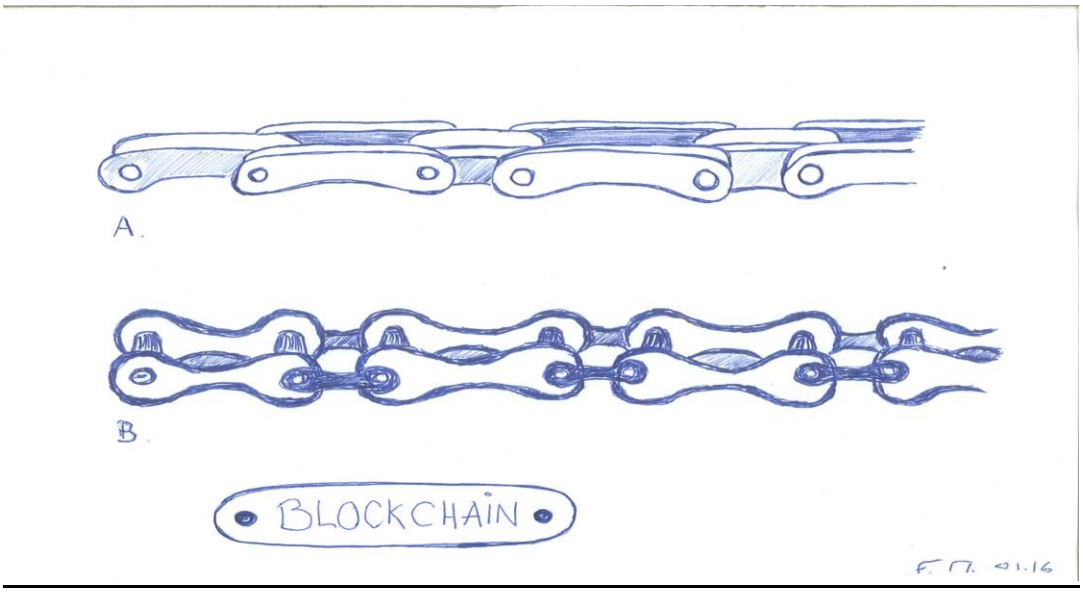
Block Chain, le buzz word deviendrait-il une réalité ?

Derrière la notion à la mode de « block chain » se cache une technologie capable de révolutionner le monde bancaire et des paiements ou même plus encore. Une menace ou une opportunité pour les trésoriers d'entreprise ? Un autre pan du business bancaire qui pourrait disparaître, victime de l' « Ubérization » ? Le train quitte la gare. Il faut peut-être pour les banques monter dedans au risque de rester à quai. Quels seront les impacts pour les entreprises ? La désintermédiation pourrait continuer à produire ses effets en créant une rupture avec le mode de paiement actuel. Que restera-t-il aux banquiers si ce business leur échappe ? Qu'est-ce qui se cache derrière ce mot tellement « geek » ? C'est ce que cet article tente de vous révéler

« The Trust Machine ?»

Le magazine « *The Economist* » titrait en octobre 2015 : « *The trust Machine* » en parlant de la technologie qui se cache derrière le Bitcoin et insistait sur le fait qu'elle pourrait bien changer la face du monde. Effet de manche ? Titre provocateur ? Idée farfelue ou réalité en devenir ? Telles sont les questions qu'il faut se poser en tant que trésorier d'entreprise. Comme on le sait, le Bitcoin souffre d'une réputation quelque peu sulfureuse. On dit que son usage est parfois détourné et dédié à des opérations illicites. On le taxe d'être hyper- volatile. Le Bitcoin est en tout cas relativement stable contrairement à l'apriori qui l'entoure (BTC/USD : +/- 440$) et peut-être moins que certaines devises par les temps qui courent. Pour le reste, il est difficile d'argumenter. La nouveauté, en plus d'intriguer dans le cas présent, dérange les conservateurs. Elle finira par graduellement s'imposer au fil des ans, soyons-en certains.

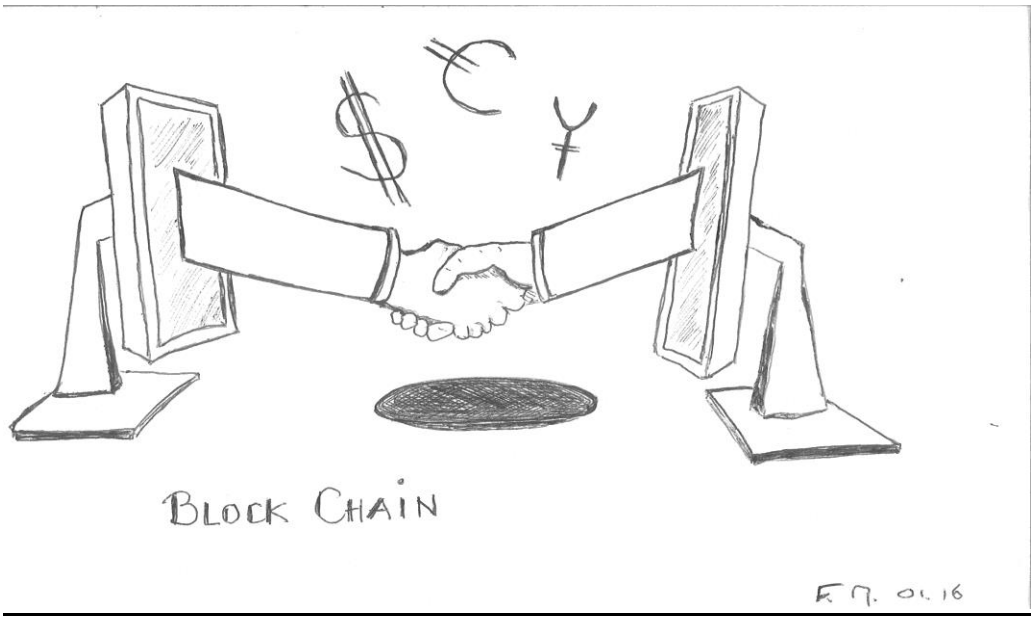
Si l'on parle de chaînes de blocs, il faut tout d'abord s'entendre sur la signification de ces termes. C'est une base de données distribuée qui gère une liste d'enregistrements protégés contre la falsification ou la modification par les nœuds de stockage. A proprement parler, une « *blockchain* » est un historique décentralisé des transactions effectuées depuis le démarrage du système réparti. On peut faire le parallèle avec internet puisque ce sont des protocoles permettant la création d'une infrastructure décentralisée. Le grand livre au cœur du Bitcoin lui accorde une sécurité et une résilience incomparables grâce à sa conception « distribuée ». En simplifiant le concept, l'enregistrement des transactions est répliqué sur de multiples machines formant un réseau de minage de la crypto-devise. Dès lors une falsification isolée n'a pas d'incidence car la vérité est établie par le consensus de la majorité. Un peu compliqué me direz-vous. Retenons que c'est public et très sûr. L'idée de la chaine de bloc est qu'une personne qui n'aurait pas une confiance particulière en une autre pourrait traiter avec cette dernière sans passer par une autorité centrale neutre. En d'autres mots, la chaine de bloc c'est une machine à créer de la confiance. Le grand livre du Bitcoin (i.e. « ledger ») permet de prévenir le risque de double opération ou de duplication en gardant continuellement trace des transactions. C'est ce qui permet d'éviter le recours à une autorité centrale. L'impossibilité de duplication et donc de fraude en font un outil remarquable. Aujourd'hui l'intérêt réside dans ce qui pourra être capitalisé sur la technologie de chaine de bloc, plus que sur les crypto-devises elles-mêmes. Cette technologie permettrait de réduire les coûts, notamment des transferts bancaires, de plusieurs milliards.



Problème des Généraux Byzantins

On décrit parfois les chaines de blocs comme la solution au fameux problème dit des « généraux byzantins ». Cette métaphore traitait de la remise en cause de la fiabilité des transmissions et de l'intégrité des interlocuteurs. La question est de savoir comment, et dans quelle mesure, il est possible de prendre en compte une information dont la source ou le canal de transmission est suspect. La solution implique l'établissement d'un algorithme (d'une stratégie) adapté. Des généraux de l'armée byzantine campaient autour d'une cité ennemie. Ils ne pouvaient communiquer qu'à l'aide de messagers et devaient établir un plan de bataille commun, faute de quoi la défaite serait inévitable. Cependant un certain nombre de ces généraux pouvaient s'avérer être des traîtres, qui essayeraient donc de semer la confusion parmi les autres. Le problème était donc de trouver un algorithme pour s'assurer que les généraux loyaux arrivent tout de même à se mettre d'accord sur un plan de bataille. Il a été démontré qu'en utilisant uniquement des messages oraux, ce problème des généraux byzantins peut être résolu, si et seulement si plus des deux tiers des généraux (messagers) sont loyaux. Ainsi un seul traître peut confondre deux généraux loyaux. De plus, le problème peut être résolu pour un nombre quelconque de généraux renégats si les messages sont écrits (et non falsifiables). Par analogie avec les systèmes informatiques, un ensemble de composants informatiques qui fonctionnent de

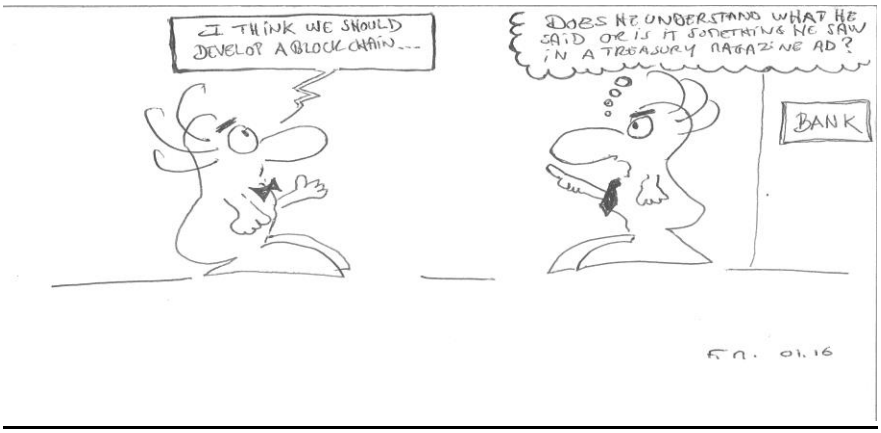
concert doivent gérer d'éventuelles défaillances parmi eux. Les défaillances ou informations erronées peuvent être accidentelles ou malveillantes. C'est à ce problème que la chaine de bloc entend répondre.



Technologie détournée et accidents salutaires

Parfois une technologie ou une idée est développée par quelqu'un avec un but précis et puis se voit détournée à d'autres fins. Le Bitcoin n'était peut-être qu'un point de départ. Par exemple, XEROX existait avant le premier MAC, tout comme Internet qui fut créé au départ comme le GPS à des fins militaires et dont on connait l'usage infini actuel. Alexandre Fleming a découvert par hasard la pénicilline en contaminant lui-même les bactéries qu'il étudiait. Il existe tant d'exemples de techniques détournées de leur objectif initial. Napster a été mis hors service mais a réussi à inspirer d'autres services « Peer-to-Peer ». L'idée d'un service P2P, pionnier illicite du partage de musique, créé en 1999, a suscité bien des émules. On a réussi à y trouver des usages musicaux ou autres tout à fait légitimes. Le « *block chain* » est peut-être une sorte de «*Skype* » en puissance, capable de révolutionner diverses industries. Et ce qui nous intéresse est que cette technologie pourrait bien créer une rupture avec le passé et changer la face du monde des paiements bancaires. Certes, il semble difficile de miser sur le

futur. Mais de nos jours, l'impossible ne devient-il pas tous les jours un peu plus réel et concret ?



«*Block Chain Buster*»

Masi d'où nous vient ce nouveau « *block buster* » qui anime les conversations des trésoriers ? La chaine de bloc fut créée en 2008 (i.e. « ***Distributed Ledger Technology*** ») et est l'algorithme sous-jacent à la crypto devises « bitcoin ». Mais au-delà de cette devise encore décriée et très virtuelle, se cache une technologie phénoménale aux applications infinies. On ne se penchera que sur les paiements, mais imaginez les registres qu'elle permettrait de tenir et de sécuriser (e.g. cadastre immobilier, registre de détention d'ouvre d'art, de brevets, etc…). Certaines banques l'ont bien compris et s'associent pour éviter d'être phagocytées (e.g. R3 consortium). Les banques s'associent entre elles ou à des sociétés dites « FinTech » afin de ne pas louper le coche et d'être sur les technologies de demain afin de ne pas être victimes de l' « Ubérization », elles aussi, puisque personne ne semble y échapper. Elles semblent avoir décidé de ne pas se comporter en victimes consentantes. Cette technologie permet à une contrepartie inconnue d'une autre de traiter et d'enregistrer leur opération ou transaction dans un registre (ou « l*edger* »). L'idée centrale serait donc, comme pour le Bitcoin, de traiter électroniquement et d'enregistrer de manière sécurisée des opérations dans le domaine public internet sans passer par des intermédiaires de confiance tels les banques et les correspondants bancaires, SWIFT ou les chambres de compensation. Magique, n'est-ce pas ?

Révolution des paiements ?

Deux éléments différenciant émergent: l'absence de tierce partie et le stockage public d'informations. La chaine de bloc est une gigantesque base de données encryptée de transactions toutes uniques. Cela signifierait des économies colossales, plus de rapidité, d'efficacité et surtout beaucoup plus de sécurité. Le cycle nécessaire pour le règlement (i.e. « *settlement* ») serait réduit à un minimum voire à quelques minutes. Même si ces changements ne se feront pas du jour au lendemain, gageons qu'ils semblent inéluctables et les intermédiaires peu ou pas proactifs auront du mouron à se faire. Les structures intermédiaires classiques qu'on connait depuis des lustres devront s'adapter pour démonter une valeur ajoutée. Avec la digitalisation de l'économie, c'est « adapte-toi ou disparais ! »

Hold-up ou qui pourrait tourner à la farce ?

Les grandes institutions financières se devaient de réagir. Mais si elles s'emparent des chaines de bloc, c'est pour préserver leur gagne-pain. Leurs vieux démons et leur volonté de préserver un territoire de chasse gardé, pourraient tuer toute initiative. Sujettes à de constantes cyber-attaques, les banques dépensent des fortunes pour se protéger. Elles ne sont donc pas insensibles à cet argument sécuritaire essentiel. Par contre, l'idée d'abandonner le contrôle absolu des données qu'elles gèrent est contraire à leur ADN et poussera une majorité d'entre elles à abandonner le concept dans son ensemble. Si l'on prend l'exemple du

réseau Swift (société coopérative détenue par les banques), il pourrait créer son propre « block chain » pour remplacer son réseau propriétaire. On se demande ce que serait le changement si Swift voulait demeurer seule responsable de la nouvelle infrastructure. Un livre de compte distribué n'a pas de sens si son code n'est pas partagé. La confiance dans ce genre d'instruments, même privés, ne peut évidemment pas se satisfaire d'algorithmes propriétaires. La croyance que ce que feraient les banques sera meilleur est peut-être à écarter une fois pour toutes. Privatiser les « *block chains* » requière des mécanismes de permission qui n'existent pas dans le fondement du Bitcoin. L'habilitation requière l'autorité centrale et les risques qui vont avec elle. Cela serait paradoxal de couper court à l'avantage d'une technologie pour protéger les intérêts d'un petit nombre. On peut comprendre l'envie d'éviter la disruption mais pas à n'importe quel prix et au détriment de l'idée même du « *block chain* »… Les banquiers ne font rien de moins que ce que tentent les taximen pour protéger leur business du phagocytage par UBER. Arriveront ils à se protéger, est une autre question. Je me permets d'en douter.

Même si plusieurs scénarii pourraient émerger (tels du « *Bank2Bank* » ou du « *Corporate2Bank* » ou même du « *Corporate2Corporate* »), on ne peut dire à ce stade lequel s'imposera. Le marché sera à moyen terme fondamentalement chamboulé dans tous les cas de figures.

« New kids on the block »

Les « *New chains on the block* » seront peut-être le « *disruptor* » de tout ce qui est centrales de règlement ou "*clearing houses*". Aujourd'hui même des gouvernements, comme la Grèce, ou des banques explorent ce type de solutions pour les substituer à l'organisation existante, avec le double objectif de renforcer la sécurité tout en limitant les coûts ou d'apporter plus de transparence et d'examens minutieux, tout à la fois. Cette technologie aurait le pouvoir de transformer en profondeur la manière dont certains businesses opèrent, se règlent et se liquident (i.e. *settlement*) Elle risque de changer complètement les règles du jeu. L'anonymat, l'efficacité, la communication « P2P » et l'indépendance de réseaux existants lui donnent ces caractéristiques spécifiques

qui la rende si intéressante et intrigante à la fois. Les grands perdants pourraient être les banques, les « *clearing houses* » et SWIFT, notamment. L'argent sera plus mobil et à moindre coût, spécialement pour les pays exotiques d'où le rapatriement est parfois très cher.

Un des problèmes principaux résidera dans la réglementation qui souvent avec les développements IT est en décalage et en retard par rapport aux outils qu'elle est censée légiférer. L'usage de pseudonyme sera aussi un point critique pour éviter l'anonymat et la fraude potentielle, à l'heure du KYC et de la transparence absolue imposée par le G20. La chaine de bloc sera un nouvel élément poussant à la désintermédiation bancaire. Cette technologie aura un impact considérable sur le futur de la banque telle que nous la connaissons. Comme le disait Theodore Levitt : « *Le futur appartient à ceux qui voient les possibilités avant qu'elles ne deviennent évidentes* ». Même si les trésoriers ne sont qu'utilisateurs, ils se doivent d'envisager ces possibilités futures et de veiller à ne pas en être de simples spectateurs. Le Président de l'EACT, Jean-Marc Servat, en a fait un sujet phare pour l'association européenne. Ce n'est donc pas la dernière fois que vous en entendrez parler, en bien ou en mal.

François Masquelier, Chairman ATEL