propositions nouvelles.

B2B : MIEUX FONDER LES BOÎTES À OUTILS DE *BLOCKCHAIN* PERMISSIONNÉES ET LES *SMART CONTRACTS*

Le secteur du B2B voir émerger des besoins croissants (de type notarial et, de plus en plus, pour des filières de logistique) de services de type *blockchain* ; en l'espèce il s'agit, essentiellement, de *blockchain* permissionnée. Point n'est besoin d'algorithmique coûteuse telle que la PoW, puisque la population d'abonnés est connue et non ouverte. Nous avons mentionné le cas de l'écosystème *Hyperledger*. D'autres initiatives similaires existent ou seront proposées.

Ces acteurs proposent des boîtes à outils de composants permettant de se faire des *blockchains* permissionnées à façon, ainsi que des *smart contracts*. Les systèmes qui en résultent restent toutefois complexes, car les services qu'ils combinent sont tout sauf orthogonaux : leur interaction est au contraire intime au sein des systèmes ainsi construits et c'est le système dans son ensemble qui procure le service attendu. C'est typiquement un cas de figure où les risques d'interactions indésirables entre composants sont les plus forts, ce qui est en soi source d'erreurs.

Favoriser le développement de boîtes à outils bien fondées pour tout type de *blockchain*

En fait, le besoin de boîtes à outils bien fondées existe, pour tout type de *blockchain*, qu'elle soit permissionnée ou non. Le risque d'interaction indésirable existe dans les deux types. Bien entendu, il y a entre ces deux types des différences de fond et les études formelles auront à le refléter.

La recommandation qui suit vaut donc pour ce point et le précédent :

Seules des études formelles permettent d'identifier les bonnes combinaisons de composants et de s'assurer que leur composition donne le résultat escompté. Cela passe par l'identification d'un modèle abstrait des éléments constitutifs de la blockchain et de leur combinaison[52].

Progresser sur l'établissement d'un cahier des charges pour un usage donné

Contrairement au point précédent, celui-ci ne retient pas « naturellement » l'attention des communautés de la recherche. Elle ne ressort pas non plus des objectifs des startups puisqu'il s'agit plutôt d'une tâche d'intérêt commun.

Trop souvent les cahiers des charges sont des collections non (ou peu) structurées d'exigences. On y trouve plein d'éléments auxquels le concepteur a pensé, mais dont l'importance est variable pour fonder les choix architecturaux pour la *blockchain* « au plus juste ». Il faut donc favoriser le développement de méthodologies guidant la construction des cahiers des charges et s'assurant que les exigences clés ont bien été fournies.

En particulier, la question centrale est le choix, pour la *blockchain* à déployer, entre *permissionné* et *non permissionné*.

52. Voir par exemple : E. Anceaume, A. Del Pozzo, R. Ludinard, M. Potop-Butucaru, S. Tucci-Piergiovanni, "Blockchain Abstract Data Type", 31st ACM Symposium on Parallelism in Algorithms and Architectures (SPAA), 2019.

Il faut donc clairement identifier si l'on veut considérer la population d'acteurs concernée par le cas d'étude comme *fermée* ou *ouverte*.

La réponse à cette question ne va pas toujours de soi dans le B2B.

– Si l'on opte pour *ouverte*, alors il faudra payer le prix par le recours à une protection forte de type PoW (sûre, mais très coûteuse), voire PoS (moins coûteuse, mais non validée au même niveau que la PoW), ou autres.

– Si l'on opte pour un cadre *fermé* (comme c'est l'hypothèse pour *Hyperledger*), alors il faut en examiner le coût juridique en termes de gouvernance (qui accrédite un candidat usager ? et comment ?).

Organismes gouvernementaux ou de régulation : évaluer et intervenir

Plus précisément, s'agissant des organismes gouvernementaux ou de régulation, il nous paraît indispensable qu'ils puissent :

– mesurer les usages des *blockchains* et des cryptoactifs de manière directe et autonome, pour avoir une information sûre et de première main[53] ;

– évaluer les risques d'une infrastructure *blockchain*, et

– disposer de moyens pour intervenir.

S'agissant des moyens de métrologie, un *nutriscore énergétique* nous paraît indispensable : une infrastructure *blockchain* devrait être tenue d'afficher les éléments qui permettent aisément une évaluation, par un organisme extérieur, de la consommation énergétique (il s'agirait d'ordres de grandeur).

53. Le leader du marché est ChainAnalysis, américain, dont il faut espérer que les rapports sont honnêtes.

S'agissant des **moyens d'intervenir**, les leviers suivants pourraient être considérés :

– pour les *blockchains* non permissionnées (pour système ouvert) utilisant la PoW, on pourrait demander des moyens de contrôle des mineurs[54]. Ou, plus généralement, de la partie la plus coûteuse de la *blockchain* ;

– demander des leviers d'action permettant d'intervenir lors de l'entrée ou de la sortie de la *blockchain* ;

– par une régulation externe, disposer de leviers permettant d'agir sur la confiance dans l'infrastructure *blockchain*[55].

Pour pouvoir intervenir efficacement, il faut comprendre les enjeux et les technologies. Or, comme ce rapport l'a amplement démontré, les *blockchains* en contexte ouvert (*permissionless*) sont complexes. De nombreuses technologies y sont combinées (cryptographie, algorithmique distribuée, incitations économiques, aspects monétaires) et le système global devient difficile à appréhender. Il est ainsi trompeur de les réduire à l'une des technologies sur lesquelles elles reposent. Il est donc rare de réunir des réelles compétences *blockchains* dans leur totalité.

Aussi, nous recommandons que soient proposées des formations approfondies pour une forte montée en compétence des acteurs de l'état (ainsi que des grands opérateurs), qui seront amenés à intervenir dans divers domaines (financiers, économiques, juridiques, législatifs, régulateurs, normatifs) face à l'industrie du domaine et divers lobbyistes.

54. Se rappeler que la Chine a banni le déploiement de mineurs sur son territoire, ce qui a conduit à leur report vers le Kazakhstan et les USA, y causant une accélération de l'activité des *data centers*.

55. Un exemple est celui de l'interaction entre la SEC et le *bitcoin* (mentionnée en fin de la Section 2.1) : la SEC aurait pu décider de maintenir ses digues et de ne pas ouvrir cette facilité.

Vers une démarche de certification

Dans la mesure où il s'agit d'une infrastructure critique, du point de vue des usages, de la consommation énergétique, et plus globalement pour la société, nous pensons que la technologie *blockchain* devrait être accompagnée d'un écosystème de *certification*, visant à instaurer une attitude plus prudentielle du secteur (comme c'est le cas pour la certification en aéronautique).

Cet écosystème serait, par exemple, compétent pour :

- reconnaître qu'une technologie est validée, par exemple parce qu'elle est étayée par un corpus publié d'études formelles (d'autres critères liés à la méthodologie de développement et de déploiement peuvent également entrer en compte) ;

- reconnaître et certifier des leviers de contrôle déposés par les concepteurs d'un système *blockchain* considéré.

Membres du groupe de travail

Académie des technologies
Jean-Claude ANDRÉ
Albert BENVENISTE (animateur)
Christian de BOISSIEU
Michel LAROCHE
Sophie PROUST
Gérard ROUCAIROL

Académie des sciences
Serge ABITEBOUL
Olivier PIRONNEAU

Experts
Emmanuelle ANCEAUME
Daniel AUGOT
Thierry CHEVALIER

Nous remercions Brigitte PLATEAU pour sa relecture du rapport,
ainsi que le Comité de la qualité, en particulier François LEFAUDEUX

La *blockchain* s'impose comme une technologie révolutionnaire promettant de transformer de nombreux secteurs, de la finance à la santé en passant par l'éducation et l'énergie. Pour l'Europe et la France, en quête de souveraineté industrielle, elle offre de nombreuses opportunités. Elle soulève également des défis majeurs, notamment en termes d'usage et d'impact environnemental.

Au cœur de la *blockchain* se trouvent les *smart contracts* destinés à asseoir les transactions et les NFT (*Non-Fungible Tokens*) permettant de définir des objets numériques. Son principal intérêt réside dans les applications qu'elle permet, lesquelles se sont considérablement élargies au-delà des cryptomonnaies, son champ d'application initial.

La *blockchain* est solution logicielle sophistiquée dont l'infrastructure est distribuée et décentralisée, et résiliente aux attaques ; elle repose sur des acquis fondamentaux de la recherche (mécanismes de consensus dans des mondes distribués ouverts, et cryptographie). Ce sont les mécanismes mêmes qui assurent la résilience d'une *blockchain* qui sont à l'origine d'une consommation énergétique souvent jugée excessive : c'est le vice sérieux qui est la contrepartie du service offert.

Comment concilier l'essor de cette technologie avec la nécessité de préserver notre environnement ? C'est la question centrale à laquelle l'Académie des technologies tente de répondre dans ce rapport destiné aux décideurs, entrepreneurs et citoyens. Elle propose six recommandations, invitant ainsi à une réflexion prospective sur cette innovation pour un progrès choisi et raisonné.

Académie des technologies
Le Ponant – Bâtiment A
19, rue Leblanc
75015 PARIS
+33(0)1 53 85 44 44
secretariat@academie-technologies.fr
www.academie-technologies.fr

ISBN : 979-10-97579-53-1

Couverture : Hessyz - Adobe stock