

École Polytechnique, Palaiseau  
Amphithéâtre Faure

# Blockchain pour les métiers

**Jeudi 21 mars 2019**



Coordination scientifique :

- Jean-Michel BATTO (Eiffage Energie Systèmes)
- David MENGA (EDFlab)



Blockchain  
pour les métiers

Partenaire:



## ***Editorial Board***

Dr. Christophe Calvin (CEA)

M. Laurent Duplouy (BnF)

M. Philippe Wlodyka (Polytechnique)

M. Pascal Pavel (CEA)

Dr. Thiên-Hiệp Lê (ONERA)

Mme Katia Castor (ARISTOTE)

# ***Blockchain pour les métiers***

Séminaire Aristote,

21 mars 2019 à l'École Polytechnique

Coordination scientifique

Jean-Michel Batto (Eiffage Energie Systèmes) et David Menga (EDFlab)



# ***Table des matières***

<u>Introduction</u> , par Jean-Michel Batto (Eiffage Energie Systèmes) et David Menga (EDF Lab).....	page 5
<u>1/ Blockchain : quelle économie ?</u> , par Xavier Dalloz (consultant).....	page 7
<u>2/ Cas d'usages pratiques de la blockchain inter-entreprises</u> , par Jérôme Lefebvre (Stratumn).....	page 11
<u>3/ L'impact d'un protocole de réservation pair à pair sur l'économie en ligne</u> , par Vidal Chriqui (BTU Protocol).....	page 14
<u>4/ Blockchain pour la transparence dans l'agro-alimentaire</u> , par Stefano Volpi (Connecting Food).....	page 16
<u>5/ Blockchain pour lutter contre la pollution digitale</u> , par Vincent de Montalivet (Digital For the Planet).....	page 19
<u>6/ La cadre réglementaire des ICO's</u> , par Diane Richebourg (DS Avocats).....	page 22
<u>7/ Blockchain pour l'énergie</u> , par Jean-Baptiste Fraysse (Blocktricity).....	page 25
<u>8/ Une blockchain éco-responsable</u> , par Sébastien Dupont-Raoseta (Uniris).....	page 27
<u>9/ Des smart contracts sécurisés par conception</u> , par Arthur Breitman (Tezos).....	page 29
<u>10/ La sécurité des cryptowallets</u> , par Pascal Urien (Ethertrust).....	page 31
<u>11/ Panel : quel avenir pour la blockchain ?</u> , animé par Mickael Champion (CEO de Data Solutions & Innovations Corporation, filiale de DSI Group), avec Nicolas Merle (Chain-Ops), François Stéphan (Be-Bound) et Xavier Dalloz (consultant).....	page 33
<u>12/ Conclusion</u> , par Daniel Menga (EDF Lab).....	page 35

# ***Introduction***

Par Jean-Michel Batto (Eiffage Energie Systèmes) et David Menga (EDFlab)



« Avec cette journée de séminaire, vous allez comprendre pourquoi, demain, vous ne pourrez pas échapper à la révolution induite par la technologie blockchain. » Jean-Michel Batto donne le ton. Il ne sera plus jamais abandonné de la journée.

La blockchain, avec ses usages multiples et ses applications variées, va, c'est une certitude, modifier de fond en comble nos comportements de tous les jours. Ce sera vrai dans la vie courante mais aussi, et de toute manière c'est très lié, dans la vie des entreprises. Rien, demain, n'échappera à la blockchain. Cette technologie vient tout chambouler, à la fois dans la perception des choses et dans leurs applications. C'est un changement clair et net de paradigme qui s'opère sous nos yeux.

Nous sommes à l'aube de cette révolution, mais révolution il y aura. « La blockchain est une technologie fondatrice, et l'heure n'est plus à se poser des questions technologiques, mais bien,

désormais, de savoir comment appliquer cette technologie dans les différents métiers, au quotidien », avance David Menga.

Tout cela pour dire que la blockchain, c'est très concret et, comme se plaît à la démontrer David Menga en sortant quelques magazines de son sac, c'est déjà dans l'actualité. « Prenons quelques magazines, s'amuse-t-il, joignant le geste à la parole. Regardez La Recherche, en une : Qu'est-ce que la blockchain et comment ça marche ? Un autre exemple avec le dernier numéro de L'Informaticien. En une, toujours : Blockchain, les grands éditeurs débarquent en force. La blockchain est partout, vous le voyez et, au travers de cette journée de séminaire, nous allons entrer encore plus dans le détail de ses applications les plus concrètes et les plus utiles aux métiers. »

Mais un mot, avant cela, sur ce qu'est la blockchain, justement. La blockchain est une technologie de stockage et de transmission d'informations sans organe de contrôle, qui a été créée en 2008 avec la cryptomonnaie Bitcoin. En dix ans, évidemment, la technologie a fait du chemin et s'est largement émancipée d'une seule application liée aux cryptomonnaies.

Pour faire simple, une blockchain peut se concevoir comme une gigantesque base de données, sécurisée et infalsifiable. Infalsifiable dans le sens où tout ce qui y est écrit est ensuite impossible à effacer. La traçabilité est donc inhérente à son fonctionnement, et le caractère décentralisé de la blockchain, couplé avec sa sécurité et sa transparence, promet des applications bien plus larges que le seul domaine monétaire.

C'est tout l'objet de ce séminaire, organisé par l'association Aristote, dont la mission est de vous aider à mesurer les enjeux et à savoir vous positionner pour ne pas subir la révolution que va créer la blockchain.

Alors que l'Internet a permis à chacun de se connecter à toutes les sources de savoir et de divertissement, la blockchain va donner la quasi-gratuité à la confiance dans les services et les outils. L'association Aristote, dans sa lecture de l'avant-garde du numérique, pose un diagnostic sans appel sur le futur : il se fera avec la blockchain et avec un coût maîtrisé.

Place donc, maintenant que ceci est posé, à un programme très riche.

# 1/ Blockchain, quelle économie ?

Par Xavier Dalloz, consultant



« Mon métier est d’imaginer ce que sera le monde dans les dix prochaines années. Je fais cela depuis 1976. Et si les technologies changent, l’état d’esprit est toujours le même, malheureusement. Il est de se dire que ça ne marchera jamais. Je peux vous faire une liste impressionnante en la matière, il en va toujours ainsi... Et pourtant ! Tous les dix ans, une innovation majeure, une innovation de rupture, vient bouleverser les champs d’actions de nos vies. Et la blockchain vient s’insérer dans cette liste. Dans dix ans, je vous le dis, on ne se posera même pas la question : la blockchain sera partout. »

C’est peu de dire que Xavier Dalloz croit en la révolution de la blockchain. Elle est, à ses yeux, partie intégrante, de la dernière révolution technologique décennale en cours, depuis 2014. A savoir celle de l’IoM, pour Internet of me, cette manière nouvelle de concevoir les choses, où ce qui compte, c’est désormais la qualité des interactions permises et générées. Cette nouvelle manière d’appréhender les choses s’inscrit donc pleinement dans la longue liste des innovations majeures qui, tous les dix ans, viennent balayer le monde ancien :

1944 : le premier ordinateur

1954 : le premier mainframe

1964 : le premier mini-ordinateur

1974 : le premier micro-ordinateur

1984 : MacIntosh

1994 : le web

2004 : la RSE

2014 : l'avènement de l'Internet of me avec les smart contracts. La création de valeur est dans la qualité des interactions.

Dans ce contexte de changements de paradigmes forts et finalement très réguliers, à chaque fois, la grande question qui se pose, et qui fait toute la différence entre les adeptes et les réticents, est celle de la confiance. Car, enfin, si à chaque fois la réaction première est de se dire que cela ne marchera jamais – alors que si, évidemment, non seulement ça marche, mais cela s'impose à nous, de gré ou de force – ce n'est pas uniquement par atavisme. C'est par manque de confiance.

La confiance... Tel est le mot clé. Et c'est là, justement, que se niche le grand avantage de la blockchain. Cette technologie a en effet pour vertu première cette idée même de confiance ! La sécurité des transactions effectuées est assurée par un réseau d'ordinateurs qui valident et certifient la transaction avant de l'inscrire de manière définitive dans un bloc. Une fois enregistrée, cette transaction devient infalsifiable et facilement vérifiable. Il s'agit donc d'un réseau distribué au sein duquel les transactions s'effectuent en pair à pair (P2P). Et ce sans qu'à aucun moment la question de la confiance soit mise à mal.

Plus besoin, en d'autres termes, de l'intervention d'un tiers de confiance (notaire, banque, État, plateforme d'intermédiation de type Uber, AirBnB, etc.) pour valider ou certifier la transaction. Cette fonction d'intermédiaire, avec la blockchain, n'a plus lieu d'être puisque tout est tout l'objet d'un consensus : le fait qu'une transaction soit acceptée ou rejetée est le fruit d'un consensus distribué et non d'une institution centralisée.

Et lorsque l'on parle de transactions, attention, cela va bien sûr bien au-delà d'une simple opération de paiement ou d'enregistrement. Cela va jusqu'à des instructions beaucoup plus complexes : on parle alors de contrats. Et puisque ces contrats sont publiés sur une blockchain



pour qu'ils s'exécutent automatiquement sous certaines conditions, on parle alors de « Smart Contracts ». Un exemple ? Vous avez une voiture, vous n'en avez pas payé les traites... elle ne démarrera pas !

Les enjeux, on le voit, sont énormes. Tous les acteurs impliqués dans l'intermédiation sont concernés : les banques, les assureurs, les notaires, les avocats, etc. C'est bien, au final, un marché de plusieurs milliers de milliards de dollars qu'il faut réinventer !

Bill Gates disait : « We need banking but we don't need bank ». C'est exactement cela qui se joue. La manière de faire des affaires change du tout au tout. Nous allons vers la destruction massive des tiers de confiance.

En clair, il s'agit de rompre avec le passé pour construire un avenir nouveau. Nous sommes dans un monde massivement interconnecté, ce qui vient directement influencer la chaîne de production de valeurs. L'objectif, in fine, est de faire passer cette création de valeurs des équipements, des biens, comme c'est le cas aujourd'hui, vers les services. C'est en cela que nous sommes pleinement dans l'ère de l'internet of me, avec un consommateur-citoyen qui se trouve désormais au cœur de tout le système. Un système, donc, basé sur des interactions multiples et décentralisées. Dans ce contexte, la place et le rôle des entreprises changent. Ce qu'elles doivent être, désormais, ce sont des plateformes.

Nous sommes dans un monde d'interactions constantes et facilitées par la technologie. Même les objets peuvent entrer en interaction entre eux et avec nous. Le monde ne peut plus se décrire autrement que comme un ensemble de réseaux imbriqués les uns avec les autres, les uns dans les autres. Le tout dans une logique de communication entre pairs, entre égaux, opposée à l'organisation centralisée, pyramidale, qui est celle de la majorité des entreprises et des administrations.

Pour les entreprises, enfin, les applications de la blockchain se résument de la façon suivante : il s'agit de créer un tissu de confiance décentralisé pour entrer dans une nouvelle ère de collaboration et d'échange de données entre les appareils, les applications, les entreprises et les utilisateurs permettant ainsi de trouver un bon compromis entre évolutivité, sûreté et sécurité des échanges.

Comment ? Les six lettres du mot « impact » viennent tout résumer : I pour identification des personnes et/ou des objets, M pour monnaie de l'échange, P pour la notarisation des échanges, A pour l'autonomie de tous les processus nécessaires à l'échange, C pour le contrat associé à l'échange et T pour la traçabilité de l'échange.

Blockchain = Impact, et cela va changer radicalement tous les modèles économiques actuels que l'on a en tête. Dans ce contexte, la clé de tout ce système qui est en train de se mettre en place, c'est la décentralisation globale et complète de tout. Cela pose quand même un problème, à tout le moins une question. Celle de savoir comment mesurer la valeur, quand même. C'est tout l'enjeu de la « PEC », pour productivité des échanges collaboratifs. C'est cet indicateur, nouveau, qui va être la clé de voûte de cette nouvelle manière de faire du business qui se crée. Le partage est l'avenir de tout.

## ***2/ Cas d'usages pratiques de la blockchain inter-entreprises***

Par Jérôme Lefebvre, Stratumn



Pour sortir de la seule association aux cryptomonnaies et trouver une utilisation innovante pour la blockchain, une poignée d'entreprises visionnaires sont en train d'inventer de nouvelles solutions mêlant cryptographie, blockchain et solutions de connectivité. L'idée sous-jacente à tout ce travail ? Rétablir la confiance qui s'est massivement altérée après les scandales divers et variés liés à la traçabilité. L'opportunité est immense. Il n'y a qu'à la saisir.

Seulement, nous sommes encore à l'âge de pierre dans de trop nombreux secteurs d'activité. On s'échange des mails pour mettre en place des protocoles d'accord, on utilise des outils manuels pour finaliser les choses, on a recours à des intermédiaires de confiance... On a même connu des entreprises où, sans le savoir, cinq commerciaux venaient démarcher les mêmes personnes. C'est mauvais pour l'entreprise qui gaspille du temps, donc de l'argent, et qui prend le risque de mettre en colère le potentiel futur client. Heureusement, toutes ces incohérences et ces procédures d'arrière-garde vont disparaître avec la blockchain. Il est urgent de changer la donne et Jérôme Lefebvre nous explique pourquoi. Et surtout comment.

Garantir la confiance, la sécurité et la confidentialité, le tout dans une transparence totale, voilà l'enjeu primordial de tout le système. Et voilà, surtout, toute la raison d'être de Stratumn.

Un mot, à ce propos, en guise de court aparté dans ce compte-rendu, sur ce qu'est Stratumn. Stratumn, c'est à noter, a remporté le prix de la Fintech de l'année, décerné par le pôle de compétitivité Finance Innovation. La start-up a développé une technologie qui couple blockchain et cryptographie afin d'assurer la confidentialité des données et la sécurité des échanges. La solution mise au point par Stratumn propose de digitaliser la collecte de données grâce à des interfaces (API) sécurisées qui viennent se connecter aux différents systèmes d'information, puis de rendre le processus traçable par plusieurs entités.

Pour résumer, le protocole de Stratumn promet à tous les participants d'avoir confiance dans un processus commun en enregistrant de manière immuable qui a fait quoi, quand, où et comment. La blockchain est utilisée pour établir un horodatage précis de chacune des étapes.

L'idée, derrière tout cela ? Permettre de créer du revenu additionnel, générer une baisse des coûts et une réduction des coûts. A la clé, une nouvelle manière de revoir l'organisation des entreprises et la manière de travailler. Telle entreprise du domaine de l'assurance condamnée à verser 40 millions d'euros d'amendes parce qu'elle n'a pas été capable de retrouver le nom des bénéficiaires de contrats d'assurances-vie en déshérence ? Voilà qui devrait faire réfléchir. C'est d'autant plus inadmissible que la solution existe. Elle est sous nos yeux. La blockchain offre toutes les garanties pour éviter cela, en temps réel qui plus est...

65% des responsables Achats se disent sans visibilité sur leurs fournisseurs de rang 2... Cela ne peut pas plus durer. Cette opacité est, en plus, génératrice de risques encourus. Dans la grande distribution, on estime ainsi à 9 milliards de dollars le coût annuel de la fraude fournisseurs.

Ce n'est pas tenable, et Stratumn propose de restaurer et de garantir cette confiance qui fait trop souvent défaut. La solution mis au point permet de synchroniser, en temps réel, toutes les données échangées entre partenaires. Le tout dans une totale sécurité et avec une complète confidentialité grâce à l'encryptage des données partagées.

A la clé, des effets très concrets, qui parleront à tous. Tel client, qui avait besoin de pouvoir disposer d'une traçabilité complète de sa matière première depuis l'Inde jusqu'aux Etats-Unis a pu, via la fluidité permise par la solution Stratumn, générer 2% de revenus additionnels. Et ce sur ces contrats de plusieurs millions d'euros.

Tel autre client, Thales pour ne pas le nommer, et cette fois sur un chantier de construction à Dubaï, était quant à lui confronté à un problème de traçabilité de tous les documents relatifs à la sécurité des opérations menées. Ce qui était fastidieux et coûteux devient, grâce à la blockchain et à Stratumn, beaucoup plus simple. Donc moins cher : 43% de réduction de coûts à la clé.

### ***3/ L'impact d'un protocole de réservation pair à pair sur l'économie en ligne***

Par Vidal Chriqui, BTU Protocol



Les plateformes de réservation telles qu'on les connaît, de type Booking ? Il est possible, désormais, de parfaitement s'en passer. Ou comment, en somme, comme il existe un circuit-court appliqué aux produits alimentaires, directement via le producteur, il est désormais loisible d'appliquer ces mêmes vertus aux secteurs du tourisme et de la réservation en ligne.

C'est ce que permet BTU Protocol. BTU Protocol entend imposer un protocole s'appuyant sur la blockchain afin de s'attaquer au marché de la réservation en ligne. L'objectif est donc de se passer des centrales de réservations, qui jouent un rôle d'intermédiaire sur ce marché.

L'idée principale du système est de permettre à un acteur qui fait de la recommandation de proposer directement chez lui un outil de réservation, sans passer par un intermédiaire. En clair, vous tenez un blog ou un site spécialisé dans le voyage, jusqu'ici vous renvoyez vers les plateformes de réservations classiques quand vous parlez de tel ou tel hôtel. Avec BTU Protocol, vous pouvez directement proposer la chambre d'hôtel depuis votre site. Appliqué à

un comité d'entreprises, bien sûr, les volumes seront encore plus grands. Et comme, évidemment, pour que chacun y trouve son intérêt, il convient d'y avoir une gratification, l'idée est de renverser le partage de la valeur. Exit les intermédiaires ! Celui qui, directement, joue ce rôle, se voit récompensé en gagnant des BTU. Pour le client final, celui qui réserve la chambre, la transaction se fait de manière traditionnelle, en monnaie sonnante et trébuchante.

Le système propose ainsi des logiciels dédiés qu'un apporteur d'affaires pourra intégrer directement sur son site. Sur la blockchain (ici Ethereum) le système se charge de répertorier les offres de réservation disponibles de manière transparente et accessible à tous. Le module de réservation se contente de récupérer ces données et d'indiquer sur la blockchain quelles réservations ont été confirmées, afin de permettre à tous de bénéficier de données à jour. La particularité de BTU est de ne pas vouloir proposer une plateforme unique et centralisée, mais de proposer des modules qui pourront être intégrés par les blogueurs, sites de recommandations ou autre qui redirigent les utilisateurs.

Ainsi, se crée un canal de distribution nouveau, ouvert et fluide, permettant à n'importe qui, en pleine confiance, de se faire « agence de voyage ».

## ***4/ Blockchain pour la transparence dans l'agro-alimentaire***

Par Stefano Volpi, Connecting Food



Connecting Food, c'est un italien et une anglaise qui, ensemble, se sont réunis pour créer une entreprise française. Mais pas n'importe quelle entreprise. Une entreprise se donnant pour mission, grâce à la blockchain, de permettre à un secteur d'ordinaire aussi opaque que l'agro-alimentaire de jouer la carte de la saine transparence.

Créée en 2016, Connecting Food est née d'un constat simple : les filières alimentaires sont complexes, et manquent souvent de transparence pour les consommateurs, qui deviennent de plus en plus exigeants. Pour répondre à ces besoins, Connecting Food a construit une plateforme de traçabilité alimentaire qui utilise la blockchain pour assurer une traçabilité en temps réel de tous les produits d'une filière alimentaire. Son système d'audit en temps réel permet de s'assurer que ces produits sont conformes à leur cahier des charges, mais aussi que les informations enregistrées sont vraies. En bout de chaîne, les consommateurs peuvent eux aussi avoir accès à ces informations, redonnant ainsi du sens à leur alimentation.



Un enjeu clé si l'on a en tête cette statistique assez effrayante : si, en 2017, seulement 44% des Américains déclaraient avoir confiance en leur alimentation, cette proportion, déjà basse, est tombée à 31% en 2018. Il faut donc agir, cela devient urgent.

Connecting Foods est là pour cela avec, comme mission clé, de rétablir la confiance des consommateurs dans les produits qu'ils achètent et consomment au quotidien.

L'idée est donc ici d'apporter une solution de traçabilité sur l'ensemble de la filière, lot par lot, grâce à la blockchain. Aujourd'hui, cette traçabilité existe, mais seulement de manière « dormante » : en cas de problème, les industriels sont capables de remonter la chaîne et, in fine, de procéder au retrait des produits qui sont contaminés par exemple. Cf le cas Lactalis ou encore le cas de la viande polonaise. L'ennui, c'est que tout cela prend du temps et ne se fait donc qu'a posteriori.


























Ce que permet la blockchain, c'est le contrôle en temps réel, et cela change tout. Concrètement, Connecting Food repose sur une idée simple : savoir ce que l'on mange réellement. Pas en faisant confiance aux promesses parfois floues des emballages, mais en auditant de manière automatique et sûre chaque étape de l'approvisionnement et de la production, en s'assurant que tous les critères du cahier des charges sont respectés. Et ce via la blockchain.

Un produit est donc dorénavant « tracé » depuis la production de la matière première jusqu'à la distribution au client final. En temps réel, et à chaque étape, il est également possible de contrôler la conformité de la production avec les critères du cahier des charges défini. L'interface Connecting Food détecte instantanément les produits non-conformes ou les erreurs de production, permettant ainsi d'éviter les rappels consommateurs, toujours désastreux pour l'image de la marque ou du distributeur.

Enfin, à l'autre bout du spectre, le consommateur, lui, via une application, peut en scannant les QR-Codes ou les Gencodes, obtenir toutes les informations qu'il voudrait, en pleine transparence : origine des ingrédients, lieux de production et de transformation, mode d'élevage, rémunération des producteurs, etc.

Connecting Foods, travaille déjà sur 25 filières. En voici la liste. Pour chacune, la traçabilité est totale et permet donc d'absolument tout savoir. Le tout avec une blockchain dite « à permission », c'est-à-dire permettant de gérer les accès.

Voici la liste de ces 25 filières :

 Œufs	 Lait
 Porcins	
 Volailles	 Sucre
 Bovins	 Café
 Ovins	 Chocolat
	 Vanille
 Blé	 Sel
 Orge	
 Riz	 Miel
 Maïs	 Eau
 Oléagineux	
 Protéagineux	 Poissons et crustacés
 Légumes secs	 Coquillages & mollusques
 Fruits & légumes frais	
 Fruits & légumes transformés	
 Pommes de terre	

## ***5/ Blockchain pour lutter contre la pollution digitale***

Par Vincent de Montalivet, Digital For the Planet



Comment la blockchain peut-elle lutter contre la pollution digitale ? Vaste question, mais cruciale. « Notre vocation est de sensibiliser à l'écologie digitale, explique Vincent de Montalivet. Elle est, aussi, de conseiller les entreprises pour les aider à réduire leur impact carbone.

Pour ce faire, un écolabel a été créé, Digital for the Planet, afin de certifier la diminution des impacts digitaux décidés par les entreprises. Vingt-cinq entreprises et villes font déjà confiance à Digital for the Planet.

Encore une fois, l'enjeu est colossal. Il faut en effet avoir en tête ce que représente la pollution numérique : c'est, déjà, l'équivalent de l'impact de l'aviation civile, pour vous donner une idée. C'est énorme. Et donc, si pour préserver l'environnement vous avez déjà décidé de ne plus prendre l'avion, il vous faudrait, pour bien faire, cesser désormais d'être connecté pour être en parfait accord avec cette décision... Cela donne à réfléchir.

Chaque heure, dans le monde, plus de 10 milliards de mails sont envoyés. Un acte qui n'est bien sûr pas neutre, pas sans conséquence : envoyer des mails, stocker des données, regarder des vidéos en streaming, autant d'activités courantes qui ne sont pas neutres pour l'environnement.

Ainsi, pour élargir le champ des informations au-delà des seuls éléments fournis à l'occasion de ce séminaire, nous vous donnons ces quelques statistiques clé, afin que chacun puisse avoir en tête ce dont nous parlons. Via les informations distillées par Digital for the Planet, nous apprenons qu'une requête Google, c'est à peu près 7 grammes de CO2 émis dans l'atmosphère. Taper l'URL du site directement dans la barre d'adresse consomme beaucoup moins. Ou alors mettre les adresses récurrentes dans ses Favoris, pour éviter ces recherches à chaque fois. Autre bonne pratique à mettre en place, de manière finalement très simple : veiller à fermer les onglets ouverts quand ils ne servent plus : chaque page se recharge en effet plusieurs fois dans la journée, ce qui multiplie à chaque fois la requête initiale, et donc l'émission de ces 7 grammes de CO2.

Sept grammes, ce n'est peut-être rien, mais mis à bout, c'est vraiment énorme. Et très mauvais pour la planète. Envoyer un mail émet ainsi 17 à 22 grammes de CO2 dans l'atmosphère. Pour rendre tout cela plus concret, il faut avoir en tête que l'envoi de trente-trois courriels d'1 Mo à deux destinataires par jour et par personne génère ainsi des émissions équivalentes à 180 kg de CO2 par an. Cela correspond à plus de 1000 km parcourus en voiture.

Ceci posé, revenons au séminaire en lui-même. Le digital, c'est déjà 16% de la consommation électrique en France. Et c'est sans parler, encore, des problématiques liées à la fabrication : en matière d'énergie consommée, produire un gramme de smartphone, c'est une consommation 80 fois plus importante qu'un gramme pour une voiture. C'est sans parler, aussi, des problématiques liées à la fin de vie de nos appareils électriques : cela représente 55 millions de tonnes de déchets par an.

Si l'on sonde la population, alors les résultats sont éloquentes : 77% des personnes n'ont pas conscience de ces impacts, allant parfois jusqu'à même ignorer ce que peut être la pollution numérique. Mais, une fois qu'on leur explique, alors elles sont 91% à dire qu'il convient de se pencher sérieusement sur ces questions. C'est là une proportion encourageante.

Mais ceci posé, reste une question : comment la blockchain peut-elle aider ? Comment peut-elle devenir un levier permettant d'apporter plus de justice et d'équité dans la distribution de la valeur ; un levier capable d'assurer que les bons biens et les bons services sont délivrés aux bonnes personnes et, ainsi, permettre de regagner la confiance des citoyens ? Simple. La blockchain facilite le travail d'accompagnement vers les bonnes pratiques digitales. Elle facilite, aussi, les techniques de certification. Cela permet des approches globales et instantanées, vérifiables en temps réel et non plus sujettes au bon vouloir des participants. Alors, oui, la blockchain peut être un outil dans cette transition écologique et économique que nos sociétés sont en train d'engager.

## ***6/ Le cadre réglementaire des ICO's***

Par Diane Richebourg, DS Avocats



Diane Richebourg, avocate au sein du cabinet DS Avocats, vient évoquer le cadre réglementaire des ICO's.

Pour mémoire, les ICO's, pour initial coin offerings, sont des levées de fonds en cryptoactifs. Elles consistent, pour une entreprise, à émettre des jetons (tokens) numériques, fondés sur la blockchain. Avec le projet de loi Pacte actuellement en discussion au Parlement, ces ICO's pourront désormais bénéficier d'une certification délivrée par l'Autorité des marchés financiers (AMF). Une manière, donc, de réglementer ce système des ICO's et ce même si ce visa ainsi délivré restera toutefois optionnel.

Ces ICO's se sont multipliés, notamment en 2017, avant que le rythme ne se ralentisse aujourd'hui, du fait des nombreuses arnaques constatées. D'où, d'ailleurs, cette loi Pacte pour leur donner un cadre juridique. Ce qui devrait donc permettre à ces ICO's de connaître à nouveau un net regain sitôt ce projet de loi Pacte promulgué.

Mais ce projet de loi Pacte, justement, que dit-il ?

Tout d'abord, et c'est bien normal, il entend définir les choses dont on parle. C'est ainsi que :

- Un jeton se définit comme étant « tout bien incorporel représentant, sous forme numérique, un ou plusieurs droits pouvant être émis, inscrits, conservés ou transférés au moyen d'un dispositif d'enregistrement électronique partagé permettant d'identifier, directement ou indirectement, le propriétaire dudit bien. »
- Un actif numérique se définit comme : « Toute représentation numérique d'une valeur qui n'est pas émise ou garantie par une banque centrale ou par une autorité publique, qui n'est pas nécessairement attachée à une monnaie ayant cours légal et qui ne possède pas le statut juridique d'une monnaie, mais qui est acceptée par des personnes physiques ou morales comme un moyen d'échange et qui peut être transférée, stockée ou échangée électroniquement. »
- Une ICO : « Une offre au public de jetons consiste à proposer au public, sous quelque forme que ce soit, de souscrire à ces jetons. » Ne constitue en revanche pas une offre au public de jetons l'offre de jetons ouverte à la souscription par un nombre limité de personnes, fixé par le règlement général de l'Autorité des marchés financiers, agissant pour compte propre. »

Les définitions étant posées, d'autres questions restent en suspens. Par exemple, ce projet de loi Pacte crée-t-il un droit au compte ? La réponse, en fait, est loin d'être évidente. « Les établissements de crédit mettent en place des règles objectives, non discriminatoires et proportionnées pour régir l'accès des émetteurs de jetons ayant obtenu le visa [de l'AMF], des prestataires [enregistrés ou ayant obtenu l'agrément] aux services de comptes de dépôt et de paiement qu'ils tiennent. Cet accès est suffisamment étendu pour permettre à ces personnes de recourir à ces services de manière efficace et sans entraves. » Voilà pour ce que dit le projet de loi.

Dans les faits, voilà un droit au compte qui n'en est pas vraiment un, la disposition n'étant pas, en l'état, assez contraignante à l'égard des banques. Reste à voir, maintenant, quelles seront les conditions d'application de cette disposition, lesquelles seront précisées par voie de décret. En septembre 2019 si tout va bien.

Cela viendra en tout cas poser le cadre réglementaire en France, mais qu'en est-il ailleurs ? L'approche américaine diffère largement de l'approche française qui, elle-même, diffère des approches initiées ailleurs en Europe... Diane Richebourg nous dresse un état de lieux très complet (et très juridique) de la situation. Mais ces aspects juridiques, pour abscons qu'ils paraissent et sont, n'en sont que plus importants. Ils définissent ce que sera le « territoire de jeu » demain.



## **7/ Blockchain pour l'énergie**

Par Jean-Baptiste Fraysse, Blocktricity



L'ambition de Blocktricity est de créer une blockchain pour la distribution d'énergie. Avec ici, comme idée, de se servir des outils de partage de l'information induits par le principe même de la blockchain pour aider à la gestion d'un bien commun : l'énergie.

Pour dire les choses autrement, la plateforme Blocktricity permet de créer une place de marché pour produits dérivés, où l'on vend et achète l'énergie, le tout couplé à des algorithmes qui font ensuite se rencontrer, de manière idéale, l'offre et la demande.

L'intérêt majeur réside dans la capacité de faire circuler les informations au bon moment, et ainsi faciliter l'échange et la vente d'électricité, dans la plus parfaite des transparences, tant vis-à-vis de l'origine que du prix de l'électricité.

Autre bénéfice permis, encore : celui de pouvoir organiser une vente d'énergie adaptée à la production et à la consommation locales.

Une application concrète de cette utilisation de la blockchain appliqué à un réseau énergétique est à venir dans le petit village de Vieux, dans le département du Tarn : 94 foyers du centre-bourg vont pouvoir bénéficier de la solution mise en place par Blocktricity. Cela va représenter 120 habitants, avec des installations photovoltaïques et des bornes pour véhicules électriques. L'idée va être de voir, in situ, comment tout cela s'organise et se vit. Un cadre d'expérimentation « en réel » pour prouver que cela marche et que ces vertus du circuit-court, pour faire simple, appliquées à l'énergie, sont viables grâce à la blockchain.

## ***8/ Une blockchain éco-responsable***

Par Sébastien Dupont-Raoseta, Uniris



Avec l'ensemble des présentations précédentes, nous prenons conscience de l'immensité de ce que la blockchain rend possible. Il nous faut maintenant nous pencher non sur ses limites, mais sur ses risques. Et voir, surtout, comment les contourner.

Un premier élément de réponse nous est apporté par Sébastien Dupont-Raoseta, de chez Uniris. L'idée forte d'Uniris est de proposer un service d'authentification biométrique infalsifiable. Par quelle magie ? Simple : il s'agit de s'identifier avec ses empreintes digitales. Il suffisait d'y penser.

Uniris, c'est ainsi d'abord une authentification universelle et inviolable avec laquelle il ne sera plus jamais nécessaire de retenir aucun login ou mot de passe. Uniris, c'est aussi un service qui permet de ne plus craindre une quelconque usurpation d'identité ou violation de la vie privée. Et pour une bonne raison puisqu'Uniris est capable de reconnaître chaque personne et de générer ses clés à partir de ses propres données biométriques. Le tout avec, pour l'utilisateur,

aussi bétotien soit-il, seulement son doigt à utiliser pour se connecter à un site web, pour ouvrir les portes de sa maison ou de sa voiture.

On le voit, les vertus de la blockchain sont immenses. Mais... car il y a un mais... Si ses possibilités sont magiques, pas sa consommation d'énergie, qui s'avère bien trop importante. Juste un chiffre pour s'en convaincre : Bitcoin consomme 38,7 milliards de Kw/an pour seulement 93 millions de transactions. Cela représente 414 Kw par transaction. C'est beaucoup trop. La technologie est géniale, mais cela ne peut pas continuer comme ça.

D'où tout ce travail aujourd'hui effectué notamment par Uniris pour arriver à une nouvelle génération de blockchain qui, selon toute vraisemblance, pourrait bien changer de manière pérenne le monde tel que nous le connaissons. L'idée maîtresse ? Mettre un peu d'IA à tout cela pour aboutir à une blockchain écoresponsable, qui soit un million de fois moins consommatrice d'énergie, le tout sans rien perdre de ses capacités de rapidité, bien au contraire (entre 1 et 3 secondes pour valider une transaction) et qui soit, enfin, illimitée (grâce à une augmentation des capacités linéaires à chaque nouveau « mineur » œuvrant dans le réseau).

## ***9/ Des smart contracts sécurisés par conception***

Par Arthur Breitman, Tezos



Comment peut-on protéger les contrats intelligents, via lesquels se négocient des montants de plusieurs milliards d'euros, contre les bugs ? Comment peut-on rendre une chaîne capable d'innover de manière sécurisée et décentralisée ? C'est tout l'enjeu qui a présidé à la création de Tezos. Tezos ? Il s'agit d'une cryptomonnaie et d'une plateforme de contrats intelligents de troisième génération construite autour de trois idées maîtresses : pérennité, sécurité et décentralisation. En d'autres termes : c'est une blockchain dotée d'un mécanisme de gouvernance décentralisée, et ce au travers d'auto-amendements.

Pas besoin de « fork » avec Tezos. La plate-forme reste compétitive en suivant les meilleures avancées technologiques, sans avoir à causer de chaos pour ses utilisateurs. Les participants ont de la visibilité et de l'influence sur la direction technique du projet.

Concernant les Smart Contracts, l'histoire des cryptoactifs nous a montré jusqu'à présent que si des montants importants d'actifs de valeur sont détenus dans un système, des hackers essaieront de trouver, et trouveront éventuellement, des vulnérabilités qui leur permettront de

mettre leurs mains sur ces valeurs. Afin d'anticiper des erreurs dans les smart contracts, l'équipe derrière Tezos a pris la décision de construire son protocole en Ocaml, un langage axé sur la sécurité en facilitant les opérations de vérifications formelles, une technique permettant de prouver mathématiquement l'exactitude de programmes informatiques.

## 10/ La sécurité des cryptowallets

Par Pascal Urien, Ethertrust



Cette présentation, très technique et pointue, s'applique à décrypter la question de la sécurité des cryptowallets, utilisés par les blockchains. Un enjeu considérable car ces cryptowallets stockent les clés privées des utilisateurs et calculent les signatures des transactions. Ils sont donc, sans mauvais jeu de mots, la clé de voûte du système de confiance qui s'instaure.

Ces cryptowallets se répartissent d'une part en « hot wallet » (avec des ressources TCP/IP) tels que PC, site web, smartphones... Et d'autre part en « cold wallet » (sans ressource TCP/IP) : par exemple jetons USB, tablettes, smartphones board, wallets, vault ou crypto-terminal. La sécurité peut être renforcée par des éléments matériels tels que « secure éléments », mémoires cryptographiques, crypto processeurs, TEEs, ou cartes à puce.

Un crypto-terminal s'attache à la sécurité des terminaux bancaires dans un contexte de blockchain. Les clés sont stockées dans une carte à puce dont l'assurance de sécurité est de niveau EAL5+. Le terminal réalise un pare-feu entre la carte à puce blockchain et le PC ou le mobile. Lors de sa livraison il ne possède aucun code, il est donc qualifié de « bare metal ». Un

jeton USB, dont l'authenticité est garantie par une sonde d'intégrité, permet de flasher le code du terminal. C'est le mécanisme dit de « BigBang », le code zéro charge une chaîne de logiciels, il peut également se cloner.

Voici ainsi détaillé les fondements mêmes de ce qu'est et permet Ethertrust. Créée en 2007, par Telecom ParisTech et l'Université Paris 6, Ethertrust est une start-up française qui développe des solutions de cartes à puce pour améliorer la sécurité web et simplifier les accès aux applications pour l'utilisateur final.

Cette dernière s'appuie pour ses services sur les technologies de cryptologie et de certification numérique. Elle développe des logiciels qui s'insèrent dans les puces que les objets connectés et les serveurs peuvent reconnaître sans problème.

Sécuriser est un enjeu de taille alors que les piratages prennent toujours plus d'ampleur. Ethertrust, avec son crypto-terminal, permet de s'affranchir de tous ces risques préjudiciables. Voici comment :

Threat\ Technology	PC Mobile	WEB Site	MCU Only	MCU+ Secure Element	MCU+ Crypto Memory	TEE	Vault	WEB Site + HSM	Ethertrust Crypto Terminal
Side Channel Attack	Red	Green	Red	Green	Yellow	Red	Red	Green	Secure Element
Malware APT	Red	Red	Green	Green	Green	Green	Green	Red	Big Bang
Firmware Software Integrity	Red	Green	Red	Red	Red	Green	Red	Green	Bare Metal
Injection	Red	Red	Red	Red	Red	Red	Red	Red	Firewall - keypad
PIN Code Password	Red	Red	Red	Red	Red	Red	Red	Red	Smartcard keypad - display
On-Line Attacks	Red	Red	Green	Green	Green	Yellow	Green	Red	Firewall Off Line



## 11/ Panel : quel avenir pour blockchain ?

Animé par Mickael Campion (CEO de Data Solutions & Innovations Corporation, filiale de DSI Group), avec Nicolas Merle (Chain-Ops), François Stéphan (Be-Bound) et Xavier Dalloz (consultant)



**François Stéphan**, de la start-up Be-Bound, présente tout ce que la blockchain peut apporter aux pays émergents. La réponse ? Tout, et plus encore. Disons, à tout le moins, beaucoup. Comme autrefois avec le téléphone mobile qui a permis au Continent africain entier de « zapper » la case téléphone fixe, la blockchain peut aider les pays émergents à franchir un cap nouveau, directement.

La question, c'est de savoir comment. La blockchain peut permettre de s'affranchir des problématiques actuelles en matière de paiement par exemple. Prenons un cas concret, aux applications potentielles colossales : celui des transferts d'argent entre pays. Là encore, comme ce séminaire l'a démontré tout au long de la journée, la blockchain peut permettre de se passer, demain, des tiers de confiance. Ici, des tiers de confiance nommé Western Union et consorts, en l'occurrence. Avec la

blockchain, il est possible de se passer de ce type d'intermédiaires, aux commissions très élevées, et donc de concevoir un système plus économe et plus rapide.

Pour expliquer plus en détail ce qu'est Be-Bound : les fondateurs de Be-Bound se sont demandé pourquoi un appel peut être passé de n'importe où, alors que l'accès aux mails est, lui, limité à certaines zones ? Si un SMS peut être envoyé, pourquoi pas un mail ? À partir de ces questions, une technologie a été développée qui rassemble les réseaux existants de GSM à la 4G et apporte une connectivité constante partout, pour tous. L'objectif ? Participer ainsi à réduire la fracture mobile digitale.

**Nicolas Merle**, pour Chain-Ops, vient présenter quant à lui la solution Chain-Ops, qui se veut être le premier opérateur de réseaux blockchain pour les entreprises.



Experte dans le développement de réseaux blockchain, la société Chain-Ops aide les entreprises à réaliser leur projet blockchain, depuis l'idée initiale jusqu'à la concrétisation finale.

**Xavier Dalloz**, consultant, qui a est déjà intervenu le matin, revient, micro en main, pour affirmer, si jamais nous n'en étions pas tous convaincus encore, « à quel point nous allons vers une blockchainisation généralisée de nos sociétés. »

## 12/ Conclusion

Par David Menga, EDF Lab



Cette journée de séminaire, en balayant toute cette série d'applications concrètes permises par la blockchain prouve à quel point nous sommes au début de quelque chose qui va venir bouleverser de fond en comble notre perception des choses, et du quotidien. « Ce n'est que le début, explique David Menga. Ce que nous voyons aujourd'hui, c'est le tout début d'une phase d'industrialisation des moteurs de la blockchain. Quand ils tourneront à plein régime, vous le verrez, ce sera encore autre chose. »

La blockchain sera au centre des modèles économiques des entreprises. Des entreprises plus agiles, décentralisées, en réseau, et entièrement tournées vers le consommateur. Nous entrons dans une ère d'industrialisation. Les technologies blockchain permettent d'apporter des réponses concrètes à des attentes consommateur ayant trait, in fine, au problème majeur de la confiance. Le tout en alliant intérêt personnel et bien commun.

Pour conclure, donc, blockchain est appelée à être demain partout. Et ce que nous vivons n'est encore que le début.