WAVESTONE

BANKINSIGHT

LA NEWSLETTER BANQUE
DES CONSULTANTS WAVESTONE

OCTOBRE/NOVEMBRE 2016

LA BLOCKCHAIN
LE BIG BANG DE LA RELATION BANCAIRE

OLIVIER SCHMITT
Directeur associé

SOMMAIRE

DÉSINTERMÉDIATION...SÉCURISÉE

Tout un chacun a plusieurs fois caressé l'idée d'un monde désintermédié où le producteur serait directement en contact avec le consommateur.

L'avènement de nombreux sites marchands, de troc, de vente de seconde main peut, par certains côté, paraître y répondre. Mais ne nous y trompons pas nous passons par un intermédiaire établi, certes discret, qui nous rassure mais prend sa dîme.

La technologie du *Blockchain* va nettement plus loin puisque l'autorité n'est plus une institution, une entreprise, un organisme mais elle est incarnée par une communauté d'acteurs informels qui tracent, certifient et sécurisent une transaction, un contrat.

Cette nouvelle répartition des rôles et des pouvoirs pourrait rapidement remettre en cause bien des modèles établis.

Olivier Schmitt

Laetitia MERCIER de BEAUROUVRE
laetitia.mercier@wavestone.com

Il y a 20 ans nous n'imaginions pas Internet… Or, aujourd'hui nous sommes plusieurs heures par jours connectés à Internet pour effectuer des transactions en utilisant des plateformes ou applications qui font office de tiers de confiance pour sécuriser ces transactions de biens contre des paiements. Et pourtant, ce qui nous émerveillait hier, semble être l'ère du crétacé avec l'arrivée de la *Blockchain* qui annonce le déclin du tiers de confiance (« *La Blockchain ou l'illustration d'un monde qui change* »).

La *Blockchain* est une technologie de stockage numérique et de transmission d'informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle.

Concrètement, la *Blockchain* constitue « un registre » contenant la liste de tous les échanges effectués entre les utilisateurs de cette *Blockchain* depuis sa création. Ce registre est décentralisé, c'est-à-dire stocké sur les serveurs de ses utilisateurs, et fonctionne sans intermédiaire, éliminant donc les frais d'infrastructure. Sa sécurité est garantie par un protocole cryptographique et il est mis à jour en temps réel indépendamment par tous les utilisateurs, ce qui permet à chacun de vérifier la validité de la chaîne (« *La Blockchain : un nouveau modèle pour la confiance ? »).*

Cette technologie pose d'ores et déjà certaines questions qui appelleront, à terme, des choix de société : dans quelle mesure accepterons-nous de remplacer les autorités de confiance historiques (banques, gouvernements…) par des programmes informatiques ? Les réponses à ces questions poseront les fondements de l'utilisation à venir de la *Blockchain (« Peut-on avoir une confiance sans limite dans la Blockchain* ? »).

LA BLOCKCHAIN OU L'ILLUSTRATION D'UN MONDE QUI CHANGE

Les technologies de rupture sont celles qui permettent l'expression d'une grande innovation.

Nombreux pressentent la *Blockchain* comme la prochaine révolution numérique, avec la promesse d'un changement radical du modèle sociétal, par une désintermédiation des échanges.

La confiance distribuée qui singularise la *Blockchain* porte une promesse d'horizontalisation de la société. On pourrait assister à une redéfinition profonde de modèles commerciaux et institutionnels qu'on pensait immuables. Cette possibilité est porteuse d'autant d'espoirs que d'inquiétudes et, pour un bon nombre d'acteurs, il s'agit de trouver la bonne approche, dans le souci de faire partie du paysage de demain.

LA BLOCKCHAIN : LE DÉPORT DE CONFIANCE

La *Blockchain* apporte une réponse nouvelle à la décentralisation de registres et à l'automatisation de contrats, qui suscite des questionnements relatifs à sa sécurisation et à sa mise en œuvre à grande échelle.

Originellement, la *Blockchain* Bitcoin fut le premier moyen de réaliser des transactions financières indépendamment de l'intervention des banques. Du fait des nombreuses crises, on observe aujourd'hui un report de la confiance, traditionnellement acquise aux institutions, vers des communautés d'utilisateurs/fournisseurs.

Cependant, se pose toujours la question de la fiabilité de ce modèle de confiance communautaire. Dès lors que cette question sera résolue, la disparition des tiers deviendra théoriquement envisageable.

L'immensité du champ d'application de la *Blockchain* ne suppose pas pour autant qu'on puisse y recourir pour tout et n'importe quoi, et surtout sans se poser la question du modèle à adopter et de la gouvernance à mettre en œuvre. Tous les usages ne nécessitent pas de recourir à la mobilisation d'une communauté importante.

DES PROMESSES ET DES POSSIBLES

Dans les secteurs marchand et financier, les promesses d'automatisation offrent des perspectives de réduction des coûts et de fluidité des transactions dont pourraient bénéficier les consommateurs, mais plus globalement, les gains potentiels qu'offrirait la *Blockchain* pourraient concerner une liste infinie de secteurs et d'usages.

Cependant, certains processus peuvent être automatisés sans recours à la *Blockchain*. Il s'agit alors de livrer une analyse globale et profonde, technique, métier et économique, pour identifier les cas d'usage *Blockchain* pertinents, en cherchant le sens avant le modèle business.

Les différentes pistes étudiées sont prometteuses et témoignent d'une énergie collective porteuse de gains tant pour les entreprises que pour les consommateurs. Pour autant, la promesse de désintermédiation absolue n'en sera pas forcément la résultante.

Dans le domaine de la société civile, la *Blockchain* est entre autres un moyen idéal de mettre en œuvre des projets collaboratifs nés du modèle des communautés et donc adhérents au concept de confiance distribuée.

L'État, quant à lui, pourrait se trouver à la fois dans une position de potentiel utilisateur, promoteur, maître d'œuvre et régulateur de la *Blockchain*.

La *Blockchain* présente donc un intérêt à la fois dans le privé et le public, reste à déterminer s'il s'agira en cible d'une *Blockchain* et de ses instanciations ou de la coexistence de différents modèles.

Anne GAUTRENEAU
anne.gautreneau@wavestone.com

LA BLOCKCHAIN : UN NOUVEAU MODÈLE POUR LA CONFIANCE ?

Qualifiée par certains visionnaires de technologie révolutionnaire, la Blockchain fait aujourd'hui de plus en plus parler d'elle. Le monde entier s'y intéresse et les investissements dans le domaine se multiplient. De nombreuses entreprises et administrations explorent actuellement les usages possibles de cette technologie prometteuse mais complexe à appréhender pour les métiers.

Pourtant, ce concept n'est pas nouveau : la *Blockchain* est la technologie sur laquelle s'appuie la crypto-monnaie Bitcoin, apparue en 2009. Mais alors, pourquoi ce regain d'intérêt ? Quelles sont les caractéristiques de cette technologie et quels usages peut-elle favoriser ? Quels sont les obstacles à surmonter pour qu'elle puisse se démocratiser ?

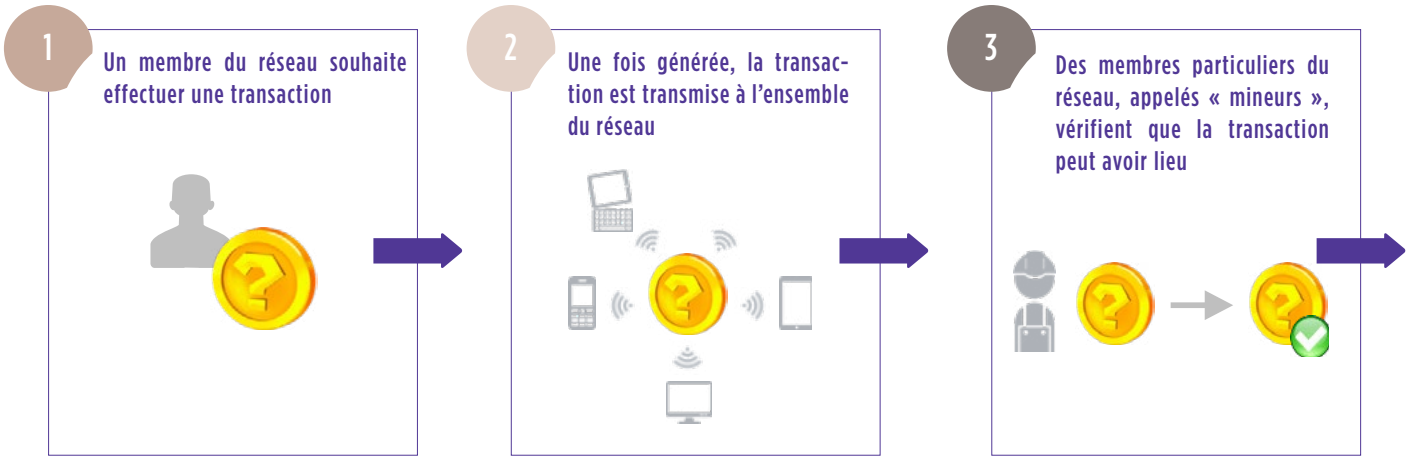
DES ALGORITHMES REMPLACENT LE TIERS DE CONFIANCE

La *Blockchain* permet aux membres d'un même réseau d'effectuer des opérations de stockage et de transmission d'informations, appelées transactions, et ce en toute confiance, sans autorité centrale de contrôle. Elle se présente sous la forme d'un registre contenant l'ensemble des transactions enregistrées depuis sa création et disposant de deux caractéristiques essentielles :

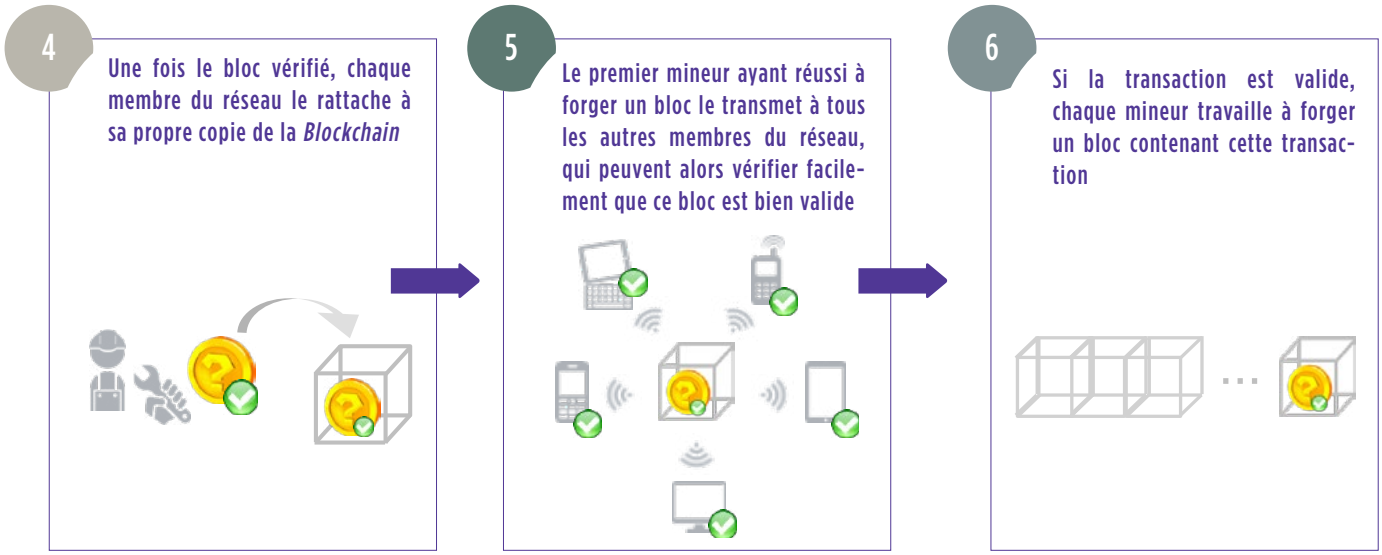
- **Il est distribué :** les membres du réseau disposent d'une copie du registre, rendant quasiment impossible sa modification par un individu sans l'aval du reste du réseau ;
- **Il est fiabilisé par les acteurs du réseau :** la confiance établie au sein du système est assurée par les membres du réseau eux-mêmes ; aucune autorité centrale ne joue le rôle de tiers de confiance.

Au sein du registre, les transactions sont regroupées dans des blocs enchainés par ordre chronologique. Le schéma ci-dessous permet de comprendre le processus de création d'un nouveau bloc, et donc l'enregistrement d'une nouvelle transaction dans la *Blockchain*.

Cinématique de rajout d'un Bloc à la Blockchain - Vision globale



Ainsi, le tiers de confiance est remplacé par des algorithmes permettant à tous les membres du réseau de vérifier facilement que les mineurs n'ont pas ajouté, supprimé ou modifié une transaction lors de la création des nouveaux blocs.



DU SIMPLE STOCKAGE SÉCURISÉ À L'EXÉCUTION DE CONTRATS INTELLIGENTS

Toute situation faisant intervenir un tiers de confiance coûteux ou faillible est une opportunité pour créer un cas d'usage *Blockchain*. Banque, immobilier, santé, transport… tous les secteurs se sentent concernés et réfléchissent actuellement aux opportunités offertes par la *Blockchain* pour améliorer ou remplacer les modèles actuels.

Trois catégories de cas d'usage se distinguent aujourd'hui :

1. **Record keeping :** *Blockchain* utilisée comme registre de stockage pour déposer des données dont on souhaite garantir la preuve de par leur existence, leur date de création et le droit de propriété, comme par exemple : des brevets, des données médicales, etc.

2. **Digital transactions :** *Blockchain* utilisée pour du transfert de valeur : transaction immobilière, crowdfunding, crypto-monnaies, etc.

3. **Smart-contracts :** *Blockchain* utilisée pour développer et stocker des smart-contracts, à savoir des contrats entre plusieurs parties, rédigés sous forme de code informatique, et qui s'exécutent sans intervention humaine selon les conditions et termes qu'ils contiennent.

Les acteurs du monde de la finance s'intéressent tout particulièrement à la *Blockchain*. Que ce soit en France ou à l'international, de nombreuses initiatives sont menées, parfois sous forme de consortium, dans le but d'évaluer le potentiel des usages de cette technologie dans le secteur et de définir des protocoles standardisés.

Bien que la *Blockchain* ait été initialement pensée comme un système public, la plupart des réflexions actuelles concernent des *Blockchains* privées (propre à une organisation) ou hybrides (propre à un ensemble de partenaires).

PERFORMANCE, ÉCOLOGIE ET RÉGLEMENTATION : LES OBSTACLES À SURMONTER

À titre d'exemple, le réseau Bitcoin permet d'enregistrer environ 7 transactions par seconde, à comparer aux 2 000 transactions par seconde de VISA. Pour s'imposer à large échelle et développer de nouveaux cas d'usage, la *Blockchain* doit donc pouvoir améliorer ses performances.

Le défi de la performance repose sur une définition et un calibrage des paramètres intrinsèques à la *Blockchain* en fonction de l'usage que l'on souhaite faire de celle-ci (taille des blocs, processus de création des blocs…).

De plus, elle s'avère très consommatrice en énergie. La consommation électrique actuelle du réseau Bitcoin est notamment équivalente à celle de 280 000 foyers américains.

La réglementation s'avère aussi être un obstacle, l'évolution rapide de la technologie et des cas d'usage amenant de nouvelles interrogations : application du processus KYC (*Know Your Customer*) ? Poids juridique d'un *smart-contract* ? Etc. Certains ministères et parlementaires français commencent à s'y intéresser sérieusement (cf. infographie p.6).

Rarement une technologie n'aura entrainé autant de réflexions. La *Blockchain* représente finalement très bien ce qu'est la transition digitale : des métiers, régulateurs, et spécialistes de l'IT qui réfléchissent ensemble à de nouveaux cas d'usage basés sur un nouveau concept technologique.

Matthieu GARIN
matthieu.garin@wavestone.com

Maxime ROCHE
maxime.roche@wavestone.com

RÉGLEMENTATION BLOCKCHAIN
en France

26 mars 2016

Bercy offre un cadre d'expérimentation de la Blockchain pour le financement des PME

Emmanuel Macron, ministre de l'Économie, de l'Industrie et du Numérique, annonce à l'occasion des Assises du financement participatif, une adaptation de la réglementation financière afin de permettre une expérimentation de la Blockchain concernant les bons de caisse et les minibons.

14 juin 2016

L'Assemblée adopte en 1ère lecture le texte de la **loi Sapin II**, habilitant le Gouvernement à prendre par ordonnance les mesures législatives nécessaires à un encadrement juridique de la technologie « Blockchain »

Sous l'impulsion de la députée Laure de la Raudière (Les Républicain - Eure et Loire), certains actes, comme les actions ou les obligations non-cotées, mais également les parts ou actions d'organismes de placement collectif, pourront utiliser la blockchain sur ordonnance.

24 juin 2016

700 millions d'euros débloqués pour la Blockchain dans le 3ème volet du Programme d'Investissement d'Avenir

L'action 9.5 du programme consiste à financer des projets entrepreneuriaux très ambitieux grâce à la structuration d'un fonds spécifique. La Blockchain est clairement identifiée comme une innovation qui bénéficiera de cet accompagnement avec plus de 700 millions d'euros débloqués.

08 juillet 2016

Le Sénat adopte avec modifications le projet de loi Sapin II et conserve l'habilitation par ordonnance du Gouvernement

Malgré la demande de suppression de l'amendement par le sénateur Pierre-Yves Collombat (RDSE), le texte est adopté et indique que "le Gouvernement est autorisé à prendre par voie d'ordonnance les mesures pour 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".

18 juillet 2016

Le Conseil Supérieur de la Propriété Littéraire et Artistique commande un rapport sur la Blockchain

Arbitrée par le ministère de la Culture, le CSPLA vient de commander un rapport d'étude explorant la Blockchain tout en analysant "les évolutions possibles en matière de contrôle de l'utilisation des œuvres, dans un environnement de services distants dématérialisés et un cadre européen et internationalisé". Le rapport consécutif à ces travaux est attendu pour le printemps 2017.

PEUT-ON AVOIR UNE CONFIANCE SANS LIMITE DANS LA BLOCKCHAIN ?

La garantie de confiance est bien souvent un argument lié à la *Blockchain*.

En effet, la *Blockchain* dispose de qualités sécurité intrinsèques : son caractère décentralisé et distribué permet une disponibilité forte du système, la traçabilité est assurée par la conservation de toutes les transactions dans le registre, et l'intégrité est garantie par les mécanismes cryptographiques.

Malgré tout, de plus en plus d'attaques sur des environnements *Blockchain* sont constatées, avec des fraudes s'élevant souvent à plusieurs dizaines de millions d'euros.

Mais alors, quel niveau de confiance peut-on vraiment accorder à cette technologie ? Décryptage des attaques visant la *Blockchain* et retour sur les mesures à prendre pour améliorer ce niveau de confiance.

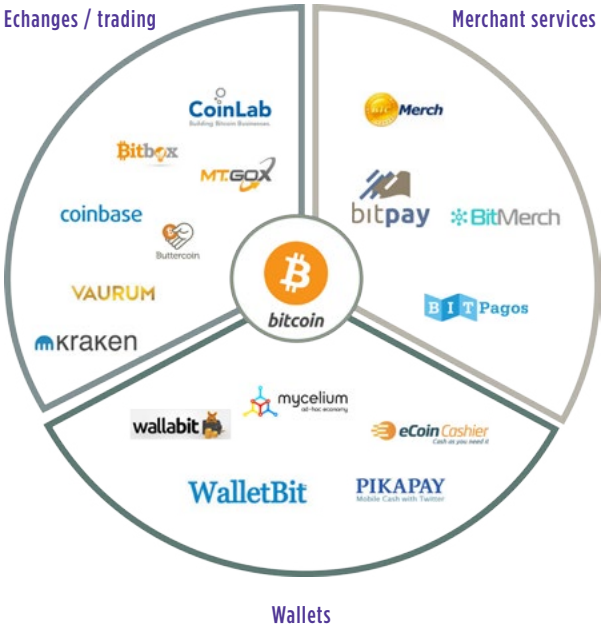
PROTÉGER LES SERVICES ET APPLICATIONS ACCÉDANT À LA *BLOCKCHAIN*

Un membre d'un réseau *Blockchain* est identifié grâce à une paire de clés cryptographiques : une clé privée, qui lui permet de signer ses transactions et de bénéficier des transactions reçues ; et une clé publique, qui permet aux autres membres du réseau d'identifier les transactions émises de sa part et de lui en transmettre. S'assurer de bien conserver et protéger sa clé privée est donc vital. Or, celle-ci est souvent stockée par son propriétaire sur son ordinateur ou téléphone, périphériques connus pour être aisément attaquables.

Aussi, de plus en plus d'utilisateurs choisissent de confier leur clé privée à des intermédiaires. Force est de constater que la plupart des attaques impactant Bitcoin ont en réalité directement ciblé ces plateformes intermédiaires. Il est donc primordial de protéger la manipulation des clés privées et plus globalement l'ensemble des services accédant au réseau *Blockchain*.

Dans le cas d'une *Blockchain* s'appuyant sur des smart-contracts, le niveau d'interaction avec l'extérieur du réseau peut être important, puisque ces derniers s'appuient sur la vérification de paramètres d'entrée, potentiellement externes au réseau. Il n'est alors plus question de sécuriser seulement les plateformes accédant à la *Blockchain*, mais également celles accédées par la *Blockchain* pour valider les conditions d'une transaction.

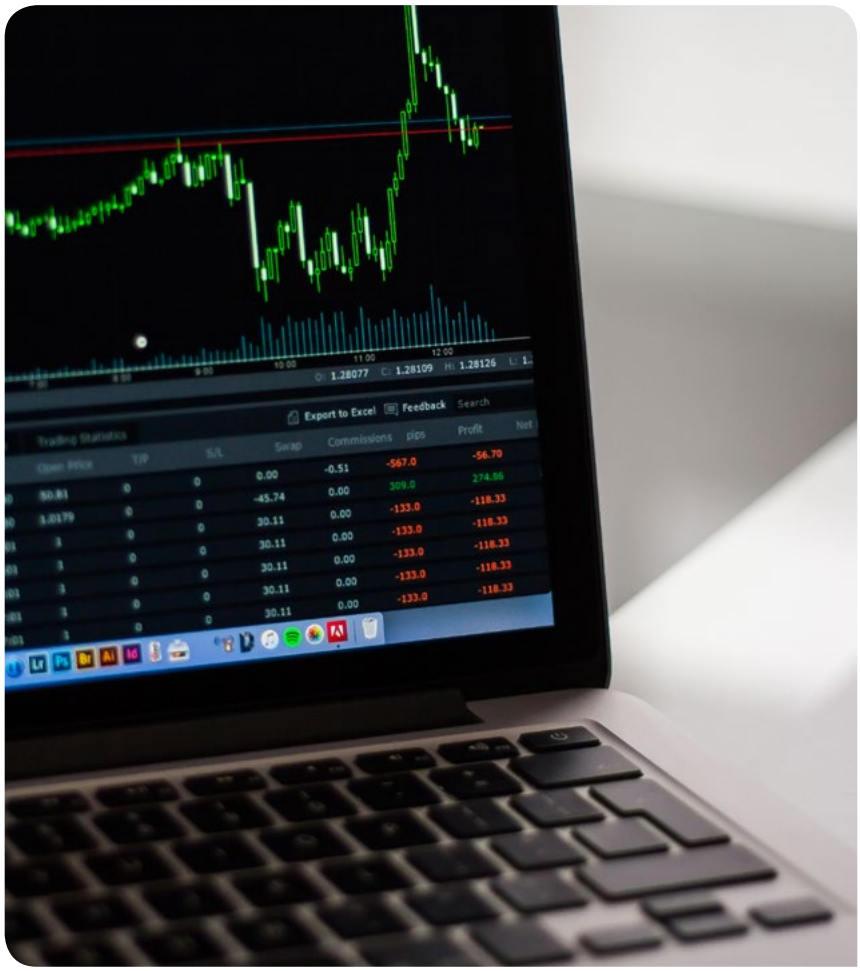
Écosystème Bitcoin : exemples de services accédant à la *Blockchain*



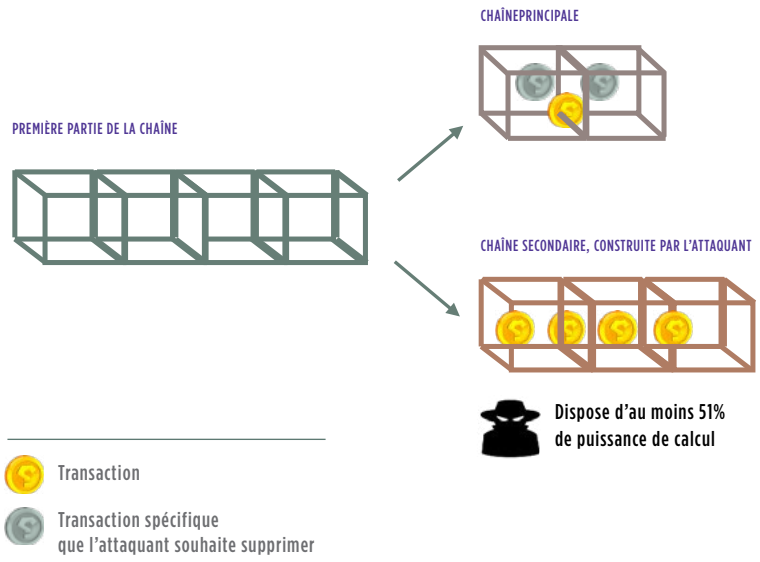
SURVEILLER LA PUISSANCE DE CALCUL DES MINEURS POUR ÉVITER UNE ATTAQUE 51%

L'attaque 51% consiste à avoir plus de 51% de la puissance de calcul du réseau dans le but d'annuler, ajouter ou modifier des transactions présentes dans un bloc. L'idée est de créer une chaîne alternative et plus longue que la *Blockchain* existante afin de la remplacer. Cela est rendu possible en exploitant un paramètre essentiel de la *Blockchain* : lorsque deux chaînes sont concurrentes, la chaine la plus longue est considérée comme la chaine légitime.

Ce risque est plus important dans le cadre de *Blockchain*s privées ou hybrides, composées d'un nombre restreint d'utilisateurs, et pouvant donc plus facilement représenter plus de la moitié de la puissance de calcul. Aussi, des mesures de sécurité doivent être mises en place pour prévenir et détecter ce type d'attaque : engagements contractuels, mécanismes de surveillance et de contrôle, etc.



Focus – L'attaque 51%, ou les limites du principe de consensus



EXPLICATION DE L'ATTAQUE 51%

Un attaquant souhaite réécrire la *Blockchain* afin d'annuler certaines transactions présentes dans un bloc

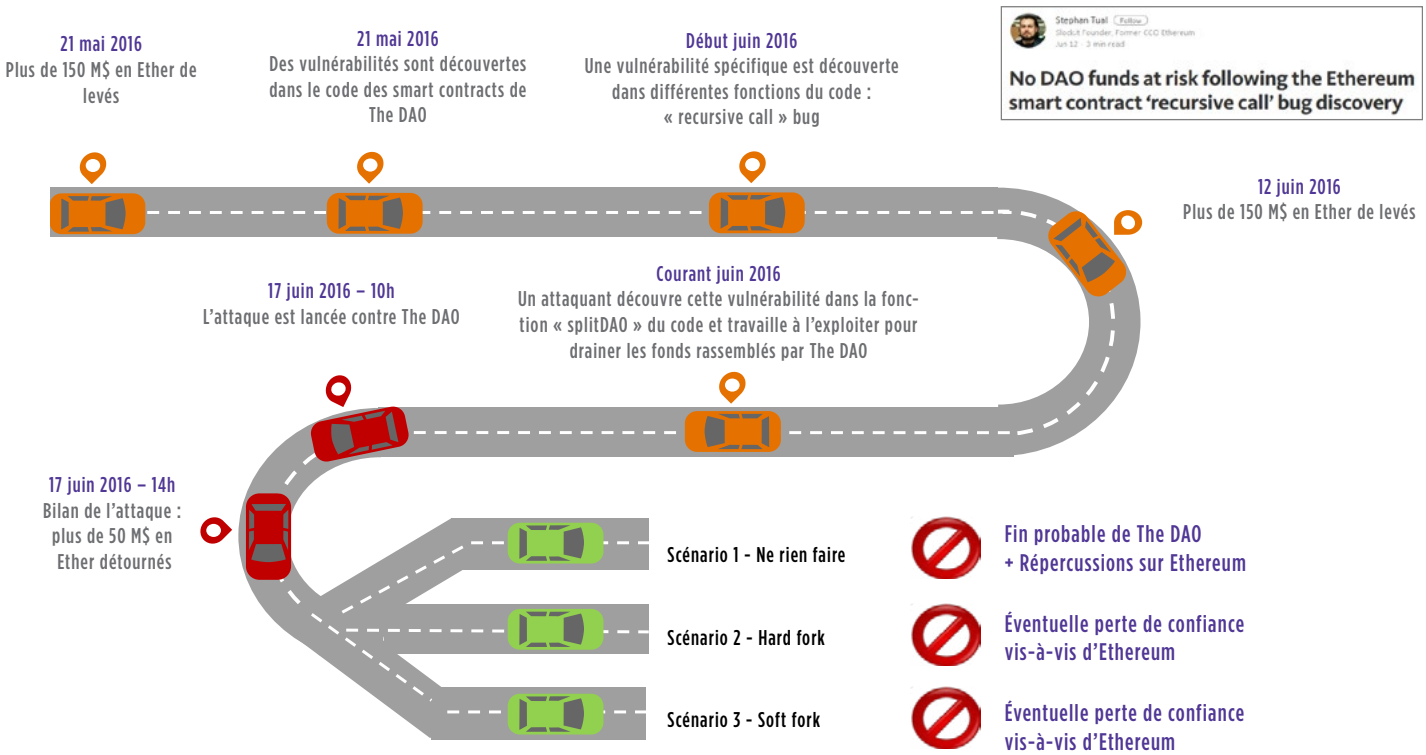
1. L'attaquant mine des blocs alternatifs, à partir du bloc précédent
2. L'attaquant publie sur le réseau la chaîne qu'il obtient dès lors qu'elle est plus longue que la chaîne existante (ce qui est possible car il possède plus de 51% de la puissance du réseau)
3. La chaîne étant plus longue, et exploitant le principe de consensus, elle remplace la chaîne existante et les transactions que celle-ci contenait sont annulées

SÉCURISER LE CODE DES *SMART-CONTRACTS*

Un *smart-contract* est un programme informatique inscrit dans une *Blockchain* et qui s'exécute de manière automatique une fois les conditions du contrat réunies.

Les conséquences d'une erreur de codage peuvent être catastrophiques et difficilement réversibles, comme en témoigne l'affaire *TheDAO* (application basée sur la *Blockchain* Ethereum et se présentant comme un fond d'investissement participatif et mutualisé). À partir d'une vulnérabilité découverte dans le code source du *smart-contract TheDAO*, un membre du réseau a pu drainer le compte principal de l'application à hauteur de 50 millions de dollars. Ces fonds furent en partie récupérés suite à une opération appelée « *hard fork* », s'apparentant à une attaque 51% concertée.

Retour sur l'affaire «TheDAO», application basée sur la plateforme Ethereum



En soi, ceci n'était pas une attaque car le contrat a été respecté, seule sa conception était défaillante. La création de cas d'usage basés sur des smart-contracts doit impérativement être associée à des mesures de sécurité applicative et un développement sécurisé.

Un système *Blockchain* est souvent considéré comme sécurisé par nature, mais les attaques présentées témoignent du contraire. La nature des plateformes accédant ou accédées par la *Blockchain*, la complexité des éventuels smart-contracts ou le nombre de mineurs du réseau sont autant d'éléments pouvant influer sur la sécurité du service fourni par la *Blockchain.*

Matthieu GARIN
matthieu.garin@wavestone.com

Stéphane GOMEZ
stephane.gomez@wavestone.com

UNE MISE EN APPLICATION CONCRÈTE DE LA BLOCKCHAIN

Interview avec Philippe RUAULT, Chief Innovation et Digital Officer chez BNP Paribas Securities Services

1.COMMENT AVEZ-VOUS PRÉVU D'UTILISER LA TECHNOLOGIE BLOCKCHAIN ?

Nous travaillons actuellement avec la société de crowdfunding SmartAngels sur la création d'une plateforme de gestion de titres basée sur la technologie *Blockchain*. Son objectif : permettre aux entreprises non côtées d'émettre des titres et aux investisseurs de pouvoir investir sur ces marchés secondaires. Son lancement est prévu pour octobre 2016.

2.POURQUOI LA BLOCKCHAIN EST-ELLE PARTICULIÈREMENT PROPICE À CET USAGE ?

La *Blockchain* est une technologie prometteuse et nous souhaitions rapidement mettre en œuvre un cas d'usage concret. Cette plateforme nous est apparue comme propice pour ce test «grandeur nature» : la traçabilité et la transparence de la *Blockchain* sont des atouts pour la tenue de titres, et les limites de la *Blockchain* en terme de performances ne constituent pas un frein (faible volume de transactions sur les marchés secondaires).

3.COMMENT AVEZ-PRIS EN COMPTE LES PROBLÉMATIQUES DE SÉCURITÉ ?

Notre plateforme se base sur une *Blockchain* privée, les mineurs étant connus et en nombre restreint. Pour l'instant, chaque client dispose de la même puissance de calcul, et il n'y a pas de rémunération spécifique pour les mineurs. Des mécanismes de sécurité classiques sont donc suffisants à ce stade : développement sécurisé, sécurité de l'infrastructure... Un potentiel changement de Business Model dans le futur (tel que la rémunération des mineurs) pourrait effectivement entraîner des mesures de sécurité complémentaires.

4.SELON VOUS, LA BLOCKCHAIN VA-T-ELLE IMPACTER PROFONDÉMENT LE SECTEUR DE LA FINANCE ?

La *Blockchain* possède des caractéristiques intéressantes et adaptées à tous les processus financiers d'échange d'actifs : traçabilité robuste, confiance dans le registre, etc. Cependant, ne nous emballons pas, il est essentiel de faire évoluer le cadre réglementaire et de travailler à l'amélioration de sa performance : il est actuellement impossible de réaliser les millions de transactions quotidiennes du secteur financier dans un système *Blockchain*.

PROPOS RECUEILLIS PAR EMILIE VAN LIERDE LE 10/06/2016

« La Blockchain possède des caractéristiques intéressantes et adaptées à tous les processus financiers d'échange d'actifs : traçabilité robuste, confiance dans le registre, etc. »

Responsable de la publication : Olivier Schmitt - Rédacteur en chef : Laetitia Mercier de Beaurouvre

Contributeurs : Anne GAUTRENEAU, Matthieu GARIN et Maxime ROCHE, Stéphane GOMEZ, Philippe RUAULT

Imprimeur : Jolly - l'impression

2016 I © WAVESTONE - ISBN : 978-2-918872-34-4 / EAN : 9782918872344

WAVESTONE

www.wavestone.com

Wavestone est un cabinet de conseil, issu du rapprochement, début 2016, de Solucom et des activités européennes de Kurt Salmon (hors consulting dans les secteurs retail & consumer goods).

Dans un monde où savoir se transformer est la clé du succès, l'ambition de Wavestone est d'apporter à ses clients des réponses uniques sur le marché, en les éclairant et les guidant dans leurs décisions les plus stratégiques.

Wavestone rassemble 2 500 collaborateurs présents sur 4 continents. Il figure parmi les leaders indépendants du conseil en Europe, et constitue le 1er cabinet de conseil indépendant en France.