dossier de VEILLE

AEC l'agence aquitaine du numérique

n°2 / décembre 2015

# BLOCKCHAIN : UN DISRUPTEUR NÉ ?

« Blockchain », ou chaîne de blocs, ce terme est sur toutes les bouches et fait la une des magazines les plus prestigieux comme the Economist qui titrait, le 31 octobre dernier « Comment la technologie derrière le bitcoin pourrait changer le monde ». Si cette technologie est encore loin de faire parler d'elle comme a pu le faire le BitCoin à ses débuts, il s'agit, selon les experts de la finance et de la cryptologie d'une véritable révolution industrielle qui est en marche et sa déferlante pourrait être encore plus forte que celle que le **web a eu sur l'humanité** depuis le milieu des années 90. **Le monde de la finance**, lui, commence à prendre au sérieux ce concurrent et les grands opérateurs, comme Orange, n'hésitent plus à **investir dans des startups disruptives** de la blockchain aux côtés de grands capital-risqueurs américains ou **Microsoft** qui vient de lancer un service basé sur la blockchain.

Histoire, décryptage d'une tendance et perspectives à plus long terme, AEC propose dans ce dossier de veille de revenir sur la genèse d'un phénomène qui semble promis à un grand avenir.

## I Le phénomène Blockchain

La technologie blockchain est apparue dans l'ombre de son premier usage, en 2009, le BitCoin. Le Bitcoin est une crypto-monnaie créée par le mystérieux Satoshi Nakamoto dont l'objectif est de s'affranchir des intermédiaires financiers classiques — à savoir les banques — lors d'échanges monétaires entre pairs. Fondé sur le principe du système distribué, le Bitcoin permet de surmonter le problème du double paiement dans les transactions financières (double spend problem) : comment s'assurer que le montant versé n'est pas encaissé deux fois ou que le chèque n'est pas un chèque en bois ? Les banques jouent traditionnellement le rôle de tiers de confiance en s'assurant (et en facturant ce service) que les deux parties sont en mesure d'honorer leur dette pour l'une et de n'encaisser qu'une seule fois la somme pour l'autre. Or, le coût du service proposé par les banques rend très difficiles les micro-paiements qui ne peuvent supporter ce coût supplémentaire. C'est alors que la crypto-monnaie intervient : les échanges (souvent de très faibles montants) sont effectués directement de pair à pair, via des plateformes d'échanges (il en existe des dizaines, comme il existe des centaines de crypto-monnaires) non centralisées. Les transactions sont alors réputées publiques, traçables, conservées de façon permanente dans le réseau Bitcoin et cela sans coût supplémentaire.

Pour réaliser cette prouesse, les crypto-monnaies se basent toutes sur la même technologie : la blockchain, ou en français, la chaîne de blocs.

### Définition

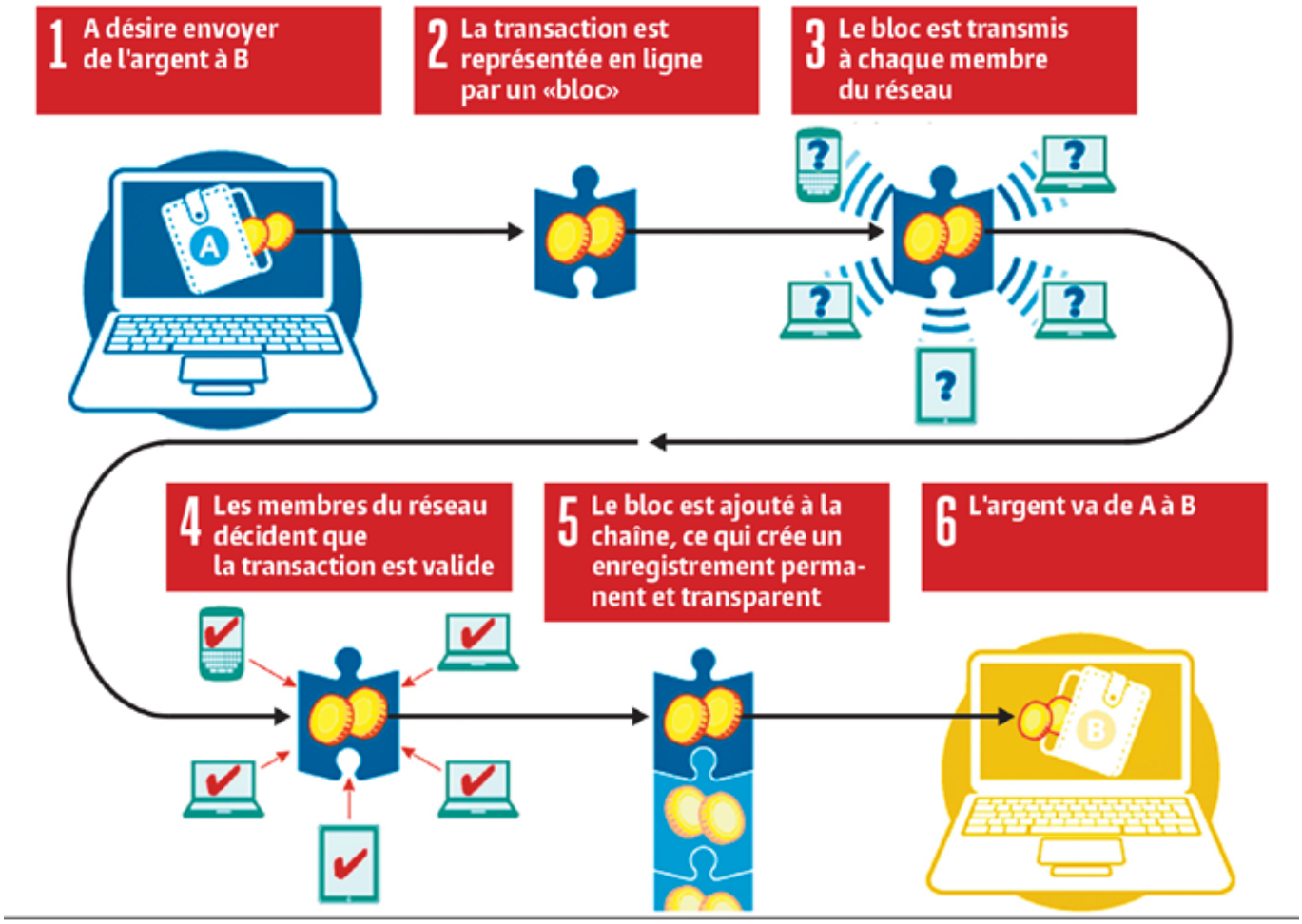
Les images ne manquent pas pour faire comprendre la blockchain : « grand livre de comptes ouvert », « **ADN mathématique** », la blockchain est en fait un registre permanent, public, inaltérable (il n'existe plus de serveur unique sur lequel sont stockées les données), crypté, infalsifiable et accessible à tous sur Internet. Ce registre permet d'identifier parfaitement l'actif, son propriétaire et toutes les informations caractéristiques de l'actif en question (notamment son transfert d'un propriétaire à un autre).

Pour s'affranchir du tiers de confiance, la blockchain doit faire appel à la puissance du réseau et à la cryptographie, deux éléments centraux qui rendent la technologie blockchain si puis-

sante et totalement sure. Contrairement au système classique centralisé (tiers de confiance), la blockchain met en œuvre la force du réseau décentralisé (réseau de millions d'ordinateurs à travers le monde, chaque ordinateur conférant sa puissance à l'ensemble de la communauté) composé de **mineurs** qui sont les nœuds de ce réseau, chaque mineur jouant le rôle d'intermédiaire dont la seule fonction est de produire — contre rémunération — des confirmations de transactions afin de les afficher dans la blockchain. Ces « Proofs of work » sont alors nécessaires pour garantir la véracité de la chaine de blocs. Pour valider une transaction, il faut attendre la résolution par la machine d'une épreuve cryptographique, nécessitant une très grande puissance de calcul (une transaction ne sera validée que lorsque la majorité des miners approuvera cette transaction). Cette épreuve fait appel à des informations contenues dans les blocs précédents, son empreinte numérique ou « **hash** ». C'est uniquement lors de sa résolution que toutes les transactions de la chaîne sont validées (on parle alors de consensus distribué), et un nouveau bloc est automatiquement crée, lié aux précédents. La blockchain est alors publique (les transactions sont consultables par tous), infalsifiable (la cryptographie permettant d'empêcher toute tentative de fraude) et inaltérable (une fois qu'une transaction est ajoutée, elle ne peut plus être modifiée ni effacée et devient donc non censurable).

La force de la technologie blockchain n'est pas seulement de se passer des intermédiaires financiers comme en rêvait Satoshi Nakamoto mais de pouvoir se défaire de tout tiers de confiance lors de transactions entre deux parties. C'est la raison pour laquelle, certains n'hésitent pas à qualifier la blockchain de plus grande innovation disruptive depuis l'invention du web.

LE FONCTIONNEMENT DE LA BLOCKCHAIN APPLIQUEE A L'ECHANGE D'ARGENT




Source: «Financial Times»

Taxonomie des domaines «blockchainables»

| Catégories | Domaines |
|---|---|
| *Instruments financiers* | *Monnaie(s), titres en actions, obligations, produits dérivés, droits de vote associés à des instruments financiers, enregistrements de transactions, enregistrements de prêts ou d'hypothèques, crowdfunding, prêts personnels en P2P, dons et donations, etc.* |
| *Documents administratifs* | *Titres de propriété foncière, cartes grises, licences professionnelles, enregistrements de faillites, casier criminel, papiers d'identité, certificats de naissance et de décès, documents d'inspection sanitaire, permis de construire, enregistrements judiciaires, bilans, etc.* |
| *Contrats privés* | *Contrats, signatures, authentifications, testaments, séquestres, données personnelles, etc.* |
| *Contrats semi publics/semi privés* | *Diplômes, certifications, dossiers ressources humaines, dossiers médicaux, ADN, arbres généalogiques, etc.* |
| *Clés d'actifs physiques (en relation avec l'internet des objets)* | *Clés physiques, serrures, voitures, boites aux lettres, chambres d'hôtels, entrepôts, etc.* |
| *Propriété intellectuelle* | *Brevets, licences, droits d'auteur, preuve d'authenticité ou de paternité, etc.* |
| *Autres types de documents* | *Tous les documents historiques, culturels ou évènementiels, Big Data, cartes sim, vote électronique, documents de livraison, etc.* |

*Adapté et traduit de « Long Finance, the chain of a life time », 2014*

# II Quels enjeux au-delà du bitcoin ?

La puissance de la blockchain réside donc dans le fait que grâce à elle, nous allons pouvoir nous passer, dans un futur proche de tout intermédiaire pour réaliser la moindre transaction et ce quel que soit le secteur d'activité. La notion de confiance disparait totalement puisqu'il n'est plus nécessaire d'avoir confiance pour réaliser un échange, la technologie blockchain se chargeant d'intégrer cette notion à son processus de validation. L'économie réelle comme l'économie du web vont être impactées par le développement et le recours de plus en plus fréquent à la blockchain. Et les disrupteurs d'hier (Uber, AirBnB, etc.) risquent à leur tour de devenir les disruptés de demain.

## Disruption des métiers traditionnels basés sur un tiers de confiance

Jusqu'à aujourd'hui, dès que nous entrions dans une transaction avec une autre partie, celle-ci devait être fondée sur une confiance réciproque dans la réalisation des droits et obligations y afférant ou si cette confiance n'était pas partagée, une personne (morale ou physique) était mandatée pour conférer un caractère authentique à tous les actes qui lui étaient demandés (notaire, banque, experts, etc.). Cependant, le recours à ce tiers extérieur à la transaction est souvent coûteux et n'assure pas contre la fraude, l'asymétrie d'information ou la malhonnêteté. Le contrat de mariage pourra bientôt être signé entre les époux sans avoir recours à un notaire pour authentifier l'acte, la blockchain et le recours au consensus distribué permettront de garder une trace authentique, infalsifiable et publique de l'engagement réciproque.

L'authentification peut également concerner les achats immobiliers, le transfert de titres de propriété étant parfois soumis à des fraudes. Le Honduras, par exemple, fait face à une fraude massive puisque 70 % du foncier n'est pas enregistré convenablement sur le cadastre. Le gouvernement a donc fait appel à une startup américaine **Factom Inc**, pour développer un registre foncier sécurisé et transparent à partir de la technologie blockchain. En enregistrant la propriété des terrains sur la blockchain, le pays sera donc en mesure de garantir à 100 % la propriété d'un terrain à un habi-

tant et par le fait même sécuriser l'hypothèque qui y est associée. D'autres startups ont également investi la gestion d'actifs immobiliers comme comme **Bitproof** ou **Blocknotary**.

Les Arts (les artistes n'auront plus besoin d'experts, de commissaire-priseurs ou d'avocat pour authentifier leurs œuvre, **la blockchain** le fera [presque] gratuitement pour eux), **l'assurance**, l'éducation (**une première école privée américaine** certifie les diplômes qu'elle délivre dans la blockchain afin de lutter contre la fraude aux faux diplômes), les **échanges contractuels entre société**, ou même sa propre **identité sur internet**, pourront profiter de la puissance de la technologie blockchain à très court terme. La blockchain pourrait également être la technologie qui révolutionne la démocratie en **sécurisant le vote par internet** (réputé non fiable et facilement piratable) et en renvoyant **le vote par bulletins aux oubliettes**; celle qui sécurise les échanges de données entre médecins et patients à travers un dossier médical personnel fondé sur la blockchain (lire à ce propos le **scénario** imaginé par l'équipe de Blockchain France autour d'une santé connectée). Celle qui permet, enfin, à chaque internaute de conserver, de sécuriser et de choisir à qui il permet l'accès à ses données personnelles et ainsi se prémunir des abus des GAFA (Google-Amazon-Facebook-Apple) dont le **modèle économique** repose sur la monétisation des données de leurs utilisateurs.

## Que peuvent Uber et AirBnB face à la blockchain ?

La blockchain promet donc la révolution dans les secteurs traditionnels qui échappaient jusque-là à la concurrence d'internet et des nouveaux disrupteurs. Demain, les taxis parisiens qui ont pris de plein fouet l'arrivée d'Uber sur leur marché pourront avoir quelques motifs de satisfaction puisque même Uber n'est plus à l'abri de la déferlante blockchain. Pour certains, en effet, la blockchain serait l'uberisation ultime de l'économie et un jour viendra où Uber se fera lui-même uberiser.

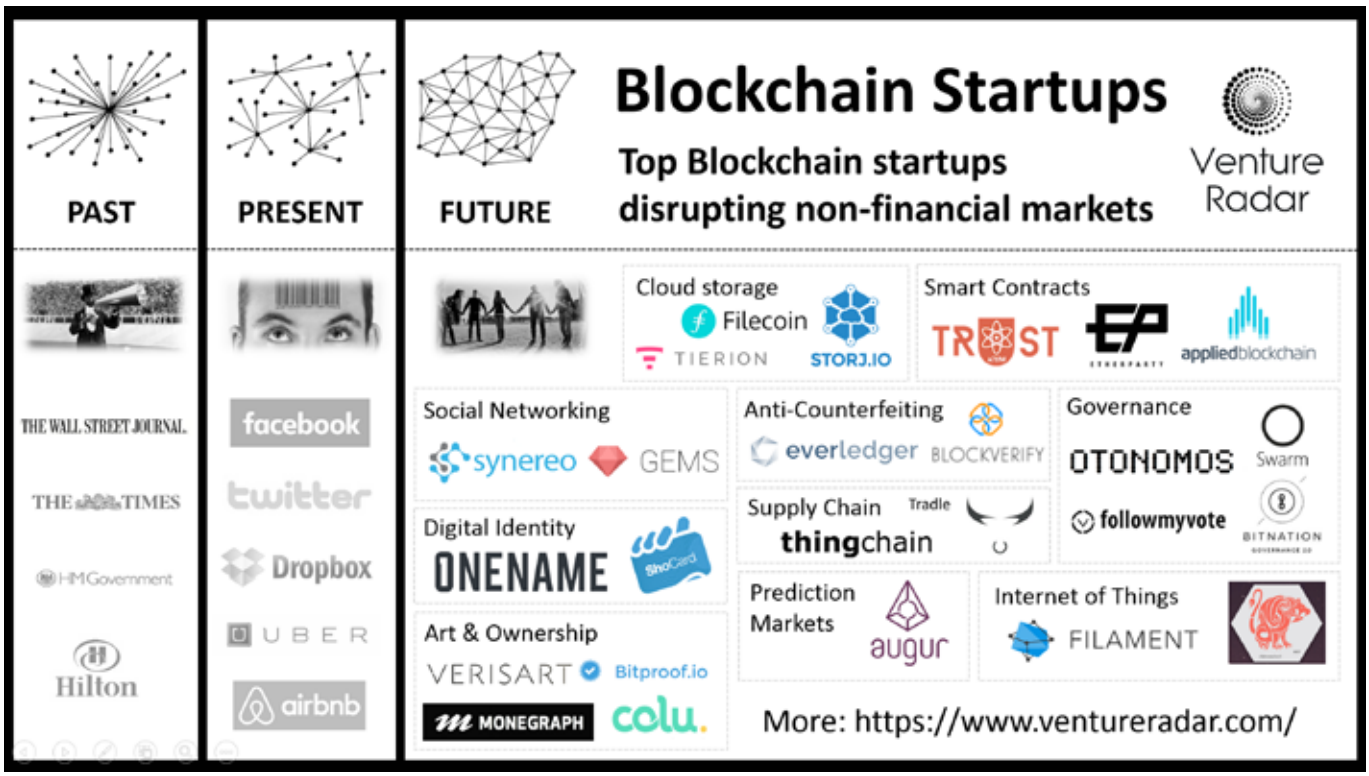
La première vague de disruption a permis à des entités (Uber, AirBnB, etc.) dont le modèle économique repose sur une plateforme de mise en relation entre particuliers, d'engranger des recettes estimées à plusieurs millions de dollars sans posséder la moindre voiture (pour Uber) ou la moindre chambre d'hôtel (pour AirBnB), c'est-à-dire en n'ayant quasiment aucun coût fixe (en dehors de la maintenance de la plateforme, entre autres). Ces sociétés proposent une offre économiquement très attractive à leurs clients et permettent aux particuliers qui

## Les contrats intelligents : l'exemple de la musique

L'une des caractéristiques principales du projet Ethereum est de reposer sur l'existence de contrats intelligents. Ces contrats intelligents sont des protocoles informatisés qui exécutent les termes d'un contrat. Leur objectif est de remplir les conditions contractuelles (comme les termes du paiement, identifier les parties, définir les termes de la confidentialité et ceux de l'exécution) en limitant les erreurs accidentelles ou frauduleuses en se passant d'intermédiaire (la blockchain permet **l'automatisation de la transaction en supprimant les tiers**). Il permet ainsi de diminuer les coûts de transaction et d'exécution en diminuant les coûts liés à l'arbitrage et à la fraude qui sont habituellement facturés par les intermédiaires. Certaines **plateformes** se sont spécialisées dans la rédaction de ces contrats intelligents.

Appliquons la blockchain et les contrats intelligents à **l'industrie musicale**. Aujourd'hui, tout artiste est entièrement dépendant d'un label, d'une société de gestion collective (de type SACEM) et d'un réseau de distributeurs qui, chacun leur tour, ponctionnent dans des termes pas toujours clairs une part des recettes issues des ventes de l'artiste. Imaginons maintenant, que ce même artiste se tourne vers la blockchain. Chaque œuvre qu'il compose peut bénéficier d'une signature unique et cryptographiée qui lui assure, publiquement, la paternité sur son œuvre et qui le protège contre une utilisation frauduleuse (notamment dans le cas d'utilisation sous forme de sample, difficilement identifiable par les systèmes de contrôle actuels). Il peut également définir les termes d'un contrat intelligent dans lequel sont stipulés les licences qu'il accorde à chacune de ses créations, quels droits il autorise et quels seront les frais. Dès qu'une radio diffuse un morceau de musique, tous les auteurs (ou leurs ayant-droits) sont immédiatement identifiés et directement rémunérés sur les bases des termes du contrat. En décentralisant totalement les modalités de diffusion toutes les transactions deviennent publiques donc parfaitement équitables.

Des plateformes émergent dans le monde anglosaxon : **UjoMusic** et **PeerTracks** semblent les mieux armés pour enclencher la révolution blockchain dans l'industrie musicale.




offrent leurs services d'obtenir des gains substantiels. Pour autant, ce modèle reste un modèle d'économie dit classique où un tiers de confiance (en l'occurrence la plateforme) met en relation deux contractants et prélève, auprès des deux parties, de quoi lui permettre de réaliser recettes et profits. La technologie blockchain met à mal ce modèle en permettant à tout contractant de négocier de pair-à-pair de manière sécurisée, transparente et non falsifiable, en dehors de toute référence à une quelconque entreprise qui facturerait quelques dollars, la mise en relation. Viennent de naître les Distributed Applications et leur nombre va croissant.

La'Zooz, startup israélienne, entend révolutionner le transport de proximité (afin de concurrencer Uber), en proposant une application open-source permettant à toute la communauté d'organiser des offres et des demandes de co-voiturage en dehors de toute instance organisatrice. Basée sur la technologie blockchain, la plateforme attire à elle, dans un premier temps, une quantité suffisante de personne sur un territoire donné en proposant des incitatifs, les « zooz token ». La valeur des jetons diminuant avec le nombre d'inscrits afin de favoriser les « early adopters » (ces derniers peuvent même être rémunérés alors qu'ils voyagent seul, dans un premier temps) et d'atteindre très rapidement une taille critique permettant de faire correspondre l'offre à la demande. Une fois le service lancé, chaque utilisateur dépense ensuite ses jetons en commandant une course, à un tarif unique, de 0,5 dollar/km.

Synereo, plateforme sociale nouvelle génération américaine, a pour ambition de concurrencer et à plus long terme remplacer Facebook. Contrairement à Facebook, l'idée de Synereo est de favoriser les échanges entre les utilisateurs dont les liens au sein d'un réseau sont distendus. En s'appuyant sur l'économie de l'attention et en valorisant les échanges entre pairs éloignés, la plateforme mise sur l'attention que les utilisateurs portent aux idées des autres et non sur leur personnalité propre. Plus un contact qui partage une de vos publications est éloigné de vous et plus cette publication est visible pour l'ensemble de votre réseau (par l'entremise d'algorithmes qui calculent l'intérêt et la pertinence des publications). Pour cela, Synereo s'appuie sur la blockchain, et crée une plateforme décentralisée, fonctionnant sur les ordinateurs des utilisateurs eux-mêmes. Ces derniers pourront créer un réseau sans avoir besoin d'un tiers de confiance, ou d'entité centrale, à l'inverse de Facebook, Google + ou encore LinkedIn. Pour son créateur, Dor Konforty, « dans 5 ans, une entité exerçant un immense pouvoir de manière centralisée – comme Facebook – n'aura simplement plus aucun sens ».

Twister (micro-blogging), storj et filecoin (stockage décentralisé), OpenBazaar (place de marché), FireChat (Chat), BitNation (gouvernance décentralisée) sont autant d'exemples d'applications décentralisées qui promettent de révolutionner le monde de l'internet. Certains acteurs sont

encore plus ambitieux et n'hésitent pas à reconsidérer totalement les modèles existant : UjoMusic, par exemple, a pour ambition de disrupter l'industrie musicale grâce à la blockchain et au contrats intelligents (voir encadré ci-dessous), Ethereum est un projet à la charnière de la blockchain et du web sémantique dont l'objectif est de créer un système économique composé d'une plateforme, d'une monnaie — l'éther — et de son propre langage de programmation afin de permettre de réaliser des transactions via des contrats intelligents. L'idée à terme serait de se passer totalement de serveurs et de construire un réseau entièrement décentralisé dans lequel chacun pourrait venir y déposer et distribuer librement des applications. Pour chaque application, des contrats seraient passés puis, à chaque contrat serait attribuée une valeur en ether.

# III Limites et défis

Si la révolution promise par la blockchain et ses nouveaux prophètes semble inéluctable certains défis restent à relever.

Des défis techniques en premier lieu. L'augmentation de la puissance de calcul des ordinateurs rend de plus en plus rapide le processus de validation d'une chaine de blocs, le système n'aura pas le temps de traiter l'ensemble des chaînes et un phénomène d'engorgement pourrait apparaître et avec lui la création de chaînes de blocs alternatives et donc un risque de confusion que le système BitCoin aurait du mal à gérer. Stephan Tual, le porte-parole d'Ethereum le reconnait « Evidemment si la planète venait à utiliser nos outils, nous aurions alors un problème, parce qu'il y aurait trop de monde. Une solution que nous regardons est d'utiliser un langage différent qui permet à chacun de ne garder qu'une partie de la chaîne de blocs et pouvoir toujours la valider. Une autre solution pourrait être de construire plusieurs chaînes et plusieurs Ethereum. Nous y travaillons encore. En fin de compte, le succès de l'aventure d'Ethereum dépendra du nombre d'utilisateurs et des outils construits. Mais si Ethereum devient trop populaire, il pourrait aussi s'effondrer par la saturation de données dans le réseau pair-à-pair. Les serveurs, après tout, existent pour une raison. »

Autre problème technique de taille : l'augmentation de la longueur de la chaine de blocs. Comme nous l'avons vu à chaque validation de transaction, un nouveau bloc est ajouté à la chaine, environ toutes les dix minutes (c'est le temps nécessaire à l'heure actuelle pour valider une transaction). Or, depuis juillet 2012, la taille de la blockchain augmente de façon exponentielle pour atteindre, en juillet 2015, plus de 45.000 Mo, entrainant de fait un ralentissement et un coût plus important du processus de validation des transactions.

Des défis liés à la sécurité et à l'anonymat ensuite. Si les grandes banques, les sociétés d'investissement et les fintechs s'intéressent aujourd'hui à la blockchain, il n'en reste pas moins que la solution proposée par les blockchains publiques ne sont pas exemptes de tout reproche aux yeux des financiers. Le coût lié au consensus anonyme (l'anonymat est relatif car si on ne peut identifier les parties qui s'échangent de la crypto-monnaie, on peut tracer l'ensemble des échanges entre ces parties) est très lourd à porter et un nouveau type de blockchain apparaît, dans lequel les processus de contrôle du registre (permission d'accès et lecture) sont plus strictes tout en garantissant l'authenticité, l'inaltérabilité et la décentralisation du processus.

Ces blockchain peuvent être totalement privées (à ce moment là un seul agent valide les blocs mais la lecture de la blockchain reste publique et transparente) ou hybride, dans laquelle le processus d'approbation des blocs est réservé à une petite quantité d'agents (les règles de la majorité pour approbation et du consensus distribué ne sont plus forcément respectées) qui organisent la blockchain. C'est ce modèle hybride ou de « consortium » qui aujourd'hui attire les grands groupes financiers et les banques. Ainsi, plus de 20 établissements financiers du monde entier, parmi lesquels Bank of America, HSBC ou encore Société Générale, ont rejoint un projet porté par la startup r2cev dont l'objectif est de créer une blockchain partagée à ce consortium, portant sur des protocoles et des standards communs, tout en garantissant aux banques participantes un contrôle sur la technologie en circuit fermé. Si un consensus se dégage, les premiers tests pourraient concerner les échanges de titres de créances qui nécessitent d'être tracées.

Les défis restent donc nombreux à relever et même si l'idéal libertaire des débuts du bitcoin semble loin, les enjeux pour l'ensemble de l'économie mondiale méritent de porter une attention sérieuse à cette chaine de caractères qui risque de refaire parler d'elle d'ici peu.

AEC est l'agence aquitaine du numérique. Elle est engagée depuis près de 20 ans dans l'émergence de projets innovant à travers :

- La veille et les publications
- l'animation et la mise en relation
- les ateliers d'innovation collaborative
- l'accompagnement de projets innovants
- l'Auberge Numérique, son incubateur dédié aux startups

Contactez-nous !

**contact@aecom.org**

**Retrouvez l'ensemble des publications de veille d'AEC :**
**http://bit.ly/aecveille**

**Prochainement : « Comment le numérique s'est emparé du secteur alimentaire : la FoodTech décryptée. »**


Pour scanner, telecharger l'app Unitag gratuite sur : **unitag.io/app**


AEC, 137, rue Achard – 33 300 Bordeaux/Tél. +33 (0)5 57 57 01 01 – Fax +33 (0)5 57 57 97 17
aec@aecom.org / www.aecom.org
@agenceAEC / https://www.facebook.com/AquitaineEuropeCommunication
https://www.facebook.com/groups/clubAEC/?fref=ts