

POUR ENFIN COMPRENDRE À QUOI SERT LA BLOCKCHAIN

La blockchain est sortie de l'ombre en 2009 avec la première transaction en Bitcoin. Les cryptomonnaies ne reflètent pourtant qu'une partie de ses potentialités. Tour d'horizon des applications possibles de ce registre distribué, inviolable et sécurisé dans notre vie quotidienne.

C'est une première en Europe. Depuis cet été, le législateur français autorise le transfert de propriété de certains titres financiers via la blockchain. Un cadre juridique est ainsi en train de s'installer autour de cette technologie qu'on a longtemps confondue avec le Bitcoin alors que ses champs d'application sont bien plus vastes que les seules monnaies virtuelles.

La blockchain est une sorte de grand cahier en ligne que tout le monde peut consulter et auquel on peut contribuer sans craindre que les informations soient falsifiées par un tiers (voir schéma). La blockchain Ethereum, en particulier, permet de faire tourner des "smart contracts", programmes autonomes censés déclencher une action



Ciprian Olteanu (M.17)



Manon Gaudefroy (H.17)



Pierre Paperon (MBA.86)

● ● ● ou un paiement dès que les conditions définies au départ sont réunies. Tout cela permet de valider des transactions sans passer par les tiers de confiance habituels (banques, notaires, SACEM...) ou les plateformes de types Airbnb ou Uber.

La preuve la plus éclatante du développement de la blockchain est le succès des ICO (Initial Coin Offerings) qui fait la une des médias cette année. Également appelées "token sales", ces opérations consistent à émettre des actifs numériques, des tokens (jetons), en échange de cryptomonnaies, durant la phase de démarrage d'un projet. Ces actifs numériques présentent deux intérêts: d'une part ils permettent d'accéder à un service (typiquement l'Ether permet d'utiliser les services proposés sur Ethereum), d'autre part ils prennent de la valeur lorsque la demande dépasse l'offre, de la même manière que pour une action. Les ICO se sont multipliées de manière vertigineuse, passant d'une soixantaine en 2017 à plus de 2000 cette année. Pour une startup dont la technologie repose sur la blockchain, une ICO peut s'avérer plus attractive qu'une levée de fonds classique car les jetons offrent aux investisseurs un accès à ses services, à la manière d'une prévente sur un site de crowdfunding. Par exemple, quand une startup ayant développé une application sur la blockchain émet des jetons, les détenteurs de ces jetons ont un accès gratuit à l'application. Les ICO permettent en outre de cibler les cryptoinvestisseurs, ces individus qui se sont enrichis grâce au boom des monnaies virtuelles (voir encadré). Trentenaires asiatiques pour la plupart, ces investisseurs d'un nouveau genre détiennent l'équivalent de 200 milliards de dollars de cryptomonnaies. Un véritable eldorado ! Mais les fonds de capital-risque et les business angels se mettent eux aussi à participer aux token sales. Au début de l'année, la messagerie sécurisée Telegram a même annulé la partie publique de son ICO car elle était déjà parvenue à lever 1,7 milliard de dollars auprès d'investisseurs institutionnels, lors de deux préventes. Et ce n'est que le début ! "De grandes entreprises françaises préparent des ICO ou des projets blockchain pour 2019", nous confie **Manon Gaudefroy (H.17)**, responsable de l'offre blockchain chez Havas. Mais pour ce qui est des nouveaux entrants, prudence, la blockchain est encore

un vaste Far West. "Attention, 50 à 80 % des ICO sont des arnaques, soit parce que la technologie blockchain n'est pas appropriée, soit parce que le porteur de projet utilise l'argent collecté à d'autres fins", avertit **Pierre Paperon (MBA.86)**, spécialiste de la blockchain.

On a tendance à réduire la "blockchain" à sa dimension technologique mais le phénomène revêt aussi une dimension culturelle forte. Cette tendance s'inscrit en effet dans la tendance "libertarienne" venue des États-Unis, empreinte de méfiance vis-à-vis des institutions. "La blockchain permettra de s'affranchir des États et de transcender les frontières", évoque **Olivier Bossard**, directeur exécutif du Master Finance à HEC Paris. "Avec la blockchain, nous pouvons reconquérir notre autonomie face aux GAFA !" renchérit **David Prinçay (MS.11)**, cocréateur du Club français de la cryptomonnaie. Preuve en est la startup Steemit, qui dénonce la captation de valeur opérée par Twitter ou Facebook et propose une plateforme de microblogging dans laquelle les contributeurs sont rémunérés par des "steamcoins" à mesure que leurs articles sont lus et likés. Explication: sur les réseaux sociaux traditionnels, vous créez de la valeur en postant des textes, photos ou vidéos; vous créez du contenu en face duquel la plateforme peut associer de l'espace publicitaire qu'elle commercialise auprès de ses annonceurs. Sur Steemit, au contraire, vous êtes directement rémunéré pour vos contributions. Dans le même esprit, la plateforme décentralisée Arcade City veut rivaliser avec Uber et Open-Bazaar avec Airbnb grâce à la blockchain: cette dernière faisant office d'intermédiaire, les commissions à payer sont beaucoup plus faibles.

La communauté HEC se mobilise sur cette thématique d'avenir. Le club Blockchain@Hec propose des conférences et des ateliers de travail à tous les diplômés qui s'y intéressent. "Je suis en discussion avec l'école pour intégrer des électifs sur la blockchain au cursus académique. Nos homologues des autres écoles (Polytechnique, Assas, etc.) constatent, comme nous, un véritable engouement sur le sujet", confie le créateur du club, **David Servais (MBA.11)**. ●



David Prinçay (MS.11)



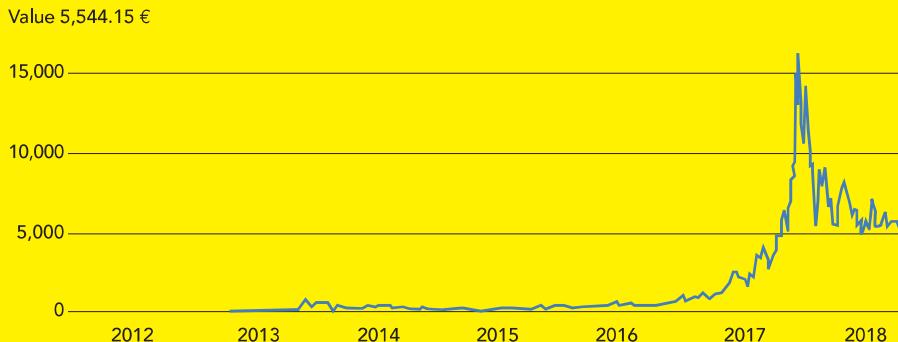
David Servais (MBA.11)

200
milliards
de dollars
La valeur des
cryptomonnaies en
circulation dans le
monde

6400
dollars
Le cours du
Bitcoin, contre 60
cents en 2010

LE COURS DU BITCOIN DEPUIS SA CRÉATION

source: courscryptomonnaies.com



UNE GIGANTESQUE BULLE

À l'heure où nous écrivons ces lignes, un Bitcoin se négocie à plus de 6 400 dollars, alors qu'il valait 60 cents en 2010. Soit une multiplication par plus de 10 000 en huit ans ! La valeur totale des cryptomonnaies en circulation (Bitcoins, ethers et les autres) tourne autour de 200 milliards de dollars. Comment justifier de tels montants ? "C'est le prix de l'alternative. Ces monnaies sont sécurisées et ne dépendent pas d'une banque centrale. Elles ne risquent pas de se déprécier parce qu'une autorité décide unilatéralement de faire tourner la planche à billets", répond David Prinçay (MS.11), cocréateur du Club français de la cryptomonnaie. Directeur exécutif du Master Finance à HEC Paris.

COMMENT ÇA MARCHE ?

La blockchain (littéralement "chaîne de blocs") est une technologie qui permet de stocker des informations de manière transparente et sûre, sans organe central de contrôle. Cela ressemble à une immense base de données contenant l'historique de tous les échanges réalisés entre ses utilisateurs depuis sa création.

La validation d'une transaction résulte d'un consensus entre les "mineurs", les machines qui constituent le noëud du réseau. Chaque nouveau bloc de transactions contient dans son code une référence au précédent. Il est estampillé d'un "hashcash", une certification par "preuve de travail" qui permet aux autres mineurs de vérifier son authenticité. Un fraudeur qui voudrait modifier un bloc devrait pour cela réactualiser l'historique des transactions, ce qui nécessiterait une puissance de calcul phénoménale et la complicité de plusieurs mineurs. Cela fait de la blockchain, en théorie du moins, un système incorruptible.

Paris, Olivier Bossard est beaucoup plus sceptique. Il voit dans la flambée du Bitcoin un phénomène purement spéculatif qui n'a rien à voir avec la technologie sous-jacente. "Les investisseurs ne s'intéressent pas au protocole de la blockchain en vue de l'utiliser techniquement, ils se sont rués sur la seule valeur faciale des jetons. C'est le fameux FOMO, "fear of missing out", qui pousse les spéculateurs à acheter les cryptomonnaies", analyse le professeur.

D'autres encore y voient un pari sur l'avenir. Les acheteurs tableraient, de manière plus ou moins intuitive, sur une utilisation croissante de ces devises dans l'économie. "Une monnaie a de la valeur à partir du moment où je crois qu'elle sera acceptée demain en paiement par d'autres personnes. C'est peut-être ce qui se passe avec les monnaies virtuelles", résume Bruno Biais (H.85/D.89), professeur à HEC Paris.

En attendant, voilà une masse monétaire considérable qui ne demande qu'à être réinvestie par les cryptoinvestisseurs, pour le grand bonheur des entrepreneurs de la blockchain. "Il suffit d'une idée pour se lancer, les investisseurs ne regardent même pas l'expérience des fondateurs, témoigne Pierre Paperon (MBA.86), fondateur de la société Solid. Ça me rappelle la bulle Internet de 1999." Cela dit, le Bitcoin a déjà connu une correction majeure depuis la fin 2017, où il culminait à plus de 20 000 dollars. Ceux qui en ont acheté à l'époque ont perdu les deux tiers de leur mise en quelques mois.

COMMENT PAYER EN BITCOINS ?



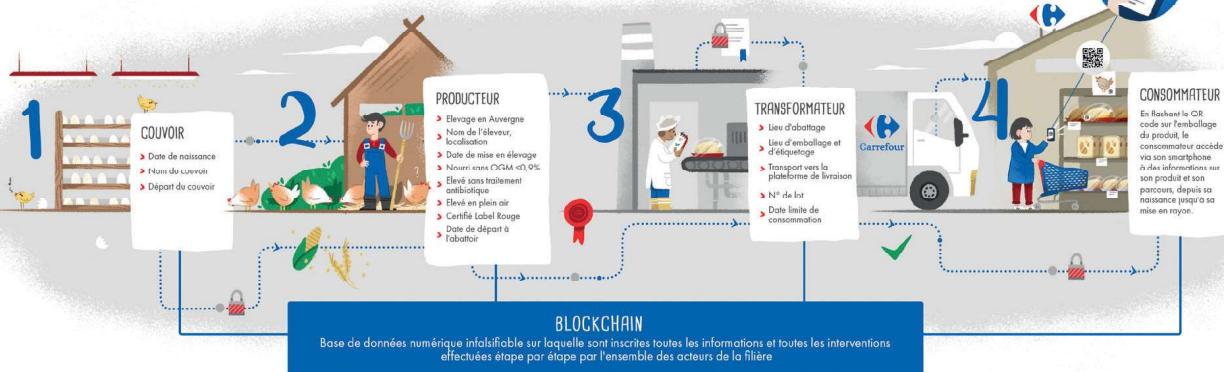
6 APPLICATIONS CONCRÈTES QUI DEVRAIENT VOUS INTÉRESSER

CARREFOUR CERTIFIE L'ORIGINE DE SES POULETS

Viande de cheval retrouvée dans les lasagnes Findus, lait pour enfant Lactalis contaminé aux salmonelles... L'industrie agroalimentaire est régulièrement fragilisée par des scandales sanitaires de grande ampleur. Les consommateurs se sentent à la merci de pratiques douteuses sur lesquelles ils ne peuvent exercer aucun contrôle, sauf à tout produire dans leur jardin. Les entreprises du secteur l'ont bien compris et cherchent des moyens de restaurer la confiance. La blockchain est prometteuse de ce point de vue. Depuis cette année, le groupe Carrefour trace l'origine de ses "poulets d'Auvergne filière qualité Carrefour" à l'aide de la blockchain. Cela représente un million d'unités par an. Concrètement, chaque maillon de la chaîne, du producteur de céréales au distributeur, en passant par l'éleveur et l'abattoir, renseigne à l'aide de son smartphone les actions qu'il a menées. "S'il y a une incohérence entre deux étapes, l'information est invalidée", précise **Manon Gaudefroy (H.17)** chez Havas Blockchain. En bout de chaîne, un QR code présent à côté du code-barres permet au consommateur de connaître le nom de l'éleveur, les traitements médicaux administrés aux poulets ou encore la date et le lieu d'abattage. "C'est une première en Europe qui garantit aux consommateurs une transparence totale sur la traçabilité de nos produits", assure le groupe, qui a également développé des filières blockchain sur les tomates et les œufs. À noter toutefois qu'il s'agit de blockchains privées, ce qui signifie que Carrefour maîtrise le protocole et décide de qui peut participer. En revanche, tout le monde peut les consulter.

TRAÇABILITÉ ALIMENTAIRE : CARREFOUR LANCE LA PREMIÈRE BLOCKCHAIN ALIMENTAIRE D'EUROPE

L'exemple du poulet d'Auvergne Filière Qualité Carrefour



SANDBLOCK RÉINVENTE LES POINTS DE FIDÉLITÉ

Votre portefeuille est encombré de cartes de fidélité ? Vous pestez chaque fois que vous oubliez, perdez une carte ou laissez expirer des bons d'achat ? L'innovation de **Sarah-Diane Eck (H.13)** devrait susciter votre curiosité. Cette trentenaire a conçu, via la blockchain, un système de jetons qui sont utilisés par les marques pour récompenser la fidélité de leurs clients. "Les points de fidélité deviennent des actifs cryptos qui circulent sur une blockchain.

La plateforme permet des échanges sans perte de valeur pour la marque et fluides pour les consommateurs", explique la fondatrice de la startup Sandblock, qui emploie une dizaine de personnes dans ses locaux parisiens. Concrètement, l'utilisateur n'est plus lésé s'il perd sa carte de fidélité ou si ses points vont expirer. Il peut échanger avec un autre consommateur ses points de fidélité auprès de la marque A par des points de fidélité de valeur identique auprès de la marque B. Il collecte des tokens en réalisant des achats dans une entreprise, mais aussi en répondant à des questionnaires de satisfaction, en suivant la marque sur les réseaux sociaux ou en participant à des chasses au trésor de points en réalité augmentée.

Forte d'un triple cursus HEC Paris, AgroParisTech et Assas, Sarah-Diane est la première dirigeante française d'une startup blockchain à avoir boudé un financement par ICO (Initial Coin Offering). Elle a levé l'équivalent de 2 millions de dollars en début d'année. Pour réussir son ICO, la startup a mis toutes les chances de son côté : l'équipe de Sandblock a conçu une application de gamification, "Stakin", afin de faire parler du projet auprès des cryptoinvestisseurs. "Dès qu'un soutien partageait des infos sur l'ICO ou participait à des jeux de connaissance sur Sandblock, il remportait des "stakes", donc un droit futur à obtenir des tokens directement en fonction de son engagement. C'était du pur growth hacking dans un écosystème qui affichait des budgets farfelus de communication pour créer leurs communautés", raconte Sarah-Diane Eck. L'outil a tellement bien marché qu'elle le propose désormais à d'autres startups pour les aider dans leur ICO.



QUIDLI

QUIDLI APporte DE LA LIQUIDITÉ DANS LE PRIVATE EQUITY

Les entrepreneurs de la tech le savent bien, la distribution d'actions est un processus complexe et chronophage. Or la rémunération de collaborateurs sous forme d'actions, qui a le vent en poupe, nécessite de pouvoir céder facilement des parts de la société. Forts de ce constat, **Justin Ahn (MBA.14)** et **Florent Bolzinger (MBA.14)** ont créé Quidli, un protocole blockchain qui permet à une entreprise de transférer des parts de son capital en un clic. Quand on sait qu'un géant comme Airbnb réfléchit à faire de ses "superhôtes" des actionnaires et qu'Uber compte faire de même avec ses chauffeurs, on imagine le potentiel de ce type de technologie... Les concurrents sont d'ailleurs nombreux sur ce créneau, à commencer par la pépite américaine Polymath, qui a levé 59 millions de dollars lors d'une ICO en février.

Comme on n'est jamais mieux servi que par soi-même, Quidli pratique elle-même le principe de "travail contre equity". "Aujourd'hui, une quinzaine de personnes travaillent avec nous. Nous les rémunérons en parts de la société. Parmi nos contributeurs, on trouve deux avocats et un juriste. Ils ont toujours rêvé d'être entrepreneurs mais ne peuvent pas se le permettre à cause de contraintes personnelles. Ça leur plaît beaucoup de "craquer" le système!" confie Justin Ahn, un grand gaillard souriant et sûr de lui.

La startup a été admise au sein de Tachyon, l'accélérateur californien de Consensys*. La jeune poussée compte réaliser une levée de fonds d'ici la fin de l'année afin de financer son déploiement en France et aux États-Unis.

*Éditeur de logiciels qui fait référence dans le monde de la blockchain.

VALYOOTRUST, LE COUTEAU SUISSE DIGITAL DE L'INNOVATION

Les plateformes d'open innovation se heurtent souvent à un obstacle de taille, les participants sont réticents à s'y impliquer vraiment. En effet, la confiance n'est pas au rendez-vous car les contributeurs craignent que la paternité de leurs idées ne leur soit pas reconnue. Cela génère chez eux de la frustration, voire de la démotivation, ce qui affecte l'efficacité de ce type de plateforme. ValYooTrust compte remédier à ce puissant frein psychologique. Accélérer, sécuriser, numériser et valoriser l'innovation, telle est sa vocation. Concrètement il s'agit d'une plateforme digitale initiée par l'Institut Mines Télécom et la Fabrique du Futur. Basée sur une blockchain, ValYooTrust sécurise les transactions intellectuelles, en assure leur traçabilité et permet ainsi un juste partage de la valeur entre les parties prenantes qui sont rétribuées. Les innovateurs l'utilisent pour créer ensemble des actifs immatériels tels que des business plans, des logiciels ou des preuves de concept (POC). Les utilisateurs sont de toutes sortes : startups, PME, fonds d'investissement, grandes organisations, collectivités publiques, hôpitaux... Les citoyens, les indépendants les patients peuvent également contribuer. "La transparence de la blockchain favorise les relations de confiance et permet de "rendre à César ce qui est à César". Cela rassure les participants et leur donne envie de s'engager" explique **Eric Seulliet (H.74)**, président de la Fabrique du Futur. L'ensemble de ce dispositif unique en France sert une vision : "assurer le développement économique par l'innovation entrepreneuriale", conclut **Patrick Duvaut**, directeur innovation de l'Institut Mines Télécom.

R3 AU SECOURS DU COMMERCE INTERNATIONAL

En ces temps marqués par les relents protectionnistes des États-Unis, voilà le genre d'innovation qui devrait mettre du baume au cœur des dirigeants de multinationales. Les banques françaises Natixis, Société Générale et BNP Paribas ont investi aux côtés de plusieurs homologues étrangères dans la plateforme Corda de la startup américaine R3 dédiée au trade finance (financement des transactions d'import-export). Sur une simple application pour smartphone, les entreprises qui importent ou exportent des produits peuvent suivre les transactions, de la validation du bon de commande à la livraison. La blockchain enregistre les étapes de façon sécurisée, ce qui limite la paperasse et réduit les délais de traitement. Premier cas concret en mai dernier : HSBC et ING ont utilisé cette solution pour sécuriser le financement d'une expédition de soja en vrac de l'Argentine à la Malaisie, pour le compte du groupe américain de négoce de matières premières agricoles Cargill. La transaction a été déboulée en 24 heures, contre cinq à dix jours pour un crédit documentaire classique.

Dans le même esprit, 15 grandes entreprises (dont des banques tricolores) ont annoncé en septembre la création d'une plateforme destinée à simplifier le financement du commerce de matières premières. Baptisée Komgo, elle sera développée sur la blockchain Ethereum.

ValYooTrust



GO

TALAO VEUT UBÉRISER LINKEDIN

Dans une dizaine d'années, la moitié de la population active dans le monde travaillera sous un statut d'indépendant ou équivalent. C'est du moins ce que prédit la jeune poussée parisienne Talao, qui met en relation des freelances et des entreprises pour des missions ponctuelles moyennant une très faible commission. Contrairement à LinkedIn où chacun peut enjoliver ses expériences et se faire mousser par des amis, la plateforme Talao est sécurisée par la blockchain et certifie l'authenticité des CV publiés : toute modification est tracée et connue de tous, ce qui limite le risque de falsification. Le candidat peut distiller les informations qu'il souhaite au potentiel client ou employeur. "Sur des marchés très tendus comme l'intelligence artificielle ou la cybersécurité, les talents les plus demandés pourront monétiser l'accès à leurs informations afin d'éviter d'être contactés par des entreprises n'ayant pas bien qualifié leurs besoins", explique **Manon Gaudefroy (H.17)**, de l'agence Havas Blockchain, qui a accompagné Talao dans le cadre de son ICO. Airbus et Thales utilisent déjà la plateforme pour répondre à certains de leurs besoins. La startup a levé 7 300 Ethereum, soit plus de 2 millions de dollars, et compte collecter en tout 60 millions de dollars. Une nouvelle émission de cryptoactifs Talao est prévue à partir de juillet 2019. La jeune société vise 5 millions d'utilisateurs d'ici à 2022.

8 AUTRES EXEMPLES D'APPLICATION DE LA BLOCKCHAIN

- Financement participatif:** Luc Jacquet, le réalisateur de *La Marche de l'empereur* (oscar du meilleur documentaire en 2006), est en train de lever 30 millions d'euros sous la forme de tokens qui donneront droit, entre autres, à des places de cinéma pour ses prochains films. "Luc Jacquet est très populaire en Asie, où se trouvent 20 millions de cryptoinvestisseurs", explique Pierre Paperon (MBA.86), spécialiste de la blockchain.
- Certification de diplômes:** la startup française BCDiploma utilise la blockchain Ethereum pour authentifier les diplômes dans un endroit sûr. Le MIT a initié un projet du même type.
- Transfert d'un titre de propriété:** la blockchain pourra se substituer aux tiers de confiance pour authentifier une transaction. "L'achat immobilier ne nécessitera plus de notaire", prédit ainsi David Prinçay (MS.11), cocréateur de Club français de la cryptomonnaie.
- Etat des lieux:** la jeune pousse marseillaise KeeeX, qui a rejoint le programme de cybersécurité de Thales à Station F, certifie grâce à la blockchain les photos prises lors de l'état des lieux d'un appartement ou du constat d'un accident automobile. Les clichés deviennent ainsi incontestables.
- Retard d'avion:** Axa a lancé l'an dernier Fizzy, une assurance automatisée qui couvre les retards de vol. Le smart contract basé sur Ethereum déclenche le remboursement dès que le retard a été acté.
- Traçabilité des médicaments:** la startup parisienne BlockPharma renseigne les patients sur l'origine des médicaments qu'ils achètent et émet une alerte en cas de falsification.
- Maison d'édition:** la plateforme communautaire Wespr se positionne en "Amazon-killer". Les écrivains peuvent protéger leurs œuvres et les lecteurs investir dans les livres auxquels ils croient. Le système redistribue automatiquement les droits d'auteur en fonction des ventes.
- Prêts entre particuliers:** sur ETHLend, l'emprunteur et le prêteur se mettent d'accord sur la durée de remboursement et le taux d'intérêt. L'accord se matérialise par un smart contract.



TROIS QUESTIONS À OLIVIER BOSSARD, DIRECTEUR EXÉCUTIF DU MASTER FINANCE À HEC PARIS

À quand remonte la genèse des cryptomonnaies ?

C'est en octobre 2008, sur un obscur forum de discussion, qu'un auteur anonyme ayant pour pseudonyme Satoshi Nakamoto a publié un article de neuf pages décrivant avec précision le protocole de fonctionnement du Bitcoin et esquissant déjà, avec un réalisme redoutable, ses implications. Trois mois plus tard, la communauté des cypherpunks [fans de cryptographie, NDLR] avait déjà implanté le code de Satoshi. Le 3 janvier 2009, la première transaction en Bitcoin était réalisée !

En quoi est-ce une révolution dans l'histoire de la monnaie ?

Au fil des siècles, nous sommes passés d'une monnaie qui avait une valeur intrinsèque (convertible en or) à une monnaie dite fiduciaire, c'est-à-dire sans valeur intrinsèque mais basée sur la confiance en un État et sa banque centrale. Puis la monnaie est devenue scripturale (littéralement, écrite sur des registres sans être systématiquement associée à un support physique), et enfin numérique.

La cryptomonnaie constitue une nouvelle étape. Elle est non seulement numérique, mais dissociée de tout organisme central de contrôle.

70%

des jetons générés via les ICO (levées de fonds en cryptomonnaies) valent moins qu'au moment de leur émission.

Source: Diar.co

Les cryptomonnaies sont-elles utilisables à grande échelle ?

Pour l'instant, non. Les premières blockchains, dont le Bitcoin, assurent la sécurisation par consensus via une méthode cryptographique dite de preuve de travail ("proof of work"), décrite pour sa consommation excessive en capacité de calcul, et donc en temps de latence et en énergie. À l'heure actuelle, les mineurs consomment autant d'électricité que l'État d'Israël ! L'avenir du Bitcoin est compromis par son manque d'évolutivité face à des volumes de transactions amenés à grandir exponentiellement. Cela dit, d'autres cryptomonnaies voient le jour avec des blockchains basées sur des méthodes de consensus plus prometteuses : la méthode dite de preuve de participation ("proof of stake") du Peercoin, la méthode hybride de deuxième génération de l'Ethereum et enfin une troisième génération de blockchains derrière les nouvelles cryptomonnaies que sont EOS.IO, Cardano ou Raiden Network. Nous ne sommes qu'au début de l'aventure !