

Livre blanc La blockchain pour les entreprises

Soyez curieux !
Comprendre et
expérimenter

Avec





Édito

Depuis le début de mon mandat au MEDEF, je n'ai cessé de mettre la transformation numérique des entreprises, et en particulier des PME, au cœur des défis à relever pour faire gagner la France dans la mondialisation de l'économie.

Le numérique et son pouvoir de métamorphose transforme les modèles d'affaires et appelle à la réorganisation de bien des domaines de l'entreprise.

Cependant, l'accélération des rythmes d'innovation fait émerger rapidement de nouveaux concurrents, de nouveaux marchés mais également de nouvelles technologies qu'il faut s'approprier. C'est le cas de la blockchain, apparue en 2008 et restée confidentielle pendant des années, mais qui laisse aujourd'hui transparaître une nouvelle disruption massive des modèles, des acteurs et des transactions. Le monde en parle, mais il est encore difficile d'en appréhender toutes les applications et leurs conséquences.

Cette technologie décentralisée permet en effet le stockage et la diffusion d'informations de manière sécurisée et à moindre coût. Longtemps associée à la monnaie numérique, grâce à laquelle elle a été introduite, la blockchain a de nombreux autres usages et participe notamment à rendre les entreprises plus efficaces.

Il est important de comprendre que la technologie blockchain n'est pas uniquement destinée aux institutions financières et peut être utilisée dans tous les secteurs d'activité. Même si cette technologie n'est pas encore mature il est essentiel de s'intéresser dès aujourd'hui aux possibilités qu'elle offre aux entreprises, afin que les décideurs d'entreprises se l'approprient le plus rapidement possible.

La France a l'opportunité de se positionner en précurseur sur l'application de cette technologie et il est indispensable de sensibiliser nos chefs et cadres d'entreprise, de promouvoir l'écosystème de start-up françaises travaillant avec la blockchain et surtout de pousser la collaboration entre ces start-up et les entreprises françaises. C'est par cette collaboration que nous co-construons les nouveaux modèles permis par la blockchain.

C'est pour cela que le MEDEF, dans la continuité des actions de la Commission Transformation Numérique a décidé de mener des actions de sensibilisation à travers la publication de ce livre blanc et l'organisation d'un BizHackathon Blockchain : afin de réunir des décideurs économiques de secteurs variés et de les faire réfléchir ensemble aux applications permises par la blockchain qui transformeront demain nos entreprises, leurs activités et renforceront à n'en pas douter la confiance et la sécurité des transactions.

Pierre Gattaz

Président du MEDEF





Sommaire

Guide de lecture	7
Liste des encarts	7
Introduction	9

Partie 1

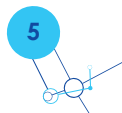
Soyez curieux ! Comprendre la blockchain 13

1. Une révolution en route : les principes de base de la blockchain	13
2. L'arbre qui cache la forêt : bitcoin ou le premier exemple à grande échelle	14
2.1. Le fonctionnement de la monnaie bitcoin	15
2.2. Les limites de la monnaie bitcoin	18
2.3. Au-delà du bitcoin	20
3. Trois éclairages sur le mode de fonctionnement de la blockchain	21
3.1. L'exploitation d'une capacité de stockage en abondance	21
3.2. La continuité virtuelle	21
3.3. L'architecture technique de la blockchain	22
4. Les limites de la blockchain	25
4.1. La confiance périphérique	25
4.2. Le passage à l'échelle	27

Partie 2

Soyez audacieux ! Expérimenter la blockchain 30

5. L'importance d'expérimenter la blockchain	30
5.1. Un intérêt croissant des acteurs économiques	30
5.2. Des attentes élevées autour de cette technologie en phase de maturation	31
5.3. Quelques éléments de cartographie de l'écosystème blockchain	33
5.4. Les modalités de collaboration au sein de l'écosystème	36
5.5. Quelques cas d'usage emblématiques de la blockchain	38
	41





6. Un écosystème non stabilisé : comprendre les enjeux des évolutions en cours	42
6.1. Le rôle des blockchains publiques et des blockchains privées	42
6.2. Le rôle clé du législateur	43
6.3. Un retour sur investissement encore lointain	46
7. Trois principes d'actions pour anticiper	47
7.1. Connaître précisément son environnement	47
7.2. Garder toutes ses options ouvertes	47
7.3. Expérimenter encore et encore	47
8. Conclusion	51
9. Remerciements	52
10. Glossaire	52
11. Références	54
12. À propos des partenaires	55
13. Annexes	58



Guide de lecture

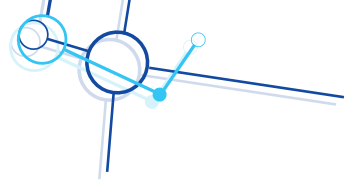
En fonction du temps dont vous disposez, plusieurs niveaux de lecture sont proposés :

- **Niveau 1** (10 minutes) :
 - > introduction
 - > blocs récapitulatifs de chaque chapitre
 - > conclusion
- **Niveau 2** (20 minutes) :
 - > niveau 1
 - > l'application à l'origine de la blockchain, le bitcoin (§2)
 - > quelques cas d'usage non financiers (§5.5)
 - > les principes essentiels à respecter pour tirer parti de la révolution blockchain (§7)
- **Niveau 3** (30 minutes) :
 - > niveau 2
 - > vue d'ensemble de l'écosystème blockchain (§5)
- **Niveau 4** (120 minutes) :
 - > ensemble du livre blanc hors encarts
- **Niveau 5** (150 minutes) :
 - > ensemble du livre blanc

Liste des encarts

1. La blockchain expliquée
2. La Poste, acteur de confiance séculaire, aborde la blockchain
3. Une première implémentation de la tenue de registre sur la blockchain sur le marché français
4. Traçabilité et blockchain
5. « Coopétition » et initiative LaBChain CDC
6. Mutualisation des ressources pour créer une start-up sur la blockchain
7. Quelques applications de l'inaltérabilité apportée par la blockchain
8. Les blockchains privées ne révolutionneront pas l'économie
9. Blockchain et Industrie, la réponse à un besoin de Confiance Numérique généralisé
10. Les apports de la blockchain pour le régulateur
11. Anticiper la blockchain
12. Penser les ruptures





Introduction

Le développement du commerce et la sophistication de notre vie en société n'auraient pas été possibles sans la faculté de noter et de mémoriser les faits et choses dont nous voulons garder trace.

Cette faculté d'enregistrer – littéralement de consigner dans un registre – a connu trois révolutions majeures qui ont chacune permis de la rendre à la fois plus accessible et plus puissante.

La première a été l'invention du papier ou, pour le dire autrement, des premiers registres qui ont révolutionné la façon de conserver et de partager l'information indispensable aux échanges sous toutes leurs formes.

La deuxième révolution a été l'imprimerie et l'industrialisation du processus de reprographie qui ont décuplé les capacités de conservation et de diffusion de l'information contenue dans les registres.

La troisième révolution est l'apparition de l'ordinateur qui a permis la numérisation du registre.

Cependant, aucune de ces trois révolutions n'avait encore apporté de réponses aux deux limites séculaires du registre en tant que facteur de confiance nécessaire aux échanges : l'impossibilité de le mettre à jour de manière collaborative et l'impossibilité de garantir son inaltérabilité et son inviolabilité.

L'apparition de tiers de confiance – par exemple le notaire dans le cas d'un transfert de propriété, ou la banque dans le cas d'une transaction financière – a eu comme rôle social de pallier ces limites, avec comme contrepartie des coûts de transaction élevés et des délais supplémentaires.

Une quatrième révolution...

Depuis son apparition il y a une dizaine d'années, une nouvelle technologie, la blockchain, nous promet de remplacer ces tiers de confiance, ou plus exactement de les déplacer, voire dans certains cas de les rendre inutiles, en garantissant que les registres soient infalsifiables tout en permettant de les mettre à jour de façon collaborative en temps réel, alors même que ces deux objectifs paraissent contradictoires.

Définie comme registre infalsifiable distribué, la blockchain lance la quatrième révolution des facultés de conservation et de partage des informations dont nous souhaitons garder trace.

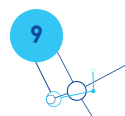
Registre *infalsifiable* parce que la blockchain permet de sécuriser et de garantir un historique de données, une inviolabilité des échanges, c'est-à-dire une source unique de vérité, alors qu'écrits, imprimés ou fichiers se limitent à porter un message sans en assurer la véracité.

Registre *distribué* parce que fonctionnant sans organe de contrôle centralisé et pouvant être mis à jour en temps réel par toutes les parties prenantes à un échange. Associée à des méthodes classiques de cryptologie, la blockchain permet aux parties prenantes de contrôler le niveau d'information partagée dans le registre.

La croissance exponentielle des données générées par nos échanges, une des dimensions du *big data*, soulève des enjeux de contrôle d'authenticité (ainsi que de maîtrise des risques de piratage) et de partage des données individuelles sans précédent, auxquels la blockchain apporte une réponse.

...qui concerne tous les secteurs

Après une première application dans le domaine des monnaies virtuelles (bitcoin), la blockchain commence à être testée dans des domaines aussi variés que l'énergie, le transport ou l'automobile. Cette nouvelle technologie possède en effet un potentiel d'une impressionnante polyvalence et ne saurait être cantonnée au bitcoin et à la médiatisation sulfureuse dont ce dernier a fait l'objet.



Parmi les nombreuses applications concrètes de la blockchain en cours de développement, nous pouvons citer :

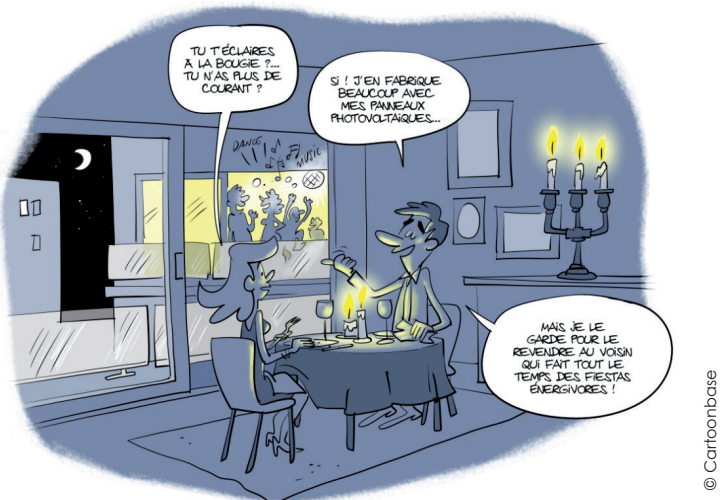
- la traçabilité du porc chinois du producteur jusqu'au consommateur (Walmart, IBM) ;



- l'ouverture d'un logement loué sur une plateforme collaborative grâce au couplage blockchain-Objets connectés (Slock.it) ;



- l'échange d'électricité en pair-à-pair (peer-to-peer) à l'échelle d'un quartier (Bouygues Immobilier et Stratumn).





Il existe en réalité plusieurs types de blockchains, des publiques, des privées ainsi que des protocoles blockchain différents, Bitcoin en étant un exemple. Cependant, dans tous les cas, la blockchain peut être techniquement considérée comme la combinaison de trois technologies : un système de partage en pair-à-pair sur un réseau (qui constitue le registre partagé), des algorithmes de validation des nouvelles entrées écrites dans ce registre, et des techniques cryptographiques avancées pour sécuriser les échanges de données ou les transactions. C'est cette combinaison qui crée une infrastructure générant de la confiance et qui permet de réaliser des échanges de valeur sans intermédiaire de confiance.

L'enthousiasme suscité par la blockchain doit cependant être modéré par trois facteurs d'incertitudes : la technologie et les algorithmes sous-jacents évoluent vite et ne sont pas à maturité ; l'horizon de rentabilité des investissements pourrait être plus lointain qu'anticipé ; et la réglementation n'est pas encore formalisée.

Face à l'impact potentiel fantastique – mais protéiforme – et malgré les incertitudes, il est essentiel que les décideurs s'acculturent sur la blockchain et en étudient les implications possibles sur leurs activités. Un sondage réalisé en mai 2017 par le MEDEF montre que 66 % des décideurs, tous secteurs d'activité confondus, s'intéressent au sujet, 69 % sont prêts à mener des expérimentations autour de la blockchain, mais seulement 16 % disent vouloir nommer un responsable blockchain, ce qui montre que la technologie et ses applications possibles doivent gagner en maturité avant qu'il ne devienne rentable d'y consacrer plus de ressources.

Au-delà du *buzzword*, ce livre blanc vise à expliquer les concepts sous-tendant la blockchain, à dresser un état des lieux de l'avancement de cette révolution et à recenser les quelques questions-clés que les acteurs économiques devront se poser pour tirer parti de cette révolution.

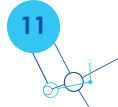
Plus précisément, ce livre blanc met en évidence, dans sa première partie, la manière dont les coûts de transaction et la confiance pourraient être redéfinis par la blockchain.

La deuxième partie du livre blanc s'attache à démontrer l'intérêt pour les décideurs d'expérimenter la blockchain, de se poser les bonnes questions sur le sujet blockchain et de s'exercer :

- Quels aspects de mon organisation sont vulnérables à la désintermédiation et quelle est la probabilité pour que celle-ci ait lieu ?
- Comment dois-je repenser et réformer mon activité actuelle avant que d'autres ne le fassent pour moi ?
- Comment tirer avantage des propriétés de la blockchain pour créer des offres et business modèles nouveaux ?
- Dois-je m'aventurer seul dans le développement de solutions fondées sur la blockchain ou dois-je collaborer avec mes concurrents ?

Ce livre blanc s'appuie sur quatre sources principales :

- le papier BCG Perspectives « *Thinking Outside the Blocks* » publié par le Boston Consulting Group le 8 décembre 2016 ;
- une recherche spécifique et des entretiens conduits par une équipe du Boston Consulting Group et d'Expand Research dans le cadre d'un sprint sur la blockchain pendant le premier trimestre 2017 ;
- un sondage réalisé par le MEDEF en mai 2017 auprès de ses adhérents concernant le niveau d'appétence des décideurs français pour la blockchain. Ce sondage visait à définir le profil du répondant ; il portait sur leur niveau d'intérêt et de connaissance de la blockchain et sur leur niveau d'engagement pour expérimenter cette technologie ;
- un BizHackathon organisé à l'initiative du MEDEF, en partenariat avec BeMyApp, le Boston Consulting Group, Blockchain Partner, le CIGREF, emlyon business school et Platinion, les 7 et 8 juin 2017, dont l'objectif était de montrer qu'en deux journées, une acculturation sur la blockchain est possible et qu'à l'issue de cet événement, des idées d'applications et de cas d'usage concrets peuvent déjà émerger chez des dirigeants d'entreprises qui ne sont pas des spécialistes du sujet, illustrant ainsi l'utilité pour eux de commencer à s'exercer sur ces technologies.





Les chiffres clés sur la blockchain

- > Âge : 9 ans
- > Croisement des courbes de recherche sur google entre objets connectés et blockchain : novembre 2016
- > Augmentation du nombre de recherches sur la blockchain en deux ans : x 10
- > Nombre de brevets sur la blockchain déposés depuis 2013 : +2500
- > Estimation de la valeur du marché de la blockchain en 2024 : 20 Md\$
- > Investissements cumulatifs dans les start-up blockchain en 2016 : 1,4 Md\$
- > Investissements réalisés par IBM dans la blockchain : 200 M\$ (~1000 Équivalent temps plein)
- > Pourcentage de banques américaines et européennes explorant la blockchain : 90 %
- > Nombre de transactions gérées chaque seconde par la blockchain : de 3 (Bitcoin) à 25 (Ethereum) contre 2500 pour Visa



Partie 1

Soyez curieux ! Comprendre la blockchain

1. Une révolution en route : les principes de base de la blockchain

Une blockchain (littéralement « chaîne de blocs ») est un registre décentralisé et infalsifiable de toutes les transactions effectuées depuis sa création et qui y sont consignées par blocs consécutifs. Ce protocole décentralisé peut trouver une multitude d'applications dès lors qu'il s'agit d'enregistrer et de certifier une transaction, un échange ou une identification.

Une blockchain peut donc être définie comme un registre actif, chronologique, distribué, vérifiable et protégé contre la falsification par un système de confiance répartie. Cela suppose la participation d'un grand nombre d'acteurs non-coalisés.

La blockchain est parfois appelée « registre distribué » (*Distributed Ledger* en anglais).

Encart 1 : La blockchain expliquée

Henri d'Agrain, délégué général du CIGREF

En 1994 était publié le rapport Théry, intitulé « Les autoroutes de l'information ». Avec une vingtaine d'années de recul, la lecture de ce rapport est particulièrement éclairante de ce que nous vivons aujourd'hui.

Pour résumer, si l'existence d'Internet est effectivement reconnue dans ce rapport, son potentiel est néanmoins rapidement écarté. On y lit en effet que « *son mode de fonctionnement coopératif n'est pas conçu pour offrir des services commerciaux. Sa large ouverture à tous types d'utilisateurs et de services fait apparaître ses limites, notamment son inaptitude à offrir des services de qualité en temps réel de voix ou d'images* ». Et plus loin dans le rapport on lit, après une liste des limites de l'Internet de l'époque, pointées par les rédacteurs du rapport, « *Ce réseau est donc mal adapté à la fourniture de services commerciaux.* » Pour mesurer la saveur de cette histoire, il faut se rappeler qu'en juillet 1994 à Seattle, au moment même où ce rapport était publié, Jeff Bezos créait Amazon qui allait devenir en moins de 15 ans le leader mondial de la fourniture de services commerciaux grâce à Internet.

Pourquoi ce retour historique sur le rapport Théry ? Parce que nous sommes probablement en train de vivre avec le phénomène blockchain un moment analogue à celui de 1994 avec l'Internet et l'émergence du web.

Le protocole blockchain s'inscrit dans une histoire de l'Internet. Dans les années 1970, le protocole de communication IP a permis de décentraliser les communications. Dans les années 1990, le web a permis de décentraliser la publication. Le web est devenu une formidable machine à copier ! Dans les années 2010, le protocole blockchain propose de décentraliser les transactions. En première approche, la blockchain offre au réseau une infrastructure de confiance permettant de garantir de manière décentralisée, dans un processus de transaction, que l'on dispose légitimement de « l'objet » que l'on compte céder, que celui qui le reçoit en dispose bien de manière légitime, que, lorsque la transaction est validée, on ne peut plus se prévaloir de la possession de « l'objet » cédé, et que celui qui l'a reçu peut s'en prévaloir. La confiance des deux parties de la transaction ne repose pas sur la confiance mutuelle, mais sur la confiance qu'elles portent dans l'algorithme.

L'innovation de la blockchain tient dans la combinaison de technologies informatiques et cryptographiques qui permettent d'assurer une confiance inaltérable dans la validité et l'intégrité des informations contenues sur le registre distribué. La confiance est portée par les algorithmes de chiffrement, l'organisation décentralisée du réseau pair-à-pair (*peer to peer* ou P2P) et les principes de la théorie des jeux.



Comment inciter à la collaboration des acteurs qui ne se connaissent pas sans passer par une autorité centrale ? Pour Satoshi Nakamoto, le fondateur du bitcoin, dans une économie basée sur la blockchain, il n'y a pas besoin d'avoir confiance en une personne, une société, un organisme, un régulateur ou une administration. Il faut juste faire confiance à l'algorithme qui permet de résoudre un problème et d'obtenir un consensus entre les parties de manière décentralisée.

La blockchain utilise les principes de la cryptographie pour s'assurer que toutes les parties contribuent à la réalisation d'un objectif commun d'une manière qui peut être validée par toutes les parties concernées.

En l'absence d'une autorité centrale, toute nouvelle transaction doit être validée par une majorité de participants avant d'être inscrite dans la base de données publique.

La majorité n'est pas déterminée sur le mode « un participant-une voix » comme pour un vote, car il serait alors trop facile de créer des participants fantômes pour valider des transactions frauduleuses. La majorité de participants s'établit en fait par la plus grande puissance de calcul collective. C'est de cette façon que le protocole blockchain permet d'établir le consensus décentralisé qui assure la validation des transactions en toute confiance.

Bloc 1 : que retenir ?

La blockchain, c'est :

- une base de données infalsifiable et partagée en ligne retraçant un historique distribué de transactions ou d'échanges de données ;
- un système décentralisé, sans organe de contrôle (consensus), qui fonde la confiance entre les parties sur des techniques cryptographiques avancées, des algorithmes pour valider chaque nouvelle entité créée dans la base partagée et la participation active d'un nombre suffisamment grand de parties pour garantir l'absence de coalition.

2. L'arbre qui cache la forêt : bitcoin ou le premier exemple à grande échelle

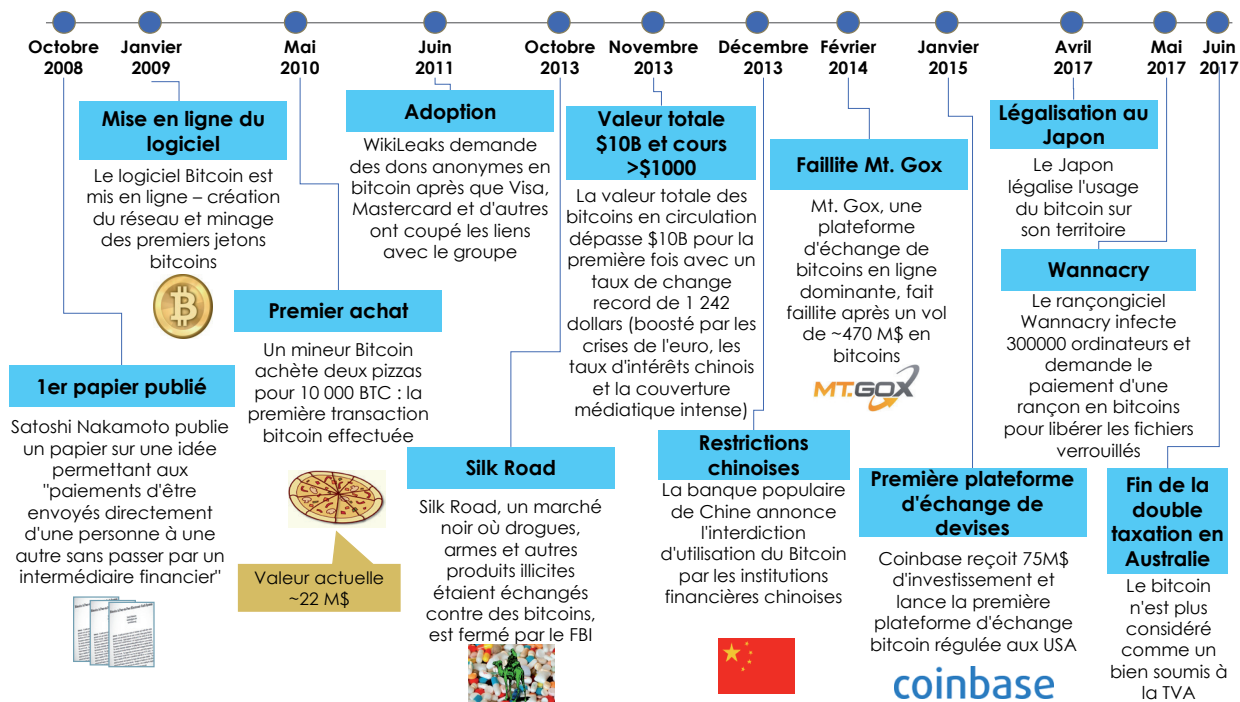


Olga Kami, via CoinDesk

Lors de l'hiver 2014, l'Ukraine était au bord de la révolution. Pour financer leur mouvement, des manifestants ukrainiens à Kiev ont montré aux caméras de télévision du monde entier des pancartes demandant des versements... en bitcoins via un QR Code pour soutenir leur mouvement de protestation. Des milliers de citoyens de par le monde ont pointé leur Smartphone sur leur écran de télévision et ont pu effectuer un don en trois clics seulement. Ces transactions, communiquées en 20 secondes et confirmées en 10 minutes, garantissaient l'anonymat (pas de surveillance possible de la part du gouvernement et origine du donateur inconnue) et étaient facturées moins d'un centime de dollar.

Cet épisode historique a contribué à rendre célèbre le bitcoin et à susciter des interrogations sur le potentiel de ce nouveau type de monnaie.

Le concept de blockchain est apparu avec le bitcoin, la plus connue des crypto-monnaies



Source : The Boston Consulting Group

2.1. Le fonctionnement de la monnaie bitcoin¹

Une transaction s'apparentant à un don via le système bancaire traditionnel aurait nécessité une multitude d'informations personnelles (potentiellement compromettantes d'un point de vue politique) concernant le compte bancaire du donateur. Cette transaction aurait engendré des coûts significatifs (10 % ou plus de commission) et aurait nécessité 3 à 4 jours de traitement. Paypal aurait pu être une solution plus rapide et moins chère qu'un virement bancaire, mais l'utilisation de cette plateforme était interdite par le gouvernement ukrainien. Une transaction en bitcoins a l'avantage d'être directe, anonyme et irrévocable, et peut être comparée au don de quelques hryvnia (monnaie ukrainienne) dans le gobelet d'un manifestant sur la place centrale de Kiev.

En effet, le bitcoin est une **crypto-monnaie**, une monnaie électronique qui utilise la cryptographie pour valider les transactions entre les acteurs du réseau. La propriété et le contrôle d'un bitcoin vont de pair. En effet, il n'y a pas besoin de « compte » bitcoin, on possède des bitcoins tout comme on possède des pièces de monnaie dans son portefeuille. Ces pièces peuvent être perdues ou volées comme des euros ou des dollars. Le bitcoin peut s'avérer dix fois plus efficace comme moyen d'échange que les moyens de paiement traditionnels. Toutefois, en incluant les coûts d'entrée et de sortie (pour repasser en monnaies classiques, imprimées par les gouvernements), ce système n'est pour l'instant pas tellement meilleur marché. Et l'anonymat, qui peut sembler noble dans le cas ukrainien, l'est moins dans des montages de blanchiment d'argent ou d'évasion fiscale.

Il est important de bien faire la distinction entre la monnaie bitcoin et le protocole Bitcoin. Le protocole Bitcoin est aujourd'hui souvent associé à la blockchain et définit les lois et le fonctionnement du bitcoin.

1. Les termes en gras sont définis dans la partie Glossaire.



- l'origine : l'adresse Bitcoin d'où provient le paiement ;
- le montant : le nombre de bitcoins à envoyer ;
- la destination : l'adresse Bitcoin du destinataire de la transaction.

Avec Bitcoin, la transaction entre Alice et François n'est vérifiée par aucun intermédiaire centralisé. Le transfert est effectué directement de personne à personne.

- Comment être sûr qu'Alice possède bien les bitcoins qu'elle souhaite envoyer à François ?
- Comment être sûr qu'Alice ne dépensera qu'une seule fois ces bitcoins ?
- Sans serveur centralisé, où sont stockés les comptes d'Alice et de François ?

Une clé privée est connue de son seul propriétaire et n'est jamais communiquée. Elle est utilisée par son propriétaire comme un sceau pour signer ses messages et comme une clé pour déchiffrer les messages lui étant adressés.

Pour dépenser l'argent reçu, il faut connaître la clé privée correspondant à la clé publique détenant les bitcoins. N'importe qui en possession de la clé privée peut avoir accès aux bitcoins envoyés, d'où l'importance de ne jamais la dévoiler.

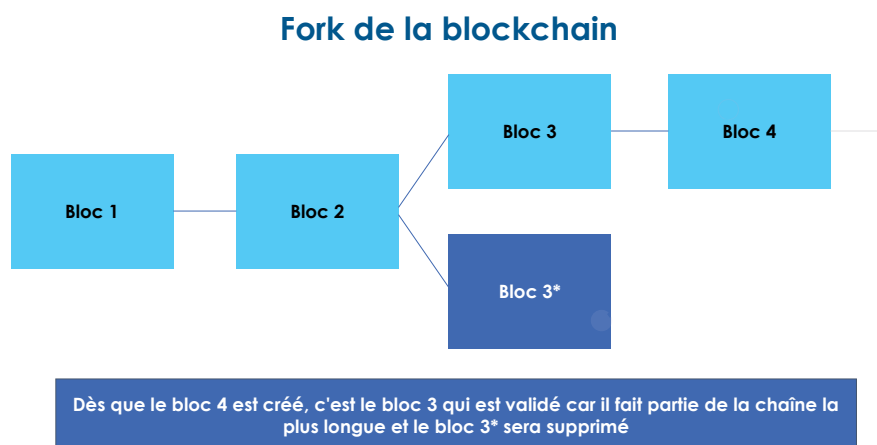
Alice ne possède pas pour autant d'endroit où sont stockés tous ses bitcoins. Lors d'une transaction, chaque jeton envoyé va référencer d'où il vient pour permettre aux nœuds du réseau (constitués de groupes d'ordinateurs mettant à disposition leur puissance de calcul) de vérifier qu'Alice en était bien la propriétaire. Étant donné que toutes les transactions sont publiées dans un registre public et distribué, chaque nœud du réseau peut retracer tous les mouvements de chaque bitcoin. Le solde d'une adresse Bitcoin est en fait la somme entre les entrées et sorties de bitcoins pour cette adresse.

Une fois initiée, la transaction d'Alice vers François va être vérifiée grâce aux signatures et à la clé publique d'Alice. Une fois validée, la transaction est ajoutée à la blockchain.

Comment éviter la double dépense ?

Si Alice essaie de dépenser deux fois ses bitcoins, elle va créer deux transactions contradictoires et simultanées. Chaque nœud décidera d'ajouter l'une ou l'autre à son bloc (groupe de transactions). Imaginons qu'il n'y ait que deux nœuds dans le réseau. Si le premier nœud parvient à créer un bloc avant le deuxième, il le diffuse au réseau et donc au deuxième nœud. C'est alors que le nœud 2 va arrêter de travailler sur son bloc pour valider le bloc créé par le nœud 1 et verra que la deuxième transaction initiée par Alice ne peut être validée. En effet, la deuxième transaction ne peut plus s'insérer, car elle devrait le faire à un endroit qui n'est plus le bout de la chaîne. Si le nœud 2 avait été plus rapide, c'est sa transaction qui aurait été validée, pas celle du nœud 1.

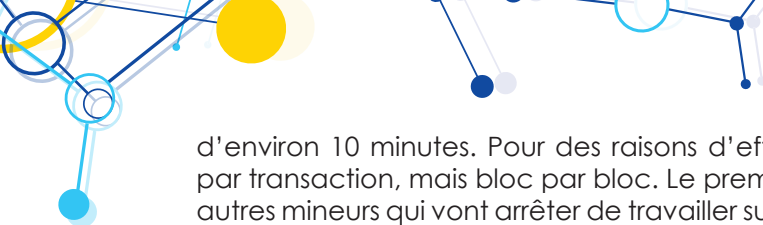
Si par hasard, les deux nœuds créent un bloc en même temps (et c'est possible), on dit que la chaîne n'est plus simple et contient un dédoublement (fork).



Les deux transactions sont alors validées jusqu'à ce qu'un nouveau bloc soit créé. Les nœuds du réseau travailleront sur les deux blocs en même temps pour en créer un nouveau. Dès qu'un nouveau bloc sera créé, le protocole Bitcoin donnera priorité à la chaîne la plus longue (celle qui a donc nécessité le plus de travail), annulant ainsi la chaîne la plus courte. Si Alice voulait travailler dans son coin et continuer à créer des blocs simultanément pour avoir de bonnes chances de valider ses deux transactions contradictoires, il faudrait qu'elle contrôle plus de la moitié de la puissance de calcul du réseau, ce qui semble difficile dans un réseau avec autant de participants que Bitcoin. Une transaction est considérée comme statistiquement irréversible après la création de six blocs supplémentaires, soit environ une heure (10 minutes par bloc).

Validation des blocs

Pour créer et envoyer un bloc de transactions à travers le réseau, un problème de calcul complexe nécessitant un ordinateur doit être résolu. Cette action est appelée « minage » et est réalisée par des groupes d'ordinateurs appelés « mineurs ». Le terme de « minage » trouve son origine dans le fait qu'il s'agit d'une action qui demande des investissements lourds et qui peut (mais pas toujours) générer une rémunération. La difficulté des problèmes à résoudre varie en fonction de la capacité de calcul du réseau pour garder un temps de résolution



d'environ 10 minutes. Pour des raisons d'efficacité, les mineurs ne valident pas transaction par transaction, mais bloc par bloc. Le premier mineur à valider un bloc le communique aux autres mineurs qui vont arrêter de travailler sur leur bloc pour vérifier celui nouvellement soumis à la blockchain. Une fois un bloc validé par plus de la moitié du réseau – ce qu'on appelle « le consensus », il est ajouté à la blockchain, et le mineur qui a créé ce bloc va recevoir une récompense en bitcoins. La récompense actuelle est de 12,5 bitcoins par bloc créé, soit plus de 28 200 dollars par bloc ou 1,5 milliard de dollars sur une année au cours du 31 mai 2017. Cependant, le nombre de mineurs est devenu tellement important que la faible probabilité de recevoir cette récompense et la quantité d'électricité nécessaire pour un mineur isolé ont rendu cette opération non rentable en dehors des pools de minage qui sont en général localisés à proximité immédiate des lieux de production d'électricité. Ainsi, environ 72 % de la puissance de calcul est actuellement concentrée en Chine où l'électricité est très bon marché.

Au départ, la récompense pour la création d'un bloc était de 50 bitcoins et cette récompense est divisée par deux tous les quatre ans. Quand la récompense aura atteint l'ordre du satoshi (plus petite division du bitcoin), soit 0,00000001 bitcoin, il n'y aura plus d'émission de bitcoins sur le réseau. Cette règle implique que la fin de la création de nouveaux jetons aurait lieu en 2141. La récompense diminuant au fil du temps, on considère que 75 % des bitcoins étaient déjà sur le marché en 2016 et 93,75 % le seront en 2024². Le nombre final de bitcoins émis ne dépassera pas les 21 millions de jetons.

2.2. Les limites de la monnaie bitcoin

Bien qu'étant la seule application de blockchain publique ayant réussi le passage à l'échelle et qui fonctionne actuellement, cette monnaie a d'ores et déjà montré des limites notables. Aux limites de la blockchain elle-même (détaillées dans le §4) – consommation électrique importante, nombre de transactions par seconde encore faible, problématique de la confiance périphérique – s'ajoutent trois limites spécifiques à la monnaie bitcoin : l'absence d'actifs sous-jacents, l'anonymat des transactions et la concentration des pools de minage.

Limite #1 : L'absence d'actifs sous-jacents

Quand on parle de bitcoin, on parle d'une monnaie digitale. La monnaie peut être définie par ces trois fonctions :

1. une unité de compte qui exprime le prix des biens ;
2. un moyen d'échange reconnu par une majorité d'acteurs pour effectuer des transactions ;
3. une réserve de valeur qui permet de reporter dans le futur l'achat d'un bien ou d'un service.

Une monnaie digitale est généralement restreinte à Internet et n'a pas de valeur sous-jacente. C'est, entre autres, cette absence d'actifs sous-jacents qui pose un problème de légitimité pour le bitcoin. En effet, cette monnaie n'a de la valeur que parce que le marché lui en donne, mais n'est soutenue par aucun État, contrairement aux monnaies traditionnelles.

Malgré cette limite, certains libertariens voient le bitcoin comme le futur « or digital » : une devise mondiale et infalsifiable qui remplacera toutes les monnaies actuelles gérées par les banques centrales et commerciales. Ses opposants, comme Jamie Dimon, le PDG de JPMorgan Chase, rappellent que les banques centrales interviendraient pour freiner cette adoption. Le bitcoin pourrait donc être destiné à n'occuper qu'une petite niche dans l'industrie des paiements.

Du fait de cette absence d'actifs sous-jacents, le cours du bitcoin est fortement influencé par la spéculation et connaît des fluctuations extrêmes. Aussi, la valeur d'un bitcoin fin 2010 était-elle inférieure à un dollar pour atteindre au 31 mai 2017 les 2 261 dollars. Entre temps, le bitcoin avait déjà dépassé le taux historique de 1 000 dollars fin 2013 avant de connaître une chute soudaine à 200 dollars début 2015. Cette instabilité du taux de change du bitcoin est due aux scandales à répétition liés à cette monnaie, ce qui décourage de nombreux investisseurs et alimente la spéculation.

2. <https://bitcoin.fr/en-quelle-annee-atteindrons-nous-le-nombre-maximal-de-bitcoins-en-circulation/>



Cours BTC/USD depuis mars 2012



Limite #2 : L'anonymat des transactions

L'anonymat des transactions promis par la monnaie bitcoin pose aussi question car, tout comme l'argent liquide, il pourrait favoriser le blanchiment d'argent, l'évasion fiscale ou le financement du terrorisme. Cet anonymat doit cependant être relativisé. En effet, comme les transactions sont publiques, car reprises sur un registre distribué accessible par tous, et qu'il n'y a pas d'anonymat à l'achat et à la vente de bitcoins, les autorités ont déjà pu retracer et saisir des fonds auprès de mafias et de trafiquants. Cela n'aurait pas été possible avec la monnaie papier traditionnelle. On parle donc de pseudonymat plutôt que d'anonymat dans le cas de la blockchain.

Limite #3 : La concentration des pools de minage

À chaque minage d'un nouveau bloc, le problème calculatoire à résoudre augmente en complexité. Plusieurs milliers de mineurs doivent alors travailler de manière collaborative à ce minage de manière à augmenter leurs chances de gain de la récompense offerte pour la création de nouveaux blocs. Pour des raisons d'efficacité, ces mineurs sont généralement regroupés au sein de pools de minage, eux-mêmes localisés à proximité de sources de production d'électricité. On assiste donc paradoxalement à une concentration alors que la blockchain repose fondamentalement sur des principes de déconcentration et de distribution.

En principe, il faut veiller à ce qu'aucun pool de minage ne concentre un pourcentage trop élevé de la puissance de calcul de tout le réseau. Si tel était le cas, un pool de minage aurait statistiquement de bonnes chances d'être en mesure d'écrire et de valider la blockchain à sa guise.

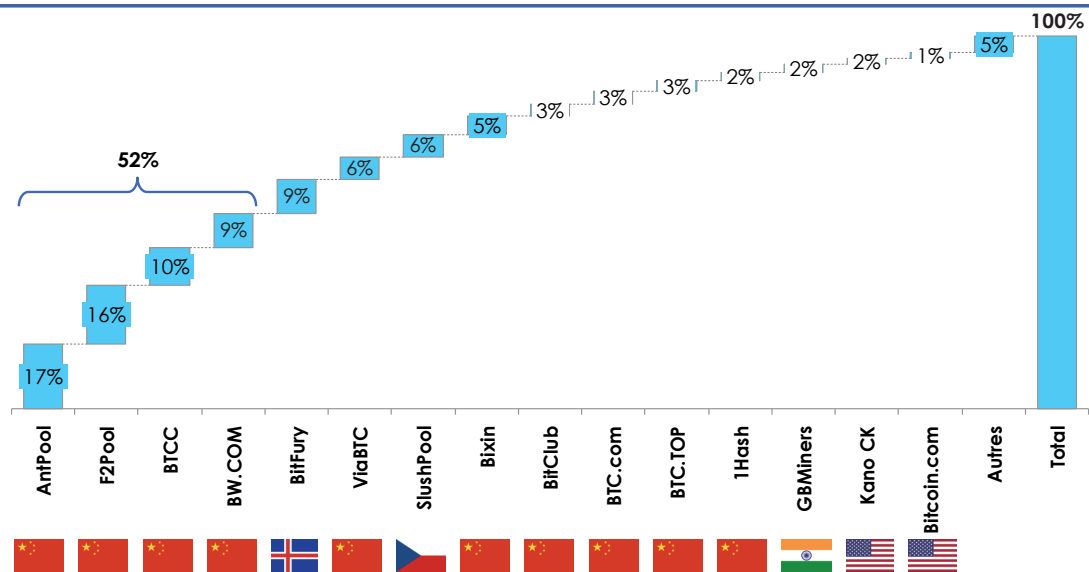
Or, à ce jour, quatre pools de minage chinois concentrent 52 % de la puissance de minage Bitcoin, ce qui pourrait poser problème en cas d'entente. On voit donc l'émergence d'un risque pays qui pourrait altérer la sincérité du processus d'inscription des transactions dans la blockchain.



Les quatre principaux pools de minage sont chinois

Ils concentrent 52 % de la puissance de minage mondiale

Pourcentage de la puissance de calcul dédiée au minage du bitcoin du 01/06/2016 au 31/05/2017



2.3. Au-delà du bitcoin

D'un point de vue stratégique, l'importance du bitcoin réside moins dans son rôle de monnaie que dans son rôle d'introduction des technologies sous-jacentes : le jeton ou token (ici, le bitcoin) et la blockchain. Un jeton ne prend pas nécessairement la forme d'une monnaie digitale, il peut être un actif digital ou représenter n'importe quel actif physique. Et une blockchain comme la blockchain Bitcoin peut servir de registre partagé, sécurisé et infalsifiable pour tout type de transaction. Même si la plupart des applications actuelles de la blockchain concernent les paiements, les technologies de jeton et de blockchain peuvent servir de points de départ pour d'autres cas d'usage.

Les possibilités d'applications de la blockchain dépassent de loin les services financiers avec des cas d'usage possibles dans les domaines de la chaîne d'assemblage, du registre cadastral, du registre de santé, de la **micro-transaction** (échanges de quelques centimes) ou encore des **smart contracts** (contrats dont les clauses sont automatiquement validées quand certaines conditions sont vérifiées).

Bloc 2 : que retenir ?

- Bitcoin est le premier cas d'usage « industriel » à l'échelle de la technologie blockchain qui s'est développée à partir de 2009.
- À ce titre, le bitcoin est une monnaie digitale qui fonctionne sans intermédiaire, avec des transactions validées par les nœuds du réseau (les « mineurs »).
- Les blocs de transactions qui composent l'historique traçable des échanges sont créés par des mineurs qui résolvent des problèmes calculatoires complexes avec des machines de minage en échange d'une récompense en bitcoins nouvellement créés à cette fin.
- Son historique est public et peut être retracé jusqu'à sa création (son « minage » d'origine).
- La principale limite de la monnaie bitcoin est qu'elle n'est pas fondée sur des actifs sous-jacents, ce qui la rend extrêmement spéculative.



3. Trois éclairages sur le mode de fonctionnement de la blockchain

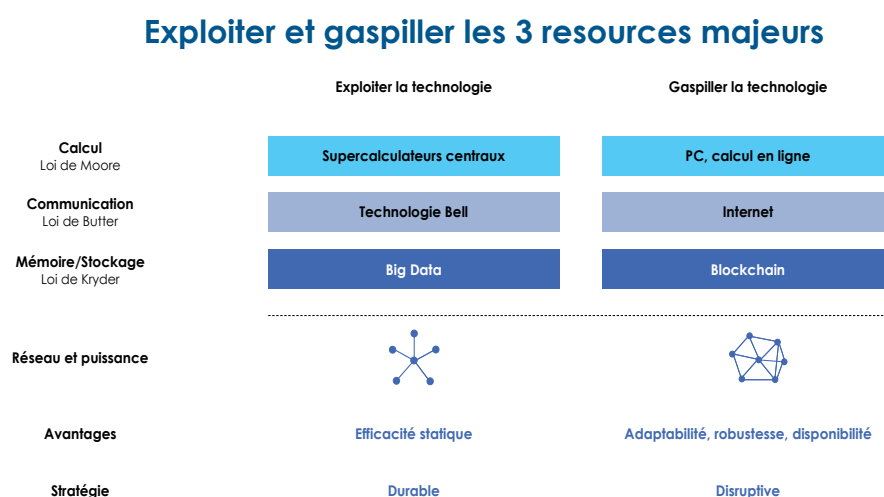
3.1. L'exploitation d'une capacité de stockage en abondance

La blockchain et les monnaies digitales « gaspillent » délibérément de la capacité de stockage numérique, dont le coût est très faible.

La révolution de l'information qui a démarré il y a une cinquantaine d'année est fondée sur les développements exponentiels (en termes de coût, rapidité et capacité) des trois fonctions suivantes : **calcul**, **communication** et **mémoire/stockage**. Ces développements ont conduit à des situations où ces ressources sont devenues si abondantes et bon marché que leur gaspillage est devenu rationnel d'un point de vue économique pour créer de nouveaux produits ou usages.

Ainsi, la division par 16 000 en vingt ans du coût du téraoctet de stockage a favorisé l'accumulation de plus en plus de données : le big data suit cette logique de gaspillage d'une ressource dont le coût devient dérisoire. La blockchain Bitcoin, par exemple, offre un enregistrement inviolable de l'historique de chaque jeton en stockant les informations sur chaque transaction plus de 6 132 fois (nombre moyen de mineurs actuellement constaté). C'est en ce sens que le registre est distribué : plutôt que d'être conservé en un endroit unique, le registre est dupliqué sur chacun des nœuds du réseau.

Gaspiller et exploiter les trois ressources principales



Source : BCG Perspectives « Thinking Outside the Blocks »

3.2. La continuité virtuelle

Ce gaspillage des capacités de stockage sur lequel repose la réplication des chaînes de blocs permet d'assurer une continuité virtuelle à des jetons digitaux comme le bitcoin.

La continuité est la faculté de certifier la propriété d'un bien en suivant continuellement le bien et son propriétaire. Cette continuité assure l'identification des biens et de leurs propriétaires et permet les transactions, les transferts de propriété et la confiance. Tout système d'échange est basé sur ce principe. Elle n'est pas suffisante pour établir la propriété et les contrats (qui supposent par ailleurs un cadre juridique pour exercer une violence légitime en cas d'infraction), mais elle est nécessaire. Les signatures, passeports, notaires et photos d'identité sont des moyens de garantir cette continuité dans les échanges réels.

Une des limites du monde virtuel est l'absence de continuité. En effet, il n'existe aucune garantie qu'une chaîne de données soit la chaîne originale ou une copie : ni les objets, ni les personnes n'ont une identité propre. Sur Internet, personne ne peut être certain que son interlocuteur est bien la personne qu'il prétend être. Dans de nombreux contextes, cette absence de continuité est souhaitable car elle permet des coûts de diffusion et de transmission de l'information proches de zéro. Mais sans continuité, l'identification, la propriété, les transactions, la confiance ou les contrats ne peuvent être garantis dans une relation de pair-à-pair.



Quand les parties ont une relation préétablie dans le monde réel, elles peuvent établir la continuité virtuelle directement grâce au **chiffrement** et au codage de données. L'absence de continuité virtuelle est actuellement compensée par l'intervention d'intermédiaires de confiance. Considérons une transaction entre A et B. A a une relation réelle avec sa banque et, de même, B a une relation réelle avec la sienne. Les banques ont également une relation réelle entre elles. Les intermédiaires (les banques n'en sont qu'un type) garantissent les identités virtuelles respectives de A et B et régulent leurs transactions.

S'il n'y a qu'un seul intermédiaire, ce dernier aura une situation de monopole et en profitera pour maximiser son profit en établissant des tarifs élevés pour ses services. En revanche, si le marché dispose d'une multitude d'intermédiaires, ces derniers auront besoin à leur tour de passer par des intermédiaires pour gérer leurs relations. Avec les systèmes multicouches de transactions internationales, un transfert d'argent vers Kiev génère donc des transactions multiples qui engendrent souvent du retard et des erreurs.

Le protocole Bitcoin établit, par sa structure, l'origine du jeton et de son destinataire. Dans les deux transactions X et Y, la structure du bitcoin permet de vérifier son ascendance : le jeton dans la transaction X est le seul « parent » de la transaction Y. L'authenticité du jeton peut donc être vérifiée en retraçant son chemin jusqu'à sa création (son minage original).

Les deux concepts sous-tendant Bitcoin, la blockchain et le jeton, gaspillent donc du stockage en répliquant cette information encore et encore pour créer la continuité virtuelle. Cette continuité garantit l'identité digitale, la propriété, les transactions et la confiance entre des parties qui n'ont eu aucune relation jusqu'à cette transaction et tout ceci, sans intermédiaire.

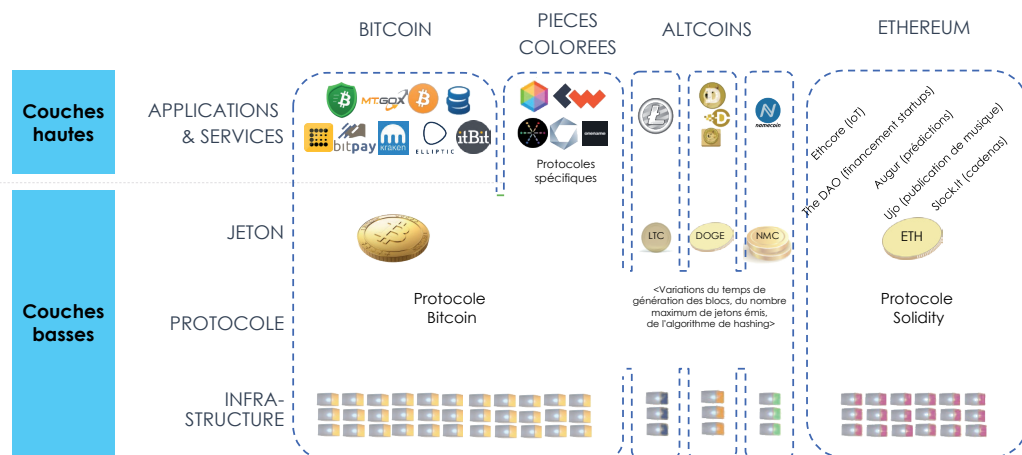
Cette technologie peut être disruptive pour tous les intermédiaires. Le potentiel de la blockchain est proportionnel au coût, à la complexité et au degré de duplication des transactions dans notre système actuel d'intermédiation.

3.3. L'architecture technique de la blockchain

La blockchain Bitcoin est construite sur une « architecture en couches », c'est-à-dire un ensemble de modules empilés les uns sur les autres. Les couches supérieures utilisent des fonctionnalités apportées par les couches inférieures, mais l'inverse n'est pas vrai. Les fonctions générales ayant besoin de fiabilité sont dans les couches basses (l'infrastructure) et les fonctions nécessitant plus d'expérimentation et de particularisation occupent les couches hautes. L'interopérabilité entre les couches du système permet la sécurité et la fiabilité (assurées par les couches basses), ainsi que l'adaptabilité (assurée par les couches hautes).

Pour illustrer cette propriété, Internet est une analogie parlante car également construit sur une architecture en couches : les couches basses concentrent le réseau et les protocoles, et les couches hautes les applications qui présentent une interface utilisateurs.

Architecture en couches du Bitcoin



Source : The Boston Consulting Group



Infrastructure/blockchain

Dans un protocole comme le protocole Bitcoin, comme c'est le cas pour toutes les monnaies virtuelles, la blockchain constitue les couches basses : un registre distribué, une base de données de toutes les transactions, regroupées en blocs et répliquées à travers des milliers de nœuds. Il n'y a par exemple qu'une seule blockchain Bitcoin et, plus il y a de nœuds et de blocs (respectivement 6 132 et 469 111 au 31 mai 2017³), plus elle est fiable et robuste. Physiquement, les nœuds sont des groupes d'ordinateurs détenus par des pools de minage.

Protocole

Le protocole est la couche juste au-dessus de la blockchain. Dans le cas de Bitcoin, il est mis à disposition de la communauté gratuitement et est géré de manière transparente par un ensemble de développeurs Bitcoin. Il couvre toute une série de services et de règles permettant de faire fonctionner l'écosystème Bitcoin. A l'instar de Linux, ce protocole bénéficie des forces d'un *business model* en *open source* : test du code par tous les participants, cycles d'améliorations rapides et confiance dans le produit car personne ne le possède vraiment. Il souffre aussi de ses faiblesses, comme la difficulté de prendre des décisions stratégiques par consensus.

Jetons (tokens)

Les **jetons** (« tokens »), bitcoins ou ethers par exemple, sont échangés au sein du système et créés par les mineurs qui les reçoivent en récompense de leur travail de validation des blocs. Comme tout moyen d'échange, le bitcoin a la valeur que le marché lui donne. Le premier achat en bitcoin a eu lieu en 2010 quand le hacker Laszlo Hanyecz a acheté deux pizzas de chez Papa John en échange de 10 000 bitcoins fraîchement minés, soit l'équivalent de 22,6 millions de dollars au cours du 31 mai 2017.

Applications et services

Les applications constituent la couche haute de l'architecture. Ces applications sont majoritairement des **wallets** (logiciels de **portefeuilles** qui permettent de détenir et de gérer ses jetons sur un Smartphone ou un ordinateur ou de consulter par exemple le solde de bitcoin sur son « compte » – adresse en réalité – bitcoin). Il existe également des plateformes d'échange (pour convertir les crypto-monnaies en devises courantes) et des services d'information. Des centaines de produits et services ont été développés par les start-up pour exploiter la blockchain.

Les couches basses de l'architecture de la blockchain sont extrêmement sécurisées. Dans le cas de la blockchain bitcoin, elles n'ont jamais été piratées avec succès malgré une valeur de 36 milliards de dollars pour les plus de 16 millions de bitcoins en circulation. Les couches hautes de l'architecture sont moins sécurisées, voire, pour certaines, reposent sur une conformité plus lâche avec les règles, lois et usages des grands pays développés, ce qui a généré des scandales de blanchiment d'argent et de marché noir tels que Mt Gox et **Silk Road**. Mais la force de l'architecture en couches est que la fragilité des couches hautes n'impacte en rien la solidité des couches basses.

Pièces colorées (Colored coins)


Le système des pièces colorées est une innovation qui utilise de l'espace de stockage disponible dans chaque jeton pour y enregistrer des données. Ces dernières sont en général associées à un objet physique particulier (voiture, œuvre d'art, part de société, etc.) et permettent donc de lier un jeton à un objet réel. Cela pourrait être utilisé pour tracer n'importe quel actif de valeur ayant un historique de transactions complexe.

Altcoin (Alternative coins)

Les **altcoins**, ou jetons alternatifs, empruntent le protocole Bitcoin et le modifient légèrement pour créer un jeton indépendant, notamment à des fins d'expérimentation. Beaucoup de ces monnaies sont exotiques et ont un nom humoristique : le BaconBitscoin (YUM), le Kimdotcoin (KOIN), le Zombiecoin (ZMB), etc.

3. <https://blockchain.info/>





D'autres sont plus ambitieuses et visent à ajuster le protocole Bitcoin. Pour Litecoin, par exemple, le protocole Bitcoin a été modifié pour produire des blocs à un rythme plus soutenu et avec moins de calculs. Enfin, des monnaies virtuelles alternatives se revendiquant 100 % anonymes et non traçables comme Monero ou Zcash ont fait leur apparition. Elles sont en outre acceptées sur la plupart des supermarchés de la drogue sur Internet.

Ethereum

Cette nouvelle plateforme, construite sur une architecture similaire à Bitcoin, a été valorisée un milliard de dollars en juin 2015, un an seulement après son lancement. **Ethereum**, qui est souvent considéré comme le Bitcoin 2.0, possède sa propre blockchain et son propre jeton (**ether**) et un protocole qui, en plus des paiements, permet de gérer les **smart contracts**. Son créateur, Vitalik Buterin, décrit Ethereum comme « l'ordinateur mondial ». Ethereum a rapidement crû et avec lui son écosystème d'applications qui a eu des résultats mitigés. The Decentralized Autonomous Organization (DAO) était une tentative de plateforme de *crowdfunding* fonctionnant avec des *smart contracts* Ethereum. En juin 2016, après avoir levé plus de 150 millions de dollars en ethers, la plateforme a été victime d'un vol de plus de 50 millions de dollars rendu possible par une faille dans le code du *smart contract* gérant la sortie des fonds en ethers de The DAO. La communauté Ethereum a par la suite voté à la quasi-unanimité la mise en place d'une *fork* pour repartir d'une chaîne parallèle redémarrant juste avant le vol, ce qui a eu pour conséquence d'annuler toutes les transactions postérieures, y compris le vol. Malgré cet épisode, Ethereum reste la plateforme préférée des développeurs d'applications *open source*.

Ripple

Ripple est un protocole open source de registre distribué qui possède sa propre crypto-monnaie appelée « XRP » (ripples). Créé en 2012, ce protocole vise à permettre des transactions internationales sécurisées, instantanées et gratuites. Ripple est la troisième crypto-monnaie en termes de capitalisation boursière derrière bitcoin et ether. Ce protocole est de plus en plus utilisé pour les transactions interbancaires. Il est notamment utilisé par UniCredit, UBS ou Santander. Pour les banques, les avantages de ripple par rapport aux crypto-monnaies traditionnelles comme bitcoin sont la sécurité et le prix.

Blockchains privées

Les blockchains privées vont à contre-courant de l'idée de départ de la blockchain Bitcoin ouverte. L'accès à ces blockchains est limité à un nombre restreint de participants, par exemple des institutions financières. Seuls les membres autorisés ont le droit d'inspecter, d'engager des transactions dans la blockchain et de la manipuler. Les blockchains privées permettent des transactions rédigées aussi bien en langage légal qu'en code informatique. Elles permettent aussi une vérification par le régulateur. Beaucoup n'en sont qu'au stade de *proof of concept* (PoC), mais des consortiums comme R3CEV ambitionnent d'utiliser des solutions s'inspirant des blockchains privées pour les transactions bancaires et financières, en particulier sur les titres et les devises.

Bloc 3 : que retenir ?

- **La blockchain repose sur l'exploitation d'une ressource bon marché - stockage/mémoire - pour créer une continuité virtuelle de données ou d'actifs échangés sur Internet.**
- **Ce système d'échanges est construit sur une architecture en couches. Les couches hautes, dites applicatives, utilisent des fonctionnalités apportées par les couches basses, formées entre autres par les protocoles blockchains.**
- **La blockchain est une technologie qui doit encore être stabilisée dans la mesure où restent ouvertes plusieurs orientations possibles :**
 - **un certain nombre de protocoles différents existent, les principaux à ce jour étant Bitcoin et Ethereum ; Ethereum ambitionnant de pallier certaines déficiences de Bitcoin ;**
 - **des blockchains privées, dont certaines caractéristiques sont aux antipodes avec ce qui fonde la blockchain, ont fait leur apparition ; leur articulation avec les blockchains publiques reste à déterminer.**



4. Les limites de la blockchain

4.1. La confiance périphérique

Les blockchains ou registres distribués sont souvent décrits comme des systèmes fonctionnant sans avoir besoin de générer de la confiance, mais ce n'est pas tout à fait le cas. Dans les faits, cette problématique de confiance est déplacée en périphérie du système.

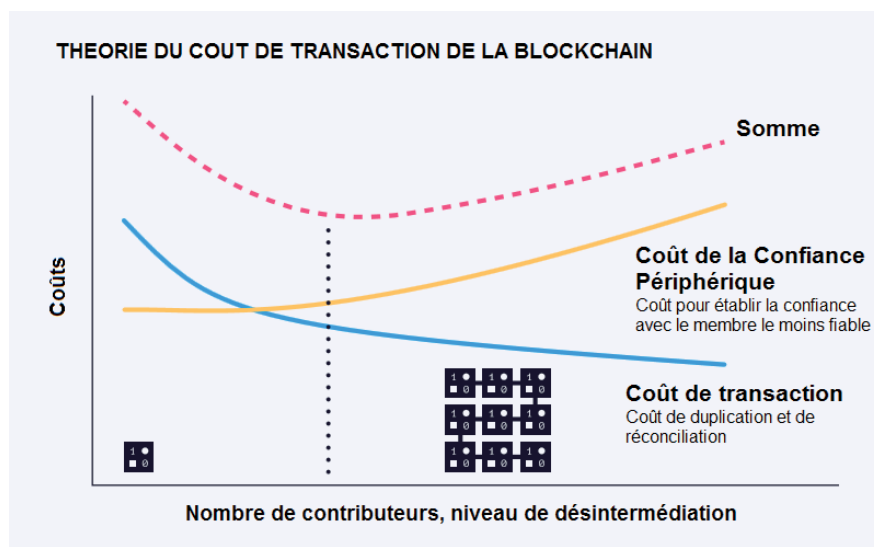
Quand l'entreprise Everledger certifie un diamant dans la blockchain, on peut être certain que le rapport a bien été posté au jour J et à l'instant T par un individu possédant la clé privée d'Everledger. Mais il faut dès lors faire confiance à Everledger quant à son analyse de la pierre précieuse. C'est pourquoi Everledger s'appuie sur un réseau de joailliers et d'experts reconnus dans le métier pour authentifier chaque diamant. L'entreprise détaille certifications, données essentielles et photographies en haute résolution pour créer le rapport de provenance digital de chaque pierre.

Prenons maintenant le cas d'un *smart contract* pour l'assurance d'une récolte agricole. Ce *smart contract* déclenchera automatiquement une indemnisation de l'exploitant si un certain nombre de conditions sont vérifiées. Ces conditions peuvent, par exemple, être une clause d'intempérie ou de catastrophe naturelle. Or ces données météorologiques sont recueillies auprès d'une source se situant en « périphérie » de la chaîne et à laquelle toutes les parties sont réputées faire confiance. Si les données fournies par cette source sont erronées, cela validera indûment les clauses des *smart contracts*.

Dans le cas de la blockchain Bitcoin, l'actif échangé est le jeton bitcoin créé dans la blockchain. Donc si l'on a confiance dans la blockchain Bitcoin, on a confiance dans la validité et la valeur unique du jeton bitcoin. En revanche, lorsque le jeton n'est pas l'actif, mais simplement une représentation digitale de l'actif, on ne peut avoir confiance dans le jeton que si l'on a confiance dans la personne qui crée cette représentation : Everledger pour les diamants ou la source (parfois appelé « oracle ») donnant les données météorologiques pour le *smart contract* de récolte agricole.


D'après la théorie de Ronald Coase, le regroupement au sein d'organisations pour travailler ensemble se justifie par le souci de faire baisser les coûts de transaction. Mais quand une organisation atteint une certaine taille, la complexité organisationnelle génère des coûts supérieurs à l'économie de coûts de transaction. Pour Ronald Coase la taille optimale d'une organisation est celle où l'économie de coûts de transaction s'équilibre avec le coût marginal de la complexité organisationnelle.

Un des avantages de la blockchain est qu'elle permet aussi de faire des économies sur les coûts de transaction : elle protège la base de données des attaques, elle élimine les problèmes de duplication, les erreurs et retards engendrés, et elle propage de proche en proche la confiance à travers le réseau. Or, plus le nombre de contributeurs à la blockchain est grand, plus se pose la question de la fiabilité des données introduites par les derniers arrivants, ceux dont la confiance n'est pas encore établie, et au-delà de la fiabilité de l'infrastructure elle-même.



Source : BCG Perspectives « Thinking Outside the Blocks »





Par analogie avec la théorie de Coase, le nombre optimal de contributeurs à une blockchain est déterminé par un compromis entre les coûts de transaction qui diminuent et la confiance périphérique qui se détériore avec le nombre de contributeurs.

Encart 2 : La Poste, acteur de confiance séculaire, aborde la Blockchain

Alain Roset, directeur innovations et ruptures du Groupe La Poste

Opérateur historique de transport de courriers créé en 1477 par Louis XI, la Poste porte la confiance des Français dès 1790 avec le premier serment du facteur, suivi en 1791 d'une loi sur l'inviolabilité du courrier. Cette confiance a aidé à lancer des produits financiers dès le XIX^e siècle (mandats, livret A), à accélérer la diffusion de la vente par correspondance sur notre territoire au XX^e siècle.

Entré dans une vielle active depuis 2014 sur la blockchain, le groupe participe aux projets et réflexions collectives françaises qui lui ont permis de comprendre quelques éléments. Les tiers de confiance resteront indispensables en périphérie des nouveaux services sur blockchain comme «oracle» validant les informations d'entrée des transactions. La gestion de la confiance par la multitude passera par une période transitoire où des initiateurs de services et des garants de dernier recours seront indispensables à la diffusion des nouveaux services.

Des efforts de R&D restent néanmoins largement nécessaires pour améliorer les premiers logiciels disponibles, combler leurs lacunes algorithmiques, vérifier la tenue en charge ou l'absence d'erreurs significatives.

Les avantages indéniables de la technologie (unicité des enregistrements, transparence, auditabilité et immuabilité des informations) feront très certainement émerger, vers 2020, plusieurs services modernisés que Le Groupe La Poste, tiers de confiance repositionné autour de blockchains, intégrera dans de nouvelles offres au service de l'ensemble des citoyens.

Un des usages les plus étudiés de la blockchain est la gestion des transactions et des transferts de titres, qui nécessite actuellement un réseau complexe de *brokers*, de banques dépositaires, d'agents de transfert de titres et de régulateurs. Un simple transfert peut exiger une douzaine de transactions intermédiaires et prend généralement trois jours. De plus, des erreurs sont à corriger manuellement dans 20 % des cas.

Avec une blockchain, deux parties pourraient lire et écrire dans une même base de données et sans erreur. Cette blockchain pourrait être accessible au régulateur, mais pas aux autres institutions par exemple. C'est le concept sur lequel repose Corda, une blockchain privée développée par le consortium R3CEV. Celle-ci permettrait l'élimination des erreurs bilatérales, et son coût serait bien moindre que le coût de modernisation des plateformes de paiement existantes.

Mais pourquoi s'arrêter là ? Les *brokers* pourraient échanger sur des blockchains plus larges pour supprimer l'intervention des banques dépositaires et donc réduire encore les coûts de transaction. Les institutions émettant des titres pourraient également les créer directement sur la blockchain et supprimer l'intermédiaire que sont les agents de transferts.

Ces projets ambitieux sont limités par la problématique de confiance périphérique. Avec cinquante banques régulées, la question de confiance ne se pose pas, mais quand on atteint des centaines de *brokers* et des milliers d'institutions, la confiance est plus difficilement atteignable. On en revient donc à ce problème de compromis entre coûts de transaction et confiance périphérique.

Encart 3 : Une première implémentation de la tenue de registre sur la blockchain sur le marché français

Yann le Floch, Blockchain Business Architect, BNP Paribas Corporate and Institutional Banking

En avril 2016, BNP Paribas Securities Services a annoncé travailler à la mise au point d'un registre utilisant le protocole blockchain qui permettra aux titres financiers émis par les entreprises



listées sur une plateforme de *crowdfunding equity* (SmartAngels) d'être comptabilisés automatiquement.

Les investisseurs achetant ces titres verront leurs paiements traités immédiatement et des e-certificats leur seront émis instantanément. Les opérations financières réalisées sur la plateforme seront ainsi effectuées de manière simplifiée, rapide, sécurisée et à faible coût. La standardisation de l'inscription des titres permettra d'offrir aux investisseurs une plus grande sécurité informatique et de traitement des transactions. Quant aux émetteurs, la plateforme blockchain opérée par BNP Paribas leur permettra de gérer leur actionnariat plus simplement.

La mise en œuvre de cette solution va permettre d'accélérer le mouvement initié il y a quelques années par les pionniers du *crowdfunding* : fluidifier l'accès des start-up et des PME de croissance au financement. La technologie blockchain se prête d'ailleurs particulièrement bien aux besoins de financement des entreprises non cotées : les volumes transactionnels sont moins importants que ceux des entreprises cotées en Bourse et les formalités administratives varient d'entreprise à entreprise, ce qui entraîne un besoin de standardisation que la technologie blockchain peut facilement régler.

La technologie blockchain présente des applications très intéressantes et fait désormais partie intégrante de la stratégie digitale de BNP Paribas.

4.2. Le passage à l'échelle

Dans la plupart des réseaux de transactions, plus le nombre de contributeurs à la blockchain est élevé, plus les coûts de transaction sont faibles mais plus la confiance envers les parties en périphérie est limitée. Le passage à l'échelle (« *scalability* ») constitue donc un challenge pour la blockchain.

Cinq problématiques liées au passage à l'échelle

La longueur de la chaîne et la question de la confiance à la périphérie ne sont pas les seuls challenges que doit relever la blockchain. Il existe cinq autres problématiques :

1. plus il y a de nœuds, plus les transactions sont sécurisées. Cela donne un avantage aux blockchains établies (Bitcoin par exemple) par rapport aux nouveaux entrants pour les applications blockchain.
2. plus il y a de jetons en circulation, plus la monnaie digitale sera liquide et son cours stable. Cela donne encore un avantage aux monnaies existantes, surtout si elles ont la masse critique. Les monnaies digitales deviennent alors un moyen d'échange acceptable et des valeurs refuges. Dans ce cas, une grande partie de leurs coûts de transaction – les commissions de change – disparaîtraient.
3. une seule « *killer app* » en couche applicative peut créer un effet de réseau sur l'ensemble des couches pour un écosystème entier d'applications. Cependant, aucune application de ce genre n'a encore émergé, et ce n'est sans doute pas le bitcoin qui va jouer ce rôle dans la mesure où il semble aujourd'hui entrer dans la phase de maturation de sa courbe en S (incubation-diffusion-maturation) ; en effet, son volume de transaction n'a crû que d'un tiers sur les douze derniers mois.
4. plus le nombre de contributeurs à la blockchain est élevé, plus leurs intérêts peuvent diverger, ce qui implique qu'il devient difficile pour les acteurs de se mettre d'accord sur une stratégie et pose des questions de gouvernance. Du côté des blockchains privées, gérer un consortium entre des entreprises concurrentes s'avère complexe. Pour ce qui est des blockchains publiques, il est difficile de faire coïncider les intérêts des développeurs, des mineurs et des développeurs professionnels. Pour les monnaies digitales, les conflits ont tendance à augmenter avec la valeur de ces devises.
5. certaines applications de la blockchain doivent faire face à un risque de régulation, notamment les monnaies virtuelles, si elles devaient atteindre des volumes d'échanges ou une valorisation faisant peser un risque systémique sur le système bancaire.

Des limites techniques...



À ces problèmes d'échelle liés au modèle économique, s'ajoutent des limites techniques liées à la capacité de traitement de la blockchain.

Actuellement, Bitcoin peut gérer 3 à 5 transactions par seconde et Ethereum 15 à 25, loin de l'efficacité de Visa (2500 transactions par seconde). Pour avoir un avenir dans le domaine des transactions financières, les blockchains doivent surmonter ce problème d'adaptabilité et d'échelle. Le problème de Bitcoin est que la vitesse de création de nouveaux blocs et leur taille sont fixes, ce qui limite la rapidité d'exécution. Des transactions validées plus vite seraient potentiellement moins sûres car une chaîne erronée pourrait se propager plus vite qu'elle ne serait validée.

Augmenter la taille des blocs faciliterait le passage à l'échelle, mais pousserait ainsi à la création de pools de minage de plus en plus grands et de plus en plus puissants. Or 52 % de la puissance de calcul totale est déjà détenue par quatre pools de minage chinois.

Les nœuds ne peuvent créer un bloc qu'après avoir fourni une « preuve de travail » (*proof of work*, PoW). Cette preuve de travail est constituée par la résolution d'un problème calculatoire complexe. Elle n'est donc pas aisée à produire, ce qui augmente le coût du travail et la consommation électrique pour produire et valider des blocs. La vérification de la preuve de travail est en revanche beaucoup plus simple que sa production. Le minage de bitcoins consomme déjà autant d'électricité qu'une ville américaine de 280 000 habitants et, selon une estimation de Motherboard (publication tech américaine), autant que l'électricité que consommera le Danemark en 2020. Le coût et l'émission de dioxyde de carbone deviendront économiquement et écologiquement non viables si le volume d'opérations effectuées par la blockchain continue de croître.

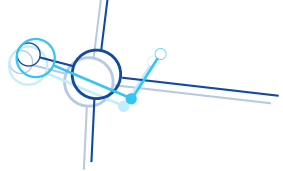
... et des pistes de solutions

Quelques pistes pour apporter des solutions à ces difficultés liées au passage à l'échelle sont à explorer :

- 1. La preuve de participation (*proof of stake*, PoS)** : contrairement à la preuve de travail selon laquelle les participants sont rémunérés pour cracker des algorithmes complexes afin de valider la création d'un nouveau bloc, la PoS implique que le participant devant valider la création d'un nouveau bloc est choisi en fonction du nombre de jetons en sa possession, c'est-à-dire de sa richesse (« *stake* »). Plutôt que de « miner » un bloc, on parle dans le cas de la PoS de « forger » un bloc. La richesse du forgeron fait que ce dernier n'a aucun intérêt à tricher, puisque cela aurait pour conséquence de faire baisser la valeur de ses jetons. Cette incitation à ne pas tricher n'est forte qu'en cas de convertibilité ou de perspective de convertibilité à court ou moyen terme des jetons. La preuve de participation peut réduire considérablement les calculs et donc les coûts de transaction de la blockchain.
- 2. Les canaux (*channels*)** : sous-groupes de participants à la blockchain qui peuvent échanger entre eux, mais qui ne soumettent qu'une petite partie des transactions à la blockchain principale pour ne pas la surcharger. Ce mécanisme pourrait permettre d'augmenter le nombre de transactions sans charger la blockchain principale tout en bénéficiant de sa sécurité.
- 3. Les chaînes latérales (*sidechains*)** : chaînes de blocs au sein de la blockchain qui créent les blocs plus vite, mais avec moins de sécurité. Cette technique permet aux utilisateurs de faire entrer et sortir des jetons de la blockchain principale vers des *sidechains*. Il peut être décidé qu'une *sidechain* appliquera une moindre sécurité pour les transactions d'un montant inférieur à un certain seuil, qu'elle créera des blocs plus rapidement ou bien qu'elle sera le support de *smart contracts*. Les *sidechains* peuvent même être des blockchains privées.
- 4. Le *sharding*** : tous les nœuds ne valident pas la transaction, et on diminue donc la sécurité en contrepartie d'un meilleur passage à l'échelle.

Ces développements sont à la pointe de la recherche et de l'expérimentation autour de la blockchain. Les leaders du Bitcoin avancent à pas mesurés dans cette direction en maintenant la sécurité comme priorité. La communauté de développeurs Ethereum avance plus vite : les versions Metropolis et Serenity, mises en production en 2016-2017 s'appuient sur les quatre principes de construction mentionnés *supra*.

Pour lutter contre les blockchains établies, les start-up essaient enfin de jouer sur une juste combinaison de ces facteurs. Elles peuvent se baser sur les codes existants de Bitcoin ou Ethereum ou en créer de nouveaux.



Encart 4 : Traçabilité et blockchain

Marc Pic, Deputy CTO Digital Activities, Surys Group

La traçabilité des biens matériels et immatériels repose aujourd'hui sur la constitution de bases de données, souvent de grande volumétrie, conservant les différents états des biens concernés. On distingue souvent la traçabilité amont – celle lors des phases de production de ces biens – de la traçabilité aval – celle de la distribution –, mais la traçabilité peut recouvrir de multiples ensembles d'étapes opérées sous le contrôle d'acteurs très différents. Ces acteurs peuvent avoir des intérêts divergents. Dans le modèle standard, la confiance dans les informations fournies par chacun de ces acteurs est alors sous le contrôle d'un tiers, souvent en charge de la base de données, dont la responsabilité est complexe vis-à-vis de chacun des acteurs.

L'introduction de la blockchain au sein d'une stratégie de traçabilité permet de déplacer la responsabilité des informations vers chacun des acteurs, chaque déclaration, signée par l'acteur la produisant, pouvant être contrôlée sans l'intervention d'un tiers. La blockchain permet alors une transparence plus importante sur les déclarations des acteurs et une meilleure association des responsabilités. Par exemple, elle peut permettre d'éviter que de fausses déclarations ne soient associées à un acteur innocent par une malversation de la base de données *a posteriori*.

Ces schémas déclaratifs multiples interviennent dans de très nombreuses applications de la traçabilité, de la sécurité alimentaire, jusqu'aux médicaments, en passant par les produits de luxe ou le *licensing* multiple. On peut donc s'attendre à un accroissement de l'usage de cette technologie dans ce domaine au cours des prochaines années. Cependant, il faut noter que des points techniques nécessitent d'être résolus. Les principales difficultés sont liées à la granularité et à la volumétrie des échanges : une traçabilité industrielle peut rapidement nécessiter la gestion individuelle de millions de nouveaux produits chaque heure, or les processus de blockchain actuels ont des latences de l'ordre de quelques secondes à quelques minutes suivant les modèles. Le coût individuel de l'insertion d'information dans une blockchain doit également être pris en considération. Des approches dites « de sidechain », avec agrégation des données, apparaissent comme une solution potentielle en faisant cohabiter base de données traditionnelles et preuve distribuée.

Bloc 4 : que retenir ?

- **La blockchain reste à ce stade une technologie non mature.**
- **Elle ne résout pas totalement la problématique de la confiance mais la déplace en périphérie.**
- **Le nombre optimal de contributeurs est déterminé par un compromis entre les coûts de transaction qui diminuent et la confiance périphérique qui se détériore avec le nombre de contributeurs.**
- **La blockchain est actuellement limitée au niveau du nombre de transactions qu'elle peut gérer par seconde : 3 à 5 pour Bitcoin, 15 à 25 pour Ethereum contre 2500 pour Visa.**
- **Il existe des obstacles à l'augmentation de cette capacité de traitement (concentration des pools de minage, consommation d'électricité), mais également des pistes de solutions (proof of stake, channels, sidechains, sharding) sur lesquelles des développements sont en cours.**



Partie 2

Soyez audacieux ! Expérimenter la blockchain

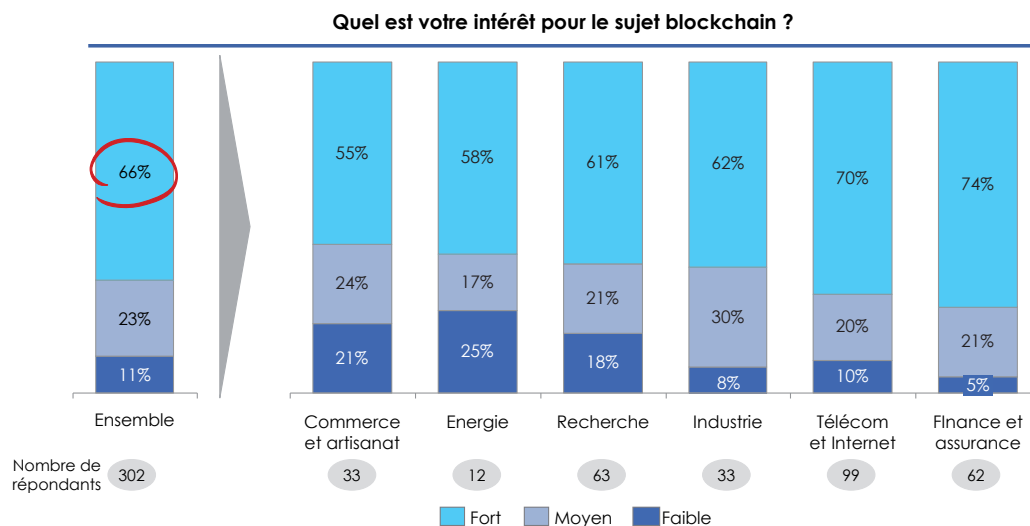
5. L'importance d'expérimenter la blockchain

5.1. Un intérêt croissant des acteurs économiques

Un sondage réalisé par le MEDEF en mai 2017 auprès d'entreprises françaises de toutes tailles et de tous secteurs d'activité montre que 66 % des décideurs s'intéressent au sujet blockchain⁴.

Un intérêt qui s'étend à tous les secteurs d'activité

66% des personnes interrogées déclarent un intérêt marqué pour la blockchain



Source : Sondage MEDEF ; Sur une échelle de 1 à 5, intérêt faible (1 et 2), intérêt moyen (3) et intérêt fort (4 et 5)

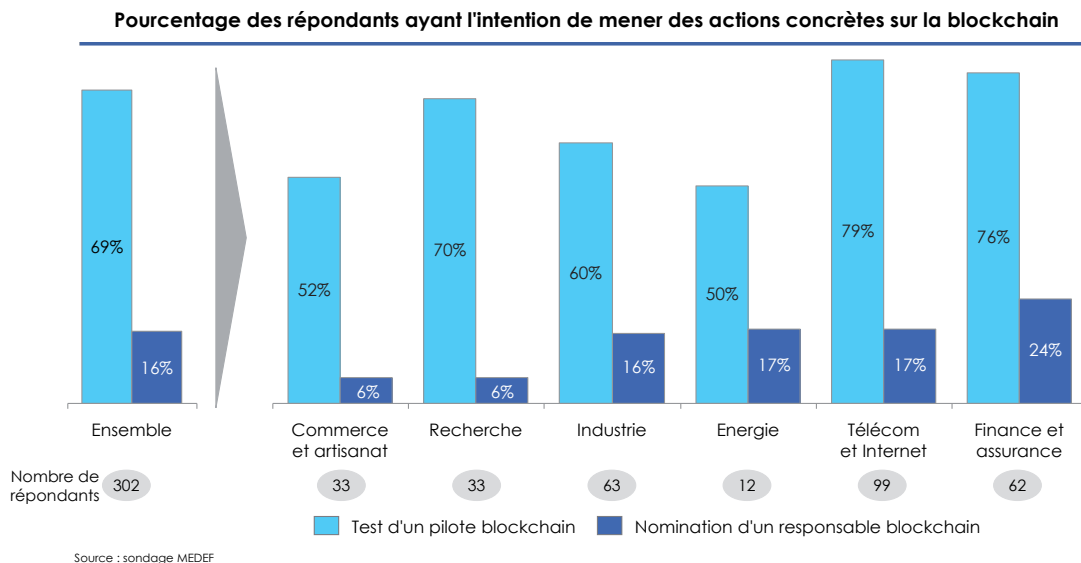
Source : sondage MEDEF

Ce même sondage montre que 69 % des décideurs seraient prêts à expérimenter la blockchain au sein de leur entreprise. En revanche, seulement 16 % pensent nommer ou ont déjà nommé un responsable blockchain.

4. Les sondés ont attribué une note de 1 à 5 à leur intérêt pour le sujet blockchain ; 1 et 2 représentant un intérêt faible ; 3, un intérêt moyen et 4 et 5, un intérêt fort. Sondage réalisé via un questionnaire auto-administré en ligne, entre avril et mai 2017 auprès de 302 répondants, qui sont des décideurs économiques répartis sur tous les secteurs économiques, adhérents au MEDEF ou à des fédérations professionnelles.



69 % ont envie de tester la blockchain... ... mais seulement 16 % souhaitent nommer un responsable blockchain



Source : sondage MEDEF

Plusieurs études internationales montrent que les cadres dirigeants ont bien intégré l'apparition de la blockchain dans le paysage économique et que la blockchain aura potentiellement un impact important sur leurs activités. Aux États-Unis en particulier, de plus en plus d'entreprises jouent un rôle actif sur le développement de technologies liées à la blockchain et un bon nombre d'entre elles se déclarent même prêtes à investir dans des projets le plus rapidement possible.

Ainsi, un peu plus de 60 % des cadres dirigeants américains interrogés déclarent avoir une connaissance solide de la technologie blockchain, 12 % ont déjà un projet blockchain en production et 15 % ont l'intention d'en lancer un en 2017⁵.

Cela se vérifie en particulier pour les institutions financières, puisque 14 % de ces dernières ont l'intention de mettre en production des solutions commerciales utilisant la blockchain en 2017. L'adoption de masse ne semble plus si lointaine puisque 65 % des banques espèrent commercialiser des services utilisant la blockchain dans les trois prochaines années⁶.

5.2. Des attentes élevées autour de cette technologie en phase de maturation

Chaque année, Gartner positionne les technologies émergentes sur une courbe du « hype » qui permet de déterminer dans quelle phase du cycle se trouvent les technologies « à la mode ».

Ces phases sont au nombre de cinq :

- phase 1 - Lancement de la technologie : émergence d'une nouvelle technologie prometteuse mais qui reste au stade du prototype.
- phase 2 - Pic des espérances exagérées : un certain emballement, médiatique en particulier, a lieu autour de la technologie pouvant ainsi aboutir à des attentes exagérées.
- phase 3 - Gouffre des désillusions : les produits développés à partir de la nouvelle technologie sont jugés décevants par rapport aux attentes qu'ils avaient générées.
- phase 4 - Pente de l'illumination : des entreprises persistent et développent des produits de deuxième génération dont les applications sont plus concrètes ; le marché se développe progressivement.

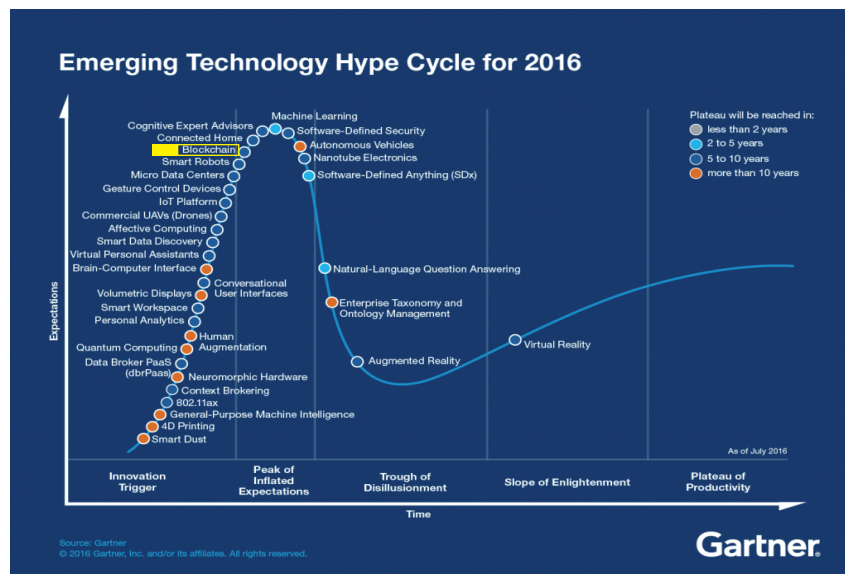
5. Deloitte Blockchain survey 2017 : www2.deloitte.com/us/en/pages/about-deloitte/articles/innovation-blockchain-survey.html

6. Enquêtes IBM : www-03.ibm.com/press/us/en/pressrelease/50617.wss



- phase 5 - Plateau de productivité : des produits de troisième génération sont développés et le déploiement de la technologie ne fait plus débat.

La courbe de Gartner établie en 2016 illustre bien cet engouement pour la blockchain et les attentes élevées qu'elle suscite. La blockchain serait même entrée dans la phase des espérances exagérées. Gartner estime par ailleurs que cette technologie atteindra le plateau de productivité dans 5 à 10 ans.

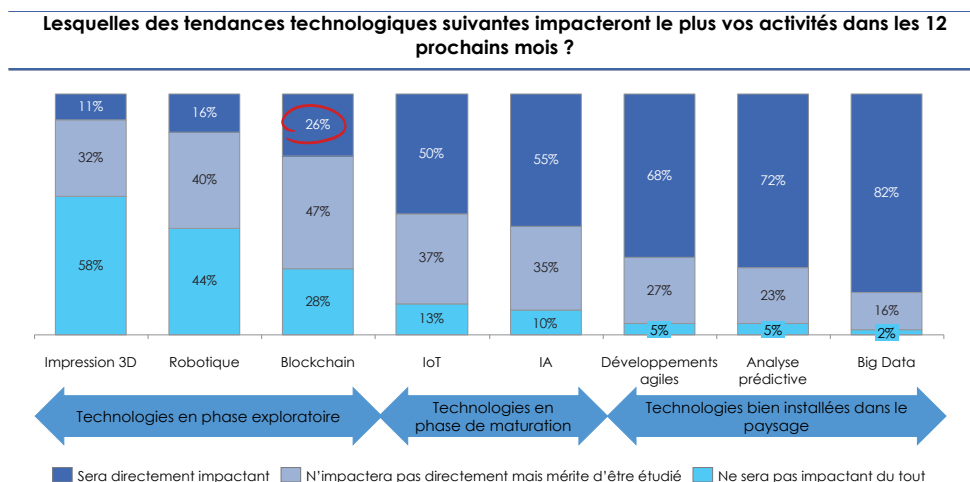


Source : analyse Gartner 2016

Un sondage réalisé par IBM-EBG-BCG en mai 2017 montre que les acteurs économiques comprennent le potentiel de la blockchain mais considèrent qu'elle n'est pas encore arrivée à maturation. En effet, 26 % des répondants considèrent que la blockchain aura un impact direct sur leurs activités dans les douze mois à venir, soit à court terme. À cela s'ajoutent 47 % des répondants qui estiment que la blockchain n'impactera pas directement leurs activités dans l'année à venir, mais qu'elle mérite d'être étudiée. Ce chiffre de 47 % est d'ailleurs le plus élevé parmi toutes les technologies sur lesquelles les répondants ont été interrogés. Cela témoigne bien d'une curiosité pour le sujet blockchain et d'une reconnaissance qu'il s'agit d'une technologie à fort potentiel, mais qui doit encore gagner en maturité.

Blockchain commence à gagner en maturité

26 % considèrent qu'elle impactera directement leurs activités cette année...



La blockchain est aussi la technologie qui soulève le plus de questions : 47% des répondants considèrent que l'impact et les applications potentiels de la blockchain doivent être étudiés

Source : Questionnaire Référentiel Digital Industrialisation (sur 776 répondants), rapport annuel sur la transformation digitale des entreprises IBM-BCG-EBG

Source : Sondage IBM-EBG-BCG

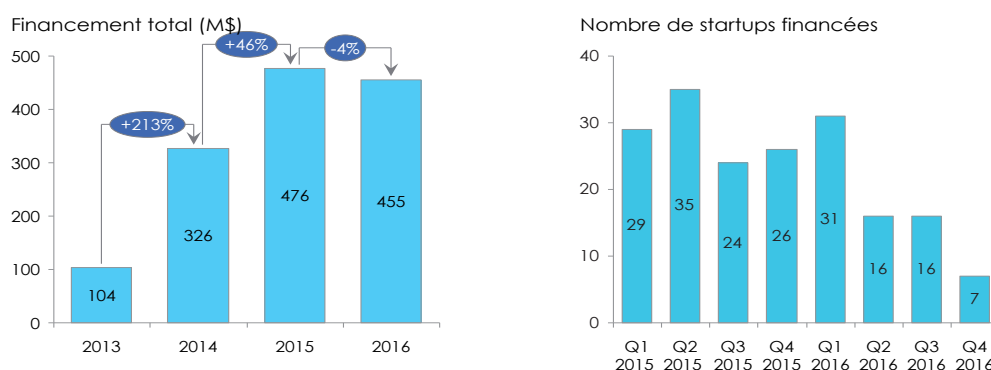


5.3. Quelques éléments de cartographie de l'écosystème blockchain

D'après les données partielles dont nous disposons, les start-up autour de la blockchain ont levé plus de 1,4 milliard de dollars de financement depuis 2013. On dénombre environ cinq cents start-up ayant décidé de se concentrer sur la blockchain. Cette technologie a réussi à attirer l'intérêt de la majorité des banques mais également d'entreprises d'autres secteurs comme l'assurance, la santé, et même de certains États.

Si les financements ont diminué en 2016, cela est surtout dû à une année 2015 exceptionnelle avec un nombre élevé de start-up ayant levé des fonds auprès d'investisseurs privés et de *business angels*.

Le financement des startups blockchain a diminué en 2016



Source : Fintech Control Tower, BCG

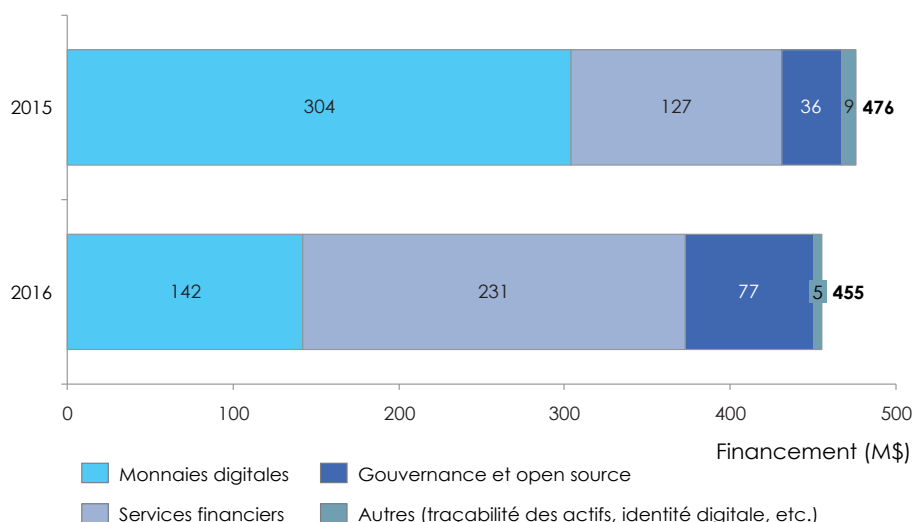
Les chiffres publiés par le World Economic Forum en août 2016 illustrent bien l'intérêt croissant pour les technologies de registres distribués :

- plus de 2500 brevets Distributed Ledger Technology (DLT) ont été déposés depuis 2013 (majoritairement par des institutions financières) ;
- plus de 24 pays sont impliqués dans des investissements DLT ;
- plus de 90 banques centrales ont commencé à discuter du sujet ;
- plus de 90 sociétés ont rejoint un consortium ;
- 80 % des banques prévoient d'engager un projet DLT en 2017.

De plus, il semble que les investissements récents se fassent moins sur les monnaies digitales et plus sur les autres applications comme les services financiers ou la gestion d'identité. Les investisseurs semblent comprendre que la vraie révolution viendra de la blockchain et de ses applications et non des monnaies digitales.



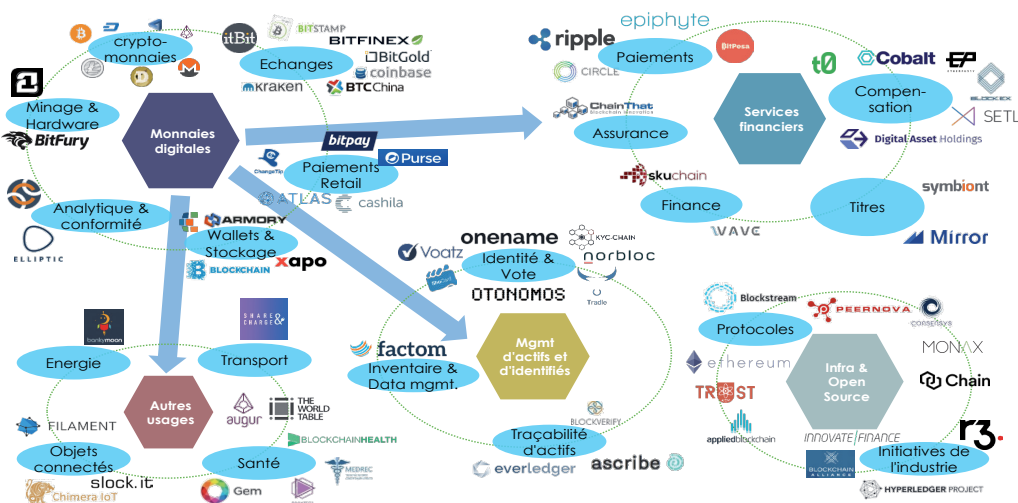
Le financement des monnaies digitales a connu une diminution par rapport aux autres cas d'usage



Source : Fintech Control Tower, BCG

Cartographie partielle de l'écosystème blockchain autour des grandes familles de cas d'usage

Les technologies blockchain se sont développées bien au-delà des monnaies digitales



Source : Fintech Control Tower, BCG

Le paysage des start-up françaises travaillant avec la blockchain est en plein essor. On dénombre une vingtaine de structures, à des stades de développement très variés, parmi lesquelles Belem, Blockchain Partner, Eureka, KeeeX, Ledger, Paymium, Postme.io, Scorechain, Stratumn, Wekeep et Woleet.

Blockchain Partner est une startup spécialisée dans le conseil sur les technologies blockchain. Ses activités reposent sur un tripôle d'expertise – stratégiques, techniques et juridiques – permettant notamment d'identifier des cas d'usage blockchain adaptés à chaque organisation, de développer des applications techniques (expérimentation & intégration), et d'évaluer la mise en conformité légale des projets blockchain.

Eureka est une entreprise fondée en 2014 proposant des cours ainsi que des certifications sur les protocoles Bitcoin et Ethereum pour les développeurs, les DSI, les entrepreneurs et les financiers. Ces formations



professionnelles visent notamment à faciliter le recrutement par les entreprises de personnes maîtrisant le sujet blockchain.

Keeex est une start-up marseillaise qui a développé un logiciel de messagerie d'entreprise fonctionnant avec des documents autosécurisés assemblés à la chaîne selon l'architecture et les principes d'une blockchain. Chaque document partagé par les employés est horodaté, signé et accompagné d'une preuve d'intégrité permettant de certifier son authenticité. Grâce à cette solution, l'archivage de données devient beaucoup plus facile puisqu'il n'y a plus besoin de coffre-fort et d'archives physiques. La blockchain garantit l'immutabilité et la sécurité des documents partagés sur le logiciel de la start-up Keeex.

Ledger est une start-up fondée en 2015 qui propose des portefeuilles pour monnaies digitales sous forme physique (« hardware »), généralement des clés USB. Ces portefeuilles apportent un niveau de sécurité supplémentaire grâce à la rupture physique avec le réseau. Le niveau de cryptage de ces portefeuilles physiques permet aussi aux propriétaires d'un produit Ledger de les utiliser sur n'importe quel ordinateur, y compris sur un ordinateur qui serait infecté par un virus. Ledger distribue ses produits dans plus de cinquante pays et veut rendre facile et sûr l'utilisation des monnaies digitales.

Paymium est une entreprise fondée en 2011 qui opère en tant que plateforme d'échange de devises et permet aux utilisateurs d'acheter, de vendre et d'effectuer des paiements en bitcoins. Paymium est la première place de marché européenne proposant un service en conformité avec la réglementation européenne sur les services de paiement. En offrant aussi ses services aux commerçants désirant accepter les paiements en bitcoins, Paymium propose à la fois du service B2C et B2B.

Postme.io est une start-up dont l'activité n'a pas encore été officiellement lancée. Elle ambitionne d'utiliser la technologie blockchain pour faciliter la gestion du processus de facturation (numérisation, comptabilité, règlement, affacturage, etc.) et d'améliorer la sécurité des données ainsi que la transparence.

Scorechain a pour ambition de fournir à ses clients des solutions pour les aider à gérer leurs actifs digitaux dans une blockchain. Depuis 2015, Scorechain commercialise une plateforme de tracking et de scoring des transactions Bitcoin et est donc l'une des premières entreprises à fournir un outil pour faciliter la gestion et la régulation des crypto-monnaies. Scorechain est impliqué également dans des projets collaboratifs dont Fundchain.lu – une initiative Blockchain menée avec plusieurs grands comptes de l'industrie des fonds – mais aussi LaBChain de la Caisse des Dépôts en France et Infrachain au Luxembourg.

Stratumn est une start-up fondée en 2015 qui se focalise sur la traçabilité des processus, via le déploiement de réseaux NaaS (*Network as a Service*) interentreprises leur permettant de sécuriser, de rendre traçable et de permettre l'audit de l'ensemble de leurs processus sensibles. Cette start-up s'est associée avec Bouygues Immobilier pour développer le premier projet français de *smart grid* sur blockchain. Ce projet, une première en Europe par sa taille, a consisté à bâtir le démonstrateur d'un réseau local décentralisé de supervision des échanges d'énergie dans l'éco-quartier Hikari, à Lyon Confluence. Le développement des énergies renouvelables et des *smart grids* a enclenché la transition d'un système de production d'énergie centralisé à un modèle décentralisé dans lesquels les consommateurs peuvent devenir producteurs. Le cadre réglementaire français y est désormais favorable, depuis l'ordonnance n° 2016-1019 du 27 juillet 2016 relative à l'autoconsommation d'électricité. La technologie blockchain déployée par Stratumn est la dernière brique parachevant cette transition, en permettant le développement de marchés locaux de l'énergie où producteurs-consommateurs et fournisseurs traditionnels peuvent entrer en concurrence. La traçabilité de l'énergie produite et consommée y est en effet un prérequis fondamental aux échanges.

Woleet est une start-up fondée en 2016 qui propose un service de stockage et de certification de données numériques sur la blockchain. La plateforme SaaS (*Software as a Service*) de Woleet propose des services d'horodatage et de signature numérique fondés par la blockchain.

Belem a développé un système de vote en ligne basé sur une blockchain et **Wekeep** est un programme d'assurance pair-à-pair totalement décentralisé. Ces start-up ne sont que des exemples parmi d'autres qui explorent les opportunités ouvertes par la blockchain.

Les start-up n'ont toutefois pas l'exclusivité des projets blockchain. Plusieurs grands groupes ont lancé des PoC, parmi lesquels PSA sur la dématérialisation du contrat d'entretien des véhicules, ou Carrefour avec la traçabilité de ses filières animales.



5.4. Les modalités de collaboration au sein de l'écosystème

Investir davantage dans la blockchain n'a de sens que si de nombreuses entités ont des coûts de transaction élevés et un niveau de confiance imparfait. C'est pourquoi la mise en œuvre de ce type de technologie doit se faire dans l'ensemble du réseau et pas chez un seul participant. Le fardeau du déploiement et du maintien de la blockchain est alors partagé.

Les multinationales de la *tech* investissent pour convaincre leurs entreprises clientes, notamment celles évoluant dans des industries fragmentées comme la santé ou le commerce international, de l'intérêt de créer des alliances autour de plateformes de transaction basées sur la blockchain. Ces projets ambitionnent de produire des résultats sur le long terme, une dizaine d'années en moyenne.

Pour soutenir des modèles alternatifs de mise en œuvre de la blockchain, les entreprises n'ont pas d'autre choix que de travailler ensemble, ce qui peut passer par plusieurs modèles de coopération.

Consortium

Selon la définition donnée par le Larousse, un consortium est une « association d'entreprises constituée dans le but de réaliser un projet commun ». Aujourd'hui, de nombreuses entreprises travaillent ensemble au développement et à l'application de la blockchain dans leurs industries respectives.

Le rôle de ces consortiums est tout d'abord un rôle d'éducation et de mutualisation de la recherche sur la blockchain. Un autre objectif poursuivi par les consortiums est la création de prototypes et le test de cas d'usage de la blockchain. De nombreux consortiums expérimentent ainsi en leur sein des applications utilisant la blockchain, avant d'éventuellement d'en lancer l'industrialisation.

On dénombre environ 25 consortiums rassemblant plus de 500 participants. La majorité d'entre eux sont américains et composés d'acteurs de l'industrie des services financiers, mais d'autres rassemblent des acteurs de l'assurance ou de la santé⁷. Les consortiums peuvent se créer autour d'une société qui en assure le pilotage ou bien autour d'un ensemble de sociétés contributrices avec une gouvernance partagée.

Les deux consortiums les plus reconnus et influents sont R3CEV et Hyperledger. **R3CEV** a historiquement été soutenu par les plus grandes banques et institutions financières de la planète pour expérimenter de nombreux projets utilisant la technologie de registre distribué. R3CEV a développé Corda, un registre distribué inspiré de la blockchain Ethereum. **The Hyperledger Project** a été créé par la fondation Linux en décembre 2015. Ce consortium a pour but de développer des logiciels de registre distribué *open source*. Hyperledger regroupe des membres comme Cisco, R3CEV, London Stock Exchange, Accenture, IBM, Intel, JP Morgan Chase, Swift ou encore Wells Fargo.

Après avoir été le consortium le plus en vue, R3CEV doit aujourd'hui faire face au départ de membres influents comme Goldman Sachs, Morgan Stanley, JPMorganChase et Santander suite à un manque de résultats probants et à des désaccords sur sa gouvernance. La plateforme Corda développée par R3CEV peine à produire des résultats concrets. De plus, lors de la dernière levée de fonds, « *R3CEV s'est certainement révélé un peu trop gourmand dans ses conditions financières en exigeant que 40 % lui reviennent contre 10 % en général dans des configurations similaires* », analyse Eric Larchevêque, directeur général de Ledger⁸.

Encart 5 : « Coopétition » et initiative LaBChain CDC

Nadia Filali, directrice des programmes blockchain et copilote du LaBChain à la Caisse des Dépôts

Au cœur de la technologie blockchain, on trouve la promesse de désintermédiation. Créant un environnement sécurisé, elle permet d'effectuer des transactions de pair-à-pair, sans tiers de confiance.

Ce fonctionnement intrinsèquement décentralisé et distribué implique qu'il y ait plusieurs parties prenantes, il est donc indispensable de travailler à plusieurs pour explorer son potentiel.

7. www.coindesk.com/state-global-blockchain-consortia/

8. Les Echos : www.lesechos.fr/finance-marches/banque-assurances/0211533384718-blockchain-les-defections-se-multiplient-au-sein-du-consortium-r3-2045899.php#inscription



Par ailleurs, un écosystème de start-up blockchain se structure en France et se positionne comme un des plus dynamiques en Europe.

C'est pourquoi la Caisse des Dépôts, tiers de confiance depuis 1816, a lancé en décembre 2015 l'initiative de place LaBChain, un laboratoire d'innovation dédié aux technologies de registres distribués afin de mutualiser les démarches d'exploration et d'anticiper collectivement les opportunités de cette rupture technologique, en priorité dans les métiers de la banque-finance-assurance. Cette initiative soutient également le développement de l'écosystème français dédié à la blockchain en organisant ses travaux autour de partenariats en mode agile entre grands groupes et start-up. Ce consortium réunit 29 partenaires : banques, assureurs et mutualistes, start-up et entreprises industrielles.

Ce modèle de collaboration innovant a permis de faire aboutir plusieurs PoC, et la Caisse des Dépôts renforce aujourd'hui ses liens avec le monde de la R&D à travers un partenariat avec l'IRT SystemX afin d'anticiper les conditions d'industrialisation, mais également au sein de LaBChain en réfléchissant notamment aux conditions de gouvernance, à l'hybridation avec d'autres technologies ou à la transposition réglementaire, en lien avec les régulateurs français et européens.

Groupes de travail

Les groupes de travail rassemblent des entreprises pour réfléchir et discuter des différents cas d'usage possibles pour la blockchain. Le MEDEF a, par exemple, lancé un groupe de travail en juin 2016. Son objectif est d'encourager la collaboration entre les acteurs de tous les secteurs d'activité liés au numérique. Ces groupes partagent leurs connaissances et avis sur cette nouvelle technologie.

Partenariats avec des start-up et fin tech

D'autres entreprises choisissent de travailler en partenariat avec des start-up ou des *fin tech* spécialisées dans le sujet blockchain. Cette approche permet un développement rapide d'applications avec l'aide de spécialistes du sujet, mais empêche la standardisation et l'adoption de masse qu'aurait pu permettre le travail en consortium par exemple.

Recherche interne

Certaines entreprises préfèrent concentrer leurs ressources sur de la recherche interne. Cela peut générer une réflexion moins riche que celle d'un consortium dans la mesure où il n'y a pas d'apport extérieur. Mais la recherche interne permet de concentrer ses ressources sur des cas d'usage qui répondent à un vrai besoin client.

BNP Paribas Corporate and Institutional Banking (**CIB**) a créé un département innovation avec quelques employés permanents et une équipe de développeurs. Selon les projets, l'équipe peut accueillir de nouveaux contributeurs qui vont travailler sur un projet donné en plus de leurs tâches habituelles.

Cette approche a permis à BNP Paribas de développer deux PoC particulièrement avancés qui pourraient être industrialisés d'ici la fin de l'année 2017. La particularité de la recherche chez BNP est qu'elle se fait en travaillant avec un client sur chaque projet. Cette implication du client rend le PoC plus réaliste et transposable à une production de masse si le projet s'avère réalisable.

Malgré ces quelques *success stories*, travailler seul sur un sujet aussi complexe que la blockchain ne facilite pas l'apport d'idées neuves et peut donc ralentir le développement de cas d'usage concrets. Une collaboration entre acteurs du marché (« coopération ») permet en revanche d'accélérer l'apprentissage et l'expérimentation.



Encart 6 : Mutualisation des ressources pour créer une start-up sur la blockchain

Nicolas Rivard, chief innovation officer d'Euronext

La blockchain va clairement transformer notre industrie ; le défi est que personne ne sait encore exactement quand, où et comment.

Pour dépasser les présentations et les prototypes, nous avons décidé de créer un consortium et de lancer un vrai projet opérationnel autour d'une ambition : améliorer le développement des PME, moteurs de l'innovation et de la croissance économique en Europe, en s'appuyant sur la blockchain pour faciliter leur financement par les marchés financiers paneuropéens.

Par sa capacité à créer sans tiers de confiance une information partagée, validée, unique et infalsifiable, la technologie blockchain ouvre l'opportunité d'une refonte des services de post-marché, essentiels au bon fonctionnement des marchés, que ce soit au service des PME ou des investisseurs. Tout d'abord, en rendant possible une gestion décentralisée du registre de titres, elle promet aux sociétés cotées d'identifier aisément leurs actionnaires, procédure longue, complexe et coûteuse aujourd'hui. Côté investisseurs, en simplifiant la chaîne de transaction, elle promet également des délais de traitement réduits et des coûts de transaction plus faibles. Enfin, elle facilite l'intégration des marchés paneuropéens.

À la poursuite de cette ambition, et dans la recherche du juste équilibre entre la nécessaire implication de l'ensemble de l'écosystème et l'indépendance indispensable à l'émergence de solutions véritablement innovantes, Euronext a créé avec Paris Europlace un consortium qui associe de grandes institutions financières dont Euroclear, la Caisse des Dépôts, CACEIS, BNP Paribas Securities Services et la Société Générale, mais aussi des investisseurs institutionnels, afin de mutualiser leurs ressources et de créer une start-up indépendante, dotée de ses propres moyens et qui sera entièrement dédiée à ce projet. La start-up sera lancée d'ici l'été 2017 et les premiers développements interviendront cette année.

5.5. Quelques cas d'usage emblématiques de la blockchain

De nombreux cas d'usage de la blockchain ont émergé ces derniers mois avec des degrés de maturité allant du *proof of concept* aux premiers déploiements, dont voici quelques exemples parmi les plus emblématiques :

- améliorer la traçabilité de la chaîne alimentaire afin de limiter la fraude sur la qualité et la nature des produits alimentaires (Alibaba, PwC, AusPost et Blackmores) ;
- améliorer la traçabilité des conteneurs et de leurs marchandises afin de réduire le temps de transport, la fraude et les erreurs d'aiguillage (Maersk, IBM) ;
- permettre l'échange de données sur la santé des patients de manière sécurisée (IBM Watson, FDA, Google, NHS) ;
- permettre d'établir numériquement des documents légaux (ex. diplômes) de sorte qu'ils soient infalsifiables et vérifiables par tous (Bitproof) ;
- développer et rendre infalsifiable le vote électronique (FollowMyVote) ;
- améliorer la transparence sur l'usage qui est fait des dons aux associations d'aide humanitaire (Start Fund) ;
- permettre le stockage *cloud* distribué pour éviter la concentration de l'information dans les *data centers* de quelques acteurs majeurs du stockage en ligne (Filecoin, Storj) ;
- permettre la rétribution des collaborateurs en fonction de leur investissement pour mieux valoriser les contributions de chacun dans le cadre d'un projet (Backfeed, Ouishare) ;



- lutter contre la contrefaçon de produits de luxe (Blockverify) ;
- protéger la paternité, la propriété et l'authenticité d'une œuvre dans la blockchain (Monegraph, Verisart) ;
- mettre en place un système de paiement direct des artistes sur une plateforme de streaming (PeerTracks, Ujo Music) ;
- permettre la communication autonome et décentralisée entre objets connectés au sein d'une maison intelligente (IBM, Samsung).

Dans ce qui suit, nous détaillons quelques exemples d'applications autour des cinq thèmes proposés à l'idéation lors du BizHackathon blockchain Paris des 7 et 8 juin 2017.

Les thématiques retenues étaient les suivantes :

- identité et authentification ;
- mobilité ;
- traçabilité ;
- objets connectés ;
- contrats et certifications.

5.5.1. Identité et authentification

Le gouvernement de la République d'Estonie a lancé en 2015 une plateforme d'e-résidence via un partenariat avec Bitnation. Cette plateforme permet aux non-résidents d'acquérir une nationalité estonienne numérique pour signer des contrats commerciaux, mais également tous types de documents comme des actes de naissance ou de mariage.

Cette initiative a pour objectif d'attirer des investissements en Estonie en y facilitant l'implantation d'entreprises étrangères. Bien que cette initiative soit basée sur la blockchain, le gouvernement n'accorde l'e-résidence qu'après contrôle d'identité et vérification des antécédents. Pour espérer donner une valeur juridique à des contrats signés et enregistrés sur la blockchain, il faut pouvoir être sûr de la véritable identité de l'interlocuteur virtuel.

Les actes de mariage et certificats de naissance ne sont pour l'heure reconnus qu'au sein de la « juridiction blockchain » et pas encore par l'État estonien. Les contrats, quant à eux, ont une valeur juridique dans toute l'Union européenne puisque les e-résidents estoniens sont également résidents européens et sont opposables devant un tribunal.

Le gouvernement travaille avec le secteur privé pour ajouter d'autres applications à sa plateforme d'e-résidence.

L'objectif de l'État est d'atteindre les 10 millions d'e-résidents d'ici 2025. Aujourd'hui, ils sont à peu près 10 000 (pour 1,3 million de résidents physiques), et plus de 500 sociétés ont été créées par des e-résidents. La population finlandaise est la plus représentée, suivie par les Russes et les Américains⁹.


Encart 7 : Quelques applications de l'inaltérabilité apportée par la blockchain

Romain Sohet, consultant SI/expert lutte antifraude

Le *cloud* soulève de nombreuses questions en termes de protection des données. La blockchain, du fait de sa possibilité de duplication à chaque nœud, va-t-elle permettre de s'affranchir des grands faiseurs de *cloud* comme Amazon ou Google ? En fonctionnant de gré-à-gré, n'importe qui peut en principe stocker les données d'un interlocuteur, à la condition d'un accord et de la mise en place des clés publiques et privées. Ces données peuvent être dupliquées en environnement crypté et sécurisé, ce qui rend leur disparition totalement impossible. Ceci peut intéresser les autorités policières et judiciaires, souvent amenées à lutter contre l'effacement ou la corruption brusque et soudaine de données sensibles.

9. www.journaldunet.com/economie/finance/1176465-estonie-blockchain/





Il en découle une application : la gestion des identités. Identités digitales à l'épreuve des manipulations et des corruptions, s'entend. Par exemple, le collectif Bitnation Blockchain Emergency ID propose un identifiant digital d'urgence pour les migrants et réfugiés qui se voient confisquer ou voler leurs passeports. Toutefois, cela implique un réseau de confiance absolue et une enquête d'état civil pour éviter toute fraude numérique.

Mais au-delà de l'inaltérabilité des données enregistrées, la blockchain libère les interlocuteurs de l'utilisation d'un administrateur de bases de données, personne tierce à l'entreprise, avec tout ce que cela comporte comme risque de maintenance et de pillage de données (ou de partage de mémoire de stockage ou de clés uniques). Certains acteurs de la santé voient d'un bon œil la mise en place de la blockchain au sein même des structures hospitalières, ce qui permet de conserver le secret médical d'un patient en toute quiétude et sans avoir recours au *cloud*. Ce secret professionnel peut s'étendre à tout type d'administration : cadastre, service de cartes grises, droits d'auteur sur prestations et créations intellectuelles, état civil et livret de famille, administration pénitentiaire... et bien sûr, le vote par Internet.

Le vote par Internet via la blockchain est tentant en termes de facilité, d'inaltérabilité des résultats, d'empêchement à la fraude... à la condition expresse que les clés uniques soient vraiment uniques, accessibles uniquement au « bon » votant, d'un nombre suffisant pour couvrir le nombre de votants, sans engorgements du réseau, et en respectant l'anonymisation du vote (la personne qui a envoyé une clé à quelqu'un qui va voter peut savoir pour qui cette personne a voté). Ainsi, autant les résultats du vote seront justes, autant l'on peut savoir qui a voté pour qui. Toutefois, ce type de vote peut aisément être envisageable dans des petites structures, des entreprises (par exemple pour élire un comité d'entreprise dans une multinationale) ou lors de primaires.

5.5.2. Mobilité

Share&Charge est une start-up allemande qui met en relation propriétaires de véhicules électriques et de bornes de rechargement. Ainsi, n'importe quel particulier possédant une borne de rechargement à son domicile peut la rendre disponible aux utilisateurs de Share&Charge. Cela leur permet de rentabiliser leur installation tout en augmentant le nombre de points de chargement pour véhicules électriques.

Share&Charge a mis au point une application de *wallet* permettant d'effectuer une transaction entre un automobiliste et un propriétaire de borne de rechargement lorsque le premier recharge son véhicule chez le second. Cette application est basée sur la technologie blockchain (et les *smart contracts*) et utilise ses principes de transparence et de décentralisation pour permettre une transaction de pair-à-pair. Une monnaie virtuelle, le « crypto-euro », est utilisée pour les transactions entre automobilistes et propriétaires de bornes de rechargement. Ce crypto-euro n'est à ce stade pas convertible en euros et ne peut donc être utilisé que pour le chargement de véhicules électriques.

5.5.3. Traçabilité

Everledger est une entreprise britannique fondée en 2015, qui est spécialisée dans la certification et la traçabilité des diamants. La start-up a construit un registre distribué qui trace et protège des actifs de valeur tout au long de leur vie.

Everledger a commencé par enregistrer des diamants sur un registre distribué en construisant une fiche d'identité pour chacun d'eux. Chaque pierre précieuse est d'abord enregistrée sur la blockchain grâce à une fiche d'identité reprenant quarante caractéristiques uniques (taille, forme, couleur, poids en carats, etc.). Par la suite, l'inscription de ces diamants dans la blockchain va permettre de les authentifier et de certifier qu'ils ne proviennent pas d'un trafic (diamants de sang, recel). Lors d'une transaction, il sera demandé de fournir une preuve cryptographique de propriété de la pierre. Aujourd'hui, le registre distribué d'Everledger compte plus d'un million de diamants.

Pour la création des profils des diamants, Everledger travaille avec des experts reconnus du secteur diamantaire. Si on est sûr que la fiche d'identité d'un diamant ne peut pas être modifiée, il faut, en revanche, faire confiance à ceux qui ont décrit la pierre dans un premier temps (déplacement de la confiance en périphérie du réseau).



En combinant blockchains publique et privée, Everledger a créé un service optimal de traçabilité des diamants qui peut être étendu à n'importe quel actif de valeur comme des montres, des bijoux ou des sacs. Everledger participe au projet Hyperledger et a construit sa plateforme sur le réseau blockchain d'IBM.

5.5.4. Objets connectés

Slock.it est une entreprise allemande qui travaille dans le domaine des objets connectés (*Internet of Things*). L'objectif de cette entreprise est de lier les objets physiques à la blockchain grâce à la plateforme Ethereum et à l'utilisation des *smart contracts*.

Grâce à la blockchain, Slock.it pourrait permettre la désintermédiation des locations de logements par exemple. Plus besoin de passer par une plateforme comme Airbnb, qui prélève une commission, pour réserver un appartement. En effet, il est possible de déverrouiller un cadenas ou une serrure grâce à la blockchain et à l'utilisation de *smart contracts*.

L'utilisateur a simplement besoin de scanner un QR code sur la serrure avec son *smartphone*. Ensuite, un paiement en ethers est validé par la blockchain (environ une minute d'attente) puis la serrure s'ouvre automatiquement. Ce système fonctionne de manière automatisée et totalement désintermédiée. Slock.it est soutenu par des partenaires comme Samsung, Microsoft et Ubuntu.

5.5.5. Contrats et certifications

La start-up Bitland travaille à l'enregistrement de registres cadastraux sur un registre distribué en collaboration avec le gouvernement ghanéen. Pour répondre à une problématique de certification de terrains parfois inexistante ou frauduleuse, la blockchain permet une immuabilité et un enregistrement fiable des titres de propriété.

Environ 90 % des terres agricoles du Ghana ne sont enregistrées dans aucune base de données officielle. Cette situation mène à des problèmes administratifs et querelles entre citoyens puisqu'il n'existe aucun moyen de vérifier la propriété de certains terrains.

Bitland se donne pour objectif d'enregistrer les propriétés sur un registre distribué pour éviter la falsification du cadastre et suivre les transactions de ces terrains afin d'en établir la propriété en temps réel. Cette ONG africaine utilise la blockchain Bitcoin pour enregistrer de manière sûre les titres de propriété des terres rurales. Bitland espère signer un contrat de quatre ans avec le gouvernement ghanéen pour répertorier toutes les terres agricoles du pays avant d'étendre son activité à d'autres pays d'Afrique. Des démarches similaires ont été entamées en Géorgie mais, cette fois, soutenues directement par le gouvernement, en collaboration avec l'entreprise Bitfury. Grâce à ces initiatives, la propriété d'une parcelle donnée peut être instantanément vérifiée¹⁰.

Bloc 5 : que retenir ?

- **Les investisseurs et business angels ont investi plus d'un milliard de dollars dans plus de 500 start-up blockchain, dont quelques start-up françaises.**
- **La prise de conscience des enjeux et du potentiel de rupture que porte cette technologie au-delà du seul secteur financier a clairement démarré : 69 % des décideurs sondés par le MEDEF se déclarent prêts à expérimenter la blockchain.**
- **Pour autant, face à une technologie complexe et non encore mature, passer le cap de la mise en œuvre d'une organisation dédiée reste difficile à envisager : seulement 16 % des sondés envisagent de nommer un responsable blockchain dans leur entreprise.**
- **De nouveaux usages potentiels, qui ne se limitent plus aux monnaies virtuelles, émergent : identité et authentification, traçabilité, mobilité, objets connectés, contrats et certification, etc.**

10. <https://blockchainfrance.net/2016/03/03/des-cadastrs-sur-la-blockchain/>





6. Un écosystème non stabilisé : comprendre les enjeux des évolutions en cours

6.1. Le rôle des blockchains publiques et des blockchains privées

Une concurrence – potentiellement conflictuelle – pourrait émerger dans les années à venir entre des blockchains privées contrôlées par des coalitions d'intermédiaires regroupés au sein de consortiums et des blockchain publiques accessibles directement par le consommateur.

Les blockchains publiques ont un avantage de taille : elles ont plus de blocs, plus de nœuds et donc une validation plus rigoureuse. Par définition, elles peuvent ajouter des contributeurs plus facilement, mais cela diminue le niveau de confiance périphérique.

Les blockchains privées ont l'avantage de travailler avec un réseau de transactions ciblé. Les chaînes privées ont besoin de moins de contributeurs et peuvent fonctionner selon des principes qui ne résistent pas au passage à l'échelle, comme celui du *proof of work*.

Les bouleversements du système et leur ampleur dépendent moins de la vitesse absolue d'avancée technique que de la vitesse relative à laquelle les implémentations publiques et privées avancent. Cette vitesse est largement influencée par le contexte politique. Sur les blockchains, les consortiums doivent travailler ensemble alors que leurs membres sont d'ordinaire concurrents. De l'autre côté du spectre, les communautés ouvertes doivent également suivre une stratégie commune alors que chaque individu a ses intentions propres. Travailler ensemble ne facilite donc pas toujours la prise de décisions...

Encart 8 : Les blockchains privées ne révolutionneront pas l'économie

Pierre Noizat, cofondateur de Paymium

Une blockchain est une base de données distribuée, sécurisée par un ensemble ouvert de valideurs qui la mettent à jour continuellement, à intervalles réguliers.

Le mot « blockchain » a commencé à gagner en popularité à partir de 2015 quand la plupart des grandes entreprises ont pris conscience simultanément de l'importance de l'invention Bitcoin et des effets disruptifs qu'elle pouvait avoir sur leurs métiers.

En gommant le réseau (Bitcoin) pour se focaliser sur la base de données (blockchain), les entreprises sont confortées dans l'idée que posséder leur propre infrastructure, un réseau privé, reste la meilleure option. Qu'en est-il vraiment ?

Avant Bitcoin, la transition numérique se concevait comme la mise en place d'une *software mediated economy* qui serait le simple reflet du monde d'avant. Pourtant, avec Bitcoin et la décentralisation qu'il permet, nous disposons bien d'un nouveau protocole.

L'utilisateur, le client et le citoyen ne sont plus à la périphérie de réseaux conçus comme des châteaux-forts, mais au centre d'une architecture horizontale et distribuée où chacun peut jouer son rôle, sans pont-levis ni garde-barrière. L'entreprise ouverte sur un tel réseau ne peut se développer que par l'excellence.

Un logiciel libre et une architecture décentralisée sont les garants d'une concurrence saine où les barrières technologiques s'effacent. Les nouveaux services permis par le réseau Bitcoin et sa blockchain tireront parti de ses propriétés de monnaie programmable et universelle : contrats d'assurance auto-exécutables, micro-paiements entre objets connectés, certification de documents accessible à tous, etc.

Ils ne remplaceront pas des services existants, mais ouvriront des marchés aujourd'hui bridés par les contraintes des réseaux centralisés. Se contenter de la blockchain pour optimiser une infrastructure privée ne suffira pas pour être un acteur durable de la nouvelle économie numérique décentralisée qui se dessine à l'orée du XXI^e siècle.



Encart 9: Blockchain et Industrie, la réponse à un besoin de Confiance Numérique généralisé

Rui Teixeira Guerra, administrateur de l'AFNET et de la Fédération des Tiers de Confiance du numérique (FNTC)

La notion de «Confiance Numérique» couvre la question de savoir de façon certaine qui peut accéder à quelle information, d'où provient chaque information, comment tracer qui y a accédé, comment s'assurer que l'information, ou les engagements sont infalsifiables et opposables, comment archiver ces informations sur des périodes courtes ou longues, comment les auditer, et comment prouver la conformité aux normes et aux règles.

D'une certaine façon la blockchain est une réponse technologique à une bonne partie de la question de la Confiance Numérique. Cette réponse arrive à point nommé, à un moment où le besoin de confiance numérique explose. La blockchain représente l'aboutissement de trois décennies d'évolution de sécurisation des échanges numériques, notamment par la cryptographie.

La blockchain c'est le «packaging» ou la «protocolisation» des technologies de la chaîne de confiance numérique. Elle porte au moins deux promesses. Avec la blockchain on peut produire et conserver facilement des traces digitales infalsifiables de «tout». En réalité on pouvait déjà le faire avant, avec des systèmes d'archivage dotés de composantes cryptographiques. Mais la blockchain facilite une traçabilité «consubstantielle» à l'infrastructure digitale. C'est en ce sens autant une révolution psychologique ou des usages, qu'une révolution technique. Ces traces peuvent être produites de façon collaborative et distribuée. Chaque partie peut donc conserver les traces des informations digitales souhaitées et ces traces font preuve de ce qui doit être prouvé. Cette structure distribuée aide à créer de la confiance là où elle n'existe pas naturellement.

La technologie des blockchains privées est une réponse simple, efficace, rassurante et adaptée à toute communauté ou filière souhaitant mettre en place un système d'échanges incluant une forte dose de Confiance Numérique. Les blockchains privées sont une voie essentielle pour l'industriel, car elles évitent les incertitudes sur la gouvernance des blockchain publiques à court terme.

Code is law vs Code and law? Certains prétendent qu'avec la blockchain, le code informatique contient la «règle» juridique et donc que le droit et le programme se confondent, voire que le système juridique n'est plus nécessaire. Ce n'est pas le cas. Quiconque côtoie le monde de la blockchain a certainement déjà entendu parler des problèmes de gouvernance. La majorité décide ? Mais cela permet-il à la majorité de voler la minorité ? Or cette gouvernance que l'on recherche implique qu'elle n'a pas encore été trouvée. Elle est même probablement contextuelle et évolutive, comme la règle de toute communauté.

6.2. Le rôle clé du législateur

Le climat actuel est étonnamment favorable, en termes de législation, au développement de la blockchain. Le bitcoin est légal dans la plupart des pays et est régulé en tant que ressource, mais pas en tant qu'instrument financier.

Le premier sujet d'intérêt pour le régulateur est la couche applicative (en particulier les plateformes d'échange de devises). En effet, les blockchains facilitent le travail du régulateur : elles réduisent le risque de contrepartie, simplifient les processus de connaissance des clients (*know your customer*, KYC) et permettent de lutter contre le blanchiment en donnant accès à l'historique des transactions.

Mais ce climat favorable est très évolutif. Les gouvernements pourraient décider de tester la blockchain eux-mêmes pour des applications dans le domaine de l'identité, de la santé et des monnaies digitales. C'est ainsi que le gouvernement britannique a commandé un rapport en 2015 sur les applications potentielles de la blockchain pour améliorer les services publics¹¹.

11. Distributed ledger technology: beyond block chain, décembre 2015





Beaucoup de dirigeants voient ce genre de technologie comme un catalyseur pour stimuler l'économie, créer des emplois et générer un avantage compétitif. Ce point de vue dépend toutefois fortement du pays.

Les jumeaux Winklevoss, connus pour leur implication dans un procès intenté contre Mark Zuckerberg à propos de la paternité de Facebook, se sont vu refuser par la Securities and Exchange Commission (SEC) leur demande de création du premier fonds négocié en bourse (*Exchange Traded Fund, ETF*) Bitcoin le 11 mars 2017. La SEC a estimé que l'ETF n'apportait pas suffisamment de garanties quant à la prévention de pratiques frauduleuses et de manipulations. La création d'un instrument financier officiel indexé sur le cours du bitcoin aurait favorisé l'adoption et les investissements dans cette monnaie digitale. Les frères Winklevoss, fervents défenseurs du bitcoin, ne désespèrent pas de voir un jour la création de cet ETF validée par le régulateur américain.

Point sur l'état de la législation française

C'est à l'été 2015 que la France, comme de nombreux autres États, a commencé à s'intéresser à la blockchain à la suite d'un intérêt croissant des banques et des services financiers pour cette nouvelle technologie. Cette période correspond à la naissance de la blockchain Ethereum et à l'arrivée des premiers smart contracts¹².

Manuel Valls, alors Premier ministre, déclarait, en juillet 2016 : « C'est en droit français que, pour la première fois en Europe, nous allons fixer les conditions juridiques et de sécurité dans lesquelles on pourra réaliser les transactions financières décentralisées sur Internet, ce qu'on appelle la blockchain ».

L'ordonnance du 28 avril 2016 a reconnu pour la première fois une valeur légale à la blockchain. Cette ordonnance permet son utilisation pour le commerce des minibons (titres de reconnaissance de dettes), certes limité, mais qui pourrait se développer rapidement. Ce texte permet la création de prêts aux PME via des plateformes de financement participatif utilisant la blockchain. Ces minibons représentent une innovation importante puisqu'ils assurent une meilleure sécurité et davantage de transparence, notamment dans les campagnes de *crowdfunding*, tout en réduisant les coûts pour l'émetteur.

Ordonnance n°2016-520 du 28 avril 2016 relative aux bons de caisse

« Art. L. 223-12 du Code monétaire et financier : Sans préjudice des dispositions de l'article L. 223-4, l'émission et la cession de minibons peuvent également être inscrites dans un dispositif d'enregistrement électronique partagé permettant l'authentification de ces opérations, dans des conditions, notamment de sécurité, définies par décret en Conseil d'État. »

Le décret n°2016-1453 du 28 octobre 2016 relatif aux titres et aux prêts proposés dans le cadre du financement participatif, pris en application de cette ordonnance, a notamment augmenté les plafonds applicables aux minibons^{xc}.

Le gouvernement français veut ainsi favoriser l'émergence de start-up en se montrant proactif sur la réglementation liée à la blockchain et servir de modèle aux autres pays d'Europe, l'Union européenne n'ayant pas encore légiféré sur le sujet.

Par ailleurs « On doit faciliter ce qu'il peut l'être, stimuler l'innovation, mais il ne faut pas mettre de freins à l'innovation tant que la technologie et ses usages ne sont pas matures. » (Lionel Tardy, député LR, 2016).

La loi Sapin 2 a suscité de nombreux amendements parlementaires pour soutenir la modernisation du paysage économique français. Quatre amendements rectificatifs (dont trois ont depuis été rejetés) ont été ajoutés pour compléter ce projet de loi pour tenir compte de l'arrivée de la technologie blockchain. L'État a souhaité, via ces amendements, la mise en place d'un système de transfert d'actions et d'obligations de sociétés non cotées grâce à « un dispositif d'enregistrement électronique partagé », soit un *Distributed Ledger*.

12. www.argusdelassurance.com/institutions/sapin-2-s-interesse-aussi-a-la-blockchain.108264



Loi du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique dite « Sapin 2 »

Art 120 : Dans les conditions prévues par l'article 38 de la Constitution, le gouvernement est autorisé à prendre par voie d'ordonnance, dans un délai de dix-huit mois à compter de la date de publication de la présente loi, les mesures relevant du domaine de la loi nécessaires pour :

1. adapter le droit applicable aux titres financiers et aux valeurs mobilières afin de permettre la représentation et la transmission au moyen d'un dispositif d'enregistrement électronique partagé des titres financiers qui ne sont pas admis aux opérations d'un dépositaire central ni livrés dans un système de règlement et de livraison d'instruments financiers ;
2. aménager et modifier toutes dispositions de nature législative favorisant la mise en œuvre et tirant les conséquences des modifications apportées en application de l'alinéa précédent. Un projet de loi de ratification est déposé devant le Parlement dans un délai de six mois à compter de la publication de l'ordonnance.

En juillet 2016, la Banque de France a annoncé avoir lancé une expérimentation de la blockchain en collaboration avec la Caisse des Dépôts, plusieurs groupes bancaires français et la start-up Blockchain Partner.

Cette expérimentation vise à automatiser et à décentraliser l'attribution des Identifiants créanciers SEPA (ICS). Actuellement, la Banque de France gère toute l'infrastructure et la gestion de ces identifiants. L'utilisation d'un registre distribué (une blockchain) permettrait à la Banque de France de ne plus être l'organe central garant de l'attribution de ces identifiants SEPA. Cette application a été construite sur une blockchain de type Ethereum privée, de sorte que seules les banques autorisées peuvent avoir accès, valider et modifier la base de données. Cette initiative illustre à nouveau la volonté des institutions publiques françaises de ne pas rester spectatrices de la révolution blockchain si celle-ci devait avoir lieu.

Encart 10 : Les apports de la blockchain pour le régulateur

Nicolas Julia, directeur du développement stratégique de Stratumn

Les technologies blockchain et leurs principales implémentations publiques (Bitcoin puis Ethereum) ont d'abord été abordées avec un regard prudent par le régulateur. Bitcoin, la première application de cette technologie apparue en 2008, soulève en effet de nombreuses questions autour de son statut juridique : est-ce un titre financier, une monnaie, etc. ?

L'apparition d'Ethereum en 2015 a soulevé un flot d'autres questions : quel statut juridique pour une inscription sur une blockchain, quelle opposabilité pour les faits juridiques afférents tels que les transmissions d'actifs ?

Il faudra apporter des réponses à ces questions dès lors que les premiers usages développés grâce à Bitcoin et Ethereum auront été validés à grande échelle et que la technologie avancera vers un niveau de maturité plus élevé, ces technologies étant encore relativement naissantes.

À l'instar d'Internet qui est resté dérégulé lors des premières années de son existence, il est souhaitable qu'il en soit de même pour les technologies blockchain. Le régulateur a besoin d'une compréhension fine des usages pour pouvoir établir un cadre clair et pertinent. Ces usages sont en cours de développement et durant cette période, il est souhaitable que le régulateur se contente de réguler les « frontières » de la blockchain, comme les plateformes d'échanges de crypto-monnaies. Des exigences réglementaires existent d'ailleurs déjà dans les domaines de la conformité client ou de la lutte anti-blanchiment.

Le législateur est également confronté à une technologie dont la philosophie même s'oppose au rôle du régulateur. Une action non coordonnée et précipitée ne pourrait que desservir le développement de la technologie et de son écosystème.



Loin d'être un fardeau complexe à appréhender et à réguler, les technologies blockchain pourraient aussi permettre au régulateur de réinventer ses missions et les moyens mis en œuvre pour les exercer. Il s'agit pour cela de se pencher sur les apports clés de la technologie : sécurité, possibilité d'être audité, traçabilité, transparence et confidentialité.

Au travers d'implémentations de blockchains privées, le régulateur peut en effet avoir accès à un réseau avec des « lunettes spéciales ». Il aurait ainsi accès en temps réel à un certain niveau d'information, le tout en préservant la vie privée des utilisateurs finaux et en garantissant un niveau de confidentialité sans égal à des acteurs ayant des intérêts divergents.

Pour ce faire, point besoin de longues heures d'évangélisation, de formation ou d'investissements lourds en termes d'infrastructure. La législation existe déjà, la technologie est prête et majoritairement *open source*.

Il s'agit dans un premier temps de s'impliquer concrètement en opérant un « nœud » au sein d'un consortium d'acteurs, dans le cadre d'un projet pilote au périmètre limité. Les bénéfices d'une « conformité en temps réel » sont visibles et mesurables aisément. Ils laissent entrevoir des promesses inégalées en termes de transparence et de traçabilité des transactions dans les écosystèmes financiers.

Après des années d'innovations sur les couches technologiques applicatives, la mutation profonde du système financier pourrait venir de l'infrastructure technologique, accompagnée de la volonté d'un régulateur de voir plus vite et plus précisément l'émergence de risques systémiques.

6.3. Un retour sur investissement encore lointain

D'après une étude réalisée par IBM en septembre 2016¹³, auprès de 200 banques et 200 institutions des marchés financiers, 52 % des banques et 57 % des institutions considèrent le manque d'un *return on investment* (ROI) clair comme une barrière à la mise en œuvre de la blockchain.

Cette question se pose également pour les fonds de capital investissement dont l'horizon de sortie du capital des start-up blockchain dans lesquelles ils ont investi pourrait être plus lointain qu'anticipé.

La maturation de la technologie blockchain et le développement de ses cas d'usage dans les années à venir devraient cependant convaincre les décideurs, au minimum, de l'opportunité d'étudier l'impact de la blockchain sur leurs activités.

Mais la révolution blockchain va continuer à produire des déconvenues. Elles sont par construction difficiles à anticiper, mais peuvent avoir trait à la valeur des monnaies digitales ou à la priorité au développement de cas d'usage ciblant la remise en question de registres centralisés existants (parce que plus évidents mais pouvant aussi générer plus de résistance) au détriment de cas d'usage moins immédiats mais prometteurs dans des champs où il n'existe pas de registres centralisés (facturation, dossiers médicaux, etc.).

Bloc 6 : que retenir ?

- **Pour arriver à des résultats probants, les entreprises doivent apprendre à travailler de manière coopérative et à entrer dans une logique de « coopération » via des consortiums, partenariats avec des start-up ou fin techs.**
- **Les organisations pourront avantageusement combiner des blockchains publiques ouvertes à tous et des blockchains privées limitées à un nombre restreint et contrôlé de nœuds et d'utilisateurs.**
- **Le législateur joue un rôle clé dans l'adoption de la blockchain.**
- **L'absence de ROI clair sur la blockchain peut générer des déconvenues et freiner son adoption, mais les expérimentations devraient se multiplier dans les années à venir.**

13. www-03.ibm.com/press/us/en/pressrelease/50617.wss



7. Trois principes d'actions pour anticiper

Il suffira d'une seule *killer app* pour enclencher une adoption massive de la blockchain, trancher les débats technologiques encore ouverts et diffuser la technologie à une multitude de services et applications. Tout ce que nous savons à ce stade, c'est que le bitcoin n'est pas cette *killer app*.

Inversement, un hacker pourrait trouver une faille de sécurité impossible à sécuriser, et qui serait rédhibitoire pour le régulateur. Les problèmes de flexibilité évoqués précédemment pourraient s'avérer impossibles à résoudre, empêchant l'essor de la blockchain.

Un scénario intermédiaire pourrait impliquer que certaines applications profitent de la vague d'innovation actuelle mais sans atteindre la révolution attendue et le succès du PC ou d'Internet.

Un constat prosaïque s'impose : personne ne sait aujourd'hui ce qu'il va se passer.

Comme avec toute technologie sujette à des effets de réseaux et à des rendements croissants à ses débuts, l'équilibre du *business model* lié à la blockchain demeure instable.

De nombreux cas d'usage de la blockchain existent, comme illustré *supra*. L'innovation peut donc venir de partout. Pour anticiper la révolution blockchain, et face aux incertitudes concernant cette technologie, trois principes d'actions ressortent pour aider les décideurs à être prêts en cas d'innovation majeure : connaître précisément son environnement, garder toutes ses options ouvertes et ne pas hésiter à mener des expérimentations.

Il est intéressant de constater que d'autres innovations lourdes comme les objets connectés, l'intelligence artificielle ou la *Robotic Process Automation* peuvent s'analyser de la même façon. En effet, ces dernières partagent une caractéristique de la technologie blockchain : une évolution selon des cycles très courts. Le paysage technologique d'aujourd'hui est fondamentalement différent de ce qu'il était il y a encore douze mois.

7.1. Connaître précisément son environnement

Chaque organisation doit connaître intimement son environnement : les technologies disponibles, les concurrents, les alliances possibles, les start-up innovantes, etc. pour être capable de cerner d'où l'innovation pourrait venir. Des protocoles de blockchains publiques pourraient annihiler les progrès réalisés par un consortium sur une blockchain privée. Certaines initiatives sponsorisées par des gouvernements de l'autre côté de la planète pourraient engendrer la création de la fameuse *killer app*. Des avancées dans les méthodes de cryptage et de décryptage pourraient apporter des solutions aux questions de sécurité. Un développement dans une industrie parallèle pourrait avoir un impact sur la technologie blockchain. Les managers doivent rester dans un processus d'apprentissage continu pour faire face à tous ces types d'événements.

7.2. Garder toutes ses options ouvertes

En stratégie comme en finance, plus le futur est incertain, plus il y a valeur à avoir des options diverses. Il y a toujours un risque à parier sur la mauvaise option, c'est pourquoi il peut être intéressant d'investir dans un portefeuille varié. Inversement, écarter d'emblée une option qui s'avèrerait *in fine* être l'option gagnante générerait un retard par rapport à la concurrence qu'il serait difficile de rattraper. Rejoindre un consortium ou une alliance industrielle peut aussi être une opportunité de participer aux premières phases d'un projet et de définir les priorités du groupe pour le développement.

7.3. Expérimenter encore et encore

Au risque de se répéter, il faut expérimenter, pratiquer, tester, s'exercer. Il est essentiel d'appliquer les principes agiles et de tester des applications blockchain au sein des entreprises. Les expérimentations sont importantes car elles permettent de décider d'une stratégie éventuelle et améliorent la capacité de réaction et la confiance des acteurs.

Ces expérimentations peuvent prendre la forme de prototypes et de *proof of concepts*, mais l'organisation d'ateliers d'idéation de hackathons, ces sessions de brainstorming et de programmation informatique collaboratives – peut également être un outil stimulant la création.



La start-up Blockchain Partner a organisé le Blockfest 1.0 en juin 2016. Cet hackathon de quatre jours avait pour objectif de décrypter la technologie blockchain, de développer des prototypes et d'en imaginer la diffusion. Ethereum France a également organisé un hackathon porté sur la création d'applications décentralisées (*decentralized Application*, dApp) sur la blockchain Ethereum.

Du côté de l'enseignement, l'École des technologies numériques appliquées (ETNA) a organisé en février 2017, un Master Code Camp d'une semaine pour se plonger dans la blockchain Ethereum. L'école supérieure Léonard de Vinci (ESILV) est quant à elle assez active dans la formation et l'éducation sur la blockchain. Elle est d'ailleurs la première école à certifier ses diplômés sur la blockchain.

Les entreprises proposent également des hackathons liés à la blockchain. Microsoft a organisé la Blockchain Hackademy, un événement pour encourager le développement d'applications blockchain. BNP Paribas a aussi organisé un hackathon blockchain avec un objectif de familiarisation pour ses employés et ses clients.



Dans le cadre de ces expérimentations, un BizHackathon centré sur l'idéation de cas d'usage de la blockchain a été organisé à l'initiative du MEDEF en collaboration avec BeMyApp, Blockchain Partner, le Boston Consulting Group, le CIGREF, emlyon business school et Platinion. Cet événement de deux jours alternait des sessions d'acculturation des candidats, des présentations de start-up et des séances d'idéation en groupe. L'objectif de ce hackathon était de montrer qu'il est possible d'amener des dirigeants d'entreprises, n'étant pas nécessairement experts sur le sujet, à imaginer des services innovants basés sur la blockchain.

La centaine de participants – représentants du monde de l'entreprise, start-uper, étudiants et indépendants – a été répartie en vingt groupes autour des cinq thématiques de l'événement (identité et authentification, mobilité, traçabilité, objets connectés et contrats) en panachant profils et niveaux de connaissance de la blockchain.

Chaque groupe devait identifier et développer, autour de l'une de ces cinq thématiques, un cas d'usage inédit et prometteur utilisant la blockchain, avec une esquisse de business plan. Ces projets ont été évalués à l'aune de leur faisabilité, de leur caractère innovant, de leur potentiel business et de l'expérience utilisateur attendue.

Trois projets ont ainsi été distingués par le jury constitué par les partenaires de l'événement.

Projet « EatOnTime »

Cette équipe est partie de l'expérience que tout un chacun a vécu de la pizza qui arrive froide car livrée en retard. Il n'y a actuellement pas de réglementation imposant le versement d'une compensation lorsqu'un repas est livré avec des délais plus importants qu'annoncés, sauf si le client le demande directement. Les réclamations sont ainsi gérées au cas par cas avec un coût élevé pour les restaurateurs. L'idée du projet EatOnTime est d'automatiser le processus de compensation grâce à une blockchain de consortium dont les contributeurs sont les acteurs de la *food delivery* (restaurateurs, sites de commande en ligne, livreurs, etc.). Cette blockchain utilise un *smart contract* pour chaque commande, à laquelle un délai de livraison est associé. Lorsqu'une pizza est commandée, le montant de la commande est déposé dans un compte séquestre. Puis, une fois la pizza livrée, le client doit flasher un QR code, ce qui permet de certifier que la commande a bien été livrée à temps. Cela déclenche automatiquement les clauses du *smart contract* : en cas de livraison à l'heure, le montant séquestré est versé au restaurateur ; en cas de retard, une compensation de 2 € est restituée au client. Ce projet d'application a pour conséquences de renforcer la confiance tout en responsabilisant les acteurs de la chaîne de livraison de repas.



Projet « Kill Bill »

Ce projet ambitionne de rendre les factures papier caduques. Il part du constat que le système actuel de gestion des factures génère de la fraude à l'assurance, du recel de biens mal acquis et des garanties non exécutées dans le cas d'une panne sur un appareil électronique. La promesse de « Kill Bill » est de fournir un accès à un référentiel unique de factures certifiées authentiques sur une blockchain. Par exemple, lors de l'achat d'un téléviseur, acheteur et vendeur valident la création de la facture dont une copie est déposée dans la blockchain. Assureurs, constructeurs et distributeurs ont alors accès à ce registre contenant des factures certifiées et horodatées et peuvent procéder au versement d'indemnités en cas de vol ou de défaillance de l'appareil. Dans le cas d'une vente entre particuliers, le vendeur peut se prévaloir de la facture présente dans la blockchain comme preuve d'achat. Ce projet d'application a pour conséquences de décharger assureurs et distributeurs de leur fonction d'archivage et de sécuriser les relations au sein de l'écosystème de la consommation.

Projet « HomeNesty »

Cette équipe est partie du constat qu'il est aujourd'hui souvent difficile lorsque l'on acquiert un logement de savoir quels travaux y ont été réalisés et à quelles dates ils ont été faits. Ceci est également vrai pour les travaux des parties communes dans le cas d'un immeuble en copropriété. La loi ALUR de 2014 crée d'ailleurs l'obligation de disposer d'un carnet d'entretien à compter de 2019 pour les constructions neuves. Cette obligation sera étendue en 2025 aux copropriétés existantes. L'idée de HomeNesty est d'utiliser une blockchain comme support du carnet d'entretien. Les travaux, en parties privatives ou en parties communes, donnent lieu à l'édition d'une facture dont une copie est déposée dans la blockchain. Cela permet d'assurer pérennité, inaltérabilité et traçabilité des rénovations effectuées et donc de sécuriser les ventes immobilières. Les acteurs de la rénovation des logements – collectivités, syndicats, artisans et propriétaires – sont également en mesure de piloter plus efficacement les programmes de rénovation à l'aune de l'historique des travaux réalisés.

Encart 11 : Anticiper la blockchain

Claire Balva, présidente de Blockchain Partner

La blockchain est une technologie en pleine évolution, et ses effets ne seront pleinement connus que lorsque ses usages se seront stabilisés autour des cas métiers et des secteurs où elle apporte une véritable valeur ajoutée. Comme toutes les innovations dites « de disruption », il est très difficile de savoir où se trouveront les nouveaux marchés et les nouveaux gisements de valeur dans cinq ou dix ans. Qui, en 1998, aurait pu prédire Facebook ou Airbnb ?

Pourtant l'enjeu d'anticipation est crucial pour les entreprises. En effet, cette technologie menace à terme de reconfigurer les marchés existants, en redistribuant la chaîne de valeur vers de nouveaux entrants, de la même façon que l'industrie musicale a vu grâce au numérique des acteurs comme Deezer ou Spotify bouleverser les marchés existants.

Les deux questions de l'entreprise qui anticipe la blockchain doivent donc être : (1) mes positions établies sont-elles attaquables à terme par un acteur qui ferait usage de la blockchain ? et (2) suis-je en mesure à l'aide de la blockchain de m'approprier de nouveaux segments de valeur ?

De plus, dans cette technologie, la prime ne sera pas nécessairement au premier entrant ; la règle qui comptera sera celle du *winner takes it all*. L'entreprise qui agira au bon moment avec le bon produit imposera le standard du métier ou du secteur et accapara la majorité de la valeur. L'entreprise doit donc à la fois se poser ces deux questions, mais aussi se donner les moyens, lorsqu'une réponse claire émerge, d'agir.

À ce stade, la construction d'un avantage compétitif en matière de blockchain ne passe donc pas par le déploiement de telle ou telle solution, mais par la mise en place méthodique d'une culture blockchain. C'est cette culture qui, au travers notamment d'une veille, de la prospection et des expérimentations pertinentes, permettra à l'organisation de se déployer stratégiquement sur la blockchain lorsque les circonstances le demanderont. Ne pas investir, ou mal le faire, c'est se condamner à subir une vague d'innovations qui s'annonce riche en bouleversements.





Encart 12 : Penser les ruptures

Thomas Gauthier, professeur de stratégie à emlyon business school

Comme beaucoup le pensent, nous avons basculé dans une ère marquée par la complexité, laquelle est indissociable des multiples ruptures qui caractérisent le monde contemporain.

Le mot « rupture » échappe encore aujourd'hui aux nombreuses tentatives qui se sont succédé pour s'approcher d'une définition satisfaisante et capable de résister à l'épreuve du temps. Au mieux, on convoque d'autres mots tels que « crise », « surprise », ou encore « révolution », pour saisir à chaque fois partiellement le sens de « rupture ».

Tous ces efforts sont voués à l'échec, au moins partiel. En occultant la complexité de la rupture, ils nient le principe d'émergence, largement décrit par Edgar Morin et d'autres, selon lequel la rupture, éminemment complexe, est un tout qui est plus que la somme des parties qui la composent.

Pour penser les ruptures et agir dans la complexité, il est désormais essentiel d'apprendre à utiliser l'intelligence collective rendue possible par les innombrables interactions entre individus reliés entre eux grâce aux technologies de l'information et de la communication.

Dès aujourd'hui, plusieurs prototypes d'intelligence collective permettent à des communautés, qu'elles soient locales ou globales, d'explorer la réalité et la possibilité de ruptures dans de nombreux domaines.

Aux États-Unis, le Massachusetts Institute of Technology s'est doté depuis plusieurs années déjà d'un Center for Collective Intelligence, véritable lieu de réflexion et d'action où chercheurs et acteurs de terrain co-construisent ensemble des dispositifs collectifs et prospectifs pour affronter les enjeux planétaires tels que le réchauffement climatique.

Plus proche de nous, emlyon business school a initié cette année, en partenariat avec l'armée suisse, un ambitieux projet pilote dans lequel 1 000 étudiants, à la fois apprenants et *early makers*, vont explorer et éclairer le potentiel disruptif de l'Internet des objets. Seuls, puis ensemble, ils vont explorer les futurs possibles de l'Internet des objets en élaborant d'abord chacun un micro-scénario prospectif puis en débattant et en enrichissant la macro-histoire de l'avenir créée en assemblant leurs contributions individuelles.

Pour finir, l'intelligence collective permettra-t-elle à l'humanité de progresser dans l'ère de la complexité et de relever ses immenses défis ? Vers quel nouvel équilibre les interactions entre hommes et machines convergeront-elles ? Est-il à craindre l'avènement d'une ère « transhumaniste » ? Est-il au contraire à espérer une ère « hyperhumaniste » qu'il nous reviendrait alors de définir et de construire ?

Bloc 7 : que retenir ?

- Une connaissance précise de son environnement et de l'écosystème évolutif de la blockchain est essentielle pour espérer détecter très tôt les innovations de rupture qui se préparent.
- Tant que la technologie n'est pas mature, les décideurs se doivent de garder toutes leurs options ouvertes.
- C'est en minant/forgeant que l'on devient mineur/forgeron ; il est donc essentiel de mener des expérimentations.



8. Conclusion

Au-delà de sa médiatisation sulfureuse et de ses limites techniques, légales ou conceptuelles, le bitcoin aura eu le mérite de faire émerger la technologie blockchain sur laquelle il s'est construit.

Les avantages de la blockchain peuvent être résumés par les cinq caractéristiques suivantes :

- la blockchain rend possible la désintermédiation et donc l'échange direct entre utilisateurs sans intermédiaire de confiance (régulateur ou autorité centrale) grâce à l'utilisation d'une technologie algorithmique basée sur de la cryptographie de haut niveau qui instaure cette confiance ;
- elle fonctionne grâce à un mécanisme de consensus décentralisé avec un registre distribué et répliqué sur tous les nœuds du réseau ainsi qu'une vérification réalisée par une communauté d'utilisateurs selon un principe majoritaire ;
- elle assure la traçabilité via l'inscription horodatée de toutes les transactions sur un registre distribué consultable par tous ;
- elle est transparente et on peut pratiquer un audit du fait de la possibilité de remonter l'ensemble de la chaîne et de retrouver l'historique des transactions ;
- elle garantit l'inaltérabilité et l'inviolabilité des informations car les blocs de transactions sont gravés de façon définitive et ne peuvent être modifiés.

La blockchain connaît toutefois un certain nombre de limites, en particulier techniques, qui restent des obstacles majeurs à son industrialisation et à sa généralisation. Elle doit donc gagner en maturité avant de pouvoir se déployer à grande échelle, et reste en attente de la *killer app* qui aura le même effet que le navigateur pour Internet.

Ce temps de maturation long est une caractéristique essentielle de ce que nous appelons *deep tech*¹⁴, c'est-à-dire les innovations de rupture fondées sur des avancées scientifiques difficiles à reproduire et qui repoussent les frontières technologiques, comme l'impression 3D ou l'intelligence artificielle. Les *deep techs*, dont les start-up sont un acteur central, ont des ressorts fondamentalement différents des innovations digitales, focalisées sur l'expérience client : besoins en financement significatifs, intensité capitalistique largement supérieure aux start-up issues du monde digital, mais aussi délais longs (et sous-estimés) de mise sur le marché des innovations.

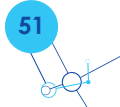
Pour répondre à ces défis, ces start-up ont des attentes vis-à-vis de l'écosystème d'innovation qui vont bien au-delà de l'enjeu du financement : elles ont besoin d'être accompagnées dans la définition des applications industrielles et commerciales de leurs innovations.

Les *corporates* sont les seuls à pouvoir y répondre dans leur intégralité grâce à leurs expertises techniques, industrielles, et commerciales (infrastructures de tests, données clients, etc.) mais surtout grâce à un accès au marché. Ils représentent donc des partenaires particulièrement attractifs. Pourtant, si la quasi-totalité des start-up *deep tech* appellent de leurs vœux un partenariat de long terme avec des entreprises pour les accompagner dans leur développement, près de la moitié estiment avoir échoué dans cette voie.

Les grands groupes doivent donc revoir leur façon d'envisager les partenariats avec les start-up dans des champs comme celui de la blockchain *deep tech* s'ils veulent se placer au cœur de cette révolution technologique.

La France a tous les atouts pour devenir un acteur incontournable de la révolution blockchain : les compétences scientifiques et universitaires, une prise de conscience réelle des enjeux de la blockchain ainsi qu'un écosystème en plein foisonnement composé de start-up, d'académiques et de *corporates*. Pour transformer l'essai, la collaboration doit être renforcée entre ces acteurs. Cela passe entre autres par le développement du *corporate venture* afin d'accompagner l'écosystème sur le temps long et par l'expérimentation. C'est sans doute sur cette dimension que la France accuse encore un retard par rapport aux grands écosystèmes d'innovation qui font aujourd'hui la course en tête.

14. From Tech To Deep Tech – Fostering Collaboration between corporates and startups, BCG & Hello Tomorrow, Avril 2017



9. Remerciements

Ce livre blanc a été rédigé par **Lionel Aré, Nicolas Harlé, Rodolphe Chevalier** et **Amine Benayad** du BCG dans le cadre d'un partenariat avec le MEDEF associant également **BeMyApp**, le **CIGREF** et **emlyon business school**.

Les auteurs tiennent à remercier en premier lieu **Christian Poyau**, président de la Commission Transformation numérique du MEDEF, ainsi que les membres du groupe de travail blockchain du MEDEF pour leur contribution décisive à ce rapport.

Les remerciements des auteurs vont également à **Guervan Adnet** et **Hadrien Cimino** (BCG) dont les analyses ont rendu possible ce travail ainsi qu'à **Norbert Faure, Régis Martin** (Platinion) et **Franck Vialaron** (Expand) pour leur implication.

Les auteurs tiennent également à remercier les contributeurs du BizHackathon blockchain des 7 et 8 juin 2017 :

Norbert Faure (Platinion), **Christian Poyau** (MEDEF), **John Karp** (BeMyApp), **Patrick Laurens-Frings** (CIGREF), **Françoise Dany** (emlyon business school), **Claire Balva** (Blockchain Partner) et **Baptiste Fèvre** (Hello Tomorrow) pour leur participation au jury.

François Stephan (IRT System X), **Pierre Noizat** (Paymium), **Pierre Paperon** (Observatoire blockchains), **Nicolas Julia** (Stratumn), **Alexandre David** (Eureka), **Nicolas Rivard** (Euronext), **Nadia Filali** (CDC) et **Thomas Gauthier** (emlyon business school) pour leurs interventions.

Gonzague Grandval (Paymium), **Cyprien Veyrat** (Keeex), **Thomas Zoughebi** (Eureka), **Laurent Friscour** (Postme.io), **Olivier Male** (Generali), **Adrien Lafuma** (Blockchain Partner), **Antoine Yeretian** (Blockchain Partner), **Hicham Skareb**, **Romain Sohet**, **Franck Vialaron** (Expand), **Pierre Gérard** (Scorechain), **Pierre d'Agrain** (EXCO), **Christelle Wozniak** (SNCF) et **Antoine Auriol** (Platinion) pour leur rôle de mentor.

Guillaume Adam (FIEEC), **Jean-Paul Amoros** (Engie), **Laurent Benichou** (AXA), **Jean-Michel Brun** (Schneider Electric), **Henri d'Agrain** (CIGREF), **Maxence Demerlé** (SFIB), **Philippe Denis** (BNP Paribas), **Julie Guillot** (emlyon business school), **Anne-Florence Fagès** (MEDEF), **Pauline Fiquémont** (MEDEF), **Erick Jonquière** (AFNet), **Jihane Khouzaimi** (Fédération Française de l'Assurance), **Ingrid Marquez** (MEDEF), **Corinne Murcia Giudicelli** (SURYS Group), **Marc Pic** (SURYS Group), **Alain Roset** (Docapost), **Romain Sohet** (Société Sohet), **Alexandre Teulade** (BeMyApp) pour leurs avis éclairés dans l'organisation de l'évènement.

Enfin nous remercions chaleureusement **emlyon business school** et son directeur général, **Bernard Bellefante**, pour avoir accepté d'accueillir cet événement.

10. Glossaire

- **Altcoin** : une « alternative coin » est une crypto-monnaie différente du bitcoin
- **Bitcoin** (BTC) : le bitcoin est une monnaie cryptographique qui fonctionne de manière décentralisée grâce à la blockchain. Cette monnaie a été créée par Satoshi Nakamoto en 2009. Le bitcoin est un moyen de paiement pair-à-pair et n'a donc pas besoin d'intermédiaires pour réguler les transactions puisque les nœuds de la blockchain remplissent ce rôle. Le Bitcoin (avec un B majuscule) désigne le protocole.
- **Bloc** : composant principal de la blockchain, un bloc est un regroupement de plusieurs transactions effectuées par les utilisateurs du réseau. Dans le cas de Bitcoin, la création d'un nouveau bloc est faite par les mineurs qui résolvent des calculs compliqués et vérifient les transactions du bloc. Sur la blockchain Bitcoin, un nouveau bloc est créé toutes les dix minutes. La blockchain Ethereum a un temps de validation plus court.
- **Blockchain** : registre public et inviolable, la blockchain est une suite de blocs qui fonctionne sans autorité centrale grâce aux utilisateurs du système. Cette technologie décentralisée permet le stockage et la diffusion d'informations de manière sécurisée et bon marché. Dans le cas d'une blockchain publique, chacun est libre de consulter la blockchain et d'en vérifier les transactions. On peut définir



une blockchain publique comme un registre comptable public, anonyme et inviolable. Inversement, une blockchain privée sera restreinte à un certain nombre d'acteurs.

- **Chiffrement** : procédé cryptographique qui permet de rendre impossible la compréhension d'un message ou d'un document aux personnes qui ne possèdent pas la clé pour le déchiffrer.
- **Clé privée** : la clé privée n'est jamais transmise à un tiers et est utilisée pour signer cryptographiquement son message.
- **Clé publique** : la clé publique est accessible à tout le monde et sert d'adresse sur la blockchain.
- **Cryptographie asymétrique** : chiffrement à clé publique et privée. L'expéditeur du message utilise la clé publique du destinataire pour chiffrer le contenu qui sera déchiffré par le destinataire avec sa clé privée de sorte que seul ce dernier puisse lire le message. Pour assurer l'authenticité de l'expéditeur, l'auteur du message utilise sa clé privée pour coder un message que le destinataire décode avec la clé publique de l'expéditeur. Ce deuxième mécanisme est utilisé par la signature numérique.
- **Crypto-monnaie** : monnaie électronique qui utilise la cryptographie pour valider les transactions entre les acteurs du réseau.
- **Ether (ETH)** : crypto monnaie utilisant la blockchain Ethereum.
- **Ethereum** : plateforme décentralisée qui utilise la blockchain pour permettre la création de *smart contracts*. La monnaie utilisée pour cette blockchain est l'ether. Contrairement à Bitcoin, Ethereum ne se focalise pas sur le seul aspect monétaire et vise à accueillir des applications variées.
- **Jeton** : toutes les blockchains publiques fonctionnent avec un *token* (jeton) qui est programmable. Ce jeton est le véhicule de l'information. Le jeton bitcoin est un exemple de monnaie programmable. Le jeton peut être l'actif lui-même (le bitcoin par exemple) ou une représentation virtuelle de l'actif (dans le cas d'un échange d'électricité par exemple).
- **Micro-transaction** : transaction d'un montant de quelques centimes qui ne vaudrait pas la peine d'être effectuée via le système bancaire actuel car les frais de transactions seraient plus élevés que le montant à transférer.
- **Minage** : utilisation de la puissance de calcul d'un ordinateur de minage pour vérifier la cohérence des transactions vis-à-vis de règles préétablies dans le logiciel et pour valider les nouveaux blocs ajoutés à la blockchain.
- **Mineur** : individu qui connecte au réseau une ou plusieurs machines de minage (pools de minage). Les mineurs sont rémunérés en fonction de la puissance de calcul qu'ils mettent à disposition du réseau. Dans le cas de la blockchain Bitcoin, les mineurs sont rémunérés en bitcoins.
- **Noeud** : ordinateur relié au réseau qui participe à la transmission et à la vérification des transactions.
- **Peer to peer (P2P)** : réseau décentralisé de pair-à-pair faisant intervenir les individus directement entre eux. Les utilisateurs du réseau interagissent sans intermédiaire de confiance.
- **PoC** : *proof of concept*, ou preuve de faisabilité, est l'expérimentation d'une idée ou d'un projet afin d'en démontrer la faisabilité.
- **Pool de minage** : regroupement de plusieurs appareils de minage qui permet aux mineurs d'unir leurs forces et d'augmenter leur chance de gain de la récompense offerte pour la création de nouveaux blocs. Dans une chaîne basée sur la preuve de travail, il faut faire attention à ce qu'aucun pool de minage n'atteigne un pourcentage trop important de la puissance de calcul de tout le réseau. Si tel est le cas, le pool de minage a de bonnes chances d'être en mesure de réécrire et de valider la blockchain à sa guise.



- **Portefeuille** (*wallet*) : application qui stocke les bitcoins (ou autre monnaie digitale) que vous possédez en ligne et qui est accessible uniquement à l'aide de la clé privée de l'utilisateur. Il existe des portefeuilles virtuels (*software*) mais également physiques (Ledger wallet par exemple).
- **Proof of stake** (preuve de participation) : procédé alternatif à la preuve de travail (*proof of work*) selon lequel les mineurs devront prouver qu'ils possèdent une certaine quantité de crypto-monnaie pour pouvoir valider des nouveaux blocs dans la blockchain et prétendre à la récompense. Si on possède 1 million de bitcoin sur les 10 millions existants, on a 10 % de chances de valider la transaction. Si on valide une transaction, on ne peut pas participer aux prochaines validations pendant un certain temps pour éviter la concentration du pouvoir au sein du réseau.
- **Proof of work** (preuve de travail) : les utilisateurs doivent exécuter et résoudre des calculs, des algorithmes et des puzzles mathématiques pour valider les transactions électroniques dans la blockchain. La difficulté de ce travail varie pour garder un temps de validation constant (10 minutes sur la blockchain Bitcoin).
- **Satoshi Nakamoto** : pseudonyme de l'inventeur du bitcoin et de l'auteur du papier inaugural disponible en ligne. La véritable identité de Satoshi Nakamoto est inconnue à ce jour. Il a donné son nom à une sous-unité de valeur du bitcoin, le satoshi, qui vaut 0,00000001 bitcoins.
- **Sidechain** : blockchain secondaire qui opère en parallèle de la blockchain principale mais qui y est attachée pour en conserver la sécurité. Ces *sidechains* permettent de décharger la blockchain principale et d'augmenter le volume d'information en circulation (normalement limité).
- **Signature cryptographique** : permet aux utilisateurs de prouver leur propriété d'un portefeuille bitcoin. Cette signature est unique pour chaque utilisateur et empêche que quiconque d'autre que le propriétaire du portefeuille ne puisse dépenser les fonds. Cette signature est visible par le réseau Bitcoin et permet donc plus de transparence dans les transactions.
- **Silk Road** : marché noir en ligne utilisé pour effectuer des achats illicites (armes, etc.) avec des crypto-monnaies comme le bitcoin. La plateforme a été saisie et démantelée par le FBI en octobre 2013. Le créateur de Silk Road, Ross Ulbricht, a également été arrêté.
- **Smart contract** : contrats intelligents autonomes qui sont exécutés automatiquement par la blockchain sans intervention humaine une fois que les conditions nécessaires à leur réalisation sont réunies. Par exemple, un smart contrat ouvrira la serrure d'un appartement loué une fois que le montant dû aura été versé par le locataire.

11. Références

Evans, P. (2016). BCG Perspective – Thinking Outside the Blocks
www.bcg.com/blockchain/thinking-outside-the-blocks.html

Bitcoin Block Explorer - Blockchain. (2017). Blockchain.info.
<https://blockchain.info/>

Blockchain Partner. (2016). Des cadastres sur la blockchain. Blockchain France.
<https://blockchainfrance.net/2016/03/03/des-cadastres-sur-la-blockchain/>

Deloitte US, (2016). Innovation: Blockchain Survey | Deloitte US. Deloitte United States.
www2.deloitte.com/us/en/pages/about-deloitte/articles/innovation-blockchain-survey.html

Drif, A. (2016). Blockchain : les défections se multiplient au sein du consortium R3. lesechos.fr.
www.lesechos.fr/27/11/2016/lesechos.fr/0211533384718_blockchain---les-defections-se-multiplient-au-sein-du-consortium-r3.htm

En quelle année sera atteint le nombre maximal de bitcoins en circulation ? (2017). bitcoin.fr.



<https://bitcoin.fr/en-quelle-annee-atteindrons-nous-le-nombre-maximal-de-bitcoins-en-circulation/>

Fredouelle, A. (2016). Comment l'Estonie booste son économie grâce à la blockchain. Journaldunet.com.
www.journaldunet.com/economie/finance/1176465-estonie-blockchain/

IBM, (2016). Blockchain Adoption Moving Rapidly in Banking and Financial Markets: Some 65 Percent of Surveyed Banks Expect to be in Production in Three Years.
www-03.ibm.com/press/us/en/pressrelease/50617.wss

Mougayar, W. (2016). The State of Global Blockchain Consortia. CoinDesk.
www.coindesk.com/state-global-blockchain-consortia/

Wong, I. (2017). Survey: Blockchain likely adopted in five years.
www.fundselectorasia.com/news/1034586/survey-blockchain-adopted

UK Government (2015). Distributed Ledger Technology : beyond block chain.
www.gov.uk/government/news/distributed-ledger-technology-beyond-block-chain

BCG & Hello Tomorrow (2017). From Tech To Deep Tech – Fostering Collaboration between corporates and startups.
www.bcg.com/publications/2017/technology-digital-joint-ventures-alliances-what-deep-tech-startups-corporate-partners.aspx?utm_source=201705Innovation&utm_medium=Email&utm_campaign=otr

12. À propos des partenaires

À propos du BCG

Le BCG est un cabinet international de conseil en management et un leader mondial du conseil en stratégie d'entreprise. Nous travaillons avec des clients de tous les secteurs partout dans le monde pour identifier ensemble les meilleures opportunités, les aider à affronter leurs défis et faire évoluer leurs activités. À travers une approche personnalisée, nous leur apportons notre vision de la dynamique des entreprises et des marchés ainsi que notre expertise à chaque niveau de leur organisation. Nous leur garantissons ainsi un avantage concurrentiel durable, des organisations plus performantes et des résultats pérennes. Fondé en 1963, le BCG est une entreprise privée présente dans 48 pays avec 85 bureaux.

Plus d'informations sur www.bcg.fr/

À propos du MEDEF

Le MEDEF est le premier réseau d'entrepreneurs de France. Plus de 95 % des entreprises adhérentes au MEDEF sont des PME. Le MEDEF met au cœur de son action la création d'emplois et la croissance durable. Il promeut l'entrepreneuriat et défend la libre entreprise. Il dialogue avec l'ensemble des acteurs de la société civile et œuvre auprès des différents décideurs en faveur d'une meilleure compréhension des contraintes et des atouts des entreprises.

Le MEDEF se mobilise pour le déploiement du numérique, notamment grâce à la commission Transformation numérique, autour de deux axes principaux :

- convaincre les entreprises des gains de productivité (et donc de compétitivité) induits par la numérisation des process et levier d'une montée en gamme des produits et services ;
- travailler sur la construction d'un contexte favorable à l'enracinement et au déploiement d'une filière numérique en France, ouverte sur un marché mondialisé.

Plus d'informations sur www.medef.com



À propos de BeMyApp

Créée en 2010, BeMyApp est une agence internationale spécialisée dans l'organisation d'événements transformationnels pour les grands groupes. Pionnière dans le domaine du Hackathon, BeMyApp est à l'origine du concept de hackathon pour les grandes entreprises et a à son actif plus de 700 hackathons organisés dans plus de 35 pays. Son leitmotiv : être un catalyseur de l'innovation en aidant les entreprises à lancer des produits rapidement. En France, BeMyApp accompagne la plupart des sociétés du CAC 40 sur leurs problématiques autour de la blockchain, de l'intelligence artificielle ou encore de l'IoT, c'est pourquoi elle s'est associée au MEDEF et au BCG pour organiser le BizHackathon Blockchain des 7 et 8 juin 2017.

Plus d'informations sur <http://agency.bemyapp.com>.

À propos de Blockchain Partner

Blockchain Partner est le leader français du conseil sur les technologies blockchain. La start-up, née de la fusion entre Blockchain France et Labo Blockchain, accompagne les organisations dans leurs démarches d'innovation sur les technologies blockchain. Elle compte parmi ses clients BNP Paribas, la MGEN, le groupe Aéroports de Paris ou encore GRT Gaz. Ses activités reposent sur un tripôle d'expertise – stratégiques, techniques et juridiques – permettant notamment d'identifier des cas d'usage blockchain adaptés à chaque organisation, de développer des applications techniques dans une logique d'expérimentation puis d'intégration système, et d'évaluer la mise en conformité légale des projets blockchain.

Plus d'informations sur <http://blockchainpartner.fr/>

À propos du CIGREF

Réseau de Grandes Entreprises, le CIGREF a été créé en 1970 et a pour mission de « développer la capacité des grandes entreprises à intégrer et maîtriser le numérique ». Il regroupe 143 grandes entreprises et organismes français de tous les secteurs d'activités (banque, assurance, énergie, distribution, industrie, services, ministères, etc.). Le CIGREF est présidé depuis octobre 2016 par Bernard Duverneuil (DSI Essilor International). Patrick Laurens-Frings (DSI groupe Caisse des Dépôts) pilote le groupe de travail « blockchain » du CIGREF.

Plus d'informations sur www.cigref.fr

À propos d'emlyon business school, l'école de la formation

Fondée en 1872, emlyon business school est l'une des plus anciennes écoles de commerce en Europe. Son objectif est aujourd'hui d'effacer la frontière entre école et entreprise pour connecter les savoirs, co-construire de nouveaux modes de collaboration et accompagner celles et ceux qui porteront la transformation des entreprises dans un monde global et digital.



Forts d'une expérience reconnue et riches de savoir-faire incontestables, les professionnels d'aujourd'hui sont néanmoins percutés de plein fouet par la concurrence internationale et l'arrivée du digital dans leur univers métier.

Les nouveaux *business models*, les nouvelles manières de coopérer, les nouveaux types de leadership... représentent autant de challenges à relever pour leur permettre de devenir les dirigeants de demain.

Il est nécessaire pour ces managers ou futurs managers de développer de nouveaux savoir-faire tout au long de leur vie. Ils doivent non seulement apprendre, mais aussi apprendre à désapprendre. Cette démarche est indispensable s'ils veulent se réinventer.

Emlyon business school leur propose ainsi de se construire un parcours de développement des compétences personnalisé, selon leurs besoins, selon leurs objectifs et à leur rythme, grâce à des formations modulaires et des méthodes pédagogiques innovantes.

Classée régulièrement dans le top 3 des écoles de commerce françaises, emlyon business school a ouvert un nouveau campus à Paris équipé des toutes dernières technologies. Situé en face de la gare de Lyon, sur un espace de 5 500 m², le campus parisien propose à la fois des formations continues et initiales.



Étroitement connecté aux autres établissements de l'école dans le monde, il offre un environnement d'apprentissage et de travail numérique ouvert sur l'Europe, l'Afrique, l'Asie et les États-Unis.

emlyon business school en chiffres :

- > 5 500 cadres, managers et dirigeants formés par an
 - > 1 600 entreprises partenaires
 - > 5 campus : Lyon, Saint Etienne, Paris, Casablanca et Shanghai
 - > 3 accréditations internationales : AACSB, AMBA et Equis
- Plus d'informations sur <http://executive.em-lyon.com>

A propos de Platinion

BCG Platinion, filiale à 100 % du Boston Consulting Group, crée et implémente les solutions technologiques de demain afin de réussir la transformation digitale des entreprises. L'équipe est composée de professionnels, passionnés de technologies partageant les valeurs d'excellence du BCG alliant conseil en stratégie IT et expertise technologique de pointe. Leur passion : « Concevoir et mettre en place des technologies qui libèrent la créativité et repoussent les limites du possible pour les collaborateurs et les modèles d'entreprises. »

Les experts de BCG Platinion permettent aux entreprises :

- de digitaliser le parcours client et les processus opérationnels ;
- d'exploiter le potentiel des données, y compris celles présentes dans les systèmes existants en les modernisant avec des architectures plus ouvertes ;
- d'améliorer les compétences et les savoir-faire technologiques des collaborateurs des DSI, notamment en généralisant l'usage de l'open source, du cloud, des méthodes DevOps et de l'agile ;
- d'accompagner le déploiement et l'appropriation de technologies de rupture (blockchain, objets connectés, bots...).

Les experts de BCG Platinion sont en recherche permanente de solutions sur-mesure pour créer toujours plus de valeurs et d'impact auprès des entreprises.

Plus d'informations sur www.bcgplatinion.com/

13. Annexes

Liste des consortiums blockchain (vision mars 2017)

Nom	# membres	Date de création	Secteur	Objectif	Participants
Hyperledger (USA)	110	Décembre 2015	Plateforme	Collaboration globale entre leaders financiers, bancaires, IoT, supply chains...	Linux Foundation & IBM (leaders), Airbus, Amex, BNP, ANZ...
R3CEV (USA)	74	2014	Financial Services	Plateforme partagée (Corda) pour créer et proposer la DLT aux marchés financiers globaux.	Barclays, BBVA, Crédit Suisse, UBS, Citi, BNP, ING, et d'autres acteurs majeurs de la finance.
PTDL Group (UK)	45	Mai 2016	Financial Services	Créer un environnement distributed ledger pour le post-trade	CME Group, Euroclear, HSBC, LSE, UBS, Société Générale
ISITC (UK)	100	Juillet 2016	Financial Services	Aider l'industrie des FS à adopter la blockchain DLT. Proposition de 10 benchmarks	Entreprises européennes
Global Blockchain Council (E.A.U.)	32	Février 2016	État	Aider les autorités et les entreprises à comprendre la technologie blockchain	Smart Dubai, Dubai Government...
Russian Banks Consortium	7	Juillet 2016	Financial Services	Développement de proof-of-concepts, recherche conjointe, approche proactive avec le régulateur russe	QIWL, B&N, Tinkoff, MDM, Otkritie Bank, Khanty-Manslysk, MDM Bank, Accenture
Ripple Japanese Banks Consortium (Japon)	30	Août 2016	Financial Services	Réduction de coûts (90 %) pour les membres et clients	SBI Holdings, Bank of Yokohama, SBI Sumishin Net Bank
Digital Asset Holdings (USA)	15	2014	Financial Services	Améliorer l'efficacité, la sécurité, la vitesse...	JP Morgan, ABN Amro, BNP, Santander, IBM...
Hyperledger Healthcare Working Group (USA)	5	Octobre 2016	Santé	Exploration de cas d'usage de la blockchain dans le secteur de la Santé (registres, identités, smart contracts...)	Accenture, Gem Hashed Health, Kaiser Permanente, IBM, Hyperledger (leader).
B3I (Suisse)	15	Octobre 2016	Assurance	Explorer le potentiel de DLT pour améliorer le service client (rapidité, sécurité).	Aegon, Allianz, Munich Re, Swiss Re, Zurich Insurance Group
ISO/TC 307 (Australie)	15	Mai 2016	Standards	DLT pour encourager l'échange de données entre utilisateurs, applications et systèmes	15 pays dont l'Australie (leader), le Canada, la Chine, les USA, la France, UK...
Fund Chain (Luxembourg)	10	Octobre 2016	Financial Services	Explorer le potentiel de la blockchain et use cases	BIL, BNP, CACEIS, PwC, HSBC...

Source : Analyse The Boston Consulting Group





MEDEF

55 avenue Bosquet - Paris 7^e

Dépôt légal : avril 2016