WAVESTONE

RISKINSIGHT

LA LETTRE DES CONSULTANTS CYBERSÉCURITÉ ET CONFIANCE NUMÉRIQUE DE WAVESTONE

BLOCKCHAIN ENTRE RISQUE ET INNOVATION, TROUVER LE BON ÉQUILIBRE

SOMMAIRE

DOSSIER

LE BLOCKCHAIN, UN NOUVEAU MODÈLE DE CONFIANCE.....2

DÉCRYPTAGE

PEUT-ON AVOIR UNE CONFIANCE SANS LIMITE DANS LA BLOCKCHAIN ?..... 5

LA BLOCKCHAIN OU L'ILLUSTRATION D'UN MONDE QUI CHANGE ?.....9

A PROPOS DE WAVESTONE.....11

AGENDA.....11

EDITO

La *Blockchain* est présentée comme une technologie révolutionnaire pour la confiance numérique. Et elle l'est ! Les usages explosent, tous les secteurs d'activités s'en emparent. Ils inventent de nouveaux modèles et réalisent des tests. Parfois évidents, parfois étranges, voir inutiles, ces tests amèneront des innovations dans notre quotidien à moyen terme !

Les fondamentaux de la *Blockchain* sont théoriquement solides et reposent sur des mécanismes cryptographiques maitrisés depuis des années. Mais ces principes restent complexes et difficiles d'accès. En regard, leur principal point faible réside dans la manière dont l'implémentation de la *Blockchain* est réalisée. Des attaques récentes ont mis en lumière ces limites, en particulier celle visant la chaîne Ethereum et ses fameux « smart contracts ».

Cette lettre Risk Insight vise à décrypter ces évolutions et leur fonctionnement, à expliquer les risques et les attaques avérées pour vous permettre de trouver le bon équilibre entre risque et innovation !

Gérôme BILLOIS
Senior manager Cybersecurity & Digital Trust

LA BLOCKCHAIN : UN NOUVEAU MODÈLE POUR LA CONFIANCE ?

Qualifiée par certains visionnaires de technologie révolutionnaire (ou « disruptive »), 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 : près d'1 milliard de dollars aurait ainsi été levé sur les 3 dernières années, dont 500 millions de dollars en 2015 (source : Magister Advisors).

De nombreuses entreprises et administrations explorent actuellement les usages possibles de cette technologie prometteuse mais particulièrement complexe à appréhender pour les métiers. Pendant ce temps, le monde de l'IT s'approprie cette technologie : les grands acteurs du Cloud comme Microsoft, IBM ou Amazon précisent peu à peu des offres de *Blockchain-as-a-Service*, pendant que de nombreuses start-ups, comme Ethereum, innovent et proposent des usages particulièrement avancés de la *Blockchain*.

Pourtant, ce concept n'est pas nouveau : la *Blockchain* est en fait 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 et les risques sécurité à adresser pour qu'elle puisse se démocratiser ?

DES ALGORITHMES REMPLACENT LE TIERS DE CONFIANCE

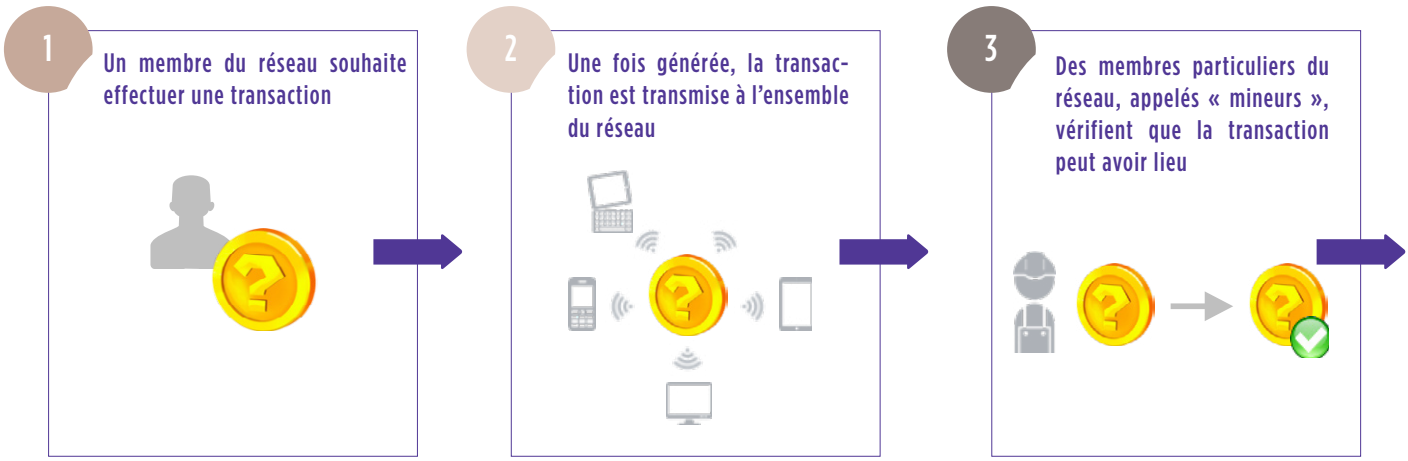
La *Blockchain* est une technologie qui permet aux membres d'un même réseau d'effectuer en toute confiance des opérations de stockage et de transmission d'informations, appelées « transactions », et ce en toute confiance, sans aucune autorité centrale de contrôle.

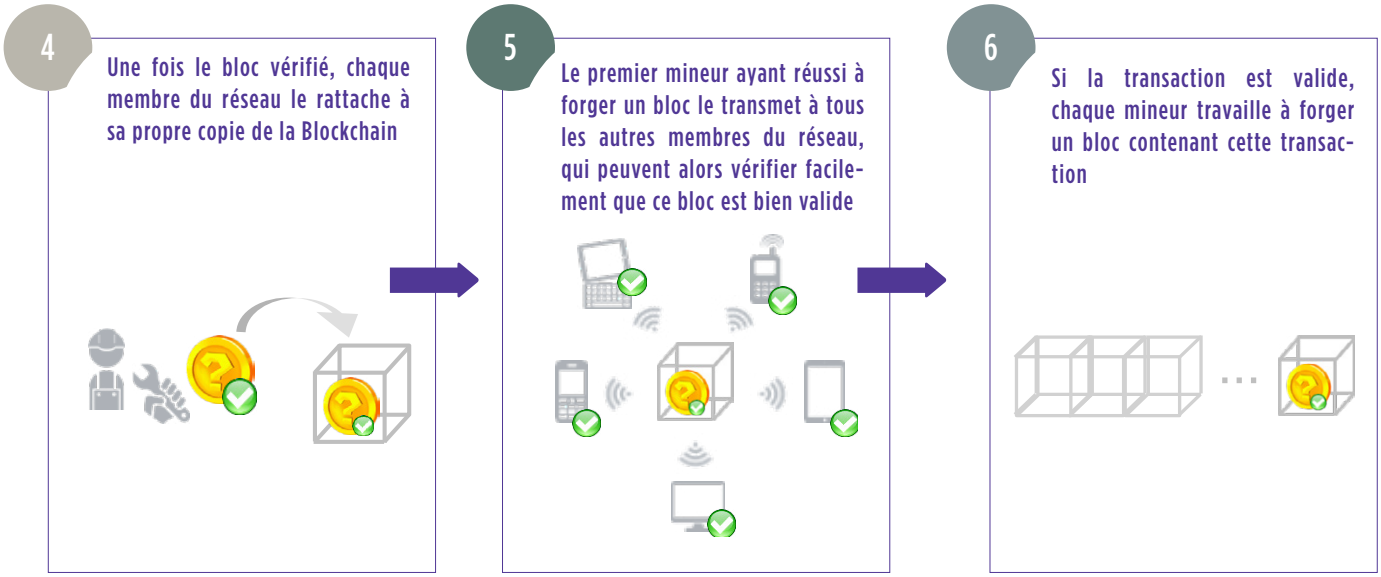
Cette technologie se présente sous la forme d'un registre contenant l'ensemble des transactions enregistrées depuis sa création (dans le cas de la *Blockchain Bitcoin*, il s'agit par exemple de l'intégralité des transactions financières effectuées depuis la création de cette crypto-monnaie). Ce registre dispose de 2 caractéristiques essentielles :

- **Il est distribué :** tous les membres du réseau disposent d'une copie du registre, rendant quasiment impossible la modification de ce registre 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 (dans le cas de la *Blockchain Bitcoin*, un bloc correspond à environ 10 minutes de transactions). Le schéma ci-dessous permet de comprendre la cinématique de création d'un nouveau bloc, et donc l'enregistrement d'une nouvelle transaction dans la *Blockchain*. Quel changement pour les entreprises ?

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, assurance, immobilier, santé, énergie, transport... tous les secteurs se sentent aujourd'hui 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 :** La *Blockchain* peut être utilisée comme simple registre de stockage pour déposer des données ou les empreintes numériques de documents dont on souhaite assurer de manière pérenne et sécurisée l'existence, la date de création et le droit de propriété, comme par exemple des brevets, des œuvres artistiques ou encore des données médicales. etc. Une fois ces données inscrites dans la *Blockchain,* elles sont distribuées à tous les acteurs du réseau et ne peuvent plus être effacées ni modifiées.

Exemple : En Afrique, près de 90% des territoires ruraux ne sont pas enregistrés dans un cadastre officiel fiable. Comment alors faire valoir son titre de propriété ou simplement disposer d'une adresse ? Pour résoudre les problèmes qui en découlent, l'ONG Bitland basée au Ghana s'est donnée pour mission de permettre aux personnes physiques et morales qui le souhaitent d'enregistrer leurs titres de propriété sur une *Blockchain,* faisant alors office de cadastre numérique.

2. **Digital transactions :** La *Blockchain* peut aussi être utilisée dans le cadre de transfert de valeur : transaction immobilière, *crowdfunding*... et bien entendu usage de crypto-monnaies (Bitcoin, Litecoin ou Dogecoin...). La *Blockchain* permet la traçabilité de chacune des transactions, et donc dans le cas d'une crypto-monnaie par exemple, la traçabilité du mouvement de chaque unité de monnaie depuis sa création jusqu'au dernier échange. Ainsi, les mineurs peuvent vérifier avant inscription d'une transaction dans la *Blockchain* que l'émetteur dispose des fonds nécessaires.

Exemple : SolarCoin est une crypto-monnaie basée sur un élément tangible : l'électricité de source solaire. Créée pour encourager la production d'énergie propre, elle permet à toute personne qui le souhaite d'être rémunérée en SolarCoin en fonction de l'électricité solaire que son installation photovoltaïque génère.

3. **Smart-contracts :** La *Blockchain* peut être également utilisée pour développer et stocker des smart-contracts, à savoir des contrats entre deux ou plusieurs parties. Il est rédigé sous forme de code informatique. Ce code est ensuite exécuté au sein des nœuds de la *Blockchain.* Une fois enregistrés dans le registre, ces programmes ne pourront plus être modifiés, et seront exécutés par la Blockchain sans intervention humaine selon les conditions et termes du contrat.

Exemple : Sur la *Blockchain Ethereum*, il existe par exemple des fonds d'investissement participatifs et mutualisés. Les membres votent pour des projets dans lesquels ils souhaiteraient investir et l'application, régie par des

smart-contracts, se charge alors automatiquement de répartir les fonds recueillis sur les projets les plus plébiscités, en fonction des règles prédéfinies dans les smart-contracts.

Les acteurs du monde de la finance s'intéressent tout particulièrement à la *Blockchain*. La start-up R3 a par exemple réuni un consortium composé des 50 plus grandes institutions financières mondiales autour d'un projet visant à développer des cas d'usages *Blockchain* dans le secteur de la finance et à définir des protocoles standardisés pour tous les marchés financiers internationaux. En France, la Caisse des Dépôts est à l'origine d'un « Laboratoire d'innovation » nommé **LabChain**, regroupant plus de 20 acteurs majeurs de la finance et autres start-ups, dont l'objectif est d'évaluer le potentiel des usages de la *Blockchain* tout en créant des synergies et initiatives de groupe sur le sujet.

Au-delà de ces consortiums, de nombreuses entreprises françaises mènent actuellement leurs propres initiatives. Le Crédit Agricole a par exemple mis en place un système sur sa plateforme CA-Store pour rémunérer en Bitcoin les développeurs qui participent à la création d'applications bancaires pour le groupe ; autre exemple, BNPP s'est donné pour objectif via un partenariat avec SmartAngels de développer une plateforme basée sur la *Blockchain* pour l'émission de titres et le crowdfunding des sociétés non cotées.

Force est de constater que la plupart des réflexions actuelles concernent des *Blockchains* privées (propre à une entreprise ou administration) ou hybrides (propre à un ensemble de partenaires). Or la *Blockchain* a été initialement pensée comme un système public : la confiance croît avec le nombre de membres du réseau. Les mécanismes techniques de la *Blockchain* devront donc être complétés afin de s'adapter à cette réalité : contrôle d'identité requis pour pouvoir intégrer le réseau, règles imposées aux partenaires, puissance limitée de calcul par mineur... Ces différents éléments doivent être définis pour chaque cas d'usage.

PERFORMANCE, ÉCOLOGIE ET RÉGLEMENTATION : LES OBSTACLES À SURMONTER

Jusqu'à très récemment, la seule application concrète de la *Blockchain* restait le Bitcoin. Pour donner un ordre de grandeur, 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.

Augmenter la taille des blocs, ou diminuer la difficulté du processus de construction des blocs, font partie des solutions étudiées pour pouvoir traiter plus rapidement les transactions. Mais toute modification de paramètre est sujette à compromis : par exemple, la construction d'un bloc est volontairement compliquée pour éviter que le réseau soit inondé de nouveaux blocs par plusieurs mineurs simultanément. 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.

En outre, la *Blockchain* s'avère très consommatrice en énergie : certaines études évaluent la consommation électrique actuelle du réseau Bitcoin à près de 350 mégawatts, soit l'équivalent de la consommation moyenne de 280 000 foyers américains. Ici encore, une solution pourrait être de diminuer la difficulté de construction des blocs (une très grande puissance de calcul est nécessaire, et plusieurs mineurs travaillent en parallèle). Toutefois, un tel changement ne serait pas sans impact sur la sécurité du système, nous le verrons par la suite.

Autre obstacle à ne pas négliger : la réglementation, alors même que la *Blockchain* trouve souvent son intérêt sur des activités régulées. Des premiers succès ont eu lieu ces dernières années, pour preuve l'application du processus KYC (*Know Your Customer*) aux principales bourses de crypto-monnaies, mais l'évolution rapide de la technologie et des cas d'usage amène de nouvelles interrogations. Tout particulièrement, quel est aujourd'hui le poids juridique d'un smart-contract ? A priori aucun, mais aucune jurisprudence n'existe à ce stade.

Rarement une technologie n'aura entrainé autant de réflexions, débats, interrogations... Certains ministères et parlementaires français commencent à s'intéresser sérieusement à la *Blockchain*. 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

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

Comme expliqué dans l'article précédent, la garantie de confiance est bien souvent un argument lié à la création de cas d'usage *Blockchain.*

En effet, la *Blockchain* dispose indéniablement 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 des transactions est garantie par les mécanismes cryptographiques.

Malgré tout, de plus en plus d'attaques impactant des environnements *Blockchain,* et pas uniquement le Bitcoin, sont constatées. Les fraudes récentes visant cette technologie, telles que TheDAO ou Bitfinex, s'élèvent très souvent à plusieurs dizaines de millions d'euros, montant comparable aux cyber-attaques bancaires les plus redoutables (Bank of Bangladesh, Carbanak...).

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

Chaque membre d'un réseau *Blockchain* est identifié grâce à une paire de clés cryptographiques : une clé privée, qui lui permet de signer les transactions effectuées et de « bénéficier » des transactions qui lui sont destinées ; et une clé publique, qui permet aux autres membres du réseau d'identifier les transactions émises de sa part et de lui transmettre d'éventuelles transactions de manière sécurisée. Pour illustrer avec l'image d'un coffre-fort, la clé privée permet de l'ouvrir d'en retirer le contenu. La clé publique, elle, permet uniquement d'ouvrir une trappe pour ajouter des éléments dans le coffre, comme une boîte aux lettres. Le propriétaire de la clé privée doit bien entendu se préoccuper de sa conservation et la soustraire à toute convoitise d'un potentiel attaquant. Ces clés sont usuellement stockées sur l'ordinateur ou le téléphone d'un utilisateur avec l'application qui lui permet d'accéder à la *Blockchain*. Et ces périphériques sont connus pour être facilement attaquables. Des codes malveillants spécifiques sont même apparus pour dérober ces clés.

Par ailleurs, de plus en plus d'utilisateurs choisissent de confier leur clé privée à des intermédiaires proposant des services tels que l'accès ergonomique au réseau Bitcoin. La plupart des attaques impactant le réseau Bitcoin n'ont en réalité pas ciblé le fonctionnement intrinsèque de la *Blockchain*, mais ont ciblé ces plateformes intermédiaires qui manipulent la clé privée de leurs clients. Nous pouvons par exemple citer les attaques ayant visé les services MtGox, Bitstamp, Bter, ou plus récemment Bitfinex.

Il est donc primordial de protéger la manipulation des clés privées (stockage, utilisation, échange, etc.), et plus globalement l'ensemble des services accédant au réseau *Blockchain.* C'est d'autant plus essentiel que l'annulation d'une transaction est en principe impossible : une fois inscrite dans une *Blockchain*, une transaction ne peut théoriquement ni être modifiée ni supprimée.

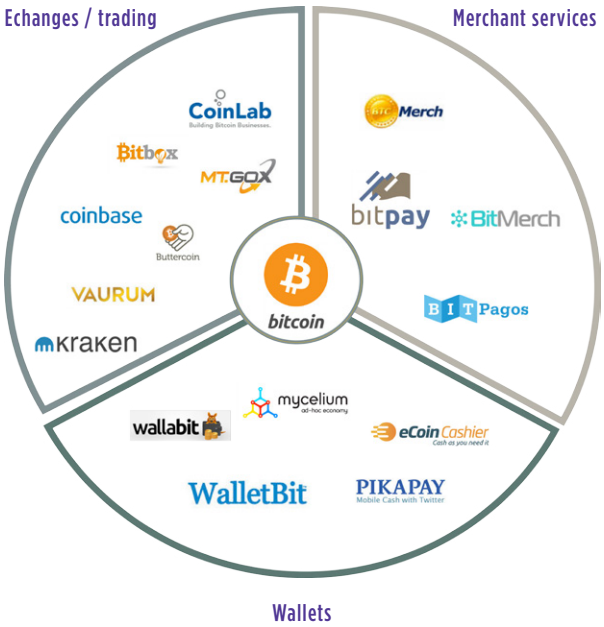
Dans le cas de *Blockchain* s'appuyant sur des smart-contracts, le niveau d'interaction avec l'extérieur du réseau peut être important. En effet, les smart-contracts s'appuient sur la vérification de « paramètres d'entrée », potentiellement externes à la *Blockchain*, permettant l'exécution du code informatique. Par exemple dans le cas d'un smart-contract « pari sportif » : la *Blockchain* vérifie les résultats d'un match sur le site « resultatsfoot.com » et effectue une transaction en conséquence. Une attaque sur le site « resultatsfoot.com » serait probablement plus simple qu'une attaque sur le réseau *Blockchain*.
Ainsi, dans le cadre d'une *Blockchain* s'appuyant sur des smart-contracts, une dimension supplémentaire doit être prise en compte : il n'est 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.

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

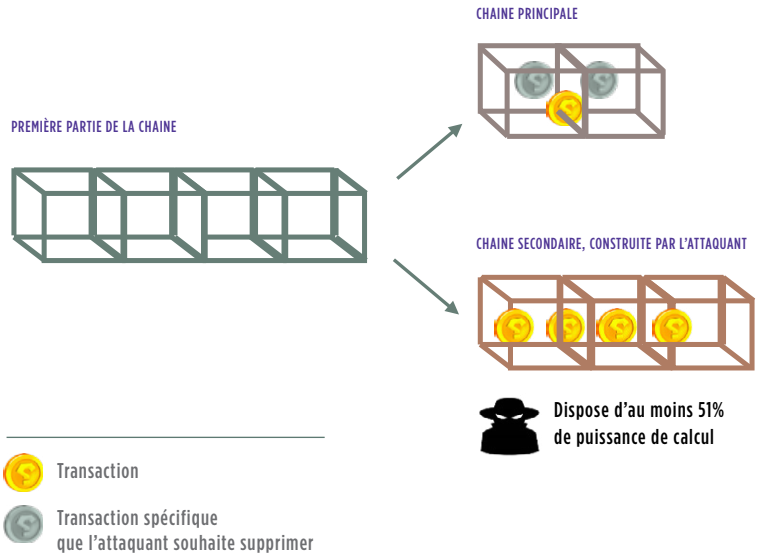
L'« attaque 51% », consiste à avoir la main sur plus de 51% de la puissance de calcul. Lors de la construction de la *Blockchain Bitcoin*, son créateur Satoshi Nakamoto l'avait d'ores et déjà identifiée : l'intégrité d'une *Blockchain* est garantie à condition qu'il n'y ait pas 51% de la puissance de calcul à la main d'une seule et unique personne, ou d'un groupe collaborant ensemble (source : https://Bitcoin.fr/public/Bitcoin.pdf).

Une fois ce niveau de contrôle atteint, les attaquants peuvent réécrire une partie de la *Blockchain* dans le but d'annuler, ajouter ou modifier certaines transactions présentes dans un bloc. Concrètement, un ensemble de mineurs s'accordent, repartent d'une version antérieure de la *Blockchain*, et minent une *Blockchain* alternative. Cette chaine alternative disposant d'une capacité de calcul supérieure va rattraper son retard et remplacer la chaine légitime, exploitant un paramètre essentiel de la *Blockchain* : lorsque deux chaînes concurrentes apparaissent sur le réseau, la chaine la plus longue est considérée comme la chaine légitime.

Écosystème Bitcoin : exemples de services accédant à la Blockchain



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

Pour pouvoir réaliser une telle attaque, l'attaquant doit disposer de plus de 51% de la puissance de calcul du réseau

Cette attaque n'est pas uniquement théorique. La plus grande coopérative de mineurs GHash.io a par exemple très fréquemment frôlé les 50% de puissance de calcul sur le réseau Bitcoin, alors que la crypto-monnaie Reddcoin a quant à elle véritablement subi cette attaque en 2014.

Des mesures de sécurité doivent donc accompagner la mise en place de toute Blockchain pour prévenir ou détecter les attaques 51%. Ce risque est d'autant plus important dans le cadre des *Blockchains* privées ou hybrides, composées d'un nombre restreint d'utilisateurs, pouvant donc plus facilement fournir plus de la moitié de la puissance de calcul.

Des engagements contractuels, et des mécanismes de surveillance et de contrôle doivent dans ce cas être mis en œuvre entre partenaires ou membres d'une *Blockchain* afin de ne s'assurer qu'aucune des parties prenantes ne dispose de plus de 51% de la puissance de calcul.

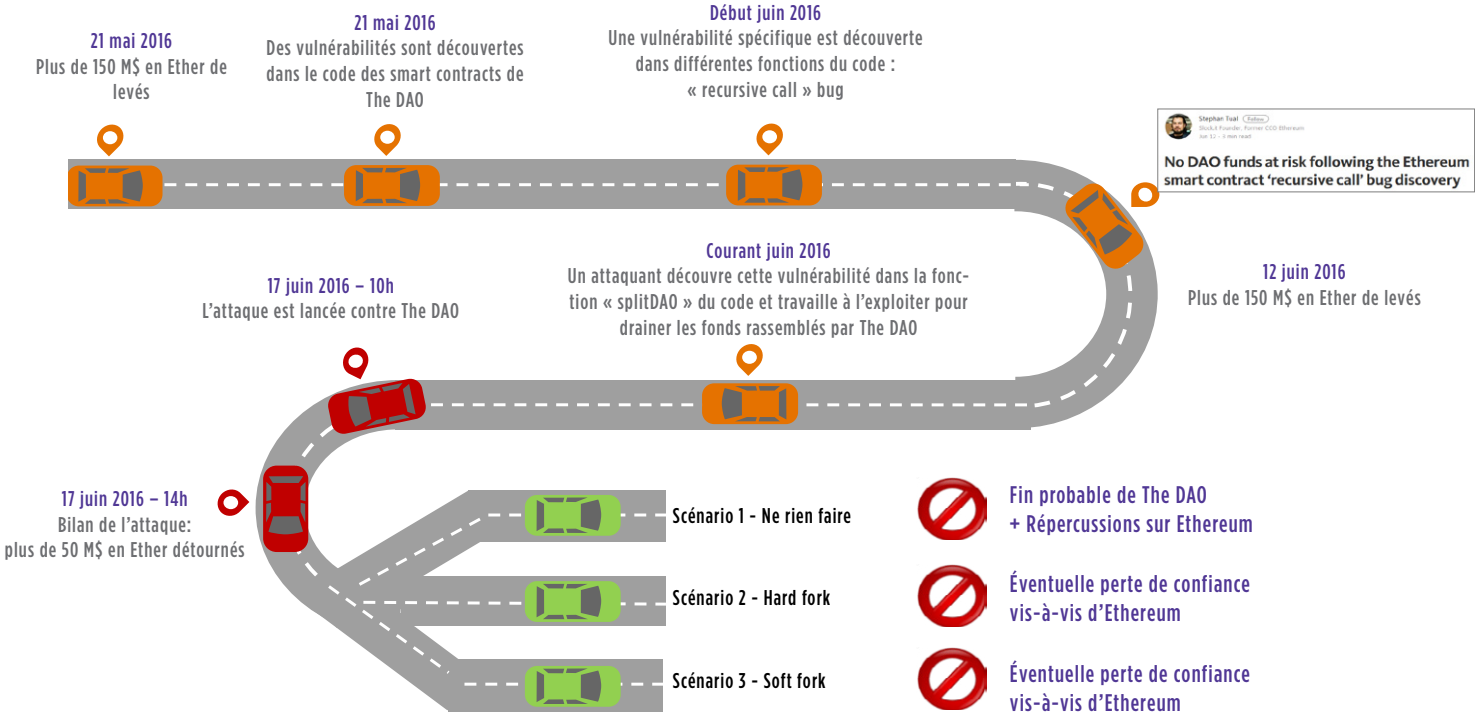
Notons que des modes de fonctionnement alternatifs de la *Blockchain* sont actuellement en cours de réflexion afin de lutter contre cette attaque 51%. Par exemple, le «*proof-of-stake* » est une méthode permettant de favoriser les mineurs « riches » en crypto-monnaie, a contrario du « *proof of work* », favorisant les mineurs disposant d'une puissance de calcul importante.

SÉCURISER LE CODE DES SMART-CONTRACTS

Les smart-contracts sont des programmes informatiques inscrits dans une *Blockchain*. Une fois inscrit dans la *Blockchain*, un tel programme ne peut pas être modifié, et sera exécuté de manière automatique une fois les conditions du contrat réunies.

Les conséquences d'une erreur de codage peuvent être catastrophiques et très difficilement réversibles, comme en témoigne la récente affaire « TheDAO », application basée sur la plateforme Ethereum. Dans ce cas précis, un membre de la *Blockchain* a découvert une vulnérabilité dans le code source du smart-contract TheDAO. En exécutant le smart-contract avec des paramètres particuliers, il 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 de la part des développeurs Ethereum, ayant mis en péril la *Blockchain* Ethereum (méthode appelée « hard fork » s'apparentant à une attaque 51% concertée).

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



Techniquement, il ne s'agit pas d'une attaque car le contrat a été respecté, c'est la conception du contrat qui avait été défaillante, et de nombreuses réflexions sont en cours quant à la réelle valeur juridique des smart contracts. Après tout, l'utilisateur a « simplement » exécuté un code informatique sur lequel tous les membres s'étaient accordés. Mais dans un objectif contraire à l'esprit du contrat… Concept qu'un code informatique ne sait pas évaluer ! De nombreuses réflexions sont en cours quant à la réelle valeur juridique des smart-contracts.

La création de cas d'usage basés sur des smart-contract doit ainsi impérativement être associée à des mesures de sécurité applicative : utilisation de frameworks sécurisés, sensibilisation des développeurs, revues de codes systématiques…

La *Blockchain* est une technologie récente, souvent considérée comme sécurisée par nature. Mais certaines attaques récentes témoignent du contraire et il est aujourd'hui indispensable de s'y pencher, d'autant plus que les mesures de sécurité à implémenter diffèrent selon le cas d'usage. La nature des plateformes accédants à la *Blockchain*, la complexité des éventuels smart-contracts ou le nombre de mineurs du réseau sont autant d'éléments de nature différente pouvant influer sur la sécurité du service fourni par la *Blockchain.*

Matthieu GARIN
matthieu.garin@wavestone.com

Stéphane GOMEZ
stephane.gomez@wavestone.com

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

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

Et les grandes innovations - celles qui modifient profondément la société - procèdent de la rencontre entre la technologie et un état de la société particulièrement réceptif. Sans ce paramètre sociologique qui donne sens et usage à la technologie, point d'innovation.

Le parallèle assez systématique qui est établi entre les prémisses de l'Internet grand public et la période actuelle d'effervescence autour de la *Blockchain* est révélateur de ce que beacoup pressentent comme la prochaine révolution numérique, disruption des transactions en écho à la disruption de l'information incarnée par Internet. Soit, non pas un nouveau catalogue d'usages émergeant à la faveur d'une évolution technologique, mais bien la promesse d'un changement plus radical de modèle de société. Ce changement étant rendu possible par la distribution de la confiance et, in fine, une désintermédiation plus ou moins importante des échanges de tout type.

Cette confiance distribuée qui singularise la *Blockchain* porte en creux une promesse d'horizontalisation de la société. En fonction des choix de gouvernance, publics et privés, nationaux et internationaux, qui seront faits, on pourrait assister à une redéfinition assez 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, entre précipitation et attentisme, adoption d'un modèle plutôt que d'un autre... dans le souci de faire partie du paysage de demain.

LA BLOCKCHAIN OU LA RÉPONSE TECHNOLOGIQUE AU DÉPORT DE CONFIANCE

En tant que technologie, la *Blockchain* apporte une réponse nouvelle à la décentralisation de registres et à l'automatisation de contrats, et en corollaire suscite naturellement des questionnements ayant trait à sa sécurisation et aux conditions de sa mise en œuvre à grande échelle. Ce qui n'est ni plus ni moins l'histoire naturelle des technologies émergentes : des espoirs plus ou moins exagérés et des obstacles à surmonter.

Originellement,la *Blockchain* est la technologie sous-jacente à l'échange de Bitcoins. Elle fut donc à ce titre le premier moyen de réaliser des transactions financières indépendamment de l'intervention des banques. Le contexte post crise financière de 2008 a son importance car l'initiative a rencontré son public et ses usages à la faveur d'un climat de perte de confiance envers les institutions financières traditionnelles. On observe aujourd'hui un report de la confiance, traditionnellement acquise aux institutions, vers des communautés d'utilisateurs/fournisseurs, dans un mouvement d'horizontalisation de la société. Le succès des plateformes en tout genre est un signal fort de ce mouvement. En effet, la confiance nécessaire avant de réaliser une transaction sur l'une de ces plateformes est désormais davantage conditionnée par les retours d'expérience de la communauté, via les systèmes de notation généralisés entre pairs, que par les autres formes de garanties.

Cependant, se pose toujours la question de la fiabilité de ce modèle de confiance communautaire : la notation à laquelle je me réfère est-elle le reflet d'une transaction réellement effectuée par l'acteur qui s'en réclame ? Cette transaction est-elle bien conforme aux caractéristiques affichées ? Comment être certain que l'information n'a pas été manipulée ? C'est dans ces questions que se niche la nouveauté de la proposition de valeur de la *Blockchain* et peut-être l'étape post plateformes : fiabilité et auditabilité distribuée via le consensus pour un modèle purement pair à pair. Dès lors que sont résolues ces questions, la disparition des tiers devient 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 forme de gouvernance à mettre en œuvre. Ainsi, tous les usages ne nécessitent pas de recourir à la « preuve de travail », qui implique une communauté importante et impose un coût énergétique plus que substantiel.

DES PROMESSES ET DES POSSIBLES

Dans le secteur marchand, les promesses d'automatisation laissent entrevoir des perspectives de réduction des coûts et de fluidité de certaines transactions dont pourraient bénéficier in fine les consommateurs, mais qui supposent également des acteurs commerciaux une capacité de transformation importante. On pense inévitablement au secteur des services financiers, déjà fortement chahuté par la concurrence des fintechs. Au-delà du seul sujet des crypto-monnaies, pour les banques, l'objectif consiste aujourd'hui à s'approprier la technologie, sans implémenter le modèle largement distribué sous-tendu par le Bitcoin, afin d'en tirer des bénéfices concurrentiels : offrir

aux clients des services à valeur ajoutée, par exemple des transferts d'argent ou de titres quasi-immédiats, moins chers puisque sans intervention humaine dans le processus, et défendre ainsi sa position de tiers et son avantage compétitif. Il en va de même pour les assureurs qui étudient opportunément les gains potentiels qu'offriraient la *Blockchain* grâce à l'exécution automatique de contrats d'assurance, ou encore la réponse qui pourrait être apportée aux problématiques de déshérence. On pourrait ainsi établir une liste infinie de secteurs et d'usages concernés, sans compter les usages qui émergeront demain et dont nous n'avons pas encore idée.

Cependant, il s'agit tout de même de rester prudent dans les projections commerciales autour de la *Blockchain.* Certains processus peuvent très bien être automatisés sans recours à la *Blockchain* et c'est bien une analyse technique et économique qu'il faudra réaliser pour effectuer le choix le plus pertinent. Dans la banque, par exemple, on peut d'ores et déjà automatiser avec profit un processus d'octroi de crédit sans *Blockchain*. En revanche on imagine des bénéfices complémentaires à disposer de moyens de dépôt de documents certifiés dans le cadre de ce processus, qui pourraient favorablement et à moindre coût être supportés par des mécanismes de *Blockchain*. C'est donc à une analyse à la fois globale et profonde, technique, métier et économique, qu'il s'agit de se livrer pour identifier les cas réels d'usage. Et, comme pour toute innovation, chercher le sens avant le modèle business.

La plupart des expérimentations en cours portent sur des *Blockchains* « privées » donc relativement en rupture avec le modèle originel de la *Blockchain* Bitcoin. Il convient d'être assez prudent sur ces choix de modèles et ne pas forcément se projeter radicalement dans l'un ou dans l'autre. En effet, si certains usages ne nécessitent pas forcément de recourir à une communauté large et diversifiée de mineurs, ni de mettre en œuvre la preuve de travail pour garantir la transaction, on peut également, en caricaturant quelque peu, se demander s'il s'agit dans ce cas d'un usage spécifiquement lié à la *Blockchain* ? Cependant, on sait aussi que les expérimentations vont apporter du recul sur le sujet et les investissements colossaux qui sont consentis actuellement vont sans doute permettre de se forger des convictions, si ce n'est voir un acteur ou un modèle s'imposer. Les différentes pistes étudiées et expérimentées actuellement sont prometteuses, elles témoignent d'une considérable énergie collective sur le sujet et laissent entrevoir des promesses de gains tant pour les entreprises que pour les consommateurs. Pour autant, la promesse de désintermédiation « absolue » ou l'uberisation des plateformes n'en sera pas forcément la résultante.

Dans le secteur non-marchand, qu'il s'agisse du domaine de l'État ou de la société civile, les promesses sont multiples et rencontrent des aspirations assez profondes des citoyens à davantage d'horizontalité, comme en témoignent le nombre grandissant et le succès des initiatives collaboratives, de même que les expériences à plus ou moins grande échelle de démocratie participative.

L'État se trouve tout à la fois dans une position de potentiel utilisateur, promoteur, maître d'œuvre et régulateur de la *Blockchain.*

- Utilisateur dans le cadre d'automatisations de mécanismes transactionnels complexes et coûteux, on peut notamment penser à des usages pour l'administration fiscale, mais également pour tout ce qui relève de l'accès aux droits.
- Promoteur dans l'accompagnement des initiatives publiques et privées, soutien à un écosystème français dynamique.
- Maître d'œuvre et régulateur d'une future *Blockchain* publique, porteur d'un modèle fonctionnel de gouvernance à l'échelle nationale et internationale.

La société civile n'est pas en reste et trouve dans la *Blockchain* un moyen idéal de mettre en œuvre de nombreux projets collaboratifs nés du modèle des communautés et donc nativement adhérents au concept de confiance distribuée. Le vaste domaine de l'échange de biens et services entre particuliers pourrait parfaitement opérer un glissement d'un modèle commercial de type plateforme vers un modèle purement associatif tendant vers un coût minimal pour l'usager/membre. Reste à savoir si le consomm'acteur, séduit par ce modèle, serait prêt à consentir une expérience transactionnelle plus dépouillée. On a du mal à projeter un parcours client très riche dans ce type de modèle, sauf à tabler sur une communauté de développeurs dévouée, ce qui n'est au demeurant pas exclu. Par ailleurs, il semble complexe de projeter un usage massif ou d'élargir le concept à une activité nécessitant une prise en charge des risques. L'autre principale promesse de la *Blockchain* à la société civile concerne toutes les possibilités relatives à une expression démocratique plus directe, notamment via les systèmes de votes qui sont explorés par différent pays actuellement. Plus proche encore, on songe aux polémiques qui ont pu naître sur la fiabilité et la légitimité des systèmes de pétitions en ligne et on peut tout à fait imaginer le rôle positif que pourrait jouer une implémentation *Blockchain* d'un système de pétition pour garantir à la fois la pétition et les pétitionnaires.

La *Blockchain* présente donc un intérêt à la fois pour la sphère privée et la sphère publique, reste à déterminer s'il s'agira en cible d'une *Blockchain* et de ses instanciations ou de la coexistence de différents modèles.

UNE INNOVATION DE RUPTURE QUI SE CHERCHE UN MODÈLE DE GOUVERNANCE

Ce rapide et non-exhaustif tour d'horizon permet de mesurer l'étendue et la profondeur des implications de l'avènement des *Blockchains*. Guy Kawasaki, éminent spécialiste de l'innovation, rappelait fort justement dans son intervention à la TED Conférence de Berkeley en 2014 les caractéristiques d'une grande innovation, entendons par là de celles qui changent le monde :

- Profondeur ;
- Intelligence ;
- Globalité ;
- Empowerment ;
- Élégance.

À coup sûr les *Blockchains* sont porteuses de ces attributs. Il est certain également que la multiplicité des opportunités ne trouvera à s'exprimer concrètement que dans une configuration où acteurs privés et publics s'emparent du sujet dans une approche ouverte et pluridisciplinaire. De là pourront émerger un ou plusieurs modèles de gouvernance qui permettront aux nouveaux usages de s'épanouir pour le bénéfice du plus grand nombre.

Anne GAUTRENEAU
anne.gautreneau@wavestone.com

A PROPOS DE WAVESTONE

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

La mission de Wavestone est d'éclairer et guider ses clients dans leurs décisions les plus stratégiques en s'appuyant sur une triple expertise fonctionnelle, sectorielle et technologique.

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

Avec plus de 400 consultants, Wavestone détient la force de frappe la plus importante en EMEA en matière de cybersécurité et de confiance numérique.

AGENDA

05-08.10.2016
Les Assises de la Sécurité : Après le château et l'aéroport, quel modèle de sécurité pour 2020 ? (Monaco)

17-18.11.2016
Conférence Zero Night : Big Data (Moscou)

25-26.01.2017
Forum International de la Cybercriminalité (Lille)

Venez découvrir nos expertises
RISK INSIGHT

@Risk_Insight

Responsable de la publication : Frédéric Goux
Rédacteur en chef : Gérôme Billois
Contributeurs : Matthieu Garin, Maxime Roche,
Stéphane Gomez, , Anne Gautreneau
Imprimeur : Axiom Graphics
ISSN 1995-1975

WAVESTONE

www.wavestone.com

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

La mission de Wavestone est d'éclairer et guider ses clients dans leurs décisions les plus stratégiques en s'appuyant sur une triple expertise fonctionnelle, sectorielle et technologique.

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