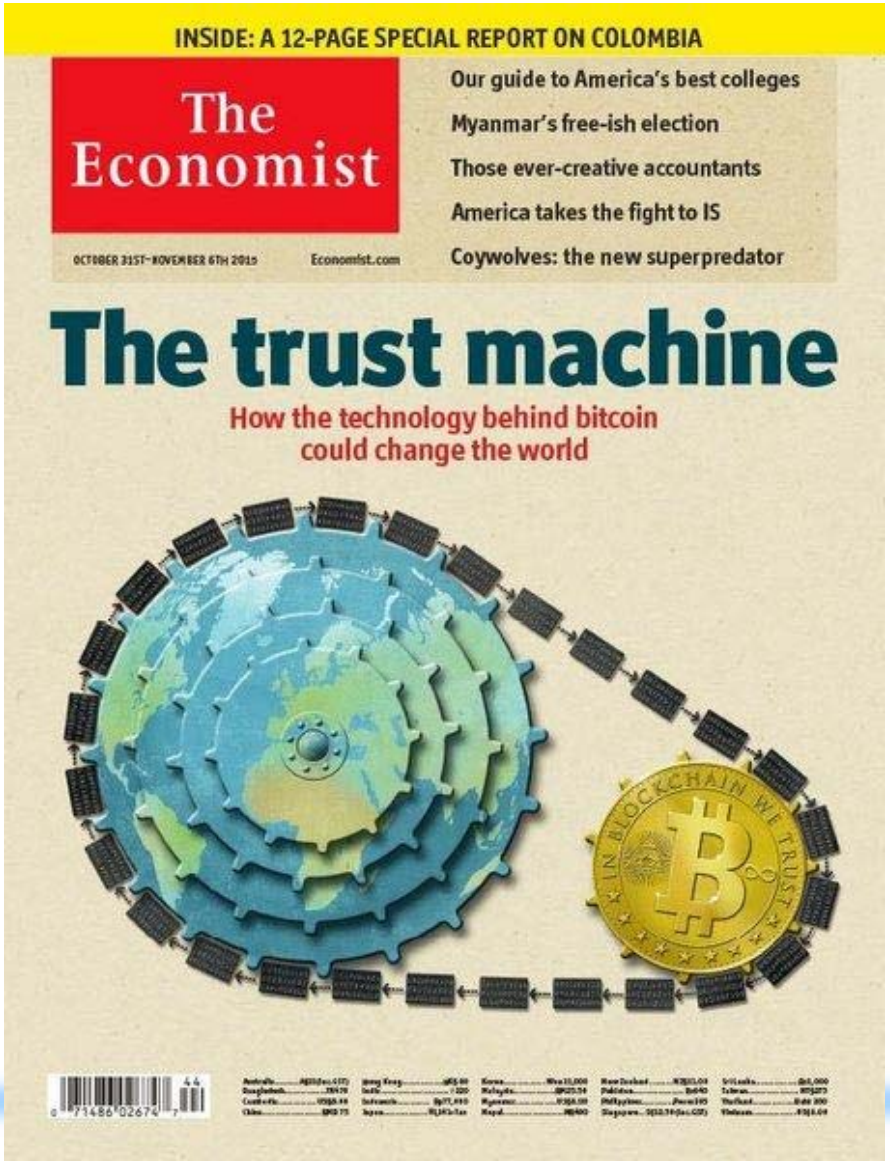
BLOCKCHAIN
Son fonctionnement

Jean-Pierre KRIMM – CEA
jean-pierre.krimm@cea.fr
Raphaël PEUCHOT – Avocat
rp@peuchot-avocats.com

Clusir Rhône-Alpes Club SSI, le 20/12/2017

En quoi La technologie Blockchain est-elle révolutionnaire ?



En quoi La technologie Blockchain est-elle révolutionnaire ?

- C'est une technologie de *stockage* et de *transmission* d'informations, un *protocole* de *gestion* de données numériques. Une *grosse base de données*, quoi.
  What else ???

Ce qui *change* la donne avec la blockchain, c'est qu'elle est :

- *Immuable* : une fois les informations inscrites dans une Blockchain, elles ne peuvent plus être modifiées ni supprimées.
- *Transparente* : chacun peut consulter l'ensemble des échanges, présents et passés.
- *Pseudonyme* : les utilisateurs sont identifiés par un « numéro de compte » rendant leur identification impossible.
- *Infalsifiable et sécurisée* : Résolution de problèmes cryptographiques pour la validation des blocs.
  Son caractère distribué lui assure également une sécurité puisque tous les blocs sont répliqués sur tous les nœuds du réseau.

C'est comme "un très grand cahier, que tout le monde peut lire librement, gratuitement, sur lequel tout le monde peut écrire, qui est impossible à effacer et indestructible." (Jean-Paul Delahaye)

Comment ça marche ?

- C'est donc une base de données numériques transparente, sécurisée et sans organe de contrôle.

Mais pourquoi une blockchain ?

- Toutes les transactions effectuées entre les utilisateurs de la blockchain depuis sa création y sont inscrites;
- Ces transactions successives sont enregistrées sous forme de "blocs" qui, mis bout à bout, forment une "chaîne";
- Les blocs sont ordonnés et hiérarchisés dans une seule et unique chaine.

Une transaction

- Une transaction est un *transfert de valeur* (monnaie virtuelle, token, etc.) entre deux comptes, deux « portefeuilles ».
- Chaque transaction est *signée* avec la clé privée du compte émetteur, fournissant ainsi
  - ✓ la *preuve* « mathématique » qu'elle provient bien du propriétaire du compte émetteur,
  - ✓ le moyen d'empêcher toutes modifications de la transaction après son émission.
- Une fois signée, la transaction est « *placée/déployée* » sur un nœud quelconque du réseau qui la diffuse à son tour, de proche en proche, sur tous les nœuds du réseau.
- À présent, tout le monde sur le réseau peut utiliser la clé publique de l'émetteur pour *vérifier* et s'*assurer* que la demande de transaction provient bien du propriétaire légitime du compte.
- Si la transaction est *valide*, elle est alors *incluse*, avec d'autres transactions en « attente », dans un bloc de la Blockchain, à son tour « exploité » par les mineurs.
- Une fois le bloc *validé*, le destinataire peut voir, dans son portefeuille, le montant de la transaction.
- Tout montant transféré est verrouillé sur l'adresse de réception et le montant à dépenser proviendra toujours des fonds précédemment reçus et actuellement présents dans le portefeuille.

Définition d'un bloc

- Un bloc contient des transactions
  = échanges entre utilisateurs de la blockchain

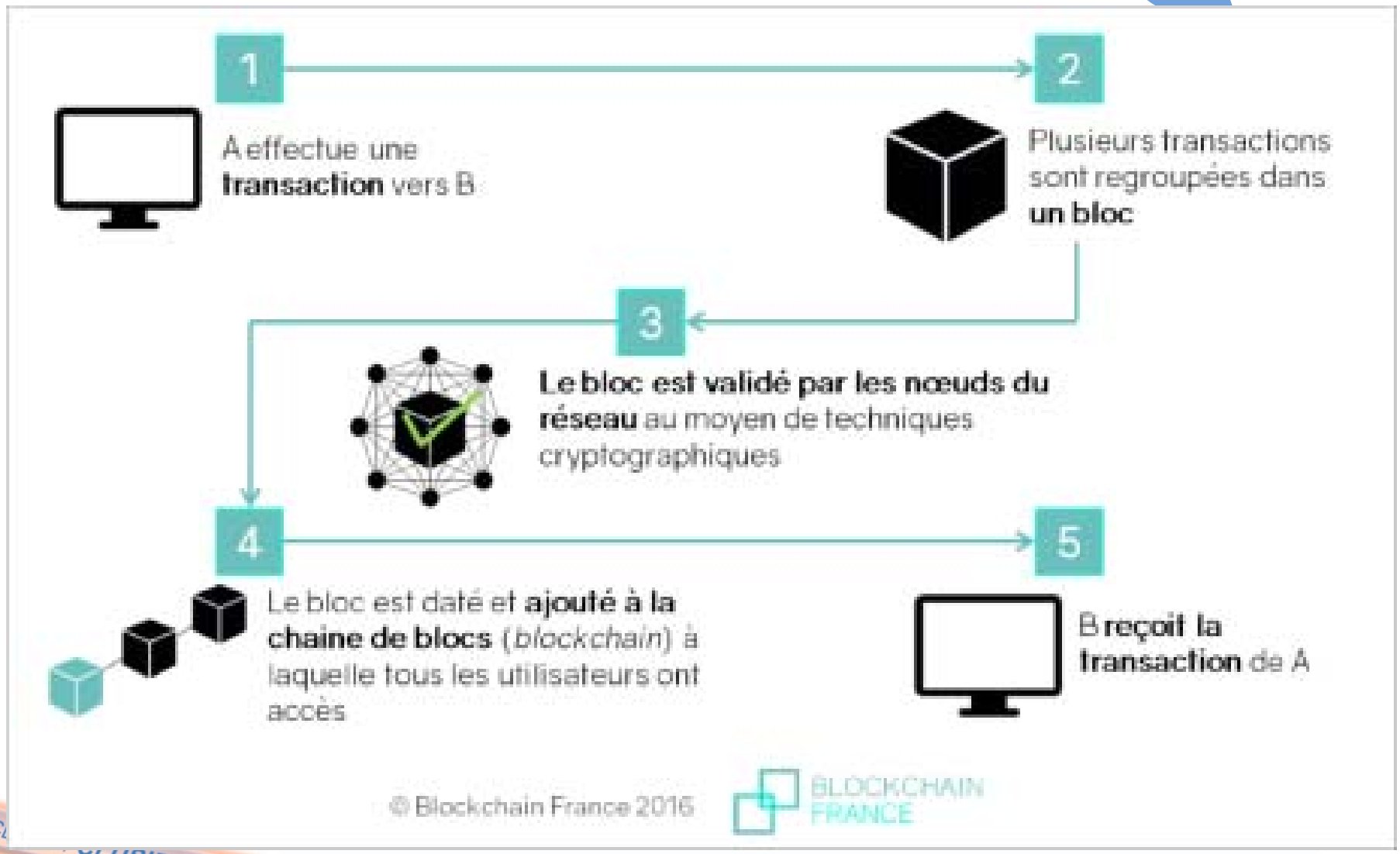
- Chaque bloc de la chaîne est constitué des éléments suivants :
  - ✓ Plusieurs transactions
  - ✓ Une ***somme de contrôle*** (« ***hash*** »), utilisée comme ***identifiant***
  - ✓ La ***somme de contrôle du bloc précédent*** (à l'exception du premier bloc de la chaîne, appelé bloc de ***genèse***) pour réaliser le chainage
  - ✓ Une mesure de la ***quantité de travail*** qui a été nécessaire pour produire le bloc. Celle-ci est définie par la méthode de consensus utilisée au sein de la chaîne, telle que la « preuve de travail », ou « preuve de participation ».

En quoi la blockchain est-elle si "infalsifiable" ?

- Répliquée sur l'ensemble des N nœuds du réseau
  => corruption simultanée > N/2

- La base de données distribuée est doublement sécurisée :
  - ✓ par un ***système cryptographique*** asymétrique;
  - ✓ par la ***résolution*** communautaire d'un système mathématique ***complexe*** qui demande une forte puissance de calcul.
    La validation de chacun des blocs est soumise à un processus baptisé "***minage***".
    Les "***mineurs***" chargés de vérifier la validité des transactions bloc par bloc sont des particuliers, ***rémunérés*** pour mettre à disposition la puissance de calcul de leurs processeurs.
    Les validations dépendent du type de blockchain (*cf. plus loin*).

Mécanisme global d'une blockchain



Les différents types de validation d'un bloc

- La Blockchain est une forme de mise en œuvre de la solution du « *problème des généraux byzantins* ».
  Ce problème mathématique consiste à s'assurer qu'un ensemble de composants informatiques fonctionnant de concert sait gérer des *défaillances* (ou *malveillances*) et arrive à produire un *consensus*.
  Le système doit pouvoir *maintenir sa fiabilité* dans le cas où une part *minoritaire* des composants enverrait des informations *erronées* ou *malveillantes* pour contourner la vérification de la double dépense.

- Le type de validation dépend de la méthode choisie pour résoudre ce problème. Il est donc lié à la blockchain :
  - ✓ Bitcoin = le "Proof-of-Work", preuve de travail
  - ✓ Ethereum = le "Proof-of-Stake", preuve de participation
  - ✓ Peercoin = un mélange des deux...

Le Proof-of-Work

- Cette méthode utilise l'*énergie* comme moyen de vérification que le « *mineur* » a bien réalisé un travail.
- Le protocole utilise un système *cryptographique* fondé sur un système décentralisé de preuves : la résolution de la preuve nécessite une *puissance de calcul informatique élevée*, fournie par les mineurs.
- Dans le cas de *bitcoin*, il faut répéter plusieurs centaines de milliards de fois l'opération (~ 10^{11}) pour espérer résoudre ce problème.
- Les *mineurs* sont des entités dont le rôle est d'alimenter le réseau en *puissance de calcul*, pour permettre la mise à jour de la base de données décentralisée.
- Pour cette mise à jour, les mineurs doivent confirmer les nouveaux blocs en déchiffrant les données.
- Une *concurrence* existe entre les mineurs pour le déchiffrement des transactions, permettant à la puissance disponible sur le réseau de croître.
- N'importe qui peut prêter sa puissance de calcul pour miner, mais plus les mineurs sont nombreux plus la résolution des preuves est difficile à s'attribuer. Ainsi, le protocole peut devenir *quasi-inviolable* dès lors que la *concurrence* est *forte* à chaque nœud du réseau, c'est-à-dire qu'aucun groupement de mineurs ne devient majoritaire.
- Dans le cas de *bitcoin*, chaque mineur est *rémunéré* pour le travail fourni à soutenir le réseau.

Le Proof-of-stake

Se base sur le *montant de crypto-monnaie* mis, à dessein, en dépôt par un utilisateur.

Le principe est le suivant :

- Un certain nombre de possesseurs de crypto-monnaie mettent en dépôt une partie de leurs « avoirs » dans le cadre du mécanisme de preuve d'enjeu. Ils deviennent alors des « *validateurs* ». Lorsqu'un nouveau bloc est proposé à l'ajout de la blockchain, un validateur est *sélectionné*, « *aléatoirement* » parmi tous les validateurs identifiés et se voit attribuer le *droit* de *créer* le prochain bloc et donc d'être rémunéré.

- La *sélection* d'un validateur est *pondérée* en fonction du montant total de cryptomonnaie (ou token) qu'il a mis en dépôt. Ainsi par exemple, un validateur avec 10 000 « unités » aura dix fois plus de chance d'être sélectionné qu'un validateur avec 1 000 « unités ».

- Si ce validateur ne crée pas le bloc dans un intervalle de temps donné, il est alors « *abandonné* » et un deuxième validateur est sélectionné, puis un troisième et ainsi de suite.

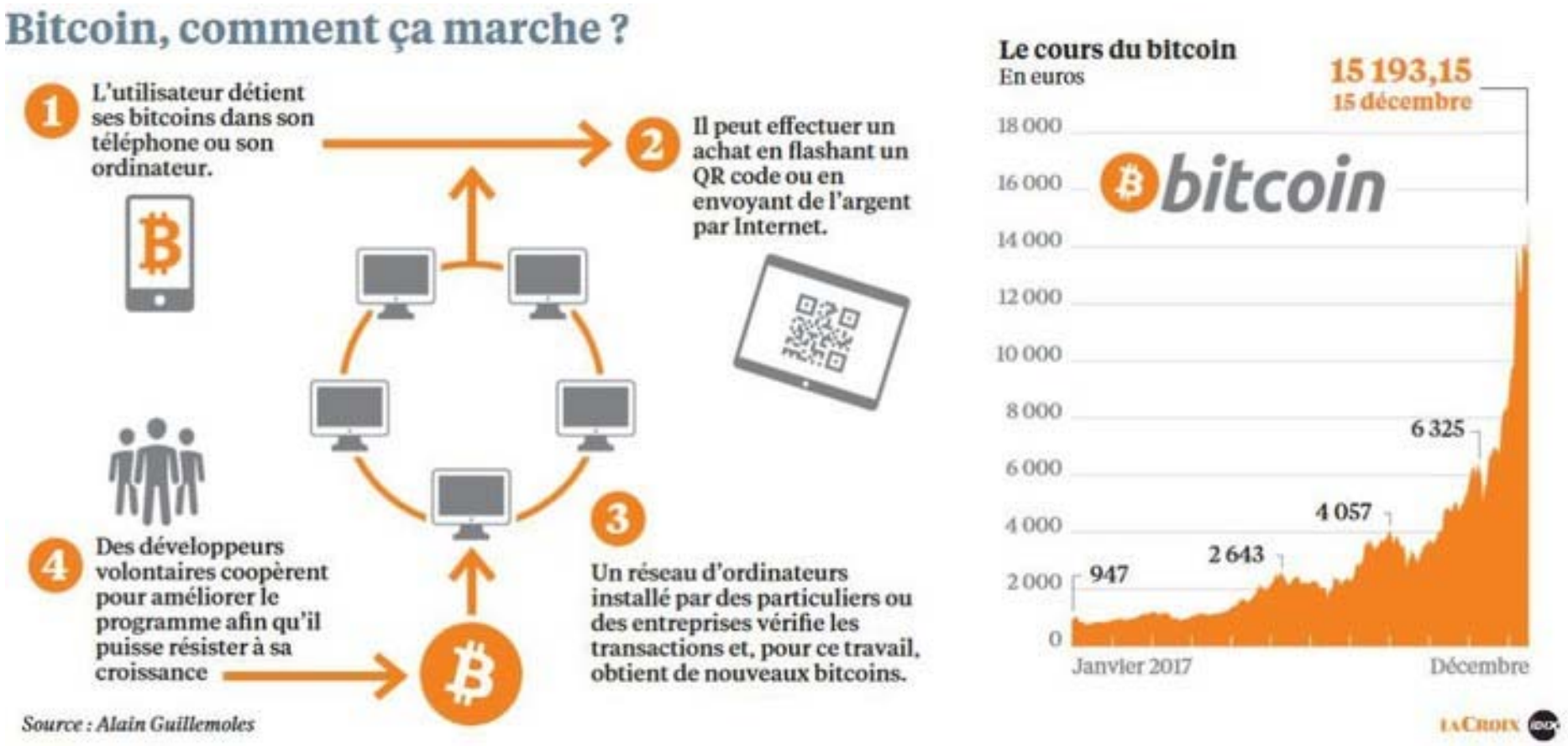
Quel est le rapport avec le bitcoin ?

- La technologie *blockchain* est "*l'infrastructure virtuelle* sur laquelle repose le bitcoin", "le protocole décrivant le fonctionnement du réseau sur lequel cette monnaie circule".
- *Bitcoin* désigne à la fois un protocole de paiement sécurisé et anonyme et une crypto-monnaie.
- La Blockchain est donc née en même temps que les premiers bitcoins, en 2009.
- Pour rappel, la première transaction avec cette monnaie, en mai 2010, était l'achat de... deux pizzas.
- Si le bitcoin ne peut exister sans la blockchain, l'inverse n'est pas vrai
  => elle a un potentiel bien plus énorme !!!

Le bitcoin

- N'importe qui peut accéder à cette blockchain (elle est publique, donc ouverte à tous) et donc utiliser des bitcoins.
  Pour ce faire, il suffit de créer un portefeuille virtuel, téléchargeable sur les stores d'applications.
  La crypto-monnaie permet d'acheter des biens et services et peut être échangée contre d'autres devises.
- Certaines plateformes proposent la conversion de dollars, euros ou yuans en bitcoins.
  C'est le cas de Paymium, une start-up française qui permet d'échanger des bitcoins contre des euros.
- Le bitcoin a un cours très volatile. Il peut augmenter ou diminuer de 20% en seulement deux jours. Cette volatilité est liée à la forte spéculation autour de cette monnaie et à l'absence d'une autorité régulatrice.
- Début décembre 2017, le cours du bitcoin a dépassé pour la première fois les 15 000 $.
- Il a augmenté de plus 1 000% depuis janvier 2017.
  Face à cette envolée, l'Autorité des marchés financiers (AMF) et l'Autorité de contrôle prudentiel et de résolution (ACPR) ont mis en garde les investisseurs sur les risques liés à l'achats de bitcoins.
- Au Japon, le bitcoin a été reconnu comme moyen de paiement légal le 1er avril 2017.
- La capitalisation de la première crypto-monnaie a atteint 191 milliards $ en novembre 2017.

Le bitcoin



Comment fonctionne le bitcoin, une monnaie virtuelle ? / Idix pour La Croix

Cours des crypto-monnaies - Top 10

All ▾ | Coins ▾ | Tokens ▾ | USD ▾ | ← Back to Top 100

* #	Name	Symbol	Market Cap	Price	Circulating Supply	Volume (24h)	% 1h	% 24h	% 7d
1	Bitcoin	BTC	$280 478 353 396	$16 761.10	16 733 887	$13 416 400 000	-0.86%	21.95%	46.11%
2	Ethereum	ETH	$44 964 495 036	$467.07	96 268 461	$1 369 030 000	-0.17%	5.74%	-0.03%
3	Bitcoin Cash	BCH	$23 868 077 353	$1 417.75	16 849 288	$846 213 000	0.93%	10.42%	-6.93%
4	IOTA	MIOTA	$11 975 939 768	$4.31	2 779 530 283 *	$481 355 000	-0.49%	4.52%	82.34%
5	Ripple	XRP	$9 498 179 751	$0.245183	38 739 144 847 *	$174 110 000	-0.29%	4.89%	-2.98%
6	Litecoin	LTC	$8 848 430 028	$163.10	54 250 233	$1 123 020 000	1.93%	19.11%	62.87%
7	Dash	DASH	$5 605 139 513	$723.59	7 746 292	$178 292 000	-0.99%	8.13%	-5.32%
8	Bitcoin Gold	BTG	$4 368 936 731	$261.61	16 699 999	$238 725 000	-2.50%	22.99%	-20.29%
9	Monero	XMR	$4 122 998 313	$266.87	15 449 232	$139 146 000	0.63%	15.47%	33.90%
10	NEM	XEM	$3 862 152 000	$0.429128	8 999 999 999 *	$68 620 000	-2.12%	20.12%	54.04%

Capitalisation et cours des dix premières crypto-monnaies du monde début décembre 2017. © Capture d'écran JDN

1.231 : le nombre de crypto-monnaies existantes
110 : le nombre de fonds spéculatifs dédiés aux cryptomonnaies

La blockchain Ethereum

- Créée en 2014, Ethereum utilise aussi sa propre crypto-monnaie : l'ether.
- Contrairement au bitcoin, qui permet seulement d'effectuer des transactions simples (principalement des paiements), l'Ethereum va plus loin.
  Il permet de faire tourner des "smart contract"
  - ✓ des programmes autonomes qui exécutent automatiquement des actions validées au préalable par les parties prenantes.
- L'Ethereum et ces contrats intelligents intéressent les acteurs de la banque et assurance mais aussi les professions juridiques. Ces acteurs pourront à l'avenir certifier
  - ✓ des transferts de propriété de manière plus sécurisée
  - ✓ verser automatiquement des indemnités.
- Axa a été le *premier assureur* à sortir une assurance basée sur la blockchain. En septembre 2017, il a lancé une *assurance automatisée* pour les retards de vol d'avion. Basée sur la blockchain Ethereum, cette assurance est en fait un "*smart contract*", un contrat intelligent qui déclenche un *remboursement automatique* une fois que le retard a été constaté.
  Cette offre baptisée Fizzy a été développée avec la start-up Utocat, qui édite une plateforme pour accélérer la conception de prototypes blockchain.

Qui a inventé la blockchain ?

- C'est l'inventeur du BitCoin, en 2008...
- Il reste inconnu à ce jour.
- Son pseudo : *Satoshi Nakamo*.
- Régulièrement, certains revendiquent la paternité du bitcoin et donc de la technologie blockchain.

Typologie

Il existe trois « types » de blockchain :

- **Publique**
  Il s'agit de blockchains accessibles à n'importe qui dans le monde.
  Aucune permission n'est à demander pour effectuer des transactions ou pour participer au processus de consensus.
  Tous les acteurs sont en situation égalitaire dans leur participation au réseau.
  Bitcoin et Ethereum sont les deux principales blockchains publiques.

- **Privée**
  Il s'agit de blockchains tournant sur un réseau privé, dans lesquelles tous les participants sont connus et pour lesquelles la gouvernance est assurée par une organisation.
  Personne ne peut y accéder et y participer sans y être autorisé.

- **Consortium** (Hybride)
  Il s'agit de blockchains dans lesquelles le processus de consensus (validation des transactions/blocs) est contrôlé par un nombre connu et restreint de noeuds.
  Certains noeuds peuvent être rendus publics (accès autorisé en lecture seule) tandis que d'autres restent privés.
  Elles sont plus adaptées aux contextes régulés.

Définition (Wikipedia)

- *Une **blockchain**, ou **chaîne de blocs**, est une technologie de **stockage** et de **transmission** d'informations **sans organe de contrôle**.*
  ***Techniquement**, il s'agit d'une **base de données distribuée** dont les informations, envoyées par les utilisateurs, sont **vérifiées** et **groupées** à intervalles de temps réguliers en blocs, **liés** et **sécurisés** grâce à l'utilisation de la **cryptographie**, et formant ainsi une chaîne.*
  *Par extension, une chaîne de blocs est une base de données distribuée qui gère une **liste d'enregistrements protégés** contre la **falsification** ou la **modification** par les nœuds de stockage.*
  *Une blockchain est donc un **registre distribué** et **sécurisé** de toutes les **transactions** effectuées depuis **le démarrage du système réparti**.*

Autre définition (BlockChain France)

- La blockchain est une technologie de stockage et de transmission d'informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle.

  Par extension, une blockchain constitue une base de données qui contient l'historique de tous les échanges effectués entre ses utilisateurs depuis sa création. Cette base de données est sécurisée et distribuée : elle est partagée par ses différents utilisateurs, sans intermédiaire, ce qui permet à chacun de vérifier la validité de la chaîne.

Le potentiel de la blockchain

- Le caractère décentralisé de la blockchain, couplé avec sa sécurité et sa transparence, promet des applications bien plus larges que le domaine monétaire (bitcoin, ether, ...).
- 3 catégories d'utilisation de la Blockchain :
  - ✓ Les applications pour le **transfert d'actifs** (utilisation **monétaire**, mais pas uniquement : **titres, votes, actions, obligations...**)
  - ✓ Les applications de la blockchain en tant que **registre**
    => meilleure traçabilité des produits et des actifs.
  - ✓ Les ***smart contracts*** : programmes autonomes qui exécutent automatiquement les conditions et termes d'un contrat, sans nécessiter d'intervention humaine une fois démarrés.

- De façon générale, des blockchains pourraient remplacer la plupart des « **tiers de confiance** » centralisés :
  métiers de banques, notaires, cadastre,...

- Les défis à relever : économiques, juridiques, de gouvernance, ou encore écologiques.

Exemples d'applications

- Réduction des coûts de paiement et des coûts de transaction
  - ✓ En 2015, 25 banques internationnales ont signé un partenariat avec une société américaine ***R3*** pour l'utilisation de *blockchains* dans les marchés financiers
  - ✓ ***Citibank*** a annoncé son souhait d'émettre sa propre cryptomonnaie : le ***Citicoin***
  - ✓ En avril 2015, la banque ***UBS*** a ouvert à Londres son propre laboratoire de recherche dédié à l'étude de la technologie *blockchain* et à ses applications dans le domaine financier.
    À travers ces recherches et ces consortiums, les banques espèrent mettre en place une technologie basée sur la *blockchain* qui deviendra une ***référence*** au sein du domaine bancaire.
    En effet, le consortium ou la banque qui parviendra le premier à sortir une technologie éprouvée sera à même de facturer son propre service auprès des autres acteurs du domaine financier
- Développement d'assurances *peer-to-peers*
- Expérimentations dans les domaines suivants :
  - ✓ industrie musicale : gestion des droits d'auteurs
  - ✓ contrôle des données : construction d'un cloud décentralisé
  - ✓ chaîne logistique : traçabilité des matériaux

Aspects sociétaux

- La *blockchain* — et ses protocoles décentralisés de vérification des échanges — pourrait avoir un impact très important sur les *États*, qui se trouvent interpellés par rapport à leur monopole sur
  - ✓ la monnaie et
  - ✓ sur les transactions financières,

  mais aussi un impact sur les banques et l'économie tout entière.

- De nombreuses voix en France et à l'étranger ont souligné l'aspect révolutionnaire de cette technologie et les changements structurels qu'elle peut apporter à la société tout entière
  MAIS
  - ✓ grande quantité d'énergie électrique nécessaire à son fonctionnement
  - ✓ environnementalement ou économiquement soutenable ?

Inconvénients

- Gouffres énergétiques dû aux validations des blocs
  - ✓ le minage du *bitcoin* avait consommé un peu plus de **30 TWh** sur les 11 premiers mois de l'année 2017.
    La production électrique annuelle de l'Irlande est de **25 TWh**.
    Les fermes de minage étant souvent en **Chine**, une part très importante de l'électricité consommée est produite par des **centrales au charbon**...

    Tout ça pour seulement 350.000 transactions par jour et 30 millions d'utilisateurs.

    Qu'est-ce que ça serait si cette "monnaie" était utilisée autant que le dollar ou l'euro ?

- Monnaie acéphale : c'est bien le problème, c'est celui qui a le moins de scrupule qui décide et utilise les autres à son profit.

Ce qu'attendent les start-up française

- Plus de 410 start-up positionnées sur la Blockchain en juillet 2016
- Les fintech qui opèrent dans le domaine veulent avant tout éviter de subir une législation trop contraignante.
- Rapprocher start-up et juristes en créant des guichets chez les régulateurs, dans le but d'aider les jeunes pousses.
  => L'Autorité des marchés financiers (AMF) et l'Autorité de contrôle prudentiel et de résolution (ACPR) ont toutes deux installé l'an dernier un pôle dédié aux start-up de la finance.
- Définir l'actif numérique, c'est-à-dire les éléments transmis par la blockchain.
- Reconnaître le bitcoin du point de vue juridique, qui permet de régler des achats sans passer par une banque et sans devoir communiquer les coordonnées de carte bancaire.
- Depuis début 2017, La Maison du bitcoin est affiliée à certaines règles de Tracfin, la cellule anti-blanchiment de Bercy. Si elle remarque des transferts importants ou des comportements étranges de ses clients, elle doit désormais le signaler à l'organisme.
- Identifier l'émetteur des opérations dans la blockchain afin de bénéficier d'une authentification numérique (assurance, papier d'identité, ...)

Aspects juridiques

- Les aspects juridiques de la blockchain portent sur :
  - ✓ le droit de la propriété intellectuelle,
  - ✓ le droit du contrat ainsi que
  - ✓ la gouvernance de la chaîne

- La blockchain publique fonctionne sans tiers de confiance => idéalisme communautaire.
- La blockchain de consortium s'en approche en sélectionnant à l'avance les nœuds participants au consensus (R3).

- Une blockchain privée fonctionne avec un cadre établi dont les règles régissent le fonctionnement,

  alors que

- la blockchain publique ne définit pas d'autre règle que celle du code constitué par la technologie protocolaire et logicielle qui la compose.
- la loi applicable à la chaîne est la loi désignée par les parties

La gestion des titres transformée

- Grâce à la blockchain, les banques espèrent se passer des tiers de confiance coûteux qui assurent la bonne passation des titres.
- Le processus d'émission et de passation de titres pourrait être complètement transformé par l'utilisation de la blockchain :
  - ✓ amélioration des opérations automatisées et de la confirmation des opérations
  - ✓ réduction des frais de garde (coût de tenue de comptes titres).

- Eliminer les risques de non-livraison des titres
  - ✓ gérer l'échange de titres cotés sur une blockchain privée
  - ✓ les contrats intelligents permettront d'éliminer les risques de non-livraison des titres après règlement
  - ✓ le smart contract spécifie que la contrepartie A va livrer tant d'actions à B contre tant d'euros, et la transaction n'est débloquée que quand l'argent est reçu sur la blockchain
  - ✓ Le fonctionnement d'aujourd'hui à deux ou trois intermédiaires s'en verrait considérablement simplifié. Plus de chambres de compensation nécessaire, la blockchain jouant le rôle de tiers de confiance.

  => diminution des coûts...

Conclusion

- La blockchain est devenue une réalité technologique et économique dépassant le simple phénomène de mode.
- Elle fait passer d'un système pyramidal à une société de réseau « d'ordre spontané ».
- La blockchain s'est affranchie des cadres financier et bancaire dans lesquels elle était cantonnée.
- Complexe et sujette à bien d'interrogations, la compréhension et la maitrise de la technologie Blockchain nécessite la mobilisation de ressources importantes (temps, humain, financier) et fait intervenir une équipe pluridisciplinaire (DSI, marketing, relation client, etc.).
- Véritable phénomène, elle repense tous les usages et impacte tous les secteurs d'activité. Elle a révolutionné la monnaie fiduciaire avec les bitcoins et elle va maintenant « disrupter » les banques, mais aussi les notaires, les avocats, les agents immobiliers, le monde de l'énergie, la santé, la culture, les administrations, ...,

En résumé, ses usages semblent illimités...

CLUSIF

CLUSIR Rhône Alpes

Merci pour votre attention