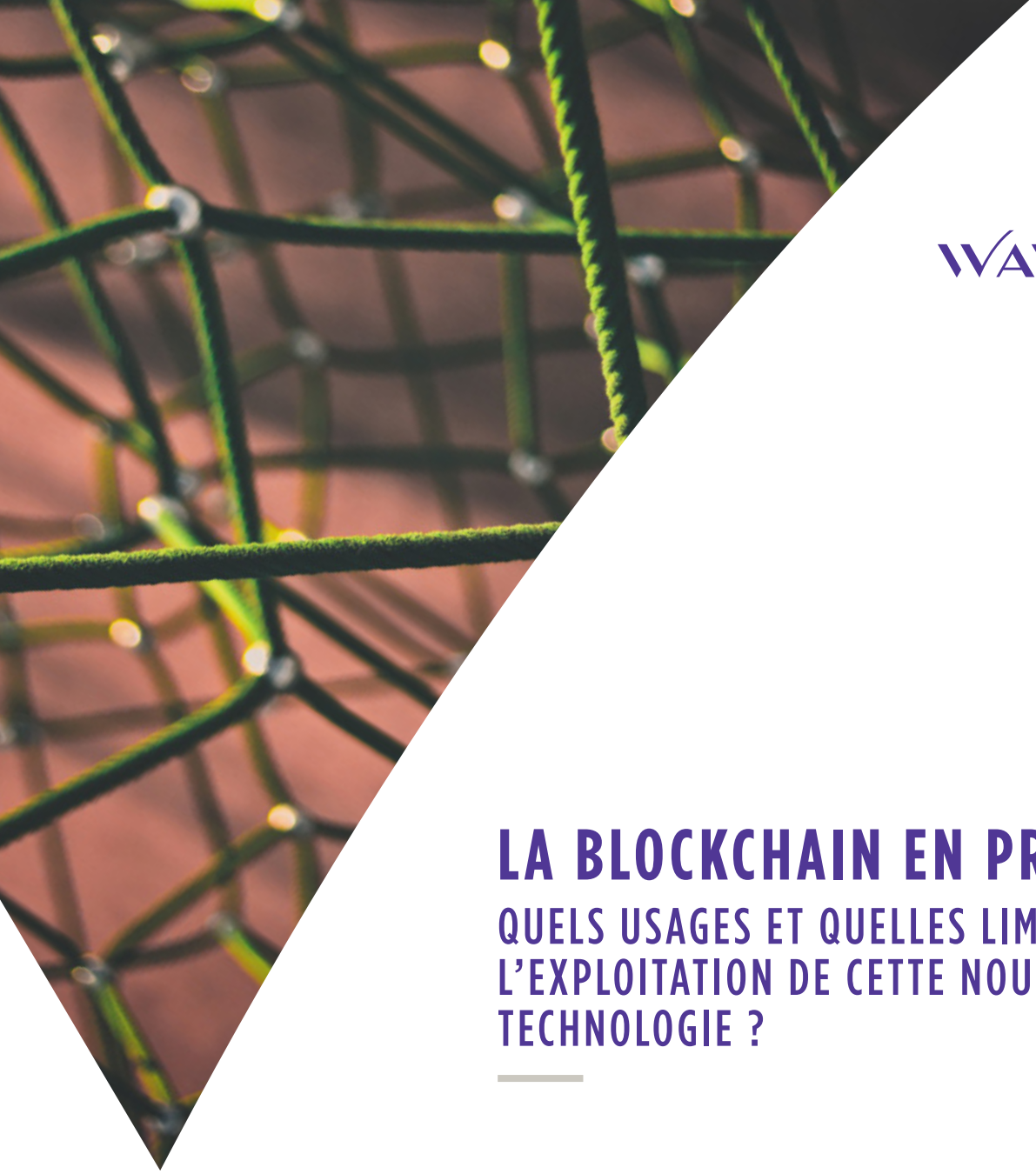


WAVESTONE

LA BLOCKCHAIN EN PRATIQUE

QUELS USAGES ET QUELLES LIMITES POUR L'EXPLOITATION DE CETTE NOUVELLE TECHNOLOGIE ?

Les services financiers et en particulier le secteur de l'assurance sont identifiés comme étant les marchés à plus fort potentiel pour l'utilisation de la Blockchain.

Les assureurs en ont bien conscience et sont d'ailleurs parmi les plus avancés dans leurs recherches sur cette technologie. Un sondage réalisé par le MEDEF en mai 2017 montre que l'intérêt des financiers et des assureurs pour la Blockchain est bien réel : 74% des décideurs expriment un intérêt fort pour cette technologie, et 76% souhaitent réaliser un test pilote Blockchain.

De par son fonctionnement, la Blockchain est à l'opposé de nombreuses technologies traditionnelles et nécessite de nouvelles compétences techniques pour appréhender tout son potentiel. Chez Wavestone nous avons étudié la Blockchain et avons construit des POC (Proof of Concept) pour mieux appréhender les concepts qui sont totalement nouveaux, en mesurer le potentiel et les limites structurelles ou conjoncturelles.

CONTACTS

LAURENCE AL NEIMI
laurence.alneimi@wavestone.com

NICOLAS MAI
nicolas.mai@wavestone.com

Cette publication a été réalisée avec les contributions de Islem BEN TAHER et Arnaud CHIKHANI.

POTENTIELS OU LIMITES ?

Grâce à des concepts technologiques innovants, la Blockchain présente un très fort potentiel pour les assureurs au travers de 3 familles d'usages : le record keeping, le transactionnel et les smart contracts..

/ **Record Keeping**
Cette fonctionnalité répond à un besoin pour des parties de conserver un historique, elle permet d'en stocker la référence de façon transparente dans un registre inaltérable.
Cette fonctionnalité permet à tous les acteurs de l'Assurance d'avoir accès instantanément aux mêmes informations infalsifiables, mises à jour en temps réel, garantie de traçabilité et d'efficacité.

/ **Transactionnel**
Chaque participant du réseau ayant une vue complète de l'historique des transactions, authentifiées et tracées, la Blockchain permet d'effectuer des transactions numériques dans un réseau peer-to-peer, notamment entre partenaires de l'écosystème assurantiel. Cette fonctionnalité ouvre des applications en matière de paiement ou de logistique.

/ **Smart contracts**
La Blockchain permet de stocker et faire fonctionner des smart contracts qui exécutent automatiquement du code stocké au préalable. Cela ouvre la voie à l'automatisation de processus comme l'indemnisation de sinistre, possiblement déclenchée par des données externes, délivrées par un oracle, tiers de confiance.

Immaturité de la technologie

Le déploiement à grande échelle constitue aujourd'hui un défi technologique. Si les expérimentations fonctionnent bien dans un environnement maîtrisé avec un nombre contrôlé de participants ; des difficultés se posent pour un usage à grande échelle.

Par ailleurs, il faut garder à l'esprit que le coût de minage (puissance de calcul x coût de traitement) d'un bloc augmente avec la taille de la blockchain, ne garantissant pas la pérennité des activités de minage. **Sur la Blockchain Bitcoin**, la difficulté pour trouver un nouveau bloc a été multipliée par 7 sur l'année écoulée[1], alors même que les frais de transaction des mineurs (en équivalent USD) sont restés sensiblement les mêmes sur la période[2]. D'une manière générale, le coût unitaire par transaction (revenu total des mineurs / nombre de transactions) a été multiplié par 10 en un an[3].

La conséquence de cette technologie naissante manipulant des concepts nouveaux est la difficulté à l'appréhender sur l'ensemble des dimensions technologiques, mais aussi ergonomiques pour présenter un parcours client simple et attractif. A ce jour, peu d'experts maîtrisent cette double compétence.

Nous notons que le développement des usages de la Blockchain passe actuellement majoritairement par des start-ups. En 2017, 70% des investissements réalisés dans la Blockchain ont bénéficié à ces dernières.

Enfin, s'il s'agit de tester et comprendre la technologie Blockchain, le cas d'usage importe peu. Par contre, pour un projet visant une industrialisation, la pertinence est structurante, notamment au regard des solutions traditionnelles. Pour s'en assurer, nous avons établi un **double filtre Wavestone®** pour conforter l'adéquation d'un projet Blockchain. Y soumettre l'idée permet de challenger le cas d'usage.

Le double filtre Wavestone® permet d'évaluer la pertinence des cas d'usage Blockchain

1/Les caractéristiques de la Blockchain sont-elles bloquantes pour certains usages?

Les consensus de distribution, l'unicité et l'incorruptibilité, caractères intrinsèques de la Blockchain peuvent-ils empêcher son application dans certains cas d'usage ?

Distribution
L'information est partagée entre l'ensemble des parties prenantes, impliquant une transparence de l'information

Unicité
La Blockchain assure l'unicité des règles et de l'information

Incorruptibilité
Les informations ne sont ni modifiables, ni effaçables

2/La Blockchain est-elle la meilleure solution disponible à date ?

L'enthousiasme suscité par la Blockchain doit être modéré par trois facteurs d'incertitude qui peuvent rendre son implémentation complexe :

Volumétrie de la participation
La résilience de la Blockchain est proportionnelle au volume de participants et d'activité

Défiance envers les tiers
Un transfert du pouvoir vers un système algorithmique conçu par des développeurs

Motivation économique
Contrairement aux systèmes centralisés, la participation même au réseau nécessite un investissement

1 : Source Blockchain.info (mars 2018) : https://blockchain.info/fr/charts/difficulty?timespan=1year
2 : Source Blockchain.info (mars 2018) : https://blockchain.info/fr/charts/transaction-fees-usd?timespan=1year
3 : Source Blockchain.info (mars 2018) : https://blockchain.info/fr/charts/cost-per-transaction?timespan=1year

Des risques entourant la technologie

L'ensemble de la Blockchain est vulnérable en plusieurs endroits, méritant une forte attention. Trois risques majeurs fragilisent particulièrement le dispositif.

/ **La qualité du code des smart contracts :** A la différence d'un programme classique, un smart contract est inaltérable. Sa programmation est donc critique. Une faille dans l'algorithme permet de les altérer ou d'en détourner aisément le fonctionnement.

/ **La gouvernance de la Blockchain :** le regroupement des mineurs en ferme de minage peut être à l'origine d'une concentration du contrôle. Entre le 20 décembre 2017 et le 20 mars 2018, 3 fermes chinoises concentraient 56% de la puissance de calcul de la blockchain Bitcoin...

/ **L'écosystème de la Blockchain :** la vulnérabilité des oracles, clés privées facilement attaquables, permettent ainsi une propagation des attaques à la Blockchain.

Un cadre réglementaire en construction

La France cherche à figurer parmi les pays précurseurs, ainsi l'ordonnance du 28 avril 2016 a mis en place les dispositions de l'article L. 223-12 du code monétaire et financier permettant de recourir à un « dispositif d'enregistrement électronique partagé » (DEEP) ainsi définis pour désigner la technologie Blockchain, pour les transactions de mini-bons. Puis, la loi n°2016-1691 du 9 décembre 2016 dite loi Sapin 2 a permis par voie d'ordonnance d'introduire la Blockchain dans le droit applicable aux titres financiers et aux valeurs mobilières. Enfin, avec l'ordonnance n° 2017-1674, publiée le 9 décembre 2017, Paris devient la première place financière en Europe à définir un cadre pour le transfert de propriété de titres financiers par DEEP, reste au Conseil d'Etat à fixer les conditions applicables à l'inscription de titres financiers dans un DEEP, qui interviendront par décret.

Cependant, pour aller plus avant dans les étapes de la régulation, il est nécessaire de disposer d'une excellente compréhension des concepts technologiques et des usages innovants. De la même façon, par le passé, Internet est également resté dérégulé lors des premières années.
Conscient de ce préalable, le législateur laisse place aux expérimentations, auxquelles il prend lui-même part.

En février 2018, l'Assemblée Nationale a lancé 2 missions d'information. La première se concentre sur les usages qui ne sont pas directement liés aux cryptomonnaies. La seconde se focalise, elle sur les cryptomonnaies ou cryptoactifs. L'enjeu est de trouver le juste équilibre entre régulation et interdiction, et d'adapter le cadre législatif français aux nouvelles habitudes financières des consommateurs et des entreprises.

Dans le même temps, Jean-Pierre Landau, ancien sous-gouverneur de la Banque de France, pilote une mission chargée de proposer des orientations sur l'évolution de la réglementation sur les cryptomonnaies en 2018.

Avec ce dispositif, les données personnelles ne sont pas littéralement effacées, mais leur accès est rendu impossible et illisible.

LA BLOCKCHAIN ET RGDP ?

Le caractère immuable de la Blockchain présente une incompatibilité de principe avec le Règlement Général sur la Protection des Données (RGPD) applicable en mai 2018, en particulier avec l'article 17 consacré au droit à l'effacement des données personnelles.

A priori, du fait de ce caractère inaltérable, traiter des données personnelles dans une blockchain publique ou privée serait contraire au règlement. Une solution de contournement a été mise en place par plusieurs start-up comme BCDiploma qui stocke et certifie des diplômes. Cette solution vise à chiffrer les données grâce à trois clés : une pour l'étudiant, une persistante et une permanente pour l'établissement. La donnée chiffrée ne peut être lue qu'avec la possession de ces trois clés. Pour rendre impossible l'accès aux données personnelles, il suffit à l'étudiant stockant ses données personnelles de demander à l'établissement de supprimer la clé de persistance.

C'est à ce type de problématique que le futur cadre règlementaire doit répondre.

DU PROTOTYPE A LA REALITE : QUELLE ORGANISATION POUR DEVELOPPER UN PROJET TOUT EN MAITRISANT L'INVESTISSEMENT TECHNOLOGIQUE ET HUMAIN ?

Du fait de la nouveauté de cette technologie et du peu de recul sur son potentiel ainsi que de l'encadrement réglementaire en évolution, il convient d'adapter son mode de fonctionnement par rapport à un projet traditionnel.

Industrialisation

La phase d'industrialisation doit se faire en s'appuyant sur des expérimentations préalables et en travaillant main dans la main avec le régulateur. Les POC et expérimentations doivent servir notamment à anticiper d'éventuelles difficultés de mise en œuvre.

Il faut veiller à s'inscrire dans le cadre législatif existant, et dans la mesure du possible anticiper le cadre à venir afin de ne pas se trouver en porte à faux avec la réglementation.

L'idée est d'intégrer le régulateur dans les cycles d'industrialisation pour accompagner les prises de décision structurantes.

Dans l'hypothèse du retrait ou du silence de celui-ci, une piste pour estimer le cadre législatif à venir est de s'interroger sur la volonté du régulateur : est-il dans une optique de protection du consommateur ? Veut-il promouvoir la concurrence en encadrant souplement les technologies Blockchain utilisées ? Vise-t-il à un équilibre entre les solutions traditionnelles et des solutions disruptives ? Quelles sont les positions des régulateurs au niveau international ?

On peut aussi obtenir un faisceau d'indices en analysant les différentes dérives : y a-t-il eu de mauvaises expériences avec la Blockchain qui conduiraient le régulateur à un encadrement plus strict ?

WAVEVOTE®, APPLICATION DE VOTE EN LIGNE SUR ETHEREUM

Afin d'expérimenter sur cette nouvelle technologie, le cabinet Wavestone a développé un démonstrateur de vote en ligne basé sur la Blockchain Ethereum. Le principal objectif était de se confronter aux contraintes techniques et fonctionnelles afin de pouvoir conseiller au mieux nos clients dans leurs propres expérimentations.

Pour des soucis d'ergonomie, ce démonstrateur est transparent ; il masque à la fois la complexité de la Blockchain et la cryptographie.

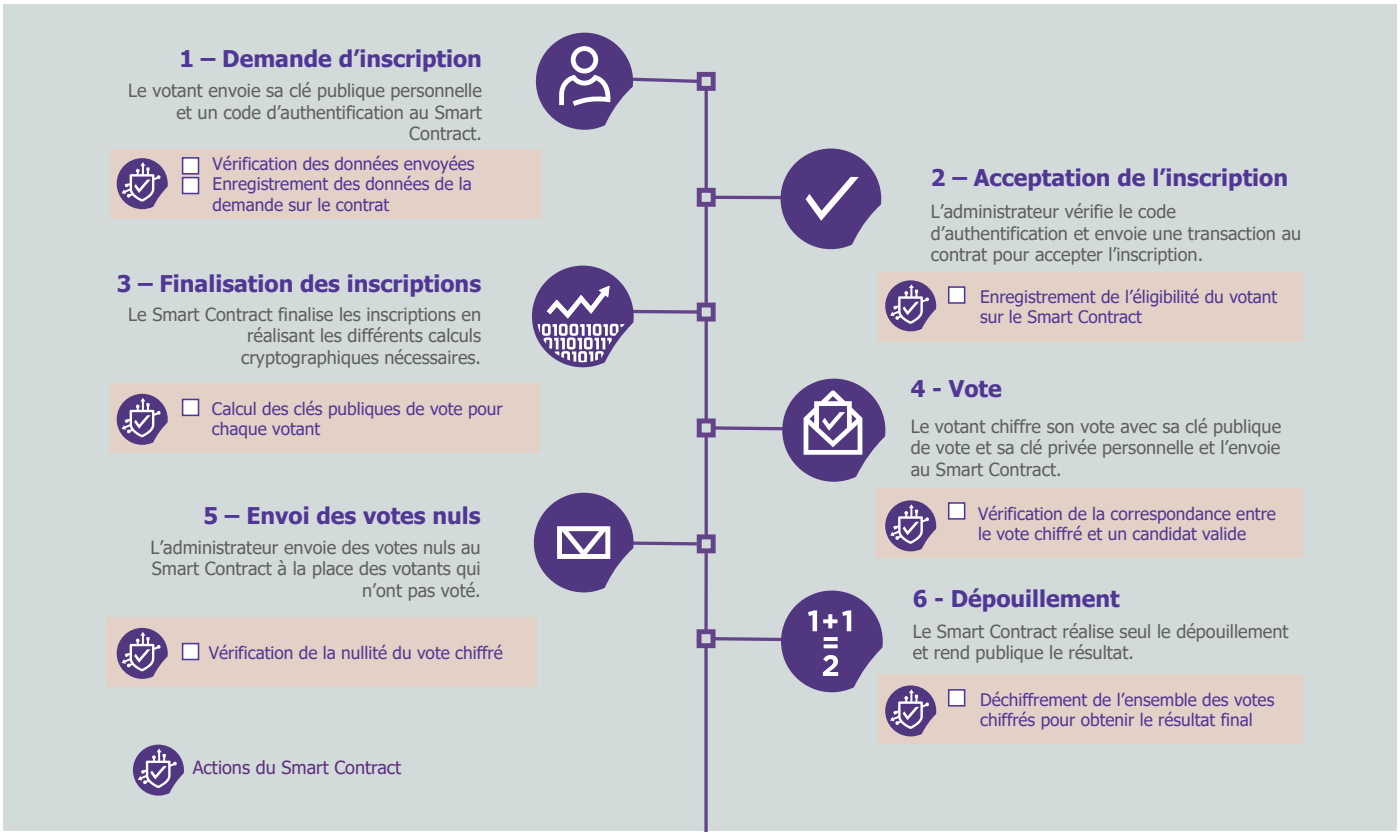
Les chiffres clés du POC

- **0** Coût de vote, hors charge de création de l'application et hébergement (serveurs)
- **1** Blockchain privée
- **2** Principales compétences techniques : back end (solidity, blockchain) et front end (interface)
- **4** Mois de développement

Pour être pertinent, le POC doit répondre à différentes contraintes pour assurer la qualité du vote

WaveVote®, application de vote en ligne sur Ethereum

Déroulement simplifié du démonstrateur WaveVote®



Contraintes et difficultés rencontrées lors du développement de WaveVote®

Dans sa configuration actuelle, l'application de vote ne pourrait pas être mise à grande l'échelle, par exemple pour des élections nationales. Il fait en effet, face à un dilemme entre Blockchain publique et Blockchain privée :

1 Publique pour la transparence du vote

Tout citoyen doit pouvoir contrôler et confirmer les résultats du vote. Cette transparence lors du dépouillement n'est pas possible dans une Blockchain privée où seule l'administration aurait accès aux résultats. Une Blockchain publique résout ce point.

2 Privée pour des limites techniques

Les opérations de fonctionnement du vote (non sécables) sont trop lourdes pour être intégrées dans des blocs classiques. L'administrateur d'une Blockchain privée peut choisir d'augmenter la taille des blocs pour qu'ils puissent supporter une transaction. Or ce n'est pas possible sur une Blockchain publique.

Même à petite échelle et sur une blockchain privée, nous avons rencontré plusieurs difficultés pour développer ce POC :

1 Développements

La technologie étant encore jeune, le POC a été développé sans interface de développement et avec un langage de programmation encore immature, rendant le débogage du programme particulièrement complexe

2 Gaz

Le Gaz représente la puissance de calcul nécessaire au minage d'un bloc sur Ethereum. Pour protéger la Blockchain, une limite de Gaz par bloc est fixée afin d'éviter les temps de calcul « infinis ». Même s'il s'agit ici d'une Blockchain privée, la limite de Gaz d'un bloc n'a pas pu être levée. Par ailleurs, les panne de Gaz, lorsque le calcul dépasse la limite sont indétectables.

3 Smart Contracts

Si les Smart Contracts permettent d'intégrer des programmes s'exécutant dans la Blockchain, leur complexité reste encore limitée. Il n'est pas encore envisageable d'intégrer des mécanismes sophistiqués dans la Blockchain.

CHIFFRES CLÉS

587 Md$
Valorisation des crypto-monnaies au 19 janvier 2018 / 814 Mds$: pic de valorisation au 7 janvier 2018

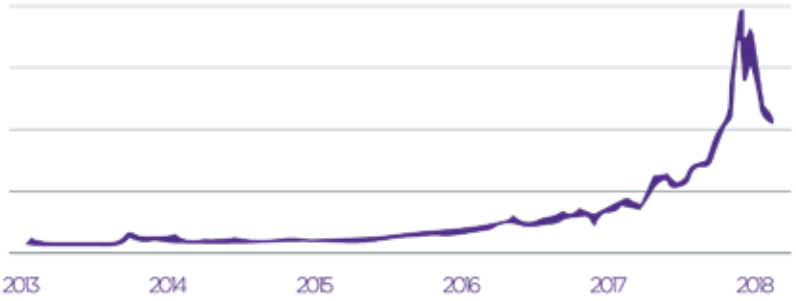
5,6 Md$
Montant des fonds levés via ICO* sur l'année 2017

* Une ICO Initial Coin Offering est une méthode de levée de fonds fonctionnant via l'émission d'actifs numériques échangeables contre des cryptomonnaies

2 Md$
Investissements cumulatifs Blockchain en 2017

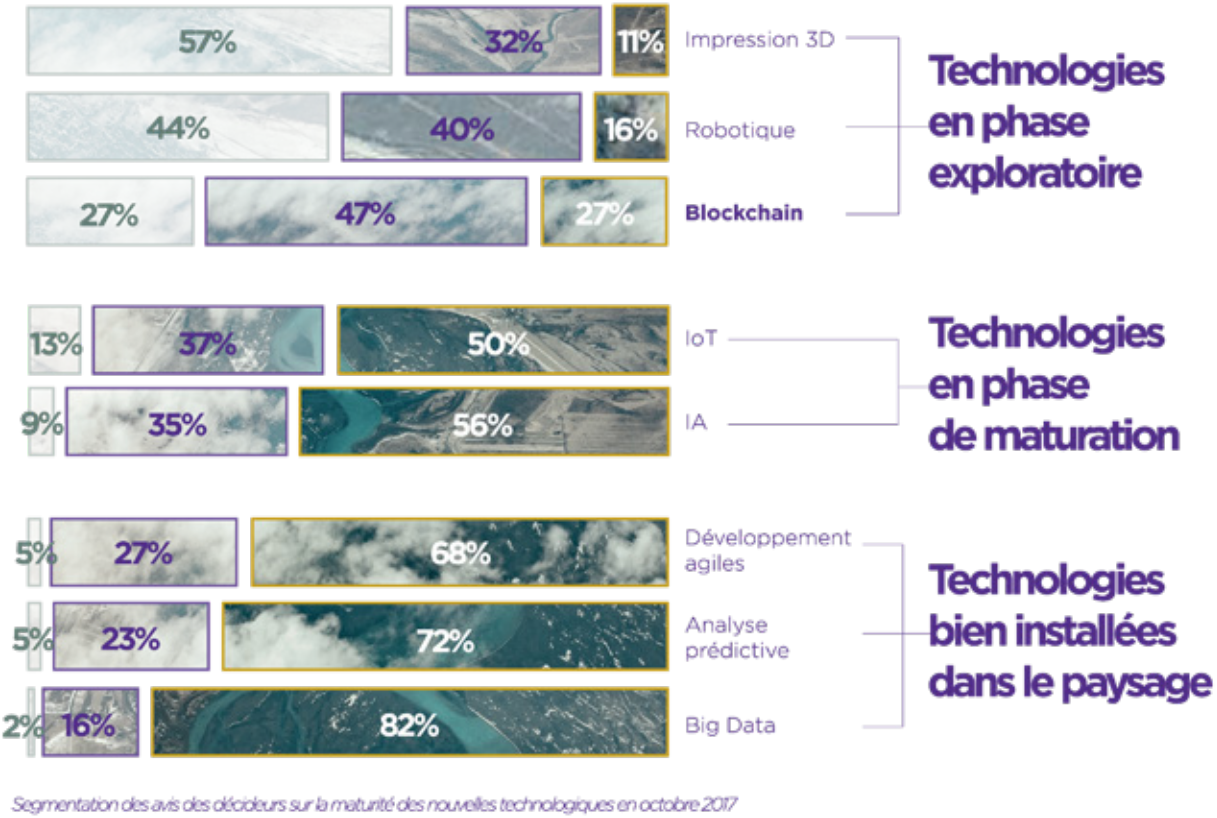
500
Nombre de startup dans le monde en 2017 qui développent des solutions à base de Blockchain

+ 2333%
Croissance des investissements dans la Blockchain entre 2012 et 2017



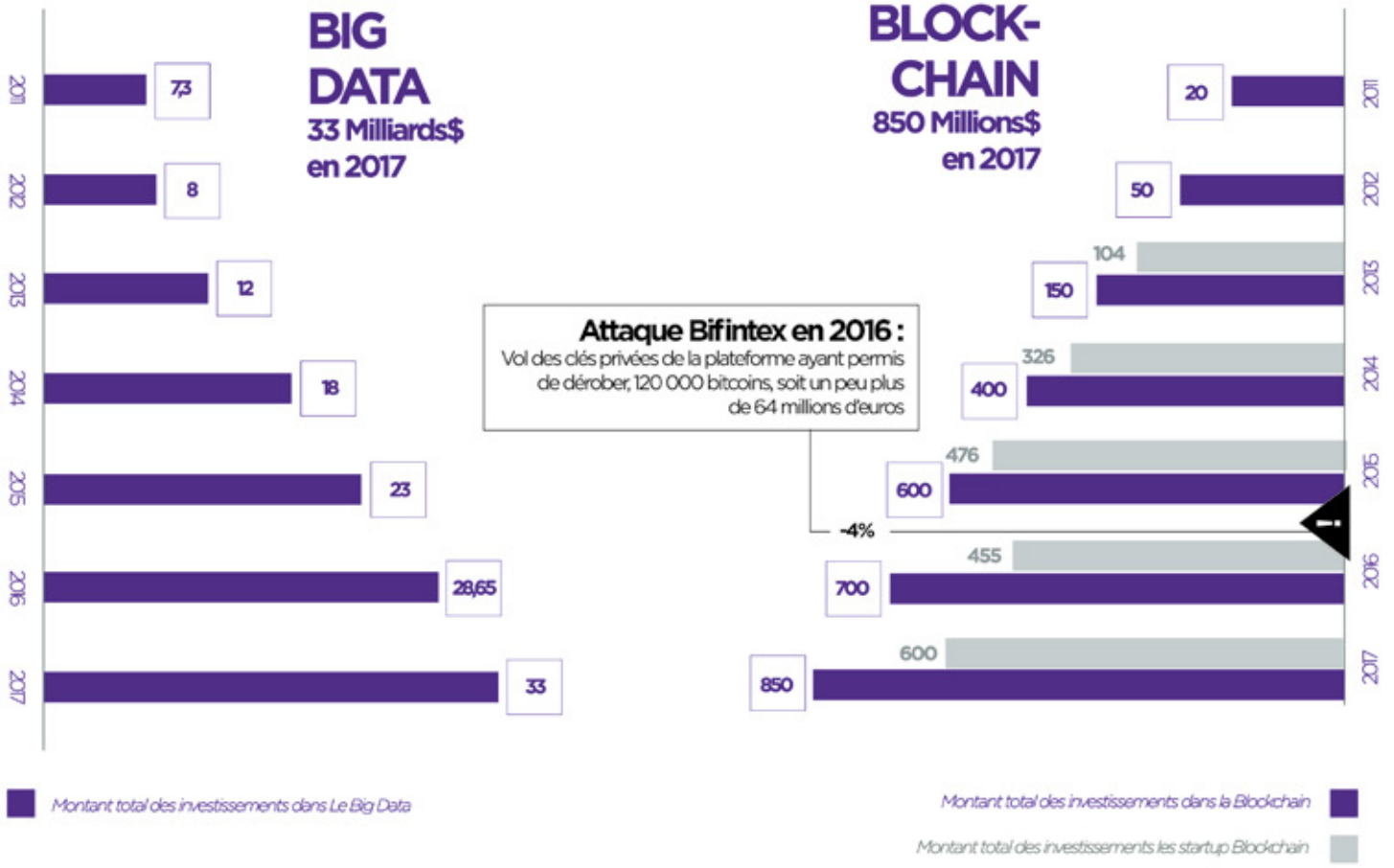
Évolution selon Google trend dans le monde de l'intérêt pour la recherche du mot Blockchain 14/03/2018

SI LES DÉCIDEURS COMMENCENT À PERCEVOIR LE POTENTIEL DE LA BLOCKCHAIN...

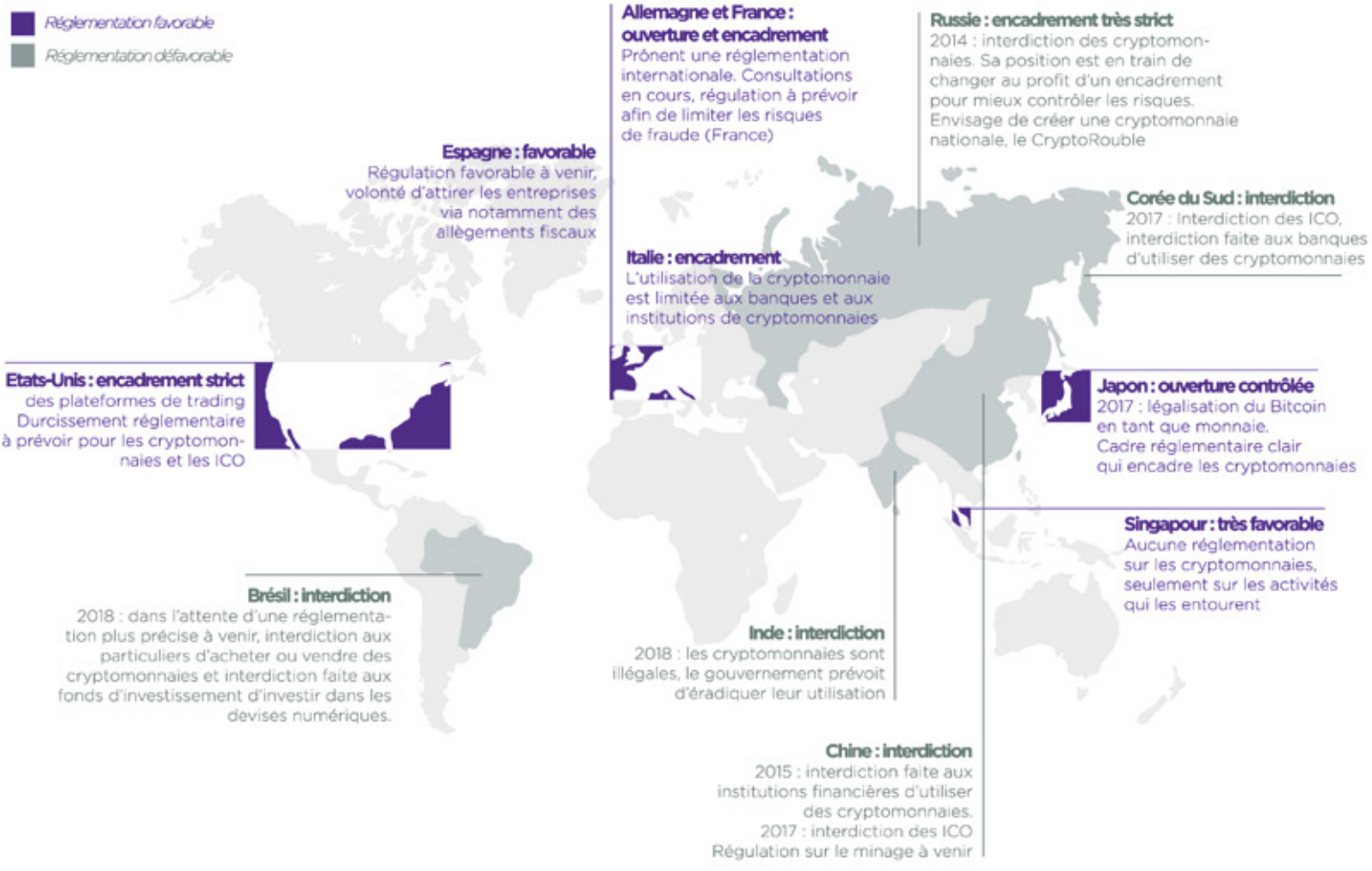


Segmentation des avis des décideurs sur la maturité des nouvelles technologiques en octobre 2017

LA BLOCKCHAIN VOIT SES INVESTISSEMENTS CROÎTRE DE MANIÈRE SIGNIFICATIVE MAIS RESTE LOIN DERRIÈRE LES TECHNOLOGIES PLUS MATURES



A L'ÉCHELLE MONDIALE, LA EST AXÉE SUR LES CRYPTRÉGLEMENTATIONO-MONNAIES



WAVESTONE EN BREF

Au croisement du conseil en management et du conseil en digital & innovation technologique, Wavestone s'est construit sur un positionnement original et une proposition de valeur différenciante parfaitement alignée sur les enjeux des entreprises et organisations à l'ère du digital.

Dans un monde où savoir se transformer est la clé du succès, Wavestone s'est donné pour mission d'éclairer et guider ses clients dans leurs décisions de transformation les plus stratégiques. Une mission que nous menons forts d'une triple conviction :

- L'innovation n'est plus une option pour les entreprises mais une nécessité au quotidien,
- Définir des stratégies d'entreprise pertinentes implique plus que jamais la maîtrise d'une forte dimension technologique,
- Les entreprises cherchant à se transformer n'attendent pas seulement un cabinet pouvant leur apporter des concepts, mais un partenaire capable de traduire ces concepts en actions concrètes.

Wavestone intervient auprès d'un portefeuille de clients de premier plan, composé notamment des grandes institutions et d'entreprises clés sur leur marché. Le cabinet met à leur service plus de 2 500 collaborateurs, répartis sur 4 continents et capables d'opérer de manière synchronisée sur toutes les géographies. Une force de frappe qui place le cabinet parmi les leaders des cabinets de conseil indépendants en Europe et à la toute première place en France.

WAVESTONE EST PARTENAIRE DE PLUSIEURS ÉVÉNEMENTS ORGANISÉS PAR L'ARGUS ASSURANCE

- **5 avril : Matinale Blockchain et assurance**
  Avec intervention de Laurence AL NEIMI, Senior Manager Financial Services
- **11 avril : Matinale Prévention Santé Prévoyance**
  Avec intervention de Laurence AL NEIMI, Senior Manager Financial Services
- **29 mai : Matinale Habitat Connecté**
  Avec intervention de Patrick DURAND, Senior Manager Financial Services
- **16 octobre : Matinale Auto Connectée**
  Avec intervention de Patrick DURAND, Senior Manager Financial Services
- **Les 3 et 4 juillet : animation d'un workshop sur l'expérience client**
  Avec intervention de Patrick DURAND, Senior Manager Financial Services

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). Il figure parmi les leaders indépendants du conseil en Europe.

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.

2018 I © WAVESTONE