

# LA BLOCKCHAIN



**A** l'image de la toute récente absorption de la société Chainspace par Facebook (cette start-up britannique étant la première acquisition<sup>1</sup> du géant des réseaux sociaux dans le domaine de la blockchain), 2019 marque un tournant dans la démocratisation des moyens autour de l'adoption de la confiance numérique dans les sphères privées et professionnelles, notamment par l'usage de systèmes décentralisés comme la blockchain. On parle de manière plus générale des systèmes de registres distribués ou DLT (*Distributed Ledger Technology*). Cette vague de déploiement à grande échelle de la technologie émergente blockchain devrait favoriser l'accélération d'une réelle transformation numérique de notre économie dans les prochaines années.

Beaucoup d'entreprises ont aujourd'hui pris conscience de la valeur transformationnelle de la blockchain pour l'ensemble des secteurs d'activité. Le cabinet IDC estime d'ailleurs à 9,7 milliards de dollars les dépenses globales liées aux technologies blockchain d'ici 2021.

Néanmoins, des obstacles d'ordre technique et de gouvernance restent à franchir en préalable d'une véritable adoption globale. C'est en cela que ce dossier spécial blockchain, réalisé avec des camarades de renom dans le domaine, se veut avant tout pragmatique, en abordant notamment les technologies blockchain à travers des cas d'usage concrets assortis d'une recherche perpétuelle de quantification de la valeur générée. Nous abordons dans un premier temps les aspects technico-économiques et juridiques de l'écosystème blockchain, avant de poursuivre par un focus sur les avancées technologiques et scientifiques du sujet. Ensuite, un éclairage sur l'enseignement de la blockchain à l'École sera apporté, notamment à travers la chaire Supply chain de CentraleSupélec.

Enfin, la diversité des cas d'usage de la blockchain est abordée au travers du prisme de l'économie, notamment dans l'énergie, dans la supply chain et à travers les cryptomonnaies. Sans oublier les perspectives particulièrement intéressantes sur le plan sociétal et dans le domaine de l'art.

Un grand merci aux auteurs des articles de ce dossier spécial pour leurs précieuses contributions.

**Ce dossier spécial a été copiloté par Julien Escribe (91), président de Centrale Numérique, et Mamy Ravelojaona (Supélec 98), président de Supélec Numérique.**

1. « Facebook Makes First Blockchain Acquisition With Chainspace », <http://cheddar.com>

## Sommaire

### ARTICLES TRANSVERSAUX

- p 26 Qu'est-ce que la blockchain ?**  
Marius Lombard-Platet (15 + 1)
- p 28 Panorama technico-économique et juridique**  
Julien Escribe (91)
- p 29 De la recherche aux applications en supply chain**  
Laurent Grégoire (78)

### CAS D'USAGE

- p 30 Réglementer les ICO**  
Léo Lemordant (ECLy 08)
- p 31 Les stable coins : le graal de la blockchain ?**  
Ossama Benbouidda (ECN 15)
- p 32 La blockchain au service des énergies renouvelables**  
Olivier Pasquier (MS 16)
- p 33 La blockchain, une opportunité pour les processus industriels**  
Bertrand Eteneau (83)
- p 34 La blockchain comme tiers de confiance : un bouleversement sociétal**  
Nicolas Videgrain (Supélec 16)
- p 35 La blockchain appliquée au monde de l'art**  
Bertrand Scache (86)

### CONCLUSION

- p 36 Une grande promesse qui a fait pschitt ?**  
Alexandre Martinelli (Supélec 00)



**Mamy Ravelojaona**  
(Supélec 98)

Après des débuts dans les télécoms, Mamy s'oriente en 2006 vers le développement business et stratégie d'entreprise auprès du groupe Alten, et complète sa formation par un cursus en Stratégie marketing & innovation à l'Essec. En 2017, il rejoint le groupe Grant Alexander pour y développer la practice Transformation & Strategy.



**Julien Escribe (91)**

Partner chez ISG, un des leaders mondiaux de l'analyse des technologies et du conseil dans le secteur de l'IT, Julien est également président de Centrale Numérique. Il enseigne en 3<sup>e</sup> année à CentraleSupélec. Julien est passionné de nouvelles technologies et plus particulièrement de blockchain.



# Qu'est-ce que la blockchain ?

La blockchain soulève les questions et attise les passions. Certains n'y voient qu'une bulle sur une technologie énergivore et peu sécurisée, d'autres ne cessent d'en chanter les louanges. Le point avec Marius Lombard-Platet (15 + 1), doctorant ENS/Almerys en sécurité de l'information sur le thème des blockchains et de l'anonymat.



**C'**est en 2008 que fut publié *Bitcoin*, sous la plume d'un auteur inconnu au pseudonyme de Satoshi Nakamoto. Son implémentation se fit la même année, faisant du Bitcoin la première monnaie décentralisée. Pour créer cette monnaie non régulée par une banque centrale (traditionnellement responsable de l'émission de nouvelles liquidités et de la validité des transactions), Nakamoto s'est appuyé sur son invention : la blockchain.

Qu'est-ce que la blockchain ? Pour donner une réponse concise, la blockchain (ou chaîne de blocs en français) est un type de registre, qui cherche à être inaltérable et décentralisé. Continuons : un registre est un endroit où l'on stocke des données ; inaltérable car toute transaction inscrite dans le registre ne peut être modifiée à moins de fournir un effort considérable ; et décentralisé car ne dépendant d'aucune autorité : les utilisateurs sont tous égaux, il n'existe pas de banque centrale.

Un registre inaltérable, on en comprend l'intérêt contre les fraudes. Mais pourquoi décentralisé ? L'intérêt est simple. Une banque peut se faire cambrioler ; mais il est difficile de cambrioler un système qui n'a pas de banque. Dans un système

centralisé, les banques sont garantes de la sécurité. Dans un système décentralisé, c'est l'ensemble des utilisateurs qui assurent cette garantie, obligeant l'attaquant à contrôler 33 % voire 50 % du système pour mener une offensive. Ce qui en théorie est improbable, et garantit donc la sécurité du système.

## Sécuriser les transactions

Cependant, sans autorité centrale, il faut que les participants soient d'accord sur l'ordre et la validité des transactions au sein du réseau. Pour ajouter un bloc de transactions, on suit un algorithme de minage : c'est un investissement (*encadré 1*) que fait le mineur sur le bloc qu'il propose. Un des blocs proposés par les mineurs sera alors adopté, par un algorithme de consensus sur le réseau, comme prochain bloc de la blockchain. Puis on recommence avec un nouveau bloc. Avec ces algorithmes, plus il y a de participants, plus il est difficile pour un attaquant de modifier une donnée déjà enregistrée. Pour réécrire l'historique Bitcoin, un attaquant doit pouvoir réécrire l'historique plus rapidement que le reste du réseau ne rajoute des blocs. Autrement dit, un attaquant doit posséder au moins 50 % de la puissance du réseau pour mener son attaque. Pour cela, l'attaquant doit augmenter sa propre puissance de calcul, ce qui augmente la puissance totale

du réseau, et accroît d'autant la difficulté pour un autre attaquant. Autrement dit, sur une blockchain, un attaquant améliore la sécurité du système contre d'autres attaquants. Pour autant, la blockchain n'est pas inviolable. Des attaques plus subtiles existent, *via* des bugs logiciels ou une attaque sur le réseau Internet de la victime. Qui plus est, en 2018 les blockchains Verge, Monacoin, ZenCash et Bitcoin Gold ont toutes été victimes d'une « attaque des 51 % », cumulant plus de 20 millions d'euros volés. Quant au Bitcoin, une telle attaque n'est jamais arrivée... pour l'instant. 58 % de la puissance de calcul du réseau Bitcoin est contrôlée par quatre entreprises chinoises : pour une monnaie décentralisée, c'est un comble !

## Une multitude d'applications

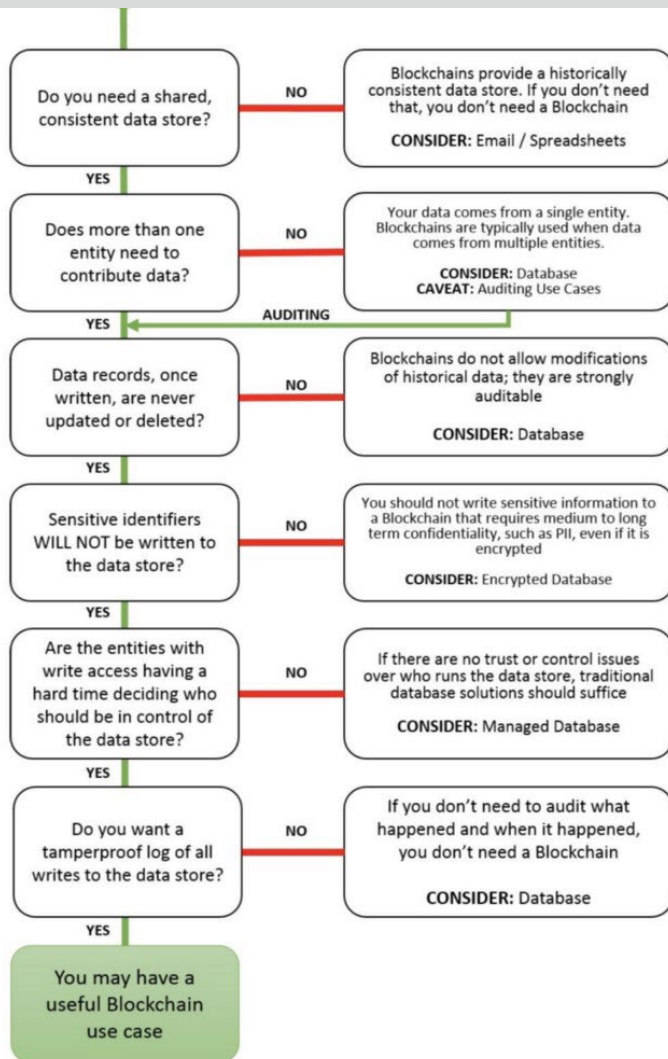
Mais trêve de questions sécuritaires. Jusqu'ici nous n'avons parlé que d'une blockchain, le Bitcoin, et que d'une application, la monnaie virtuelle. Le paysage est pourtant bien plus varié. Une blockchain peut servir de support à toute application qui a besoin d'un registre inaltérable et décentralisé. Parmi ces applications, on compte le vote électronique, la gestion d'identité (passeports électroniques), le suivi de produits dans une supply chain, le contournement de censure (puisque la blockchain, inaltérable, ne peut pas être censurée)... Pour chacun de ces exemples, au moins une blockchain existe déjà.

Suite page 27

### Marius Lombard-Platet (15 + 1)

Après avoir longtemps hésité entre physique et informatique, Marius Lombard-Platet s'est finalement tourné vers l'informatique et est actuellement en 2<sup>e</sup> année de thèse en sécurité de l'information dans un partenariat Cifre ENS/Almerys. Il s'intéresse entre autres à la gestion de l'identité et à l'anonymat.

→ Quand utiliser une blockchain ?



© DHS

De plus, le potentiel des blockchains est immense : grâce aux *smart contracts*, des programmes qui s'exécutent sur une blockchain (qui sont donc inaltérables et décentralisés), on peut coder à peu près ce que l'on veut. Par ailleurs, une blockchain peut être publique ou privée, et ouverte à tous (anonyme, ou *permissionless* en anglais) ou accessible aux membres authentifiés seulement<sup>1</sup> (*permissioned*). Chacun de ces modes correspond à un besoin précis : une cryptomonnaie sera publique et anonyme, un système d'échange monétaire entre banques sera authentifié et privé. Bref, le monde des blockchains est riche et varié. Mais gare aux sirènes ! La blockchain n'est pas une panacée, n'en déplaise à ceux qui l'utilisent à tort et à travers. Ainsi, la blockchain est une technologie dure à implémenter. Dans de nombreux cas, une simple base de données sera plus simple, moins chère et bien plus susceptible d'être un jour déployée sur le marché. En

effet, une blockchain nécessite de mettre en place un réseau – avec son lot de contraintes organisationnelles – entre divers acteurs, sur des technologies encore jeunes. Dans la charte du DHS (Department of Homeland Security), reprise par le NIST (National Institute of Standards and Technology), sont présentées plusieurs alternatives (*encadré 2*). Par exemple : « My Health, My Data » est un projet européen H2020 qui permet aux hôpitaux de consigner les demandes d'accès à des données médicales. Les hôpitaux étant très soucieux de la confidentialité de ces données, aucun tiers de confiance n'est envisageable. Seules les entités accréditées peuvent accéder au système, ce qui implique l'utilisation d'une blockchain authentifiée privée. À l'opposé, un système de suivi de supply chain d'une seule entreprise n'a aucun intérêt à utiliser une blockchain : la blockchain est décentralisée, mais il n'y a qu'une seule entité dans le système. À quoi bon ?

En résumé, la blockchain est un nouvel outil de stockage de données (transactions financières, *smart contracts*, fiches de suivi...) qui offre de fortes garanties en termes de sécurité. Si ce n'est certainement pas l'outil miracle qui résoudra tous les problèmes de notre société, il n'en reste pas moins que c'est un outil extrêmement utile dans de nombreuses situations... à condition de savoir quand s'en servir. ■

1. Le sujet fait débat : une blockchain authentifiée dépend d'une autorité qui filtre les utilisateurs, mais pas les échanges. Peut-on toujours parler d'un système décentralisé ?

→ Consensus et investissement

L'investissement peut être du temps de calcul, comme pour la *proof of work* du Bitcoin : l'ordinateur du mineur effectue de nombreux calculs (inversion partielle de SHA-256) avant de pouvoir proposer un bloc. Citons également :

- **proof of stake** : investir une partie de ses ressources dans la cryptomonnaie pour parier sur quel sera le prochain bloc. C'est ce qui est utilisé pour la blockchain PeerCoin ;
- **proof of space** : investir une partie de son espace de stockage sur disque dur (c'est le cas de Chia) ;
- **proof of elapsed time** : investir du temps de disponibilité de processeur (Hyperledger Sawtooth) ;
- etc.

Pour encouragement, un mineur gagne de l'argent à chaque bloc accepté qu'il a proposé. Sur le Bitcoin, la récompense est actuellement de 12,5 bitcoins par bloc.

Il est à noter qu'à l'heure actuelle, la *proof of work* est l'algorithme le plus commun, même s'il est le plus énergivore : on estime qu'actuellement le réseau Bitcoin consomme 73 TWh d'électricité par an, autant que l'Autriche. Seuls 39 pays consomment davantage.



# Panorama technico-économique et juridique

**Les blockchains ont aujourd'hui démontré leur application pratique dans l'économie. Ces systèmes décentralisés, dont les technologies ne cessent de gagner en maturité, promettent de transformer tous les processus pilotant notre quotidien. Le point avec Julien Escribe (91), partner chez ISG et président de Centrale Numérique.**



## Julien Escribe (91)

Partner chez ISG, un des leaders mondiaux de l'analyse des technologies et du conseil dans le secteur de l'IT, Julien est également président de Centrale Numérique.

Il enseigne en 3<sup>e</sup> année à CentraleSupélec. Passionné de nouvelles technologies et plus particulièrement de blockchain, il copilote ce dossier.

**L**e marché mondial des blockchains – ou plutôt des Digital Ledger Technologies (DLT) – pourrait dépasser les 300 milliards de dollars d'ici 2025 et les 2 000 milliards de dollars d'ici 2030. Cet ovni technologique a largement dépassé le challenge technique initial qu'on peut résumer par un cocktail détonant de cryptologie, d'arbre de Merkel et d'absence de confiance dans les entités de régulation.

L'erreur à ne pas faire est d'associer la blockchain au Bitcoin, car ce lien initial est aujourd'hui largement dépassé. Un des intérêts du protocole derrière le Bitcoin est de permettre d'appréhender une technologie particulièrement complexe. Par analogie, cela revient à ajouter une pièce au puzzle d'Internet, permettant de passer d'une logique d'information copiable à l'infini à une logique de valeur, cette dernière étant non duplicable par essence. Faire un panorama technico-économique

est un challenge, tant les blockchains ont aujourd'hui envahi notre espace numérique (*encadré*).

## Sociétal et juridique

La blockchain génère de la valeur en exploitant les données synchronisées d'un grand nombre de chaînes de valeur et les acteurs de l'écosystème veulent comprendre où sont les opportunités, quelle est la valeur de ces opportunités et qui sont les meilleurs fournisseurs de technologie pour répondre à leurs besoins. D'un point de vue sociétal, le sujet est particulièrement complexe. Les gouvernements se positionnent, prenant conscience que les blockchains pourraient devenir un nouveau type d'Internet. On cherche à mieux qualifier juridiquement les ICO, à définir la fiscalité autour des crypto-currencies et à créer des normes qui favorisent la confiance. L'idéal se place sans doute entre le « 100 % régulé » et le « laisser-faire », parfois synonyme de la ruée vers l'or en Californie. On ne peut laisser à l'écart le problème juridique de la relation antinomique entre blockchain et « droit à l'oubli », cher à toutes les mises en place de RGPD. Ce droit au déréférencement est fortement limité car les blockchains sont *a priori* non modifiables. Gageons que les nombreux outils en gestation autour de ce thème fourniront une réponse adéquate. La bonne nouvelle est que nos écoles d'ingénieurs commencent à intégrer les blockchains dans leur enseignement. CentraleSupélec en fait partie en proposant un électif dès la 2<sup>e</sup> année du cursus. ■

## → Le potentiel de la blockchain

**La blockchain est partout. Au-delà de la découpe effectuée par Blockchain France (applications pour transferts d'actifs, registres, smart contracts), voici quelques exemples concrets de ses applications :**

- les *smart contracts*,
- l'économie du partage, pour dépasser les intermédiaires numériques (Uber, AirBnB...) avec des solutions de paiement *peer to peer*,
- le *crowd funding*,
- la gouvernance sociétale, pour apporter de la transparence aux processus de vote,
- la capacité d'audit de la supply chain,
- le stockage de fichiers universels,
- le marché des prédictions (Augur),
- la protection de la propriété intellectuelle,
- l'Internet of Things,
- le marché de l'énergie (microgrids),
- la gestion des identités numériques,
- la lutte contre le blanchiment d'argent,
- le KYC (Know Your Customer) des institutions financières,
- le data management (projet Enigma du MIT),
- les registres des titres de propriété,
- les marchés financiers,
- et bien sûr les crypto-currencies, avec un marché particulièrement agité en 2018.

# De la recherche aux applications en **supply chain**

**Depuis cinq ans, des chercheurs travaillent aux applications de la blockchain en supply chain. Les premières utilisations ont porté sur la traçabilité des produits, puis sur la désintermédiation des échanges. D'autres applications sont en gestation, en lien avec les smart contracts. Le point avec Laurent Grégoire (78), responsable du partenariat Entreprises de la chaire Supply chain de CentraleSupélec.**

Il est sans doute utile de rappeler<sup>1</sup> la signification de ces deux termes : la *logistique* porte sur la gestion des flux physiques et des informations qui s'y rapportent dans une organisation ; le *supply chain management*, plus large, inclut conception, planification, exécution et maîtrise de l'ensemble des activités relatives aux flux physiques, informationnels et financiers au sein de l'entreprise étendue (des fournisseurs les plus en amont jusqu'au consommateur final) pour répondre à un taux de service fixé en assurant responsabilité sociétale et rentabilité optimale. Après l'apparition des monnaies virtuelles et des premières recherches sur d'autres applications financières de la blockchain, c'est à partir de 2014 que le monde académique s'est intéressé aux applications possibles pour la logistique et la supply chain. En France, avec les premières expérimentations en entreprise, s'est tenue en novembre 2016 la première conférence nationale « Blockchain et supply chain ». Depuis lors se multiplient les mémoires d'étudiants, lesancements de thèses, les partenariats recherche-entreprises, voire les

premières utilisations concrètes, même si ces dernières restent encore de dimension modeste.

## De la traçabilité aux smart contracts

L'application la plus concrète concerne la traçabilité des produits tout le long de leur vie dans une économie circulaire, depuis l'extraction des matières qui les composent jusqu'à leur destruction finale. La blockchain répond aux défis de la traçabilité : grand nombre d'acteurs, sécurisation, confidentialité et longévité des informations récoltées.

De nombreuses autres applications sont aujourd'hui en cours d'étude, de test ou de mise en œuvre. Elles concernent notamment la gestion documentaire de tous les transports de produits, l'automatisation des vérifications et la désintermédiation des transactions financières entre entreprises, le partage d'informations confidentielles, notamment pour la gestion de la demande, la reconnaissance et la sécurisation du



transfert légal de propriété (application sur smartphone qui a reçu un prix de l'Innovation supply chain en 2018) ou encore – mais nous n'en sommes qu'au début – l'amélioration et l'accélération du processus décisionnel de la supply chain. Sur ce dernier point, il s'agit de développer les *smart contracts*, ces contrats automatisés entre acteurs d'une supply chain, qui pourront régir, *via* une blockchain, tous les flux d'une façon non seulement réactive mais aussi prédictive. Cette utilisation conjointe de *smart contracts* et de blockchain inclura de l'intelligence artificielle pour mieux gérer la complexité croissante des supply chains. Il ne faut plus penser aux applications de telle ou telle nouvelle technologie de façon séparée mais, par une approche systémique (naturelle pour les experts en logistique et supply chain), travailler sur les utilisations croisées des nouvelles technologies : blockchain, intelligence artificielle, mais aussi DDMRP, big data, Internet des objets, véhicules autonomes, robotisation, réalité virtuelle, sans oublier l'Internet physique, la prochaine révolution technologique en logistique. ■

1. Lire le dossier « Supply chain » de la revue *Centraliens* dans le n° 630 de décembre 2013.



## Laurent Grégoire (78)

Consultant formateur après trente-cinq ans de direction logistique puis supply chain dans l'industrie, Laurent est en charge des partenariats avec les entreprises qui participent à la chaire Supply Chain de CentraleSupélec. Il a fondé puis présidé la section thématique Logistique et supply chain de la Commission nationale des services, au ministère de l'Économie.



# Réglementer les ICO

**Les ICO (*Initial Coin Offerings*) subissent un déficit de confiance. Alors que l'objectif de la blockchain est de supprimer les tiers de confiance, il semble opportun de réintroduire des tiers dont le rôle ne serait pas de certifier les transactions, mais les acteurs. La loi devrait faciliter cette évolution souhaitable. Le point avec Léo Lemordant (ECLy 08), président et fondateur de WeToken.co.**

**4,2** milliards de dollars américains. C'est le plus grand montant levé à ce jour par voie d'« *Initial Coin Offering* » (ICO). Ce nouveau mode de levée de fonds, qui s'apparente à une offre au public de titres sous forme de crypto-actifs, a fait son apparition il y a cinq ans. Ce n'est qu'en 2017 que le nombre d'ICO et les montants collectés par opération ont crû très significativement. Des milliards d'euros ont été injectés dans ce secteur au cours d'une frénésie largement irrationnelle.

Sans surprise, les dérives et arnaques en tous genres n'ont pas tardé à faire les gros titres. Même l'opération d'EOS à 4,2 milliards n'est pas exempte de tous

Le secteur a pâti de la conjonction de trois facteurs : une crise de confiance envers la qualité des projets, une prise de bénéfices des investisseurs et des prises de position fermes des régulateurs.

## Retrouver la confiance

La crise de confiance ne s'est pas seulement traduite par une baisse des montants investis. Elle a aussi eu pour conséquence une augmentation drastique des frais engagés pour réaliser une levée de fonds, passant de quelques centaines de milliers d'euros à quelques millions d'euros pour lever une somme parfois équivalente. Il est en effet devenu crucial pour les projets de se démarquer de la masse de projets



**Léo Lemordant (ECLy 08)**

Centralien de Lyon et docteur

en hydrologie diplômé de l'université de Columbia (New York), Léo a été en charge du développement de concessions hydroélectriques. En 2014, il a fondé Enerfip, une plateforme d'épargne participative dédiée à la transition énergétique. Aujourd'hui, il applique un modèle similaire pour les projets blockchain avec WeToken.co.

fournit aujourd'hui ce type de prestations<sup>1</sup>. Le traitement des aspects juridiques est également devenu une source importante de dépenses, et tous les grands cabinets d'avocats sont positionnés sur ce thème avec des équipes dédiées. Les États ont en effet commencé à ébaucher des doctrines, parfois incohérentes entre elles. Un même crypto-actif pourra être qualifié aux États-Unis de titre financier, auquel s'appliquera donc toute la réglementation classique de l'offre au public de titres, là où la Suisse ne fixera aucune règle. La loi Pacte, votée à l'Assemblée nationale en octobre dernier<sup>2</sup>, définit des régimes optionnels. Les crypto-actifs utilitaires<sup>3</sup> pourront être proposés au public à travers une réglementation qui ne s'appliquera qu'aux volontaires. L'espoir est de ne pas décourager le secteur, y compris vis-à-vis des régimes juridiques étrangers, tout en favorisant les pratiques vertueuses.

Compte tenu de l'évolution de ce contexte, il est possible que soit réintroduite la notion de tiers de confiance, non pas pour certifier les transactions mais plutôt... les utilisateurs de cette technologie. Il serait paradoxal que le secteur de la blockchain ne puisse se passer de tiers de confiance, alors qu'il a l'ambition de précisément éliminer tout type de tiers de confiance ! ■

1. « ICO : Havas crée une solution clé en main pour lever des cryptomonnaies », article de Grégory Raymond publié le 29 mars 2018 dans *Capital*.
2. Articles 26 et 26bis du projet de loi relatif à la croissance et la transformation des entreprises.
3. Ceux représentant la prévente d'un service.



reproches relativement aux standards de la réglementation financière et de la protection de l'investisseur. C'est également sans surprise que les montants investis ont connu un net recul à la mi-2018, entraînant un krach qui se prolonge depuis cette date.

« concurrents » et d'inspirer confiance. Le marketing est donc devenu une clef particulièrement importante de la réussite d'une ICO. Les dépenses de communication ont ainsi été décuplées. Signe des temps, le numéro un de la communication en France

# Les stable coins : le graal de la blockchain ?

Inventés afin de permettre aux marchés d'échange d'intégrer des cryptomonnaies indexées sur les monnaies-fiat<sup>1</sup>, les *stable coins* seraient aujourd'hui la clé du développement du secteur. Le point avec Ossama Benbouidda (EC Nantes 15), senior consultant Stratégie & Opérations pour les services financiers chez Deloitte.



**Ossama Benbouidda**  
(ECN 15)

Senior consultant Stratégie & Opérations pour services financiers chez Deloitte, Ossama travaille notamment sur des sujets de transformation numérique (blockchain, RPA, IA) pour divers acteurs bancaires et assurantiels. Il accompagne entre autres des clients souhaitant se lancer sur de nouveaux moyens de financement comme les ICO.

Depuis l'instauration des accords de Bretton Woods en 1944, le système monétaire international repose sur le dollar américain comme monnaie de référence. Bien que fonctionnel aujourd'hui, les différentes crises économiques ont montré sa défaillance et plusieurs économistes s'accordent pour lui prédire un avenir funeste. Et si la blockchain, via les *stable coins*, pouvait améliorer et rendre ce système plus performant ? Il est communément admis que le développement de la blockchain est intimement lié au développement des cryptomonnaies. Or, si ces dernières offrent des avantages non négligeables pour l'échange et la réalisation

des transactions entre pairs (rapidité, faibles frais), plusieurs grands acteurs du système financier mondial refusent de les utiliser à cause d'un défaut majeur : leur volatilité. Les cours peuvent varier brutalement du jour au lendemain, à la hausse ou à la baisse, et les deux scénarios se sont répétés maintes fois dans l'histoire de la crypto-industrie. Face à cette volatilité (en un an le bitcoin est passé de 20 000 à 3 000 dollars par exemple), des poids lourds du commerce en ligne, comme Showroomprive ou Microsoft, ont décidé d'arrêter les paiements en bitcoins.

## Les stable coins, la solution ?

Pour remédier au problème de volatilité des cryptomonnaies, nous assistons depuis quelque temps à l'effervescence d'une nouvelle classe d'assets appelés *stable coins*. Hormis le manque de volatilité, les *stable coins* tirent leur réputation de leur technique de construction : leur stabilité est vérifiée informatiquement grâce à des *smart contracts* et non grâce à des indexations sur des matières premières comme l'or.

## Limites et futur de cette cryptomonnaie

Cette nouvelle cryptomonnaie fait l'objet de nombreuses controverses. Le *stable coin* le plus connu, Tether (*encadré*), est ainsi au cœur de plusieurs polémiques. Sa maison mère Bitfinex est accusée par la communauté blockchain de ne pas détenir l'équivalent en dollars des 2,2 milliards de Tether émis et n'a jamais apporté la preuve du contraire. Fin janvier, l'entreprise a même annoncé la fin de sa collaboration avec le cabinet d'audit Friedman qui assurait jusque-là

l'équivalence des tokens de Tether émis en dollars américains sur le compte bancaire de la société Tether. Enfin, une récente étude de chercheurs de l'université du Texas affirme que le cours du bitcoin a été manipulé par le Tether entre mars 2017 et 2018, et qu'il serait même à l'origine de la grosse bulle de 2017.

Autre point, non négligeable, le *stable coin* n'a jusqu'ici été adopté que par un seul pays, le Venezuela.

Cela suffit-il à hypothéquer l'avenir de cette cryptomonnaie ? Non, et l'on verra sûrement la création de *stable coins* aux formats et utilisations diverses dépassant la fonction première des monnaies classiques, telles que des applications d'assets financiers ETF indexés sur des *stable coins*, des monnaies-fiat et, éventuellement, des matières premières ! ■

1. La monnaie-fiat est une monnaie fiduciaire entièrement contrôlée par les États.

## → Les différents types de stable coins

Il existe une vingtaine de *stable coins* sur le marché, chacun avec ses propres spécificités. Parmi ces cryptomonnaies, les plus utilisées sont :

- **Dai**, qui fonctionne sur la blockchain Ethereum et est indexée sur le dollar ;
- **Tether**, également indexée sur le dollar ;
- **TrueUSD**, construite en *smart contract* et bénéficiant d'un cadre juridique.



# La blockchain au service des énergies renouvelables

**Produire de l'électricité renouvelable nécessite de passer d'un monde de grands producteurs nationaux à un système de production délocalisée. Mais comment gérer ce monde où chacun sera producteur et consommateur ? Le point avec Olivier Pasquier (MS 16), directeur marketing de QOS Energy, sur le potentiel extraordinaire offert par la blockchain.**



**Olivier Pasquier (MS 16)**

Membre de Centrale Numérique,

Olivier est directeur marketing de QOS Energy, une start-up nantaise de data intelligence dans les énergies renouvelables.

La start-up Electron, en partenariat avec EDF, fait des tests au Royaume-Uni. La régulation du réseau sera également facilitée : le régulateur pourrait imaginer non pas d'arrêter sa turbine à gaz un jour de surproduction, mais de demander à une microgrid de le faire pour un bon prix. Ces échanges – et ces tarifs – seront écrits dans une blockchain. Le système a été testé avec succès à New York en 2016. D'autre part, si l'avenir du transport passe par des véhicules électriques, le monde entier devra déployer une quantité phénoménale de batteries. On peut donc imaginer l'automobiliste chargeant sa batterie quand l'électricité est abondante, avant de la réinjecter dans le réseau lors des pics de consommation. Cela permet également de baisser le coût d'acquisition des véhicules, en rémunérant le propriétaire pour sa capacité de stockage.

La production d'électricité reste universellement un secteur très encadré. L'adoption de technologies blockchain n'est donc possible qu'avec des changements législatifs profonds. D'autre part, la technologie actuelle reste chère à déployer (matériel, électricité). Or les coûts de transaction ne doivent représenter qu'une fraction infime du prix des kilowattheures échangés par des petits producteurs. Sur le Bitcoin, les transactions sont cadencées à 10 minutes par block. Même si Ethereum est plus flexible, la technologie blockchain doit encore s'améliorer. Plus de 300 millions de dollars ont été investis dans des start-up blockchain du secteur de l'énergie en 2017. Cette promesse de nouveaux outils de gestion pour réussir la transition énergétique semble donc bien lancée. ■



**L**es systèmes de production d'électricité ont été conçus de manière pyramidale : de grosses centrales de production délivrent leur puissance aux utilisateurs au travers de réseaux nationaux, pour produire de l'électricité avec certitude au moindre prix.

L'accord de Paris – et les changements climatiques – obligent les États à investir massivement dans les énergies nouvelles pour produire 10 % de renouvelable dans les cinq ans. Les consommateurs demandent également de l'électricité verte. Or les électrons sont injectés sur le réseau indépendamment de la source de production : nucléaire, turbine à gaz ou éolienne. Comment prouver aux clients que l'électricité qu'ils achètent est bien « verte » ? C'est la première application possible de la technologie blockchain en énergie. Chaque producteur d'électricité renouvelable peut inscrire sa production

dans un grand registre qui permet de prouver sa provenance verte. Engie déploie les outils de la start-up Ledger exactement pour cet usage. On peut aussi imaginer un marché d'échange de certificats d'énergie verte, fondé sur la blockchain.

## Gérer la transition énergétique

La généralisation du renouvelable achoppe sur l'intermittence de production. L'idée est donc de développer des microgrids. Imaginons que chaque foyer ou entreprise deviennent producteur (par des panneaux solaires sur les toits par exemple) et consommateur. Comment gérer alors la complexité de la facturation croisée ? Les cryptomonnaies apparaissent comme une solution pour financer ces échanges. Chaque transaction est écrite dans une blockchain, un décompte mensuel est effectué, tout reste dans le virtuel et on s'affranchit ainsi d'un cycle complet de facturation.

# Une opportunité pour les processus industriels

**Quels bénéfices en termes d'efficacité, de fiabilité et sécurité, une technologie telle que la blockchain peut-elle apporter aux secteurs de la production et de la supply chain ? Le point avec Bertrand Eteneau (83), directeur associé chez BCG et spécialisé dans l'industrie 4.0, les technologies de l'information et la transformation numérique des organisations.**



livraison sont gérées automatiquement, entraînant rapidement une baisse des coûts de vérification des documents et une augmentation de l'efficacité opérationnelle.

## **Gagner en efficacité, productivité et sécurité**

Dans la lutte contre la contrefaçon, l'opération d'enregistrement du produit dans le système d'authentification est majoritairement réalisée dans les ateliers de fabrication et non dans le reste de la chaîne de distribution. Ceci soit pour des raisons de coûts, soit parce que cette opération engendre des manipulations supplémentaires qui nuisent à l'efficacité des processus. Or, cette information d'authenticité est à la fois nécessaire pour des besoins internes tels que le service après-vente, mais aussi pour les clients qui veulent

s'assurer d'acheter un produit authentique. La blockchain est précisément ce socle de confiance entre tiers qui permet d'échanger et tracer l'information, de manière cryptée, inaltérable, non répudiable et partagée par tous (certificats de conformité, documents douaniers, traçabilité des produits, des flux de marchandises dans un réseau mondial de partenaires...). Dans le manufacturing, l'avènement de l'usine 4.0 s'appuie sur l'utilisation des objets connectés (IoT) et des machines connectées. Pour assurer la capacité de production de ces usines, la maintenance préventive et prédictive est un enjeu clé entraînant un besoin de coordination d'opérations nombreuses et complexes. Or, plus nombreux sont ces objets ou machines, plus compliquée est cette planification. En capitalisant sur le *smart contract* grâce aux informations générées, ces opérations seront anticipées et planifiées sans intervention de collaborateurs. Enfin, l'impression 3D couplée à la blockchain permettra de mettre à disposition des industriels des pièces de rechange plus rapidement. La propriété intellectuelle sera respectée et les lignes de fabrication plus efficaces. En sécurisant les données, de nouveaux services s'offriront aux entreprises, par exemple la machine *as a service*, qui permettra de payer une capacité consommée. Ces gains d'efficacité et de productivité sont une aubaine et doivent être considérés comme les clés de la mise en œuvre des blockchains dans l'industrie et l'ingénierie.

Investir dans la blockchain est un pari qu'il faut considérer : mieux vaut y entrer trop tôt que trop tard. ■

La blockchain, véritable eldorado pour certains, confinée à quelques applications et mystérieuse pour beaucoup, a tous les atouts pour devenir incontournable. Par la disponibilité, la sécurité, l'authenticité de l'information et la mise en place de *smart contracts* qui s'exécutent automatiquement selon des règles prédéfinies, elle permettra des économies d'échelle tant opérationnelles que financières aux grandes organisations travaillant en réseau. Les supply chains font face à plusieurs défis, géographiques, opérationnels et légaux. Le secteur doit également assurer la lutte contre la contrefaçon et s'adapter en permanence à la clientèle. Le plus souvent, les entreprises tentent d'y répondre en adoptant des systèmes adaptés à chaque problématique. Non seulement ces solutions ont un coût élevé en maintenance et formation, mais elles sont également souvent difficilement exploitables car non synchronisées en temps réel. En choisissant une blockchain, l'organisation gagne en agilité et en fluidité. En s'associant à IBM, le grand armateur Maersk a mis en place une blockchain lui permettant d'avoir tous les documents nécessaires aux expéditions. Grâce au *smart contract*, les capacités de



**Bertrand Eteneau (83)**

Après une carrière dans différents secteurs industriels : la production de composants électroniques et la vente chez IBM, le transport et la logistique (SDV et Geodis), le retail aux 3 Suisses et l'industrie automobile (Faurecia), Bertrand a intégré le Boston Consulting Group en 2017. Professeur à Centrale Paris de 1996 à 2001, il fut responsable de l'option SIET (Systèmes d'information, électronique et télécoms).



# La blockchain comme tiers de confiance : un bouleversement sociétal

**On résume souvent la blockchain au Bitcoin ou à la spéculation financière. Parfois, on met en avant l'efficacité de cette nouvelle technologie qui amène les entreprises à repenser leur structure de coûts. On évoque plus rarement le bouleversement sociétal qu'elle engendre. Le point avec Nicolas Videgrain (Supélec 16), directeur opérationnel à VP Santé.**



**Nicolas Videgrain  
(Supélec 16)**

Après l'obtention de son diplôme et d'un second en industrie des réseaux et économie du numérique à l'université Paris-Saclay,

Nicolas a été amené à travailler dans les secteurs de la blockchain, l'IA, puis la santé où il évolue à présent. Aujourd'hui, il garde la passion de ces deux technologies, dont il pense qu'elles vont changer notre société.

La première caractéristique de la blockchain est qu'aucun tiers de confiance n'est nécessaire à son maintien puisque tous les processus sont décentralisés : l'information est en effet détenue et modifiée par toutes les parties prenantes. Ainsi, au lieu d'utiliser les services d'une entité en laquelle on doit avoir confiance pour consulter ou modifier une information, on passe par des milliers et des milliers de petites entités appelées des mineurs. Alors qu'est-ce que cela change ?

D'une part, le risque que l'information soit altérée disparaît : des algorithmes cryptographiques rendent les données sur les blockchains presque impossibles à modifier sans l'accord des autres utilisateurs. D'autre part, l'information contenue sur une blockchain peut rester réellement privée : si la blockchain est bien construite, les mineurs ne peuvent pas accéder librement aux données qui sont dessus, alors qu'un tiers de confiance peut consulter les données qu'on lui confie. Derrière ces deux principes généraux et

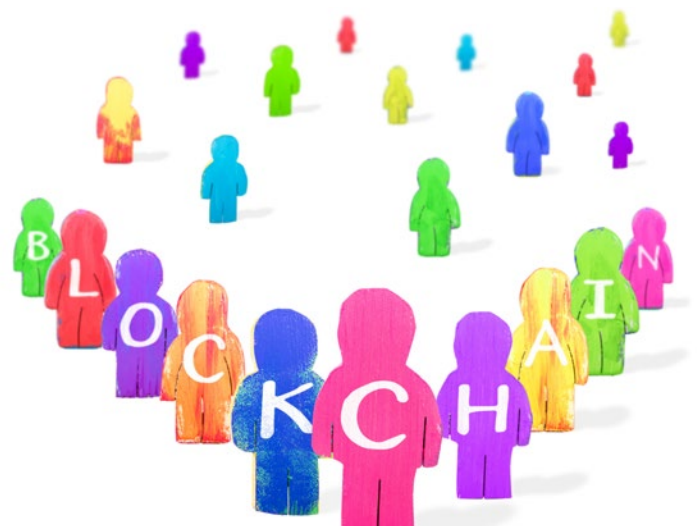
abstrait se cache un paradigme sociétal de la gestion des données véritablement nouveau.

## Rétablir la confiance dans « le système »

Dans une société moderne à l'aube de la blockchain, Cambridge Analytica n'est qu'un scandale parmi d'autres qui nous rappelle qu'on ne peut même pas faire confiance aux cerveaux de Facebook pour la gestion de nos données. À l'heure où en France les gilets jaunes font les gros titres en appelant à retirer massivement des espèces, on se rappelle que la défiance vis-à-vis du système bancaire sclérose le débat social depuis des générations. Avec la blockchain, la société dispose d'un ensemble de lois mathématiques à qui elle peut confier ses données et son argent. Rétablir la confiance dans ces domaines permettra de lever les réticences actuelles à l'adoption des nouvelles technologies, ainsi que les freins à l'évolution socio-économique.

D'aucuns trouveront le changement induit par la blockchain trop maigre pour être qualifié de « bouleversement sociétal », mais c'est regarder le monde à travers le prisme des sociétés avancées. En 2016,

*The Economist* a recensé 51 pays sous un régime autoritaire, soit près d'un tiers (32,7 %) de la population mondiale. Le dénominateur commun de ces régimes est l'étendue du pouvoir dont disposent les autorités, bien plus que la répression ou la privation de libertés. Or, il faut bien voir que ce pouvoir est en partie issu de celui que les habitants sont obligés de confier au tiers de confiance. Un exemple simple est celui de la propriété : la capacité qu'ont certaines entités à s'attribuer les biens d'autrui provient souvent soit d'une absence de plan cadastral, soit du fait que ce plan est aux mains d'une entité libre



de les modifier à sa convenance. Avec une blockchain, cette modification ne serait pas possible. Ainsi la blockchain n'est pas seulement une véritable opportunité de repenser les business models des entreprises, c'est aussi un outil qui permettrait d'émanciper la société, et pas seulement dans les pays suffisamment avancés d'un point de vue technologique. ■

# Blockchain et monde de l'art

**Source d'inspiration pour les artistes, la blockchain ouvre également de multiples perspectives au marché de l'art. On pourra acheter des œuvres avec des cryptomonnaies, établir des registres globaux de toutes les transactions ou encore utiliser les *smart contracts* pour garantir la sécurité et traçabilité des ventes. Explications avec Bertrand Scache (86), CTO de Monart, première plateforme mondiale de blockchain consacrée à l'art.**



**Bertrand Scache (86)**

Bertrand a articulé sa carrière autour du numérique, de l'innovation et de la créativité. Après une expérience variée au sein de grandes entreprises (Thales, L'Oréal, Danone) et de PME, il est depuis dix ans consultant expert en innovation numérique, associé dans des start-up, et enseigne à Sciences Po. Il participe à l'aventure Monart en tant que CTO.

Le monde de l'art est réputé opaque, géré de façon non transparente par un petit nombre d'acteurs, galeristes de renom, critiques d'art et experts, seuls à même d'authentifier des œuvres, de suivre leur vie et de leur attribuer une valeur. La blockchain peut dans ce cadre jouer son rôle d'un registre de transactions distribué, transparent et infalsifiable. À partir de l'identification initiale d'une œuvre sur la blockchain, puis des enregistrements successifs de toutes les transactions, se constitue ainsi un cahier de bord d'une œuvre. De nombreuses start-up tentent de répondre à cet usage, de l'historique Ascribe dès 2013 aux plus récentes Verisart ou ArtChain Global. Reste que la validité de l'enregistrement initial de l'œuvre impose la confiance dans l'acteur l'ayant réalisé, et dans son processus d'authentification.

## Les *smart contracts* pour sécuriser les ventes

Une fois l'œuvre enregistrée de façon authentique sur la blockchain, le « *smart*

*contract* » permet de gérer sous forme entièrement dématérialisée les multiples transactions possibles sur cette œuvre : transfert de propriété, permanente ou temporaire, multipropriété d'une œuvre individuelle ou d'une collection, création de produits dérivés (impressions...), vente aux enchères. Seuls la puissance du langage de ces *smart contracts* et la capacité des développeurs spécialisés à mettre au point ces différents types de transaction limitent le champ des possibles. Là encore, la confiance dans ces transactions vient de la capacité à prouver la validité formelle et légale de ces *smart contracts*. De nouveaux enjeux pour les systèmes de preuves de programme, les auditeurs et les juristes spécialisés !

## Valoriser le talent des artistes

Le marché de l'art est aussi un marché financier, dont les performances sont supérieures à la plupart des marchés actions ou autres. La valeur créée par la croissance du marché n'est cependant que faiblement captée par ceux qui en sont à l'origine, les artistes eux-mêmes. D'où l'émergence de cryptomonnaies spécialisées sur le marché de l'art. Ces cryptomonnaies sont alors capables de rémunérer les artistes pour toutes les transactions dérivées, ainsi que

les acteurs ayant contribué à la valorisation des œuvres par leurs recommandations ou curations. Plusieurs start-up telles qu'Artex, Artlery ou Monart abordent l'ensemble de ces usages de façon intégrée, en créant différents types de tokens adaptés à chacun. Enfin, les artistes se sont emparés de la blockchain comme d'une nouvelle technique pour créer. *Plantoid* (photo), élaborée par Primavera de Filippi, est un exemple d'œuvre fondée sur la blockchain<sup>1</sup>. Cette plante de forme hybride, physique et numérique, est capable de se reproduire elle-même, en activant un *smart contract* exécuté sur la blockchain Ethereum, lorsqu'elle est suffisamment nourrie en bitcoins par des humains (ou d'autres entités). ■

Quand la blockchain inspire les artistes. *Plantoid*, une œuvre de Primavera de Filippi.



1. <http://okhaos.com/plantoids/>

## → Monart, la blockchain au service de l'art

Monart développe une place de marché et une communauté autour de l'art contemporain en exploitant toutes les potentialités de la blockchain. De l'authentification des œuvres, réalisée par les artistes eux-mêmes, aux multiples possibilités d'échange offertes par ses *smart contracts*, Monart permet à sa communauté de savourer la création artistique en partageant la valeur créée.



# Une grande promesse qui a fait pschitt ?



**Depuis son émergence en 2008 avec le Bitcoin, la blockchain a beaucoup fait rêver : suppression des intermédiaires, traçabilité des échanges, décentralisation de l'exécution de transactions via les « smart contracts »... Pourtant, les passages à l'échelle restent rares. Aujourd'hui, quel bilan et surtout quels enseignements en retirer ? Le point avec Alexandre Martinelli (Supélec 00), CEO et cofondateur de La Javaness, accélérateur numérique spécialisé en IA.**

**S**elon de nombreux observateurs, 2018 devait être l'année de l'adoption massive de la blockchain grâce à un cadre juridique adapté et la fin des problèmes techniques de ces « Distributed Ledger Technologies ». En fait, elle a été l'année des grandes désillusions : baisse massive du cours du bitcoin, pratiques douteuses autour du fonctionnement des ICO (pyramide de Ponzi), lancement de nombreuses PoC<sup>1</sup> par des entreprises, des administrations ou des consortiums, mais quasiment aucune industrialisation.

Plus largement, les premières initiatives autour des technologies blockchain visaient soit les consommateurs (le « C ») – c'est typiquement le cas du Bitcoin, qui a été adopté initialement par des consommateurs attirés par la promesse d'une véritable monnaie décentralisée – soit le remplacement de systèmes existants dans le business (le « B ») comme l'initiative R3. Pourtant, dix ans après son émergence, l'utilisation du Bitcoin par le grand public reste très limitée, notamment à cause de sa forte volatilité. Quant à R3, c'est jusqu'ici un fiasco... Nous pouvons d'ailleurs en témoigner à La Javaness puisque nous avons été sollicités pour participer à de nombreux projets blockchain : mise en place avec une grande banque d'une marketplace de vente de voitures d'occasion permettant de sécuriser les paiements (les chèques de banque font en effet l'objet de nombreuses fraudes), mise en œuvre par un consortium industriel d'un système

de « contract management » sécurisé, déploiement d'un dispositif de gestion de l'identité numérique... Ces projets en sont malheureusement restés au stade de l'expérimentation.

## Une question de temps

Cette trajectoire est en fait complètement normale. La blockchain n'a en effet que dix ans de maturité et risque de suivre la même courbe d'adoption que les autres technologies de rupture : une période de vingt à trente ans alliant découverte, emballement, déception puis appropriation très progressive de la technologie par des « pure players », suivie d'une seconde période

de déploiement et de passage à l'échelle d'une durée similaire. C'est d'ailleurs précisément ce qui s'est produit avec les technologies Internet qui datent des années 1970 ou avec l'intelligence artificielle : après un renouveau théorique dans les années 1980, la phase d'industrialisation n'a commencé qu'à partir de l'émergence du deep learning en 2012. Cela explique que les « bricks and mortar »<sup>2</sup> du B2C, mal conseillés par les cabinets de conseil en stratégie depuis de trop nombreuses années, aient mis plus de vingt ans pour prendre conscience qu'Internet n'était pas une simple technologie mais bien le socle de transformation de leur *business model* (via les logiques de plateformisation et d'expérience client augmentée par l'IA).

Pour autant, la transformation digitale du B2B n'en est encore qu'à ses balbutiements. Nous avons donc la conviction que le cycle d'adoption de la blockchain va s'accélérer. Elle sera pour le B2B ce qu'Internet est au B2C pour les grandes entreprises : le socle de la transformation de leurs business models. Et c'est une très bonne nouvelle, car le B2B représente près des trois quarts de l'économie mondiale : il n'est donc pas trop tard pour que des GAFAB/BATX à l'européenne puissent émerger, dès lors qu'ils se focaliseront sur le B2B, la blockchain et l'IA. ■



**Alexandre Martinelli (Supélec 00)**

Ingénieur chez Capgemini, puis directeur chez Eurogroup Consulting, Alexandre a cofondé La Javaness en 2015. Vainqueur de Big Data Paris en 2018 et opérateur du programme start-up de Facebook à Station F, La Javaness accélère l'innovation numérique des grandes organisations et développe des solutions cognitives fondées sur sa technologie de *real-time machine learning*.

1. Proofs of concept.

2. Entreprises ou enseignes commercialisant leurs produits ou services dans des magasins physiques.