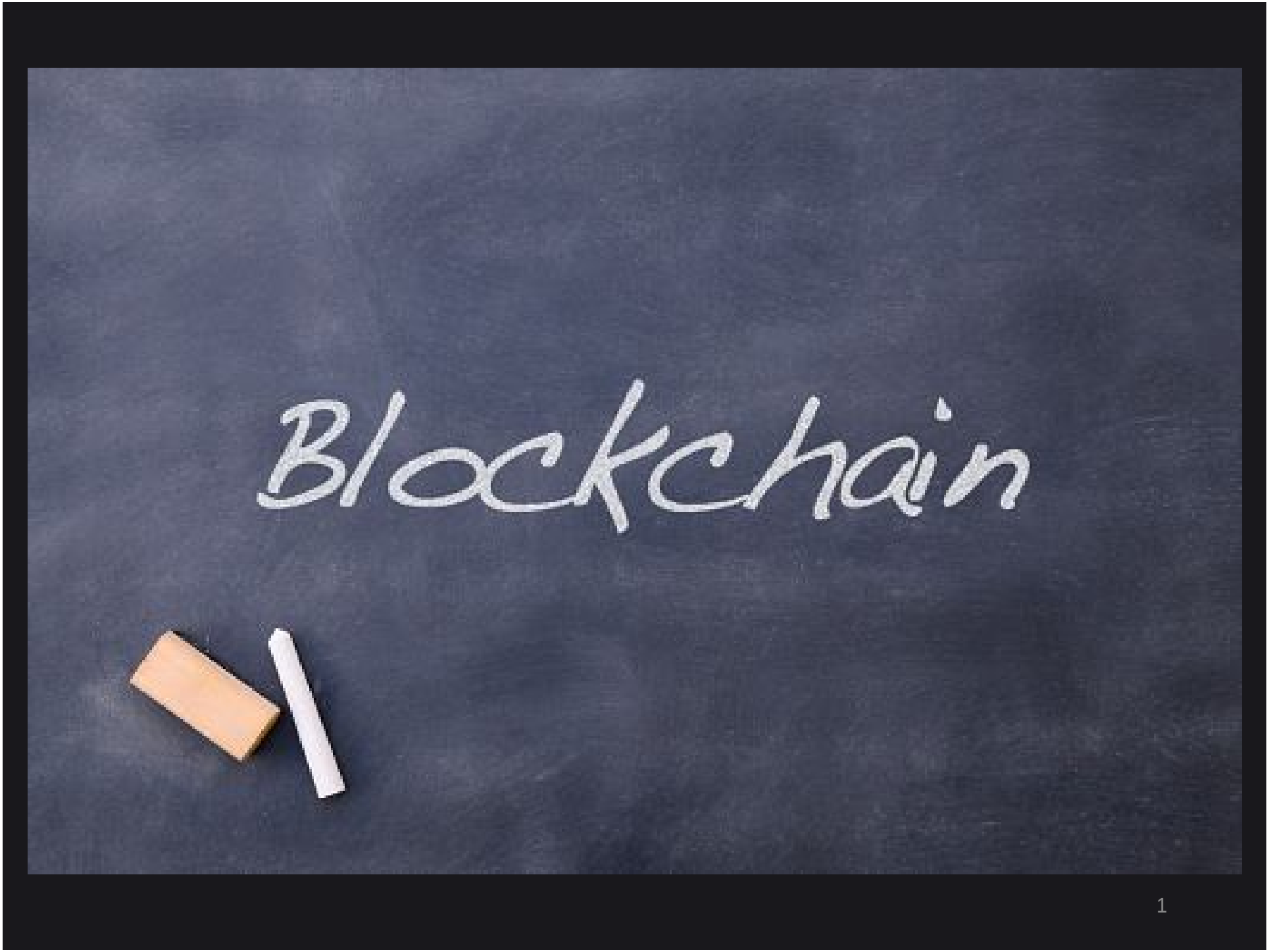

Blockchain

Laurent Leloup / Blockchain Addict

- Fondateur Finyear & Blockchain Daily News (médias & évènements)

- Expert blockchain auprès du Pôle de compétitivité mondial Finance Innovation

- Cofondateur-CEO Blockness (Blockchains for Business)

- Cofondateur & président de France Blocktech (association française de l'écosystème blockchain)

ll@finyear.com
ll@blockness.io
ll@franceblocktech.org

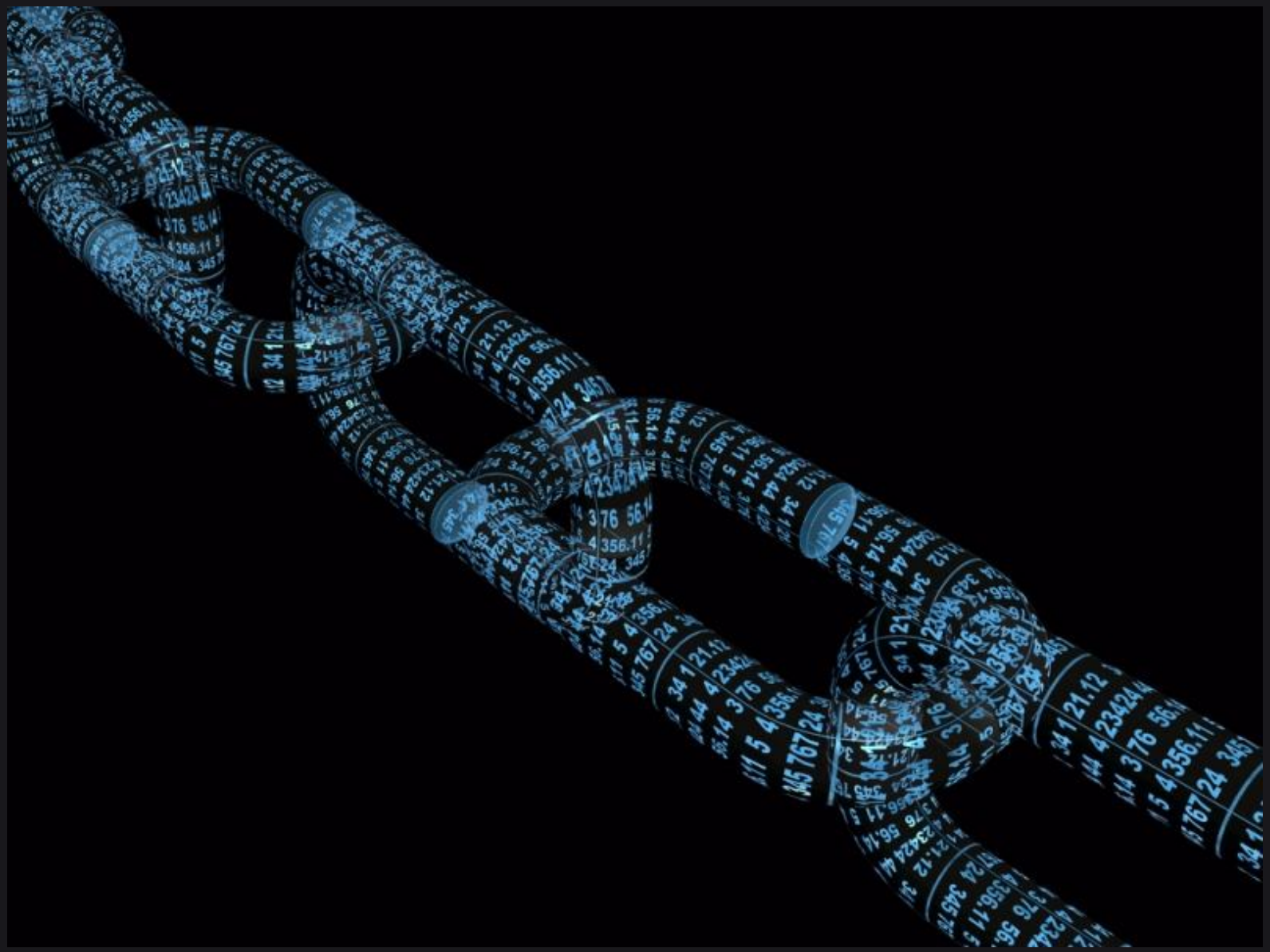
FINYEAR

BLOCKCHAIN DAILY NEWS

BLOCKNESS

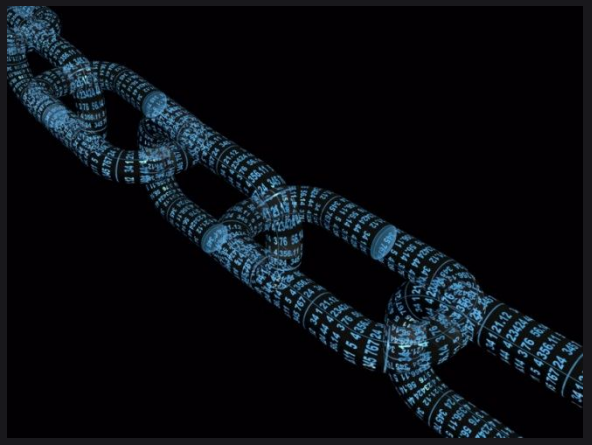
FRANCE BLOCKTECH

Finance Innovation
Pôle de compétitivité mondial



1. Blockchain

Blockchain | définition



Une blockchain est une base de données transactionnelle distribuée, comparable à un grand livre comptable décentralisé et partagé, qui stocke et transfère de la valeur ou des données via Internet, de façon transparente et sécurisée, et sans organe central de contrôle.

Ce registre est actif, chronologique, distribué, vérifiable et protégé contre la falsification par un système de confiance répartie (consensus) entre les membres ou participants (nœuds).

Chaque membre du réseau possède une copie à jour du grand livre (en temps quasi réel) et le contenu est toujours en phase avec l'ensemble des participants.

Blockchain | définition (suite)

- Elle permet l’automatisation de la transaction en supprimant les tiers.

- C’est un système de consensus distribué.

- C’est une infrastructure de certification et de notarisation.

Ainsi, la blockchain apporte une infrastructure de confiance algorithmique distribuée ou consensus-as-a-service (consensus à la demande).

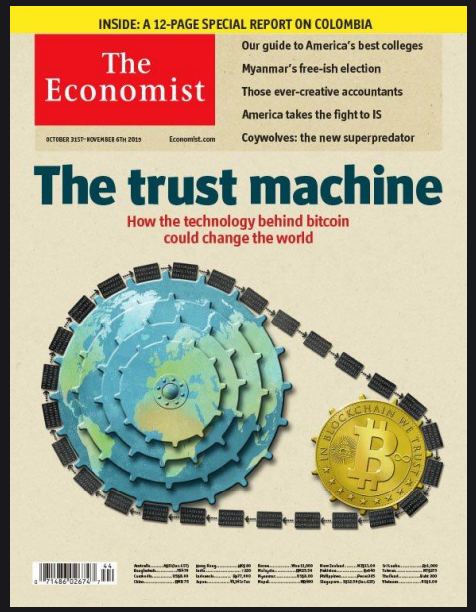
Blockchain | principes

La décentralisation & la distribution : aucune autorité centrale ne contrôle la blockchain. Pas de tiers de confiance.

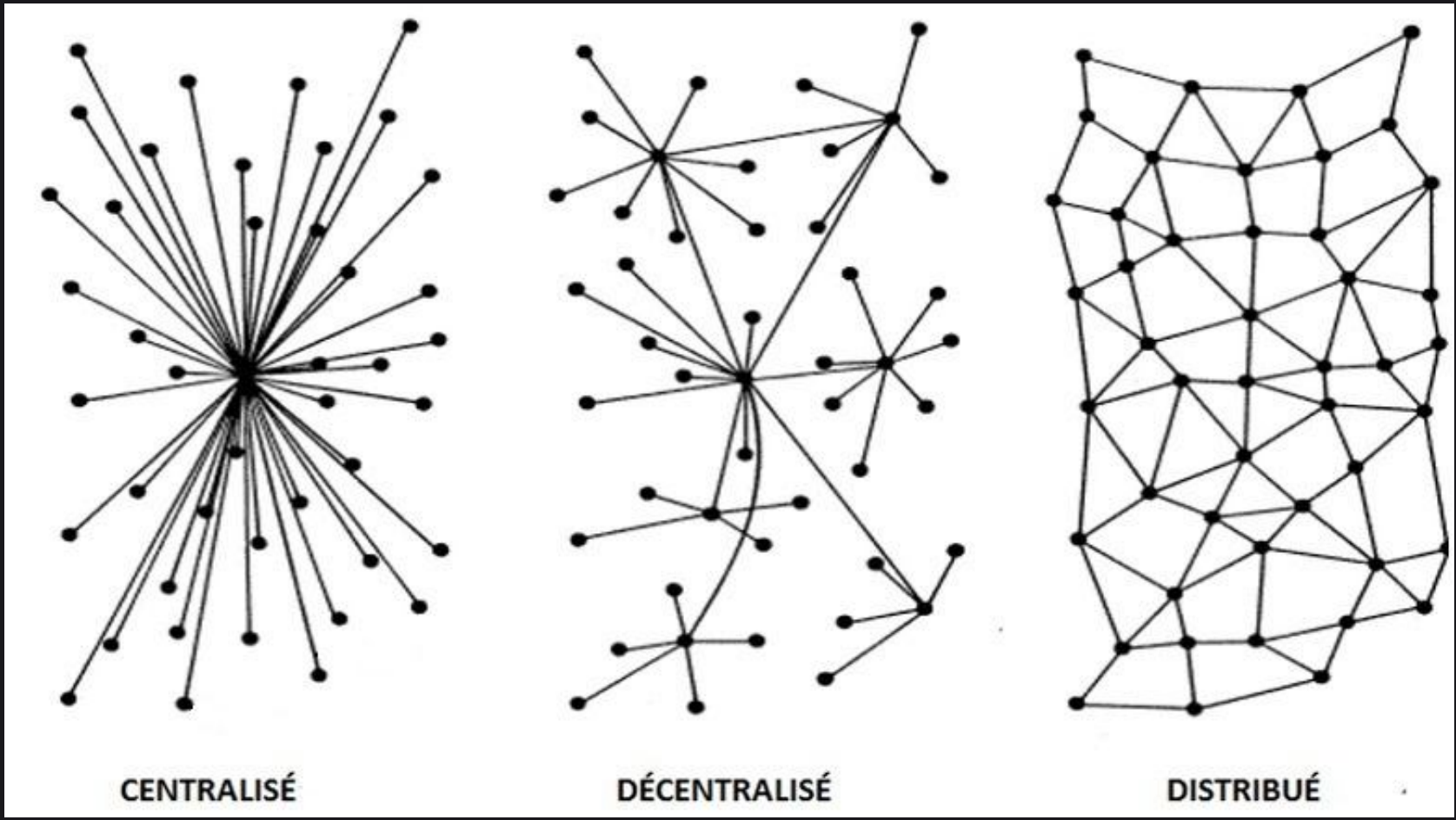
Le grand livre : reprendre le modèle des ledgers (livres comptables) mais se débarrasser de l'intermédiation financière.

Le consensus : le fait qu'une transaction soit acceptée ou rejetée est le fruit d'un consensus distribué et non d'une institution centralisée.

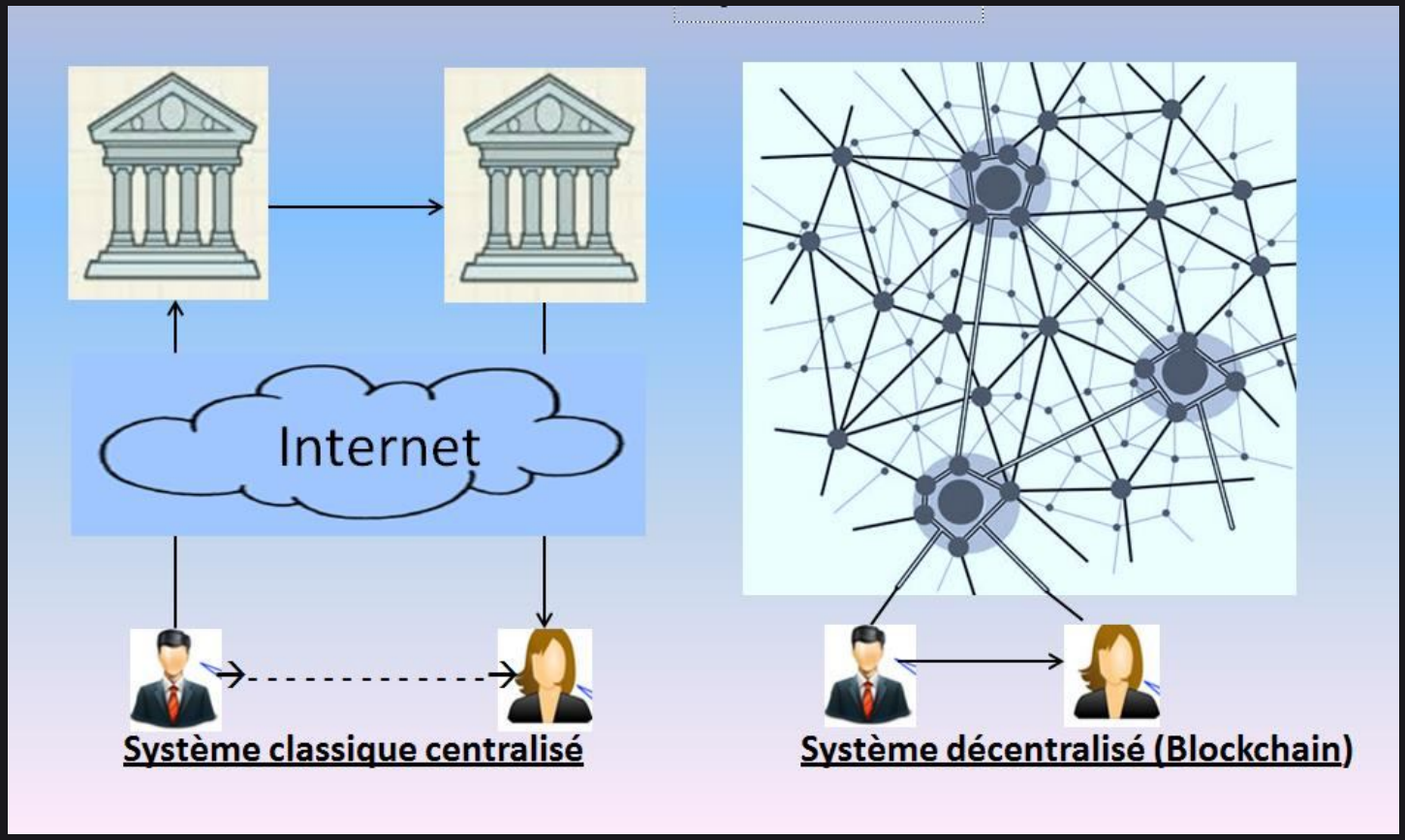
Passer par un mécanisme de consensus collectif
+ utiliser un grand livre ouvert, décentralisé et partagé
= CONFIANCE, TRANSPARENCE, PARTAGE.



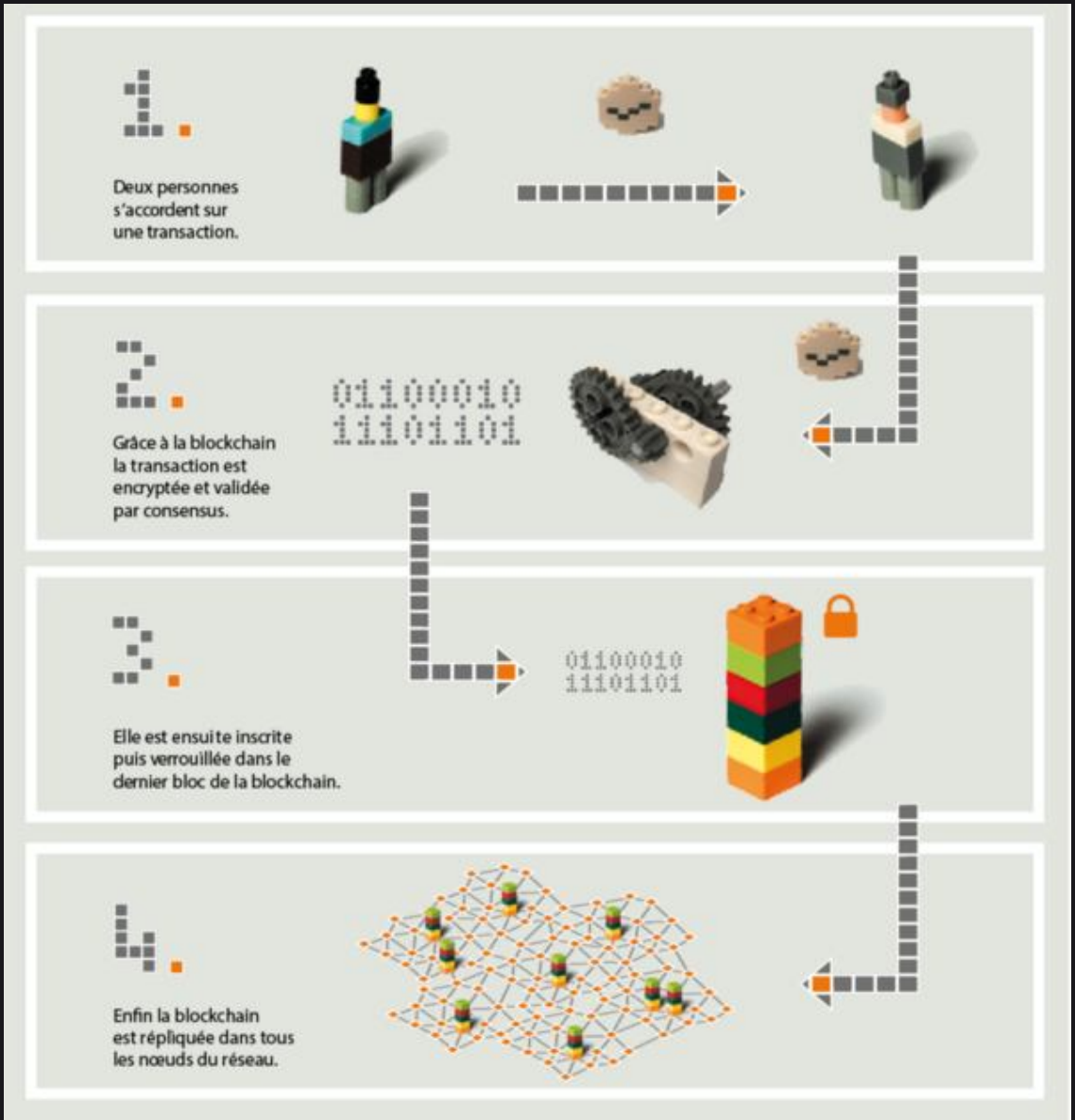
Blockchain | distribution / réseau P2P



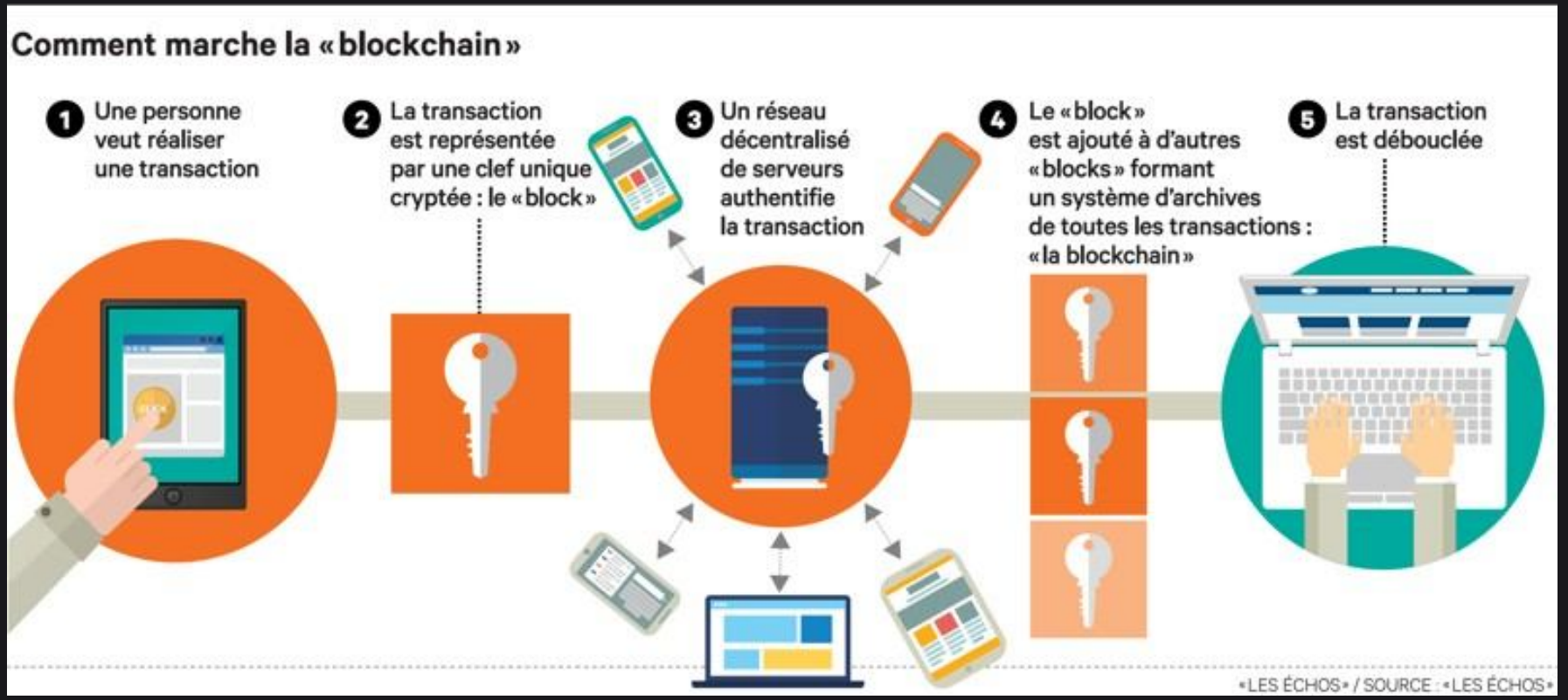
Blockchain en images (1/5)



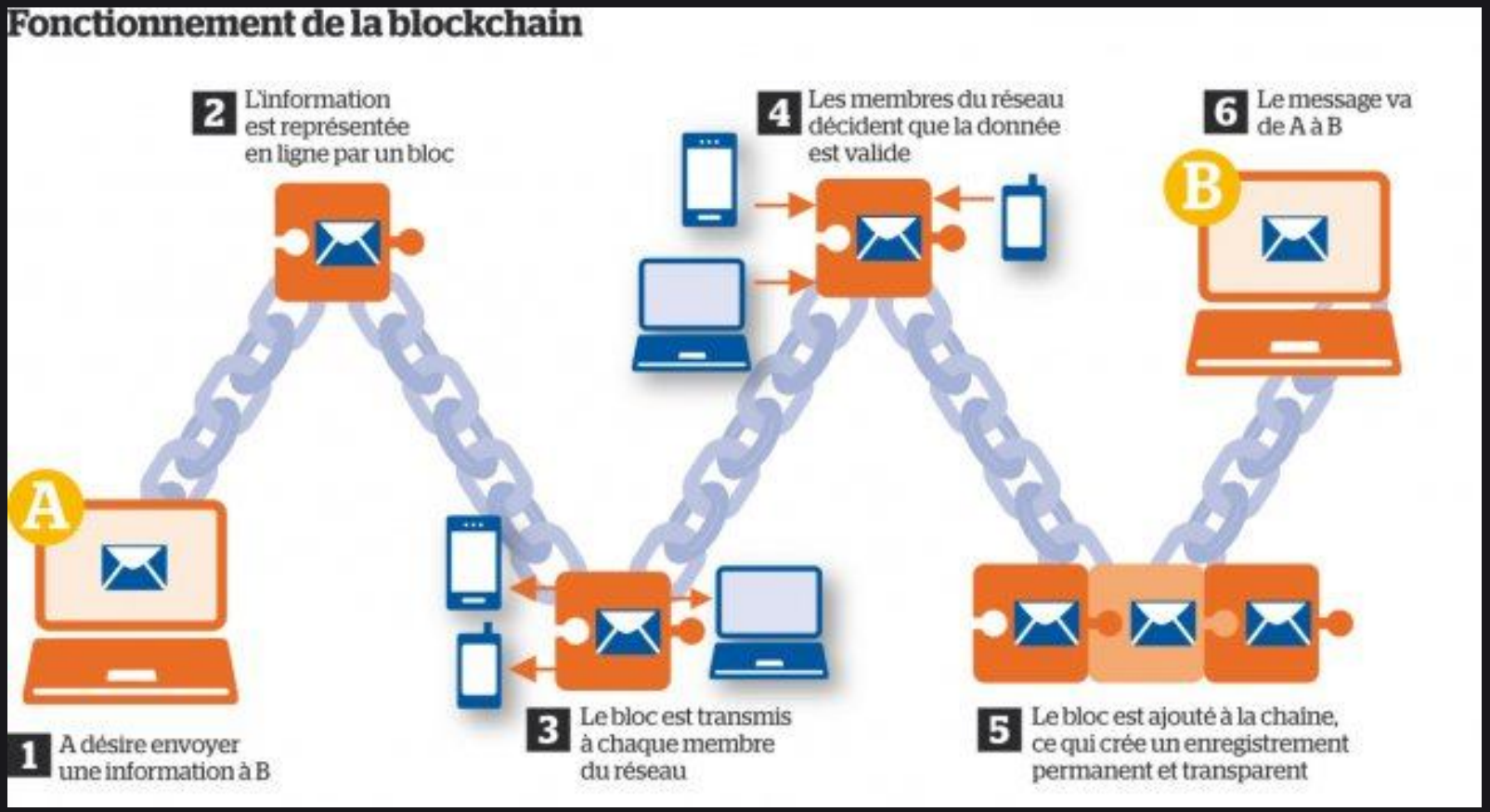
Blockchain en images (2/5)



Blockchain en images (3/5)

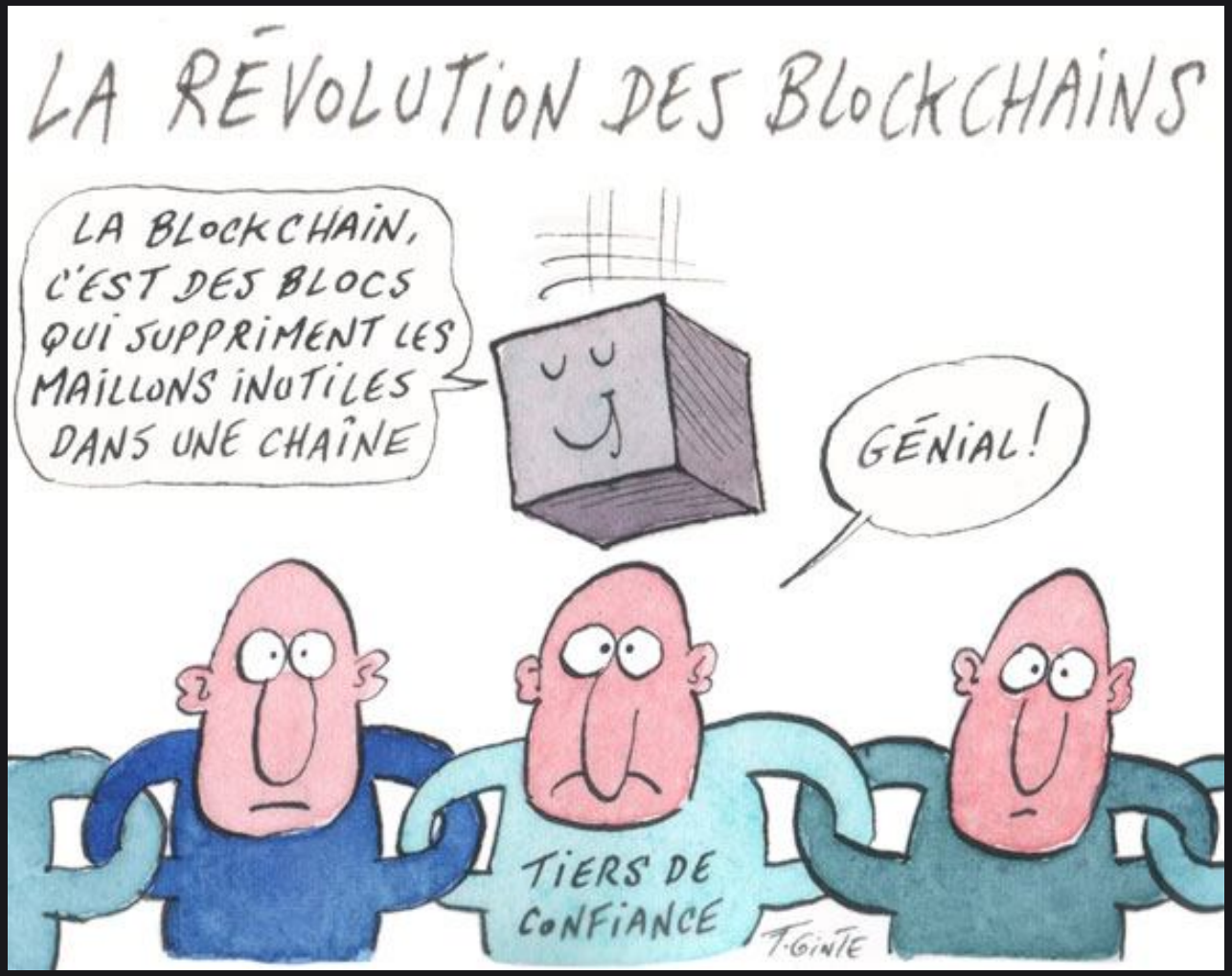


Blockchain en images (4/5)



© C. Dubos - Schéma présentant le fonctionnement de la blockchain / Le Moniteur

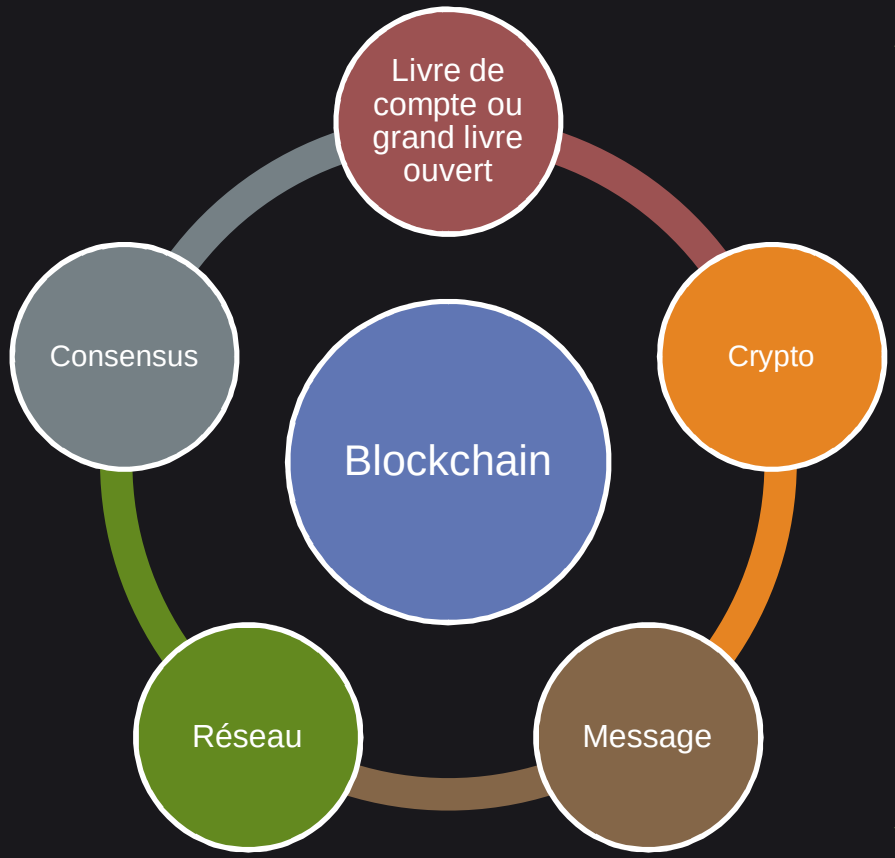
Blockchain en images (5/5)



Par François Cointe Cartoonist / LeMagIT /
http://www.techtarget.com/fr/auteur/Francois-Cointe

Blockchain | éléments clés

Constituants



Avantages

- Vitesse
- Sécurité
- Transparence
- Facilité
- Coût

Blockchain | catégories

Chaque blockchain est définie par :
- sa communauté,
- le type de transactions qu'elle permet,
- la méthode qu'elle choisie pour assurer que le consensus est honnête,
- et son caractère privé ou publique.

Bitcoin Blockchain
- Monnaie bitcoin : Bitcoin (BTC)
- Autre monnaie : Factom (Factoids), Mastercoin (MSC), Couterparty (XCP), Namecoin (NMC)

Non-Bitcoin Blockchain
- Monnaie bitcoin : Blockstream, Truthcoin
- Autre monnaie : Ethereum (Ether), BitShares (BTS), Truthcoin (cashcoin), Litecoin (LTC), PayCoin (XPY)

Non-Blockchain
- Consensus : Ripple (XRP), Stellar (STR), NXT (NXT), Hyperledger, Tendermint, Pebble, Open Transactions, aeChain (aeDeus Group)

Blockchain Neutre
- Services Intelligents : Eris Industries, PeerNova, Codius, SmartContract, SAE Tezoz, Tillit

Blockchains consortium

Une blockchain consortium est une blockchain dans laquelle le consensus est contrôlé par un ensemble présélectionné de noeuds. Exemple : le consortium R3 CEV dont 45 banques sont membres.

Blockchain | web vs blockchain

WEB

- Il a permis l'automatisation de la relation (et de la mise en relation),
- C'est un système de publication décentralisé,
- C'est une infrastructure de publication.

BLOCKCHAIN

- Elle permet l'automatisation de la transaction en supprimant les tiers.
- C'est un système de consensus distribué.
- C'est une infrastructure de certification.

Ainsi, la blockchain apporte une infrastructure de confiance algorithmique distribuée ou consensus-as-a-service (consensus à la demande).

2. Consensus

Consensus | intro

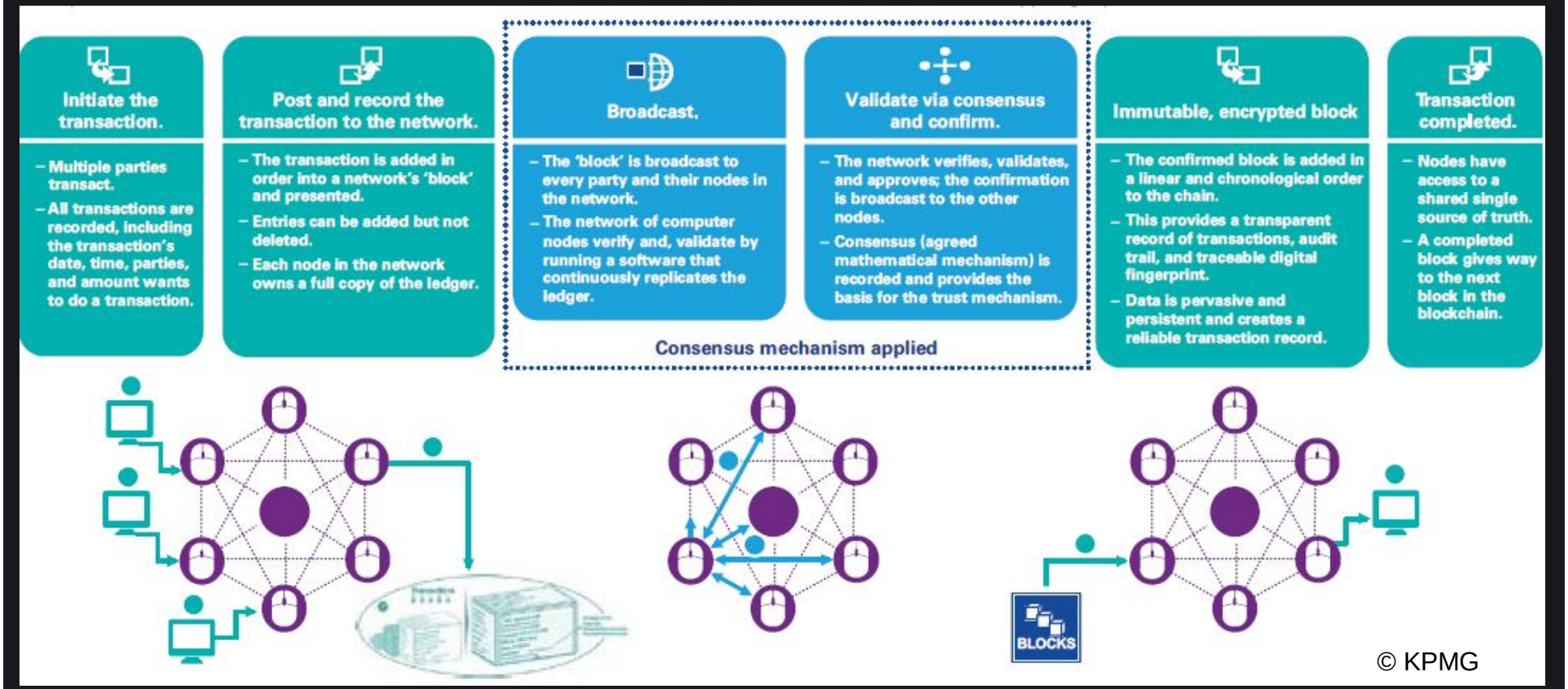
Le consensus informatique dans le domaine des systèmes distribués est un moyen pour les nœuds de se mettre d'accord sur la validité d'une transaction et de mettre à jour le grand livre avec un ensemble cohérent de faits confirmés (source : KPMG – George Samman).

La blockchain est une machine à transparence et à confiance.

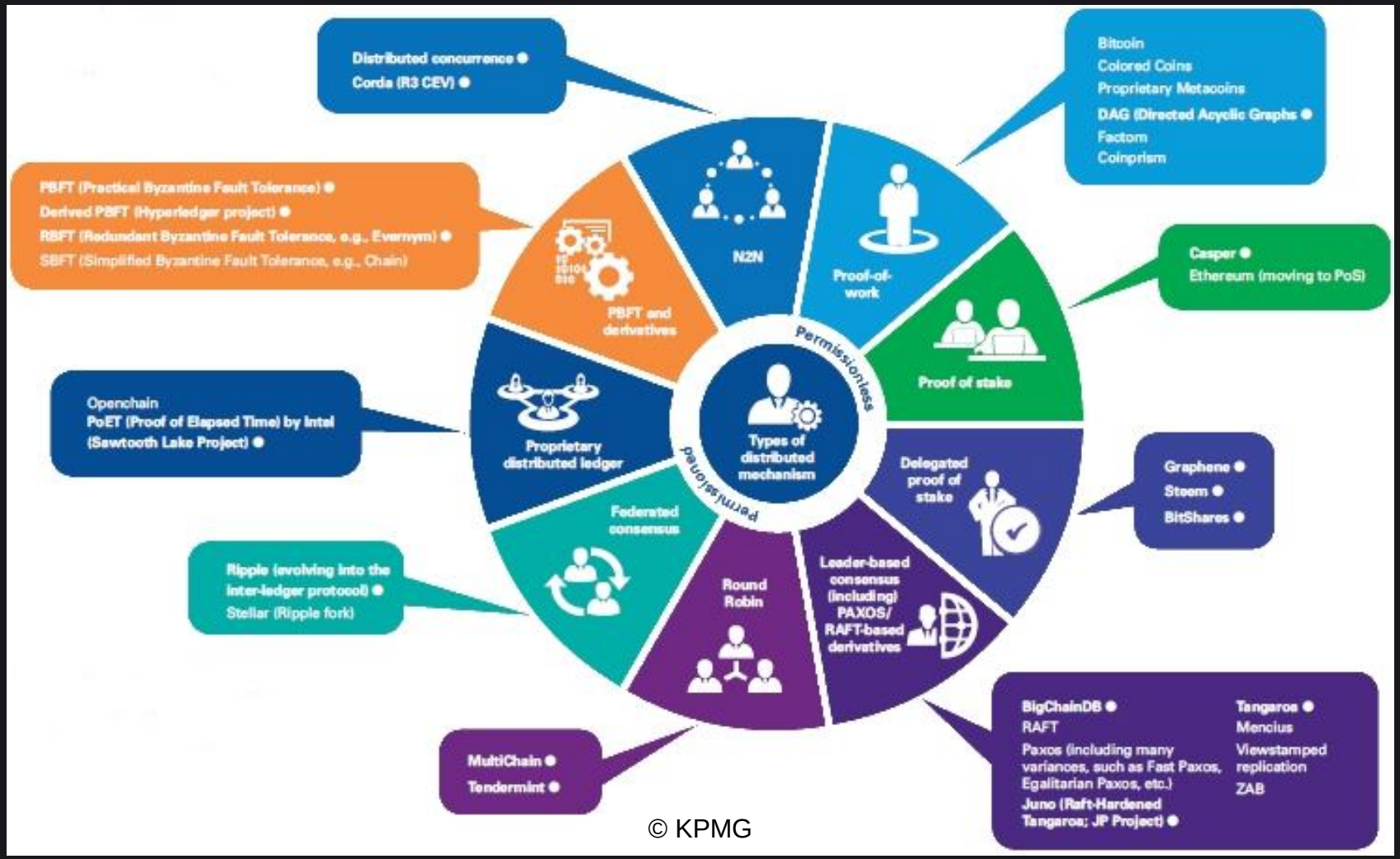
Pour déterminer le consensus et les types d'autorisations que nous souhaitons configurer dans notre expérience blockchain, nous devons répondre à 3 questions :
1) Qui sommes-nous ?
2) Qu'est-ce que nous voulons atteindre ?
3) Qui seront les nœuds ?

Consensus | Bitcoin

Mécanisme mathématique de la blockchain Bitcoin

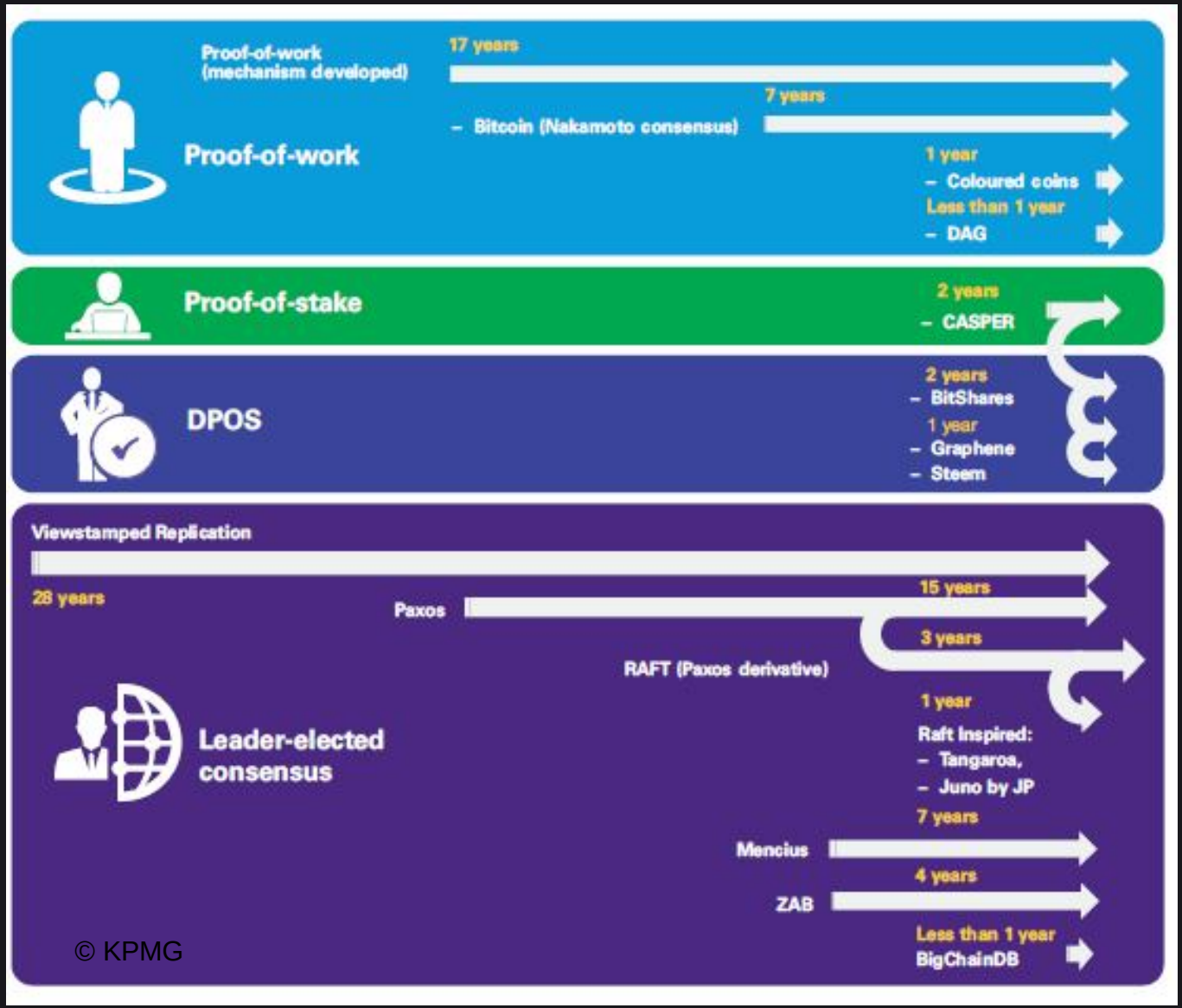


Consensus | mécanismes (1)

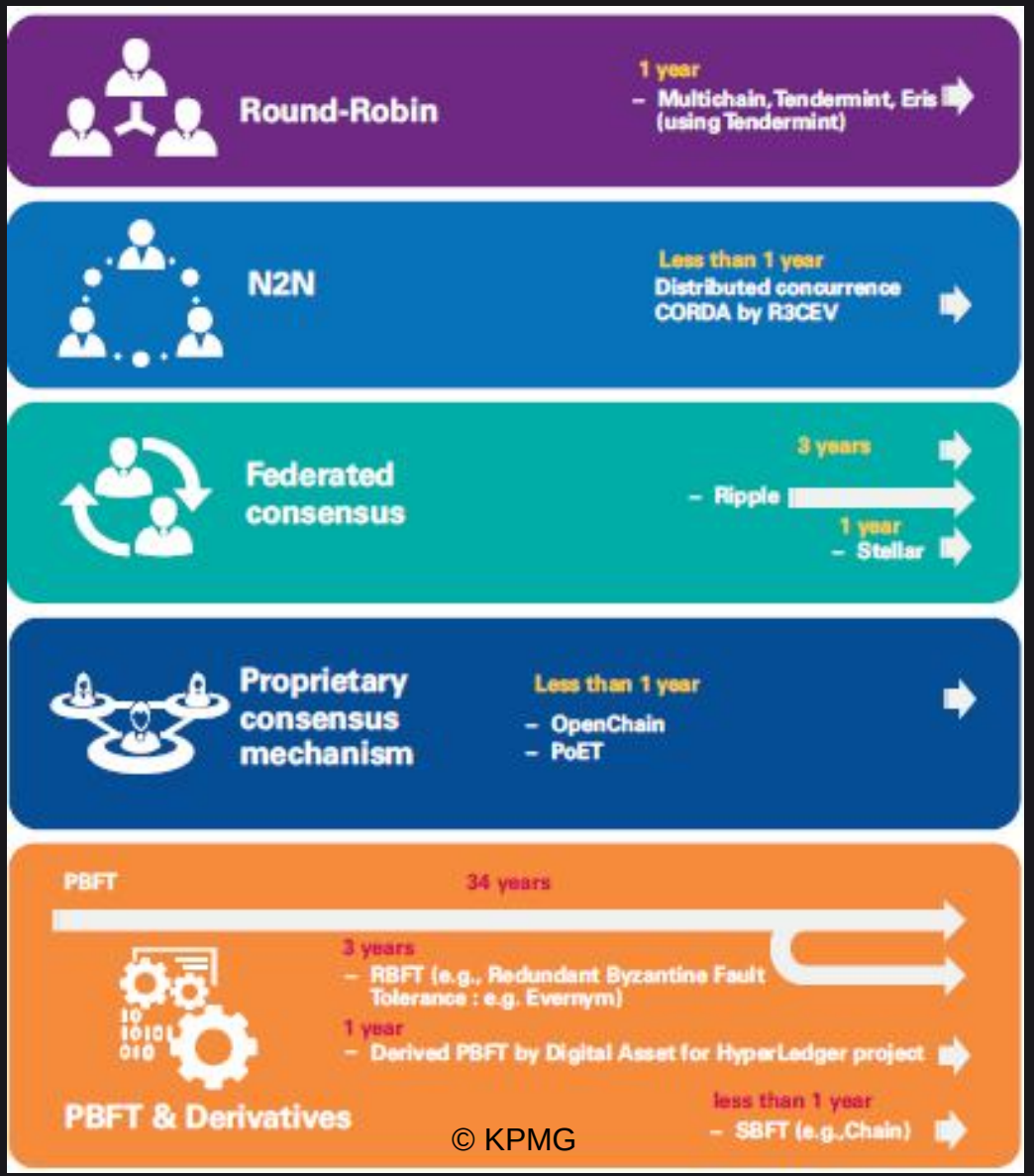


© KPMG

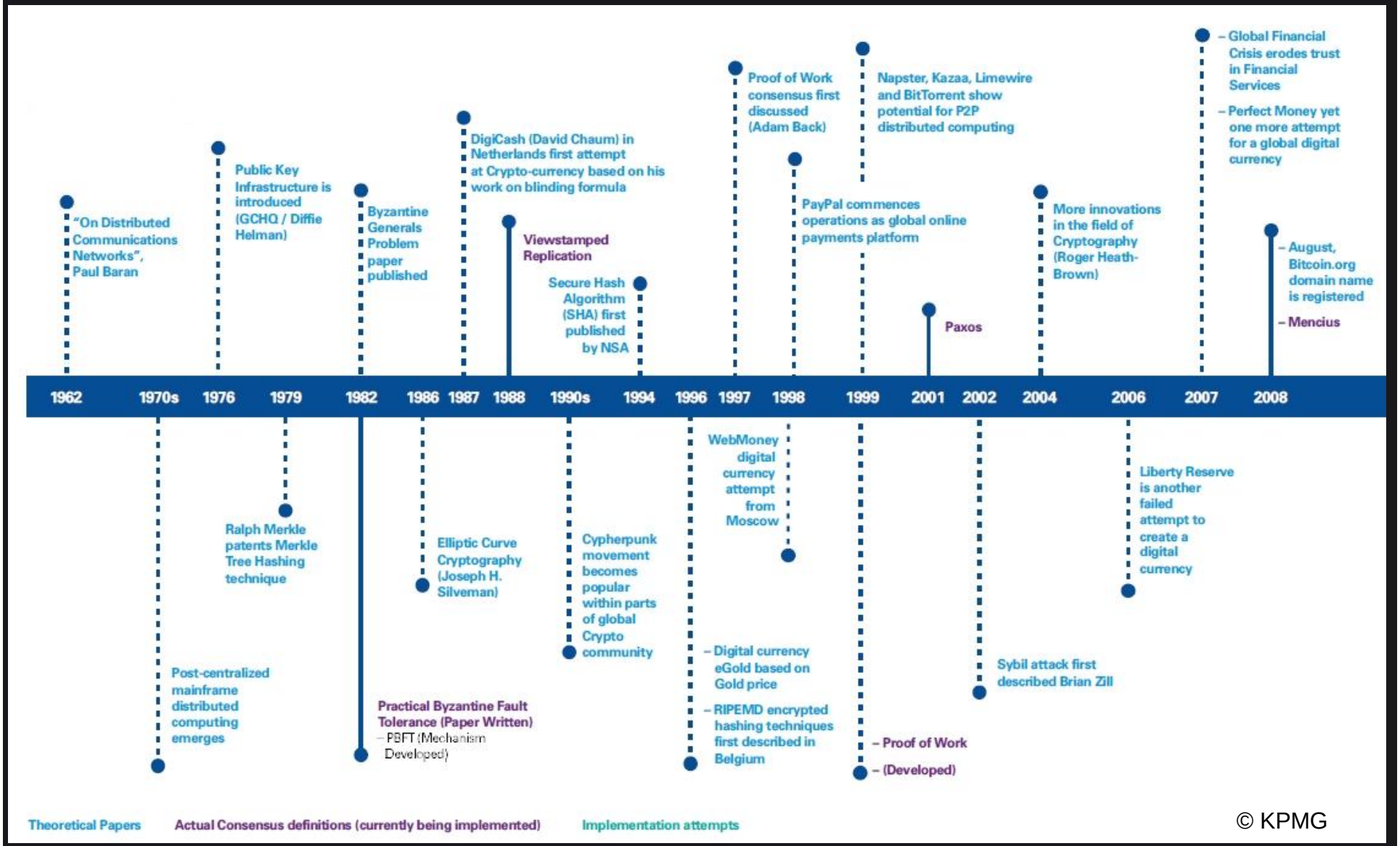
Consensus | mécanismes (2)



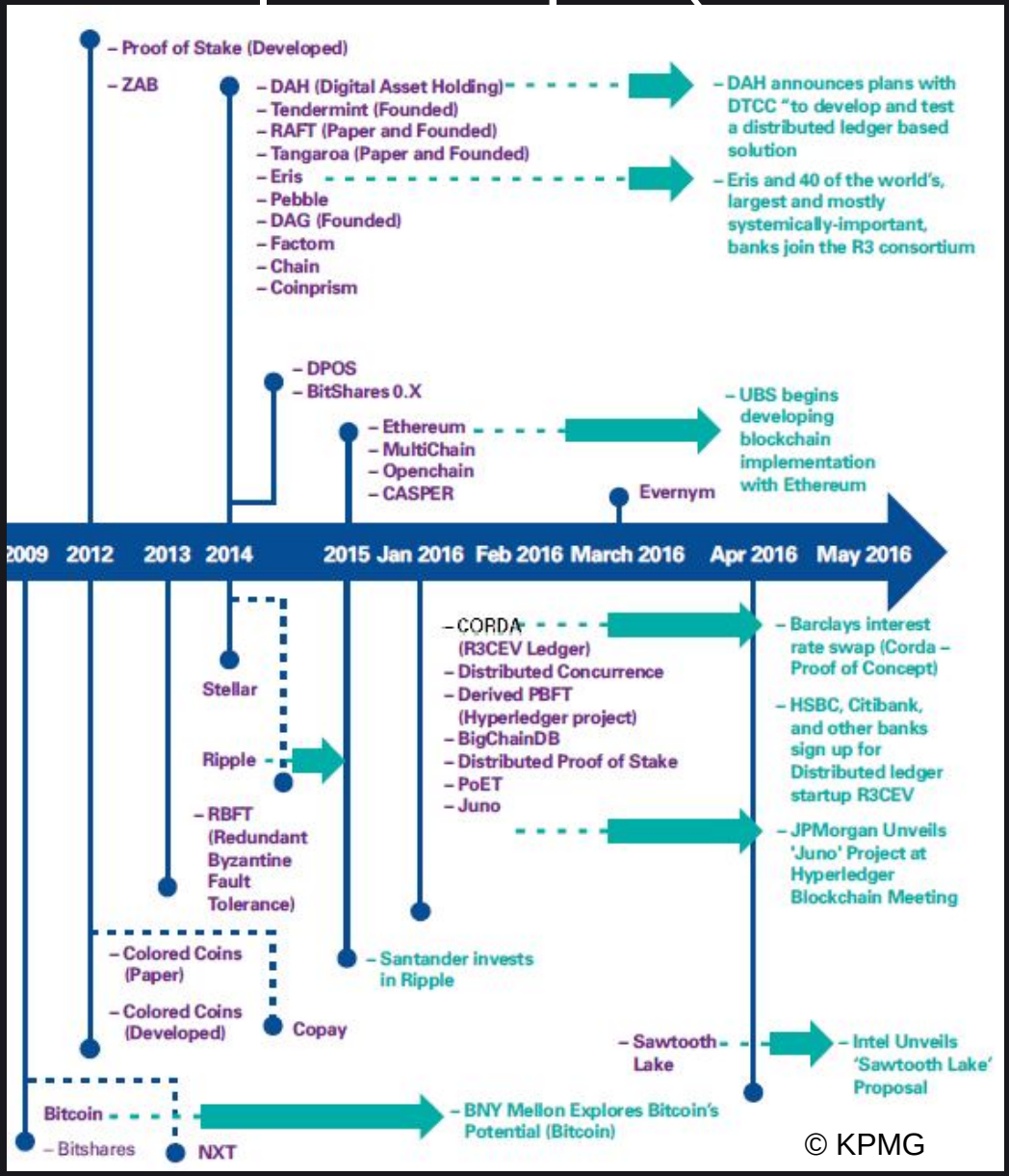
Consensus | mécanismes (3)



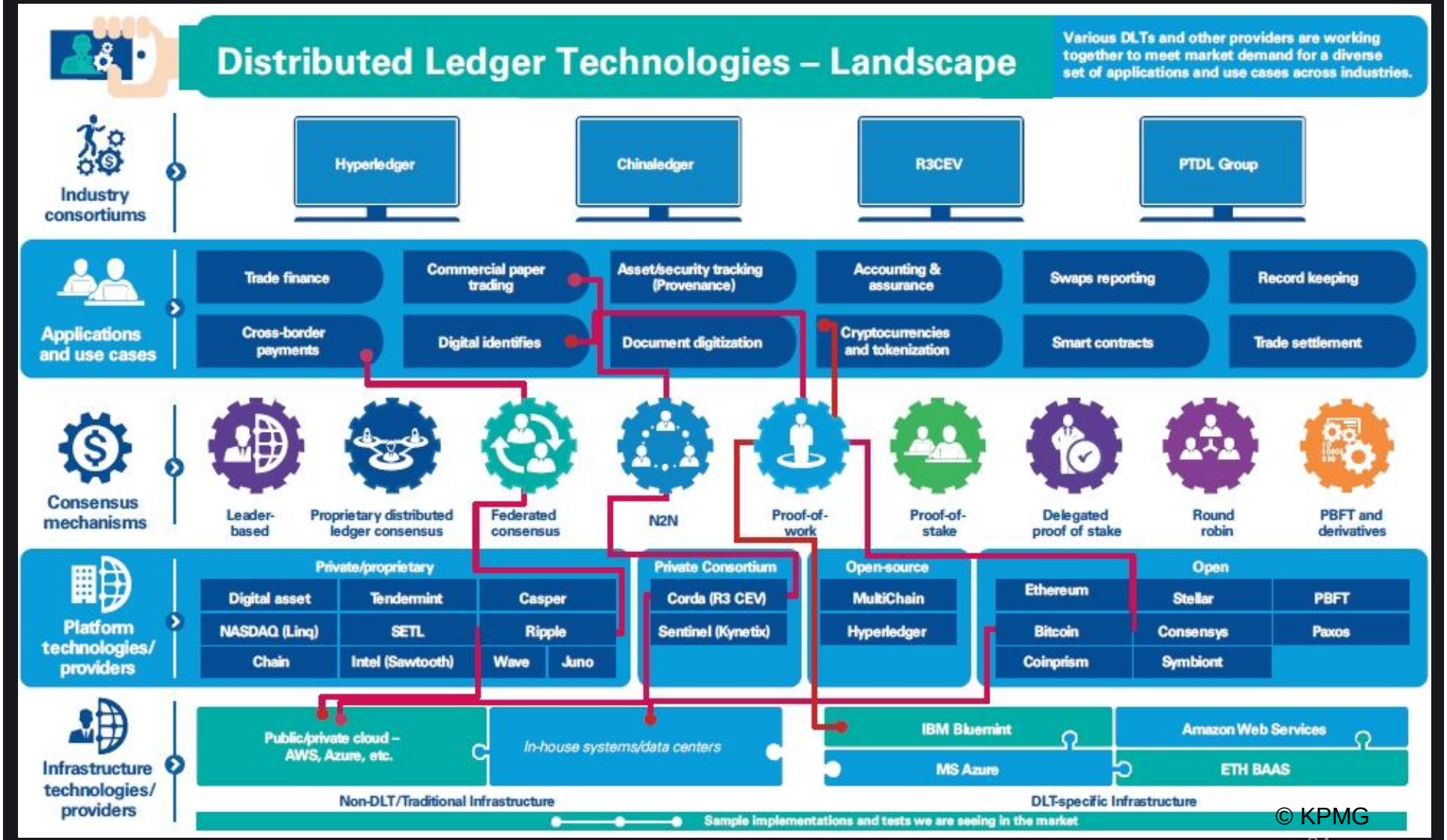
Consensus | historique (1962-2008)



Consensus | historique (2009-2016)



Consensus | DLT



3. Bitcoin, altcoins

Bitcoin | définition

En 2009 la technologie blockchain a permis l'émergence de la crypto-monnaie bitcoin.

Le terme **bitcoin** provient de l'anglais :
- « bit » : unité d'information binaire et
- « coin » : pièce de monnaie.

Bitcoin désigne à la fois
- un protocole informatique (Bitcoin) à travers le réseau Internet et
- l'unité de compte (bitcoin) utilisée par ce système de paiement.

Le principe de ce système de paiement est de tenir à jour sur un très grand nombre de nœuds (participants) du réseau, un registre (ledger ou blockchain) à la fois public et infalsifiable de toutes les transactions dont le montant est exprimé dans l'unité de compte bitcoin.

NB : un protocole informatique est un ensemble de règles qui permettent à des ordinateurs de coopérer pour accomplir une tâche (SMTP, HTTP, Bitcoin, etc…).

Bitcoin | définition (suite)

Chaque bitcoin est identifiable depuis sa création, par un historique dans un grand livre de comptes (base de données sécurisée ou chaîne de blocs) de toutes les transactions dans lesquelles il est impliqué.

Les transactions, émises en clair, sont reconnues valables par les signatures cryptographiques correspondantes qui ainsi les avalisent.

Le nombre de bitcoins est limité à 21 millions d'unités.

Chaque bitcoin est divisible jusqu'à la huitième décimale. Donc le plus petit montant qui puisse être transféré est de 0.00000001 (10-8) bitcoin, nommé « satoshi » par la communauté Bitcoin, en hommage à l’inventeur de cette monnaie.

Bitcoin | problème des Généraux Byzantins

Le consensus “Practical Bizantine Fault Tolerance” (PBFT).

Des généraux disposants chacun d’une armée doivent se coordonner pour assiéger une ville. Les généraux communiquent via des messagers fiables.

Mais certains généraux sont des traitres et visent à faire échouer le plan d’attaque.
L’attaque n’a lieu que si les généraux arrivent à un consensus.
Il faut donc trouver un algorithme pour s'assurer que les généraux loyaux arrivent tout de même à se mettre d'accord sur un plan de bataille.

Coordonner la confiance

Utiliser des messages écrits et signés (non falsifiables) entre les généraux.

Partager des intentions entre tous les généraux.

Byzantine Generals Problem

Bitcoin | Satoshi Nakamoto (中本哲史)

- Depuis 2007 Satoshi Nakamoto (中本哲史), la mystérieuse figure derrière l'invention de Bitcoin, a affirmé qu'il avait travaillé sur Bitcoin.

- En 2008 : il publie « Bitcoin: A Peer-to-Peer Electronic Cash System ». Il y expose une méthode pour résoudre un problème cryptographique sur lequel achoppait la recherche depuis plusieurs décennies, le problème du double paiement ou problème des Généraux Byzantins.

Celui-ci empêchait à deux agents d'échanger des actifs, comme une monnaie par exemple, sans le passage par un tiers de confiance.

Bitcoin | 中本哲史 (suite)

3 janvier 2009 : un bloc genesis est créé,

Block 0

Short link: http://blockexplorer.com/b/0

Hash: 000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

Next block: 00000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048

Time: 2009-01-03 18:15:05

Difficulty: 1 ("Bits": 1d00ffff)

Transactions: 1

Total BTC: 50

Size: 285 bytes

Merkle root: 4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b

Nonce: 2083236893

Raw block

Transactions

Transaction	Fee	Size (kB)	From (amount)	To (amount)
4a5e1e4baa...	0	0.204	Generation: 50 + 0 total fees	1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa: 50

12 janvier 2009 : 1ère transaction bitcoin

Bitcoin | 中本哲史 (suite)

- Février 2009 : il diffuse la 1ère version du logiciel Bitcoin sur le site P2Pfoundation et crée les premiers bitcoins,

- Mi 2010 : les développeurs et la communauté Bitcoin perdent progressivement contact avec Satoshi Nakamoto,

- 12 décembre 2010 : un dernier message est posté par Nakamoto sur le principal forum. Peu de temps avant son évanescence, Nakamoto installe Gavin Andresen comme son successeur en lui donnant accès au projet SourceForge Bitcoin et une copie de la clef d'alerte qui est une clef cryptographique privée unique permettant d'atténuer les effets d'une attaque potentielle sur le système Bitcoin, comme la découverte d'une faille cryptographique permettant de modifier *a posteriori* les transactions, ou la prise de contrôle de plus de 51% des nœuds du réseau.

Histoire du bitcoin sur : http://historyofbitcoin.org/

Bitcoin | transactions / fonctionnement

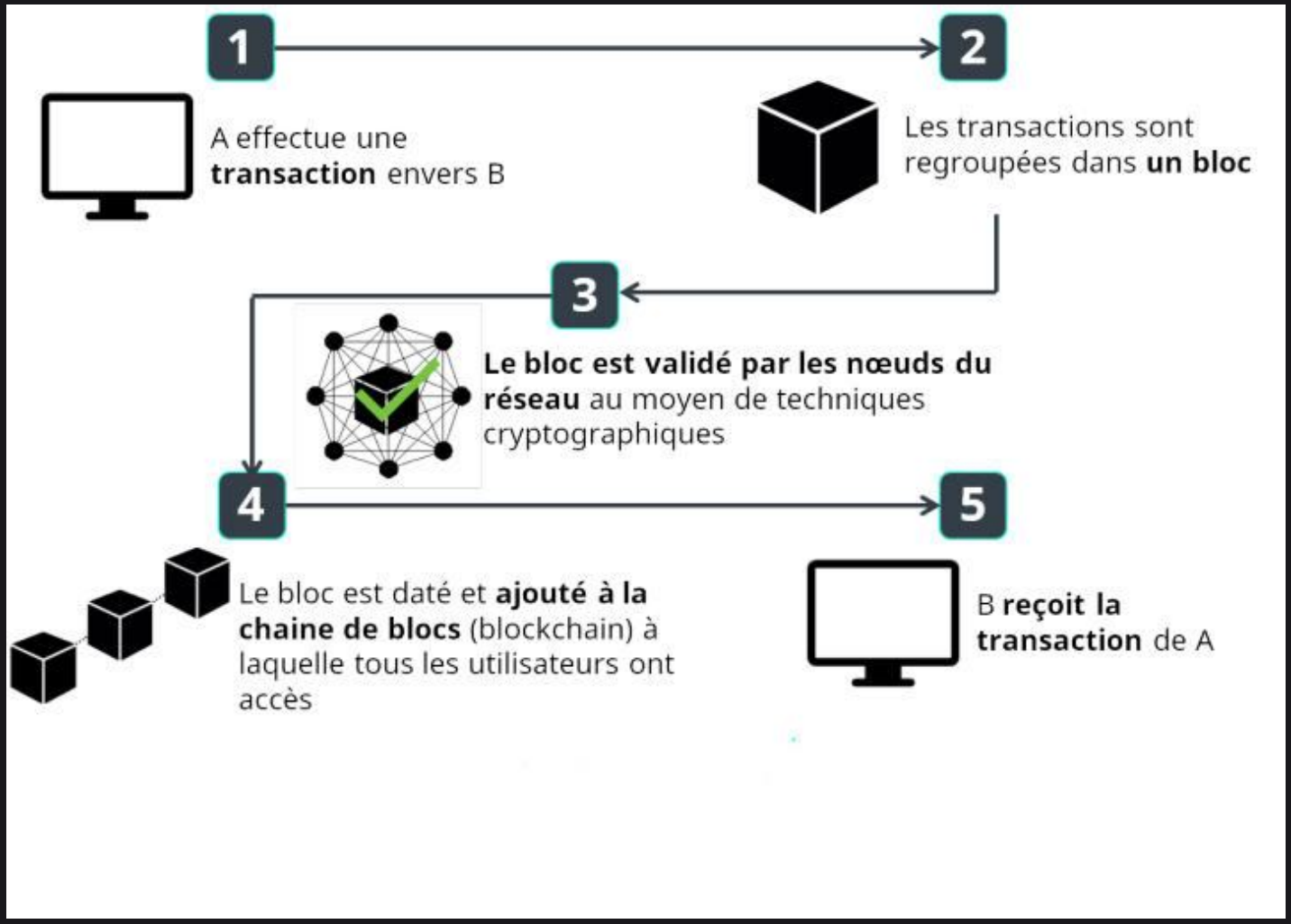
FONCTIONNEMENT :

1. deux personnes s'accordent sur une transaction,
2. grâce à la blockchain la transaction est encryptée et validée par consensus,
3. elle est ensuite inscrite puis verrouillée dans le dernier bloc de la blockchain,
4. enfin la blockchain est répliquée dans tous les **nœuds** (participants) du réseau.

Pour être valide, chaque transaction doit être signée, au sens cryptographique du terme en utilisant de la cryptographie asymétrique (clé privée / clé publique).

Trois informations sont donc nécessaires pour effectuer une transaction :
- la clé privée de l'adresse débitée,
- la clé publique de l'adresse créditée,
- et le montant de la transaction.

Bitcoin | transactions (dessin)



Bitcoin | transactions / format adresse

Une adresse est représentée au format ASCII grâce à un codage dédié sur 58 caractères alphanumériques : les chiffres et les lettres majuscules et minuscules, à l'exception des lettres et chiffres l, I, 0 et O, que Nakamoto a exclus car ces caractères se ressemblent dans certaines fontes.

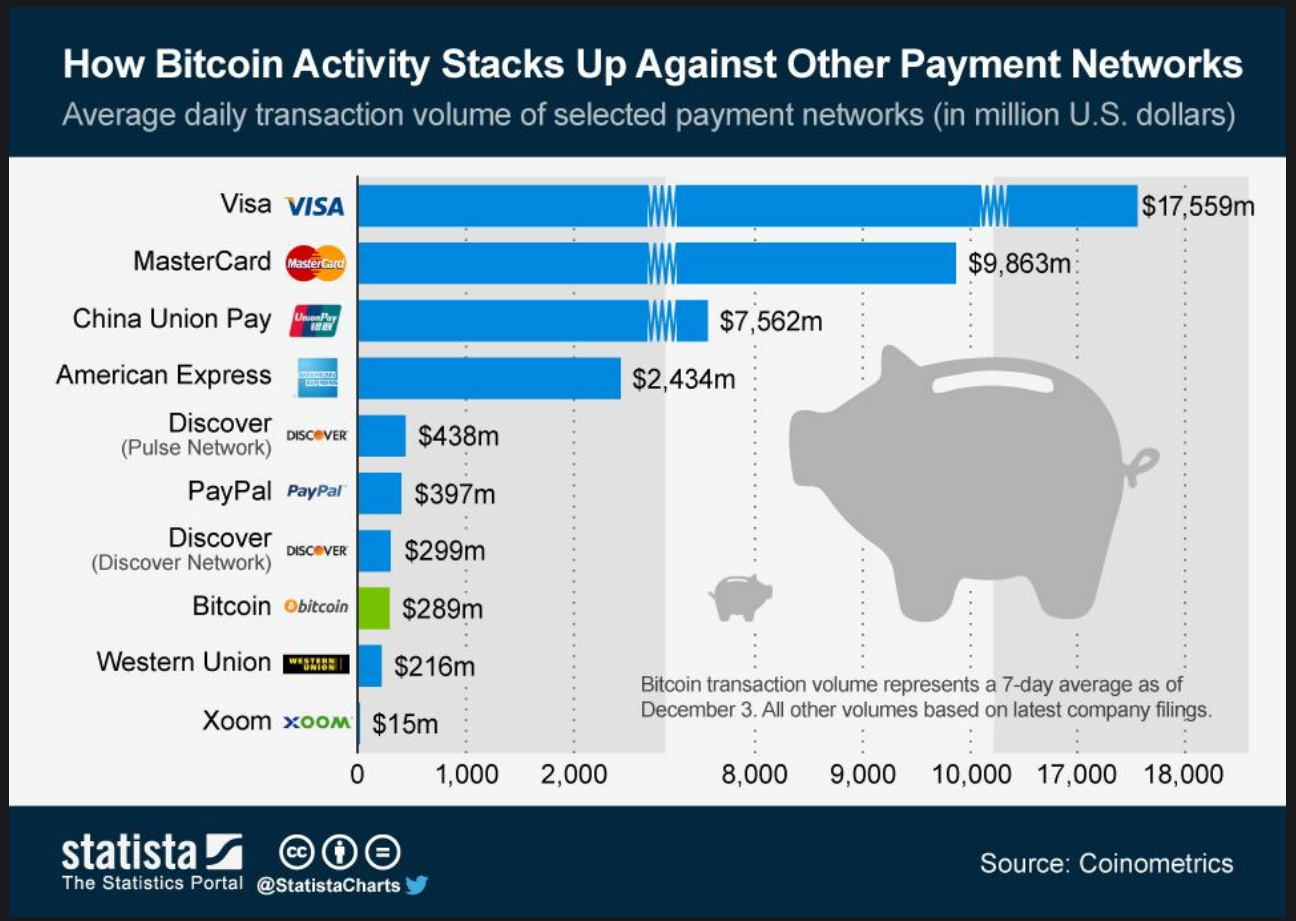
La 1ère adresse créée est : 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa44

Une adresse Bitcoin est la seule information nécessaire pour recevoir des bitcoins. Il n'est pas nécessaire d'exécuter le logiciel Bitcoin pour la réception, il suffit de communiquer une adresse et seul le payeur se charge d'envoyer la transaction complète au reste du réseau.

Pour exemple mon adresse Bitcoin est : 112BekzNCw8xEfwtpwDgKr3zEfUgyuxUZV

Bitcoin | transactions par jour (2009-2016)

Bitcoin | transactions / volumes par jour



Le système Bitcoin a toutefois des limites en terme de performances : le réseau ne peut traiter que 7 transactions à la seconde pour le moment alors que Visa tourne “régulièrement” à 480 transactions par seconde.

Bitcoin | minage (intro)

Pour ajouter une transaction dans la blockchain Bitcoin il faut miner…

Certains utilisateurs (nœuds) mettent à contribution leur puissance de calcul informatique (les CPUs) afin de vérifier, d'enregistrer et de sécuriser les transactions dans la «blockchain».

Chaque bloc est le fruit d’un consensus machinique et algorithmique.
Ce processus est appelé : Proof Of Work (PoW) ou Preuve de travail.

La difficulté change à chaque 2016 blocs.
Le réseau essaie d'assigner la difficulté de telle sorte que la puissance de calcul mondiale prenne exactement 14 jours pour générer 2016 blocs.
C'est pourquoi la difficulté augmente de pair avec la puissance du réseau.
En théorie, tout le monde peut être mineur. Mais en pratique, le minage est l’affaire de véritables entreprises essentiellement basées dans des zones géographiques où le coût de l’électricité est (quasiment) nul.

Bitcoin | minage (Proof of Work)

Un mineur pour arriver à confirmer un bloc de transaction, doit passer par un processus appelé : Proof Of Work (PoW) ou Preuve de travail.

Cela consiste en un décryptage de données ou calcul mathématique (c'est pour cela qu'on parle de crypto-devises ou crypto-monnaies car pour arriver à les produire il faut passer par un processus de décryptage).

Le minage est un protocole (algorithme) de consensus distribué et décentralisé mais d'autres formes de consensus existent (voir chapitre blockchains plus loin).
Exemple : Proof of Stake (preuve de détention), etc…

Les algorithmes de hashage sont SHA-256 et RIPEMD-160. Un double hash en SHA-256 est utilisé pour obtenir le hash des blocs et donc la preuve de travail, tandis qu'un SHA-256 suivi d'un RIPEMD-160 est utilisé pour construire les adresses bitcoins.

Blockchain | minage / les récompenses

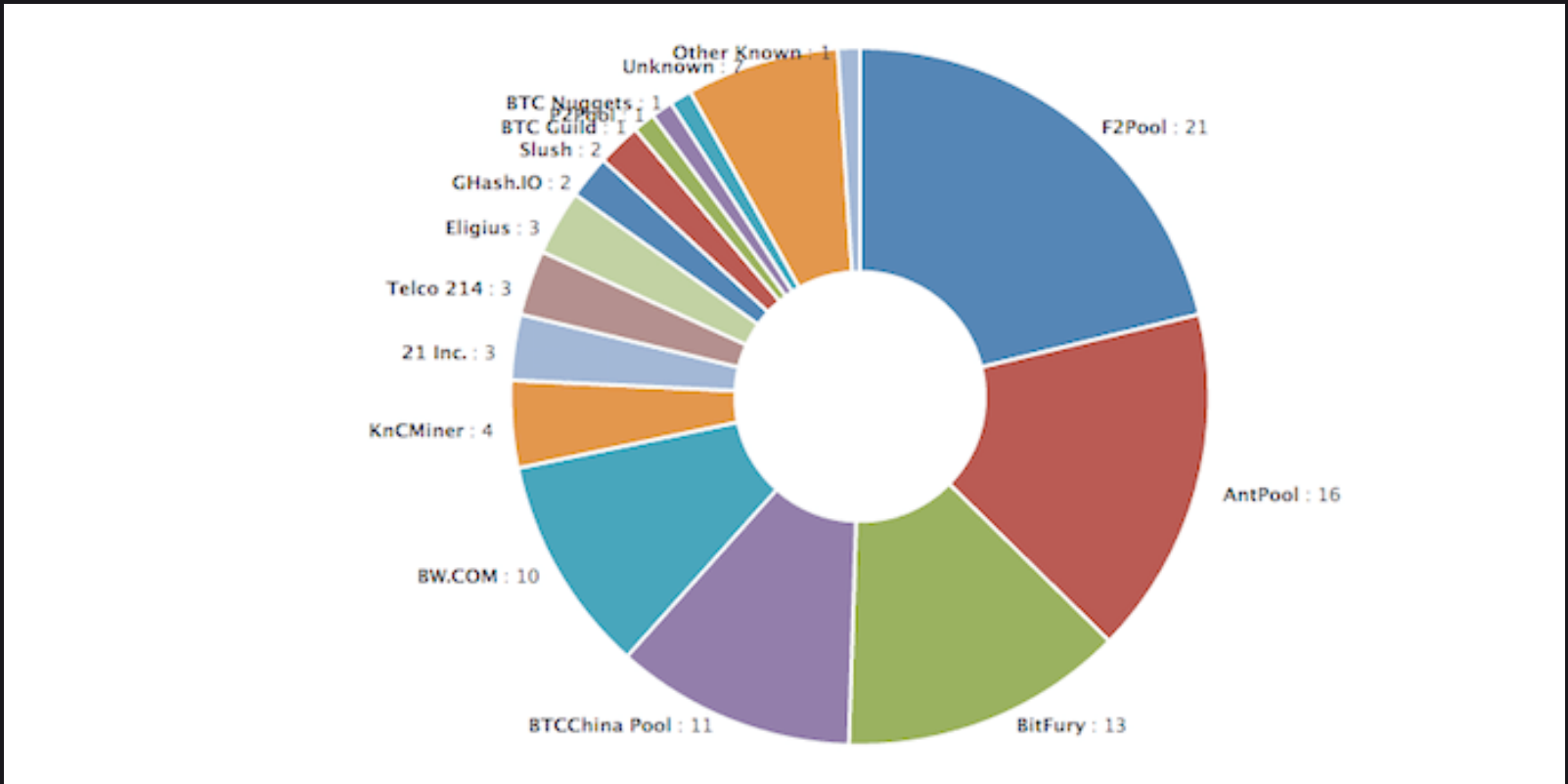
Dans la blockchain Bitcoin, un bloc = actuellement 1.000 transactions avec une taille limite de 1 Mégaoctet (la taille moyenne des blocs échangés oscille entre 600 et 700 Ko) soit environ 7 transactions par secondes.

Quand le mineur arrive à confirmer un bloc de transactions, ils remportent les 25 nouveaux bitcoins qui se créent toutes les 10 minutes.

Bitcoin existant depuis janvier 2009, la récompense pour la résolution d'un bloc était à l'origine de 50 bitcoins, mais elle est automatiquement divisée par deux tous les 210.000 blocs (environs tous les 4 ans) :

- les mineurs reçoivent aujourd'hui 25 bitcoins par bloc,
- 12,5 BTC à partir de 2017,
- 6,75 BTC à partir de 2021,
- etc…

Bitcoin | minage / pools de mineurs



Aujourd'hui une poignée de mega pools (GHASH. IO, AntPool, BW.COM, F2Pool …) ont le monopole de l'extraction de bitcoin. Il suffit de regarder sur le site blockchain.info dans la colonne « Relayé par » quel est le pool qui a réussi l'exploit de casser les derniers blocs. (les chiffres expriment des %)

Bitcoin | nœuds & réseau

GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Fri Sep 23 2016 13:46:25 GMT+0200.

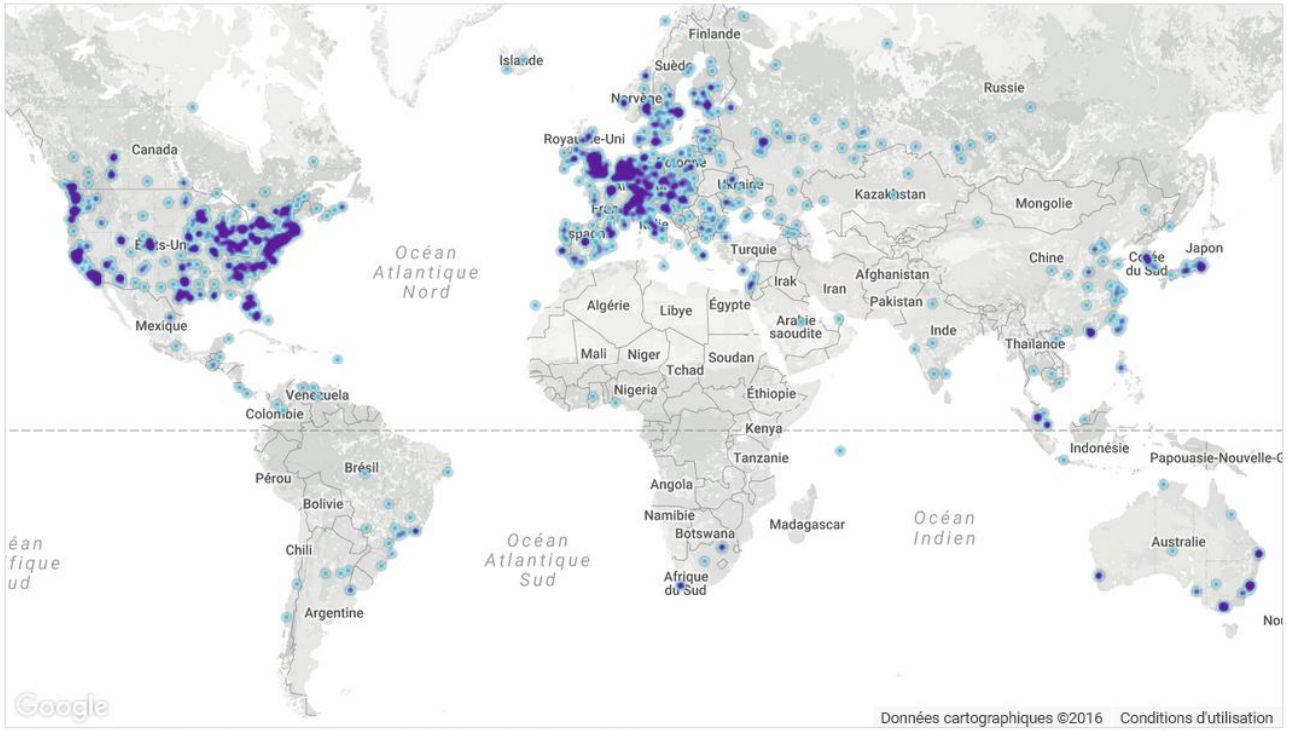
5181 NODES

24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	United States	1490 (28.76%)
2	Germany	862 (16.64%)
3	France	440 (8.49%)
4	Netherlands	299 (5.77%)
5	United Kingdom	223 (4.30%)
6	Canada	222 (4.28%)
7	China	170 (3.28%)
8	n/a	150 (2.90%)
9	Russian Federation	139 (2.68%)
10	Switzerland	91 (1.76%)

More (82) »



Map shows concentration of reachable Bitcoin nodes found in countries around the world.

LIVE MAP

Un nœud Bitcoin, c'est un client Bitcoin accessible depuis l'extérieur (port 8333 ouvert). La force du réseau réside le nombre de nœuds, qui en supporte tout le trafic.
Au 9 février 2016, le nombre de nœuds était de 5.787 (https://bitnodes.21.co/)
Tous les nœuds ne sont pas des mineurs…

Bitcoin | acteurs

Crypto-monnaies, altcoins

Plus de mille crypto-monnaies répliquant le modèle de la bitcoin-blockchain sont désormais disponibles, chacune d'elles se spécialisant dans un service ou une fonction spécifique.

On peut citer :

- le Litecoin (deuxième crypto-devise en terme de capitalisation plus de 200 millions de dollar de market cap),
- le Namecoin (qui offre la possibilité de créer un réseau de noms de domaine décentralisé basé sur la technologie des blockchains),
- des cryptos-devises communautaires comme (Potcoin et Mazacoin),
- des projets très prometteurs comme BitShares, Darkcoin, Blackcoin et Viacoin etc…

Les « alternative cryptocurrencies » sont nommées des Altcoins.

Colored coins

Les Colored Coins : « colorier » certains des bitcoins en circulation et leur assigner des propriétés spécifiques, dont la valeur peut être différente du sous-jacent bitcoin.

Le système est donc séparé en deux niveaux :
- le système Bitcoin tel que nous le connaissons,
- un réseau dépendant du protocole Bitcoin mais autonome.

Cette dissociation permet d'émettre des instruments d'échange distinct du réseau Bitcoin. Il s'agit d'un « protocole dans le protocole », pouvant être utilisé comme une monnaie alternative, des produits dérivés, des actions ou obligations, voire de la propriété intelligente, tout en utilisant l'infrastructure et le réseau Bitcoin.

Par exemple, on pourrait très bien imaginer la création d'un fonds de sécurité sociale indépendant et décentralisé à partir de ces colored coins, et géré par la communauté qui y souscrit.

ethereum

4. Ethereum

Ethereum | Introduction

La technologie derrière Ethereum est grosso modo la même que celle utilisée par le bitcoin : il s'agit d'ordinateurs individuels qui « participent » à une unique base de données globale publique, et donc partagée entre tous.

Un livre de comptes, ou un tableau Excel géant dans lequel on entre les données que l'on souhaite et auquel tout le monde a accès.

Ethereum est une décentralisation d'applications. Ces applications fonctionnent sur le réseau Ethereum, qui est constitué de plusieurs milliers d'ordinateurs qui communiquent en permanence. Ils partagent une même base de données, la blockchain. Cette base de données peut être comparée à un tableau Excel, qui serait rempli ligne par ligne par les participants au réseau.

Ethereum | smarts contracts

La Blockchain ne se limite pas à des transactions monétaires ou statiques sous forme de monnaie numérique : les contrats passés entre deux agents peuvent inclure des variables, comme la performance ou la valeur d’un actif par exemple.

Ainsi on peut anticiper l’émergence de contrats d’un nouveau type, des contrats dits intelligents ou smart contracts ou programme informatique ou encore algorithme qui éxécute automatiquement un contrat entre deux parties.

Aujourd'hui, on voit déjà apparaître ces nouveaux concepts dans des domaines aussi variés que la finance, la protection de la propriété immatérielle, ou encore les paris sportifs.

L’utilisation de la Blockchain permet d’injecter une crypto-monnaie dans les termes du contrat et démultiplie les possibilités de contrats privés indépendants du contrôle d'un tiers.

Ethereum | les DApps

Mais une blockchain peut également exécuter des programmes. Sur Ethereum le réseau permet l'utilisation de «smart contracts» , qui sont en réalité des lignes de code informatique (programmation solidity) programmables, qui correspondraient à des macros dans l'analogie avec un tableau Excel.

Ethereum a été déployé par la Fondation en août 2015 et le protocole est encore en développement. La version 1.0 a été déployée le 14 mars 2016, mais les outils permettant au « grand public » de l'utiliser n'ont pas encore été développés.

Source pour cette introduction : ETHEREUM France
https://www.ethereum-france.com

Ces applications qui reposent sur des contrats intelligents sont appelées des Applications Décentralisées, ou DApps.

Ethereum | DAO

Un contrat intelligent est capable d'opérer sans être adossé à une institution de référence. Et que se passe-t-il quand plusieurs contrats intelligents s'articulent les uns aux autres autour de règles communes ?

Certains programmes peuvent ainsi définir leur propres règles de gouvernance, ils deviennent en quelque sorte une organisation à part entière, entièrement contrôlés par les programmes dans la Blockchain, on parle alors de Decentralised Autonomous Organisation ou DAO.

Exemple : La startup BoardRoom.to fournit des DAO à destination des conseils d'administration.
Le passage par une DAO rend les règles de fonctionnement (respect du quorum, validation, procuration, etc) inaltérables, libres de toutes interventions humaines et transparentes (chaque membre peut consulter le code informatique). En outre, à titre d'exemple, les cotisations annuelles sont transférées automatiquement à partir du compte Bitcoin des membres.

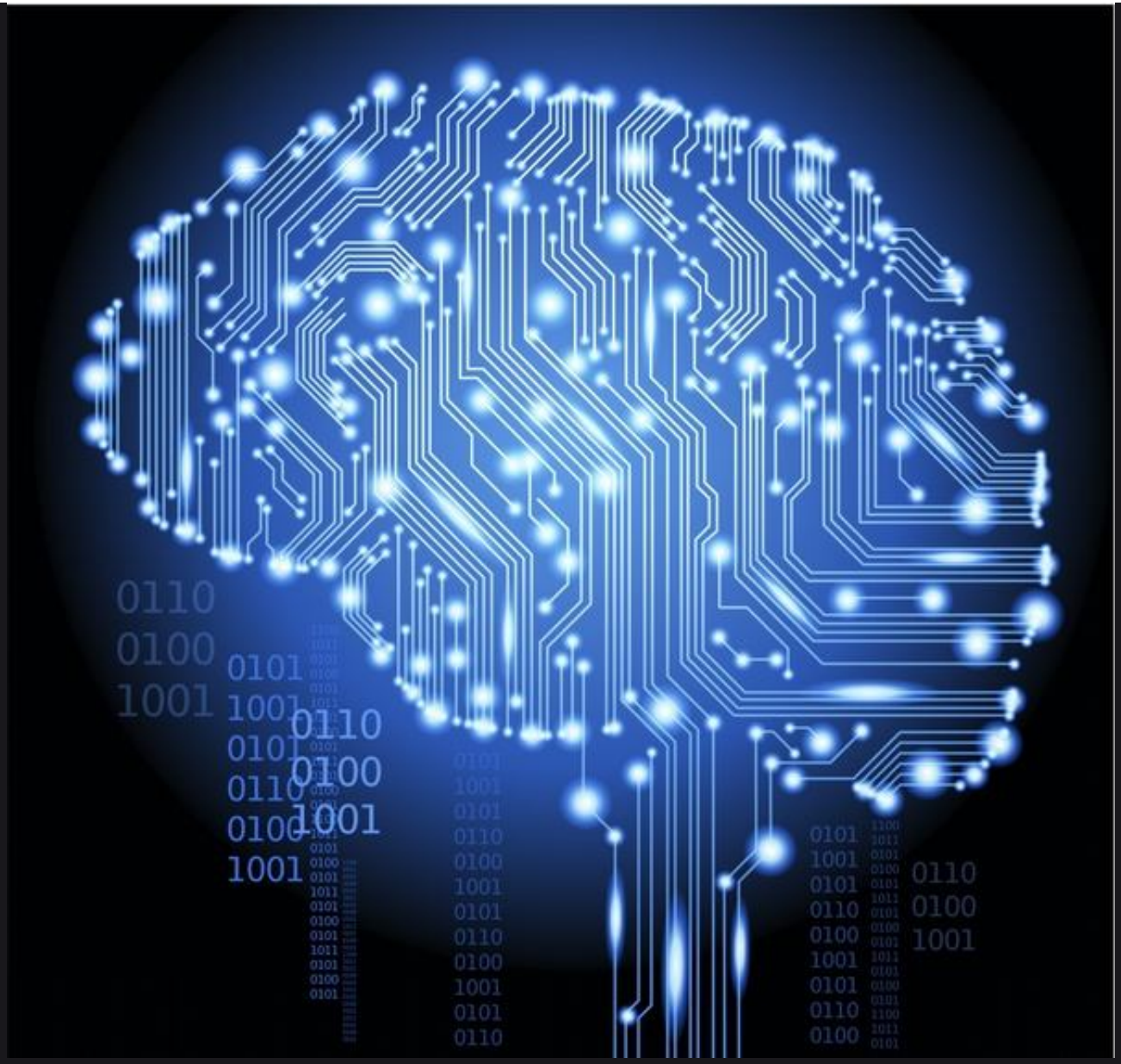
Ethereum | DAO (suite)

À l’instar des smart-contracts, ces programmes sont auto-exécutoires (self-enforced en anglais), ce qui les rend autonomes vis-à-vis d’une intervention humaine.

Certaines organisations décentralisées autonomes génèrent des tokens (voir lexique) pour rémunérer les utilisateurs en fonction d’une activité donnée.

Ici, la création monétaire ne provient plus (uniquement) du minage mais, par exemple, de la production d’énergie comme SolarCoin ou des kilomètres parcourus comme la solution de covoiturage La’Zooz.

Cette rémunération permet alors à l’organisation d’assumer seule ses besoins d’infrastructure.



5. Blockchain + IA + IoT

Blockchain | les agents intelligents

Le fait que la technologie blockchain puisse servir d'infrastructure a de nouvelles applications amène à parler de DApps, pour « Distributed Applications » .

Des premières initiatives existent, tels que :
- OpenBazaar dont l'équivalent centralisé est Craiglist ;
- lazooz dont l'équivalent centralisé est Uber ;
- Twister dont les équivalent centralisés sont Twitter ou Facebook ;
- Storj dont l'équivalent centralisé est Dropbox ;
- Etc…

Ainsi il serait possible d'avoir des agents intelligents (au sens de l'intelligence artificielle) qui pourrait exécuter des tâches pré-spécifiées selon certains conditions ou évènements ajoutés à la blockchain (source Christian Faure).

Blockchain | intelligence artificielle

IBM tente actuellement de fusionner intelligence artificielle et blockchain.
C'est-à-dire Watson + Hyperledger.

La blockchain est une technologie permettant l'échange de valeur sans friction.
L'intelligence artificielle a la capacité d'analyser d'énorme volume de données.

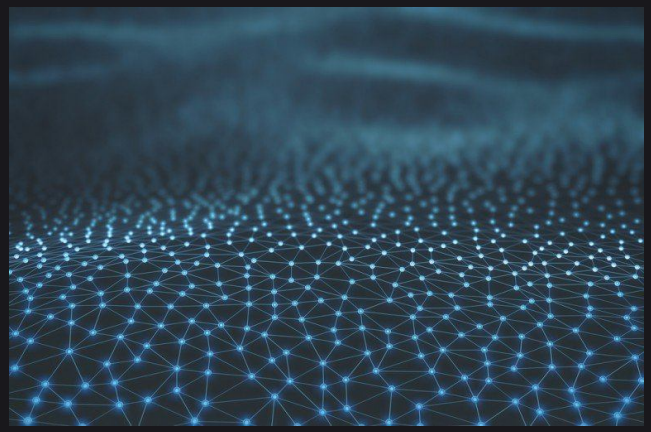
Le mariage des 2 pourrait marquer le début d'un nouveau paradigme.

Ainsi récemment à Singapour, Randy Walker, chairman & CEO d'IBM Asia Pacific, a déclaré "*Watson and blockchain are two technologies that will rapidly change the way we live and work, and our clients in Asia Pacific are eager to lead the way in envisioning and creating that future*."

D'autres acteurs lui emboitent le pas (Microsoft, SAP, etc…).

Blockchain | les objets connectés

Alors que les transactions commerciales ou financières sont bien souvent réalisées par les hommes ou les machines, l'Internet des objets donne aux objets la possibilité de participer directement aux transactions.



OCTO nous dit : « Les cas d'usage sont en cours de découverte, mais citons par exemple, la serrure qui s'ouvre si le droit de passage est bien acquitté, le colis qui valide la transaction de transport quand il arrive sur le site de destination, … le radiateur électrique qui souscrit à un contrat tarifaire avec délestage…

Ainsi l'objet connecté entrant dans la transaction étend l'impact concret de cette dernière car il a une emprise physique sur le monde.

Blockchain | les objets connectés (suite)

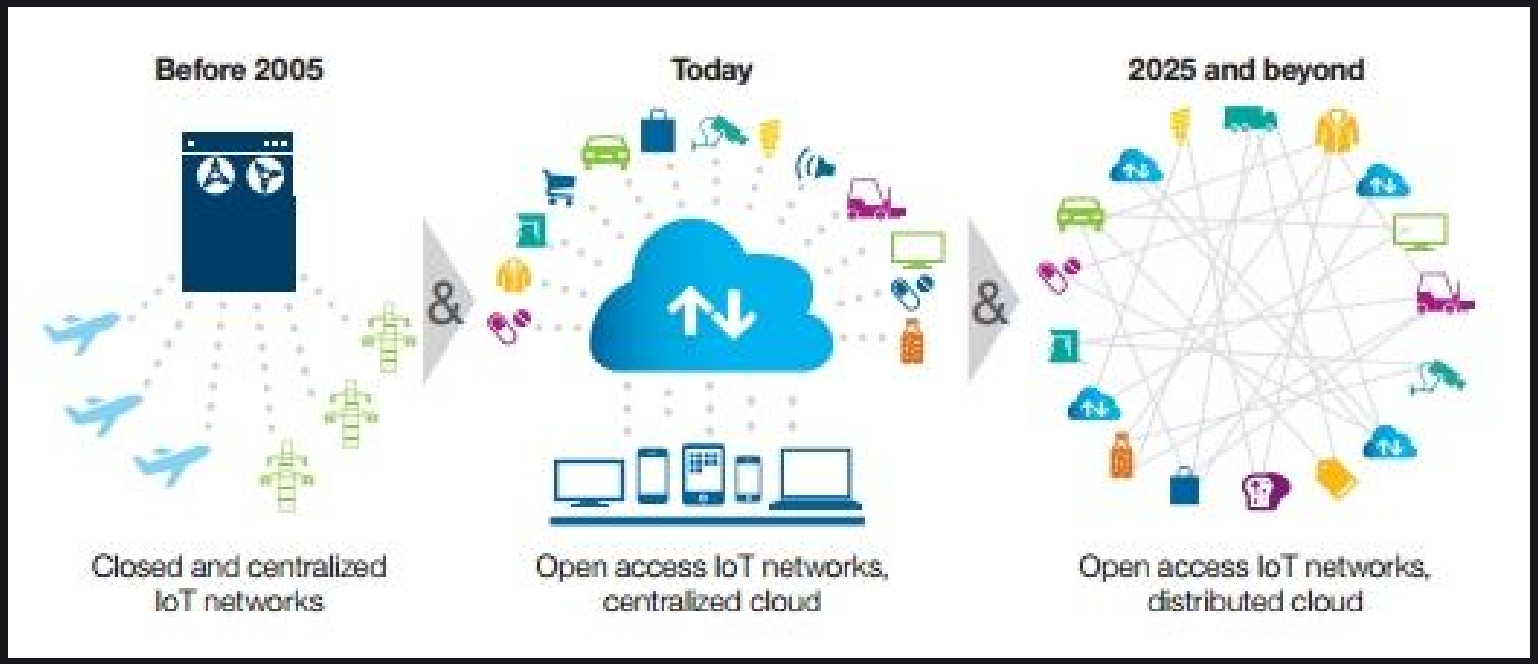
Et la blockchain dans tout cela ?

Dans l'Internet des objets (IoT) les objets connectés à Internet pouvent communiquer et faire des transactions avec tous les autres objets dans le monde. L'aspect décentralisé et mondial de la blockchain cadre parfaitement avec cette vision universelle de l'IoT (source OCTO).

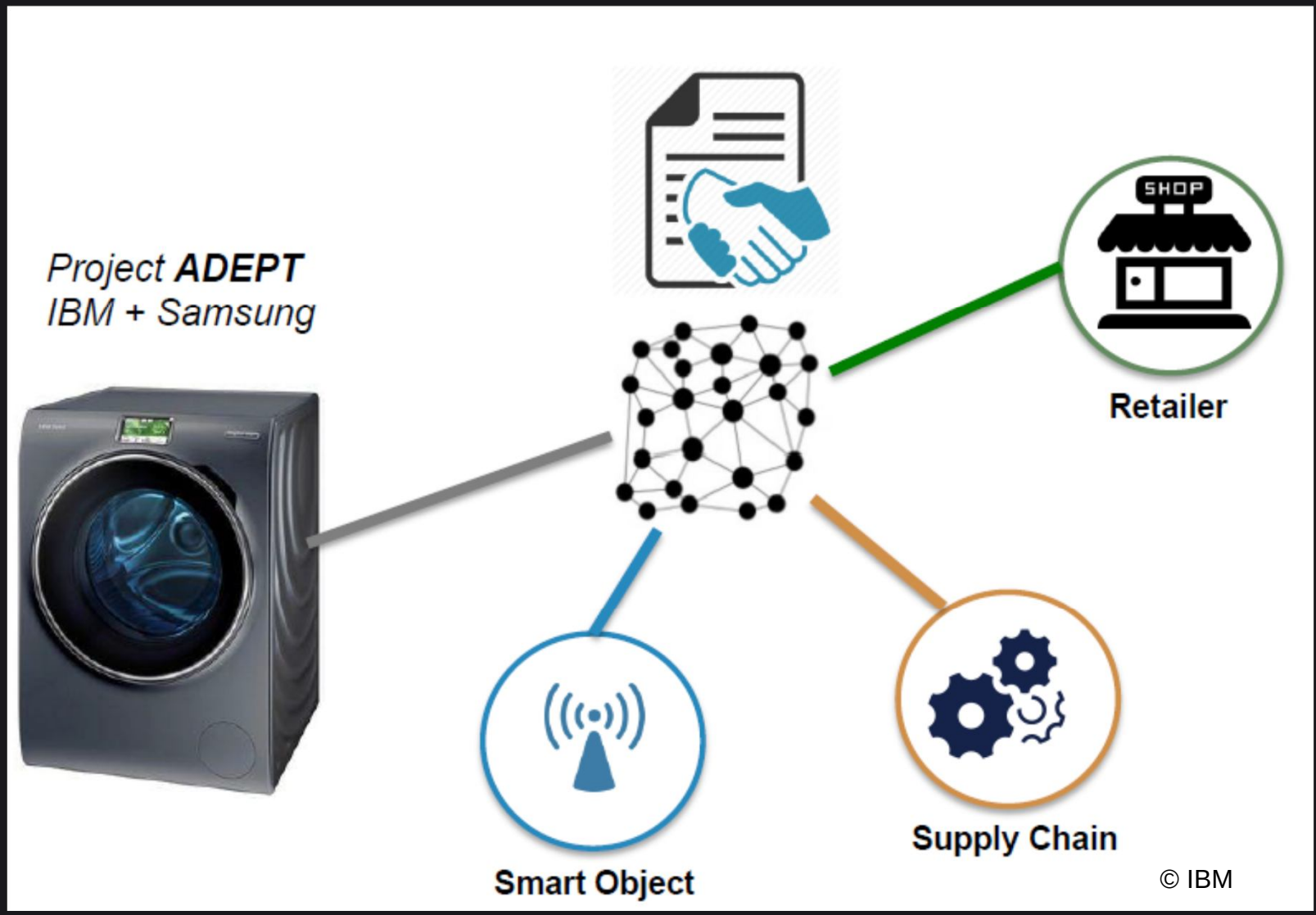
Les objets déroulent des processus automatisés entre eux et prennent part aux transactions s'appuyant sur la blockchain.
Cela induit 4 grandes conséquences :
- Les objets manipulent de l'argent;
- Les objets entrent dans des mécanismes de preuve;
- Les objets doivent consommer les protocoles de la blockchain;
- Les objets peuvent créer eux-mêmes leurs contrats de transactions.

Blockchain | IoT

IoT : la blockchain comme outil essentiel au développement de l'Internet des Objets



Blockchain | IoT (exemple)



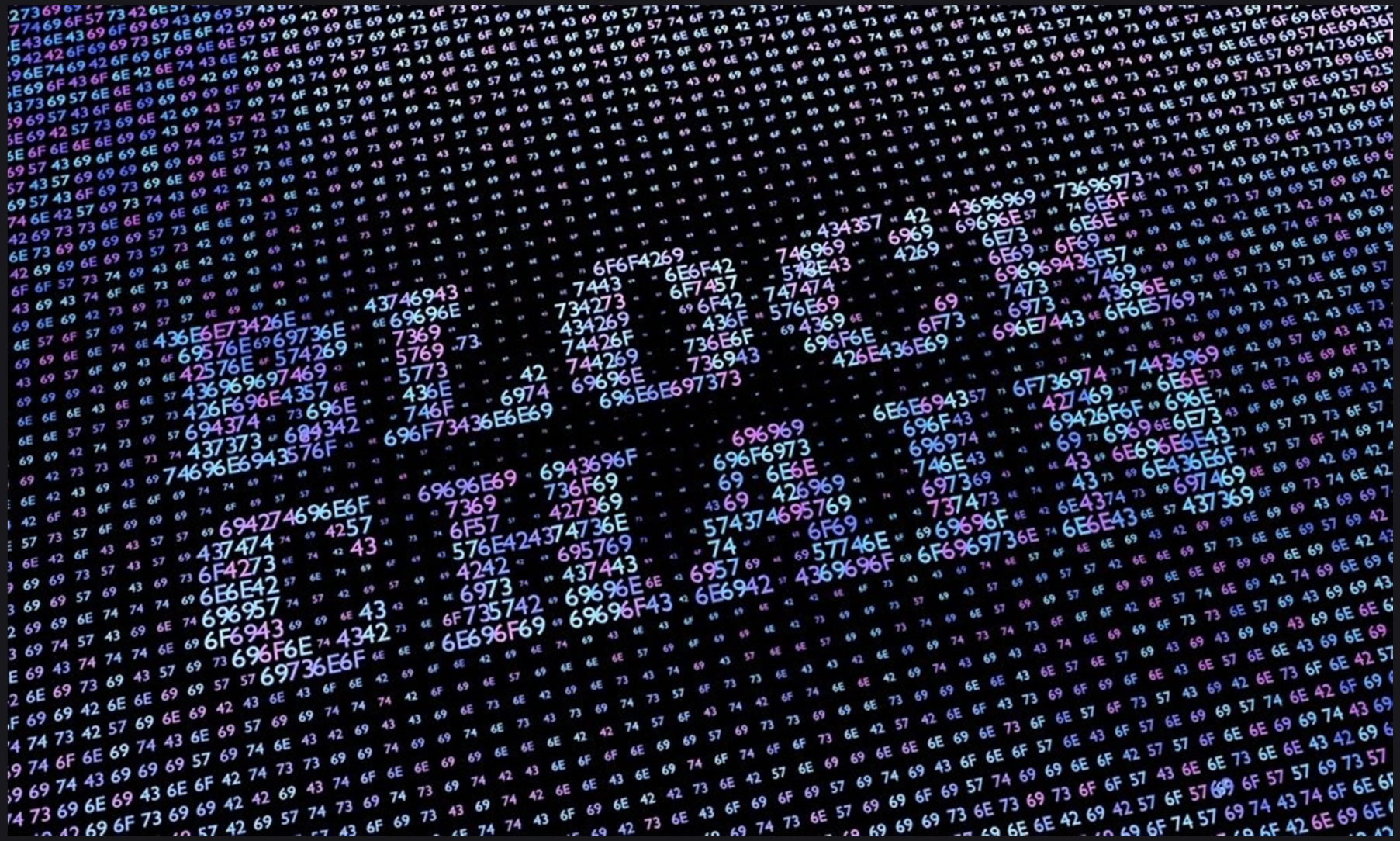
Blockchain | et demain ?

Les solutions les plus récentes offrent des algorithmes capables de gérer les consensus mais également les contrats entre les parties et ce, sans aucune autorité centrale.

Mais ce n’est qu’un premier pas…

Pour France Blocktech :

Blockchain + Objets connectés + Intelligence Artificielle = la révolution de demain



6. Blockchain Écosystème

Blockchain Solutions | courbe d'adoption 1

Accenture (février 2016)
La technologie blockchain sera massivement adoptée par les marchés de capitaux en 2025.

Influence de la Blockchain sur les banques ?

2015: apprentissage et expérimentation

2016 : développements et élaboration de normes (R3, Open Blockchain, etc.)

2017 et au-delà : Les grands projets. La Blockchain devient une composante des architectures informatiques des banques.

Blockchain Solutions | courbe d’adoption 2

Oliver Wyman & Euroclear (février 2016)

Il faudra environ dix ans pour que la technologie blockchain (distributed ledgers) pénètre le marché de la finance et disrupte la grande majorité des autres marchés.

Accenture & Oliver Wyman semblent s’accorder sur cette courbe d’adoption.

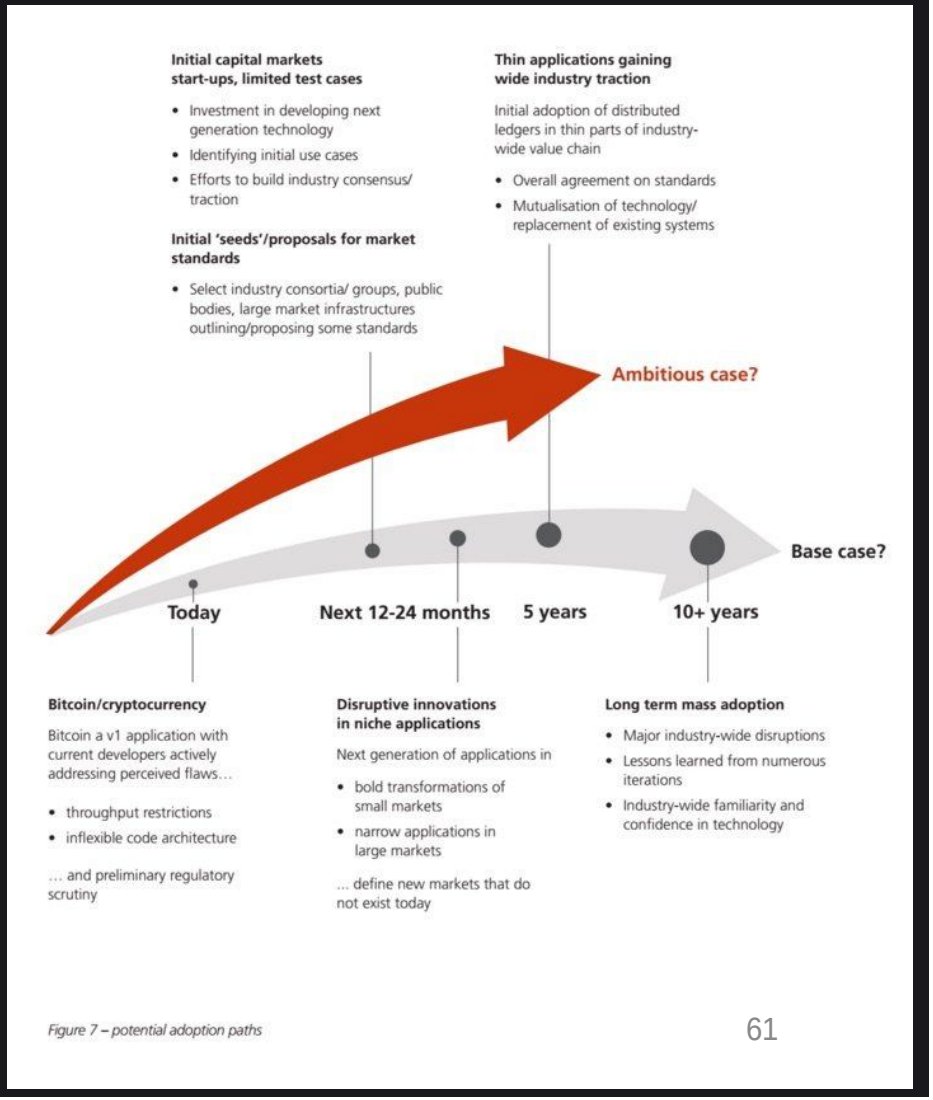
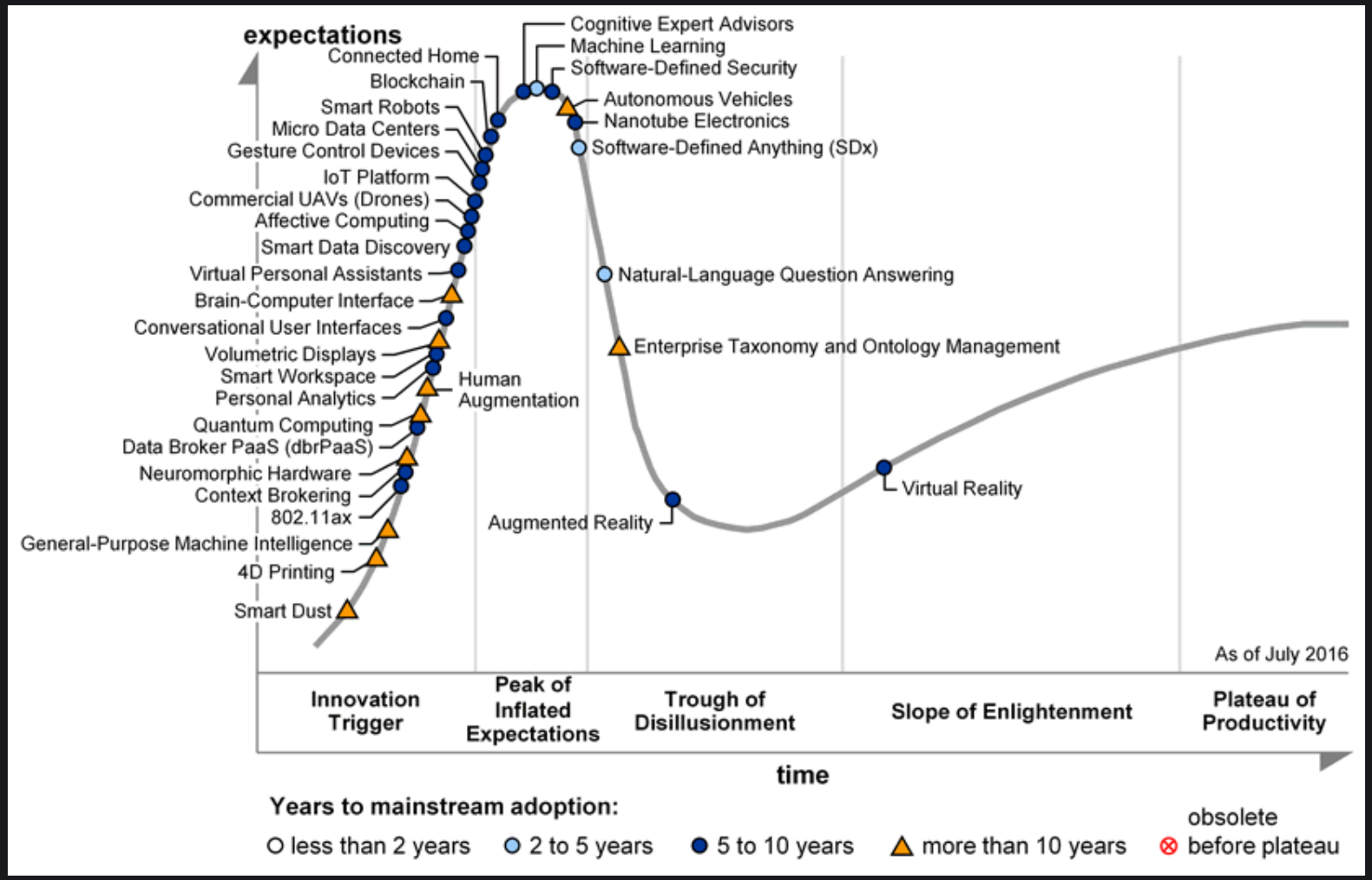
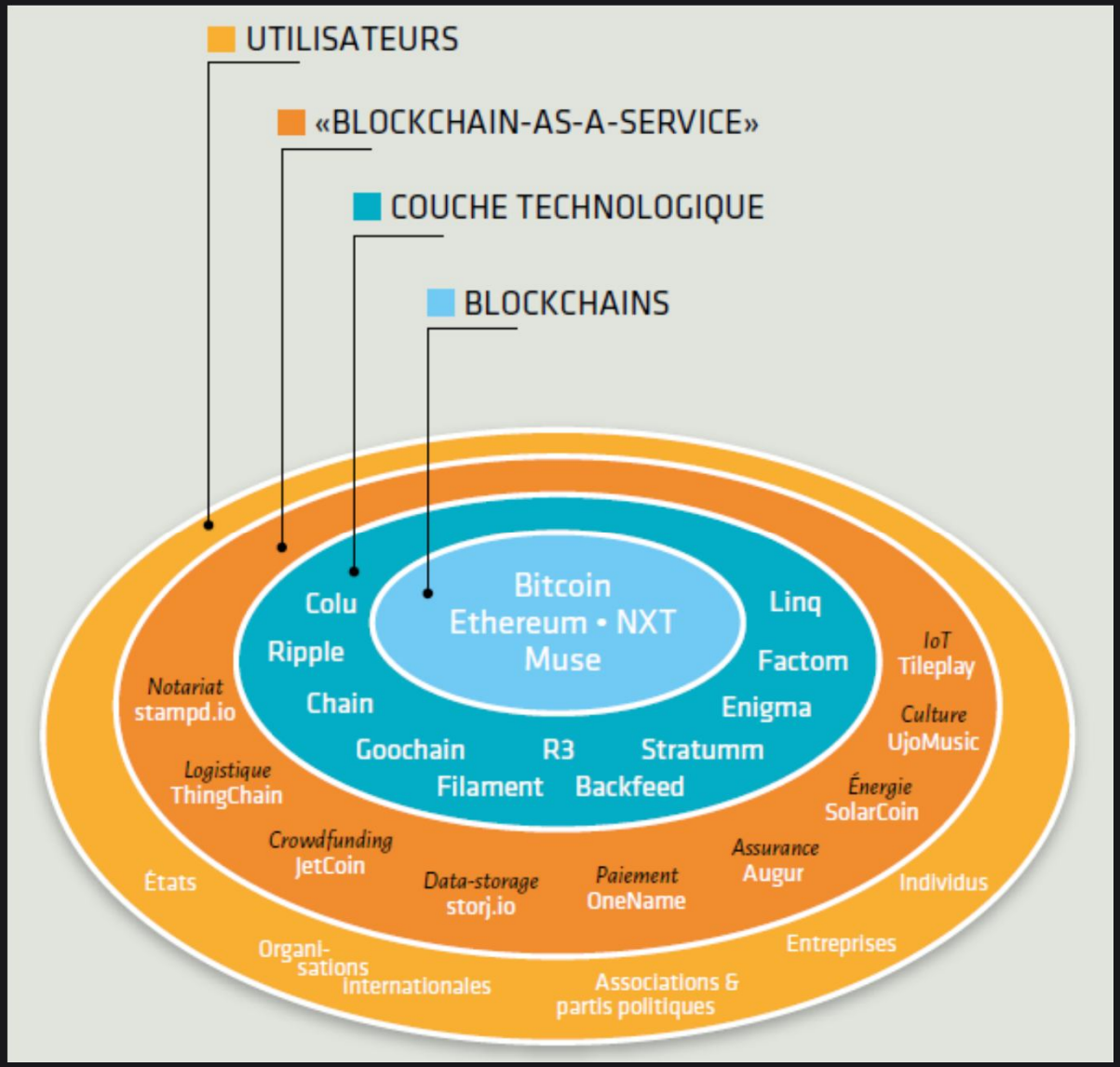


Figure 7 – potential adoption paths

Blockchain Solutions | courbe Gartner



Blockchain Solutions | écosystème



Blockchain solutions | écosystème (suite)

Les blockchains

Les différentes blockchains sont les « livres de comptes » qui enregistrent les utilisateurs et les transactions d'un service donné : par exemple, les détails des transactions de la monnaie Bitcoin sont enregistrés sur la blockchain Bitcoin [voir focus page 26].
Une blockchain peut posséder des spécificités techniques qui favorisent des types d'applications particulières ; c'est le cas de la Blockchain MUSE pour la rémunération des droits d'auteurs [voir fiche Culture page 39].

bitcoin ethereum NXT GENERATION OF CRYPTOCURRENCY MUSE

La couche technologique

Ces entreprises agissent comme l'interface technique entre une blockchain et les services qu'elles proposent. Elles traitent les informations contenues dans une blockchain pour les rendre actionnables par des services tiers.
Cependant, la croissance du modèle de blockchain privée [voir focus page 15] tend à brouiller la séparation entre une blockchain et cette couche technologique, à l'instar d'entreprises comme Ripple ou Linq.

colu. Your Assets, Made Digital. ripple Chain FILAMENT

Goochain R BACKFEED enigma factom

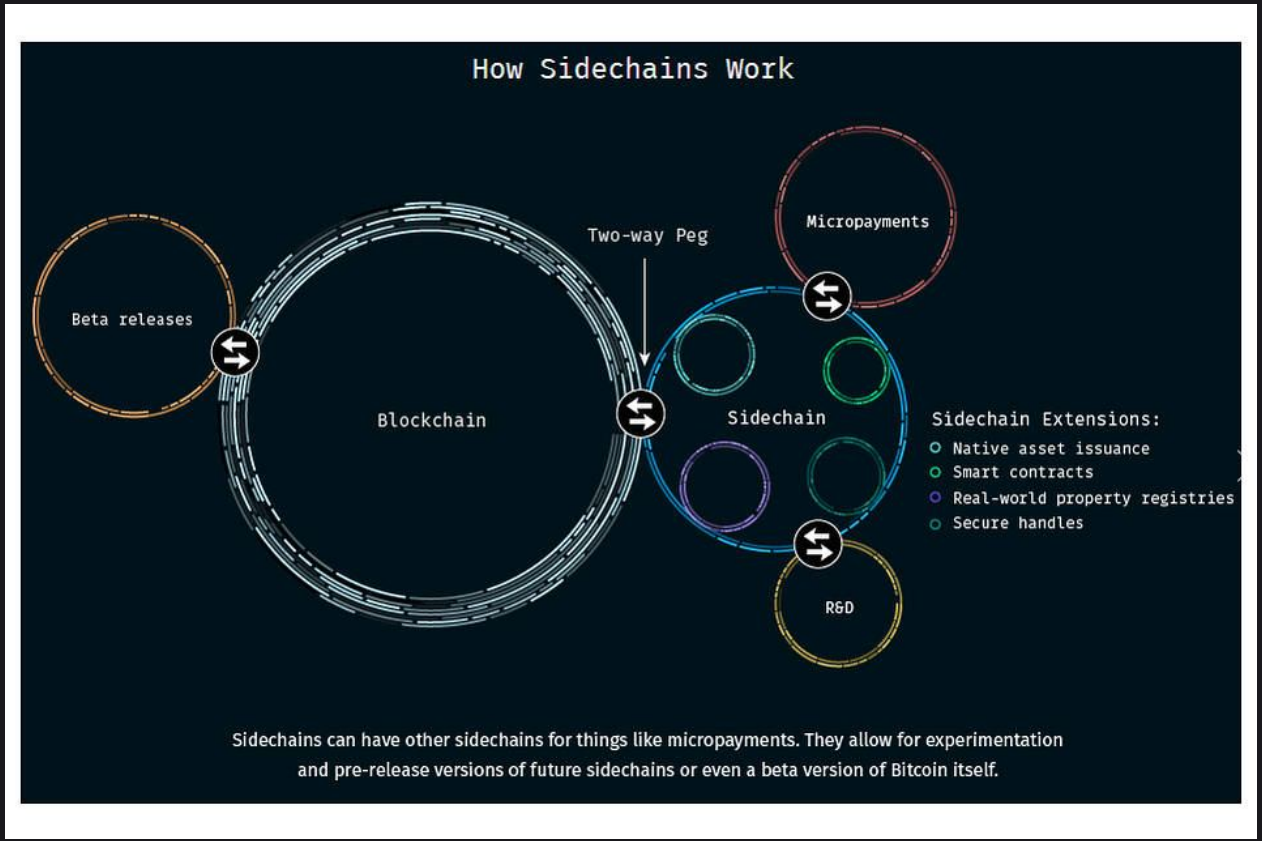
Blockchain Solutions | écosystème (suite)

■ **« Blockchain-as-a-Service »**
Il s'agit d'applications utilisées directement par l'utilisateur final : leur fonctionnement technique est transparent.

■ **Les utilisateurs**
Les structures étatiques, acteurs privés, associations et particuliers qui bénéficient de services Blockchain.

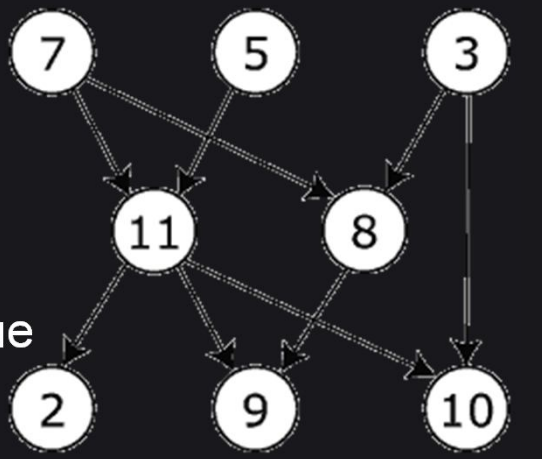
Images extraites du livre blanc « Blockchain » de Uchange.co

Blockchain Solutions | sidechains



- SIDECHAINS : blockchains qui se greffent sur la bitcoin-blockchain pour effectuer les tâches les plus disparates.
Pas de plateformes séparées, juste des une ou plusieurs blockchains multiples toutes connectées avec la bitcoin-blockchain et éventuellement entre elles.

Blockchain Solutions | IOTA



2015 : le projet IOTA.
Pas de blocs, pas de mineurs et pas… de blockchain.

Au lieu d'une suite linéaire de blocs, on est conduit à voir l'ensemble des transactions comme un graphe orienté acyclique que nous appelons tangle. IOTA est une tangle-based cryptocurrency.

Les transactions émises par les noeuds du peer-2-peer vont former le tangle, c'est-à-dire que les transactions forment le grand livre (ledger) sous forme de DAG. Lorsqu'une nouvelle transaction arrive, il doit approuver deux transactions précédentes. Ces approbations, représentées par des arêtes, contribuent à sécuriser le réseau.

Plus d'infos sur : http://blogchaincafe.com/iotatoken-une-tangle-crypto-currency#more-1057

Blockchain Solutions | LISK

Lisk est une plate-forme de nouvelle génération qui permet le développement et la distribution d'applications décentralisées écrites en Javascript.

Avec Lisk, les développeurs peuvent construire, publier, distribuer et monétiser leurs applications avec une cryptomonnaie interne.

Le système ainsi construit utilise une custom blockchain, des smart contrats, le stockage dans le cloud et des noeuds de calcul, le tout à l'intérieur d'une seule solution d'industrielle.

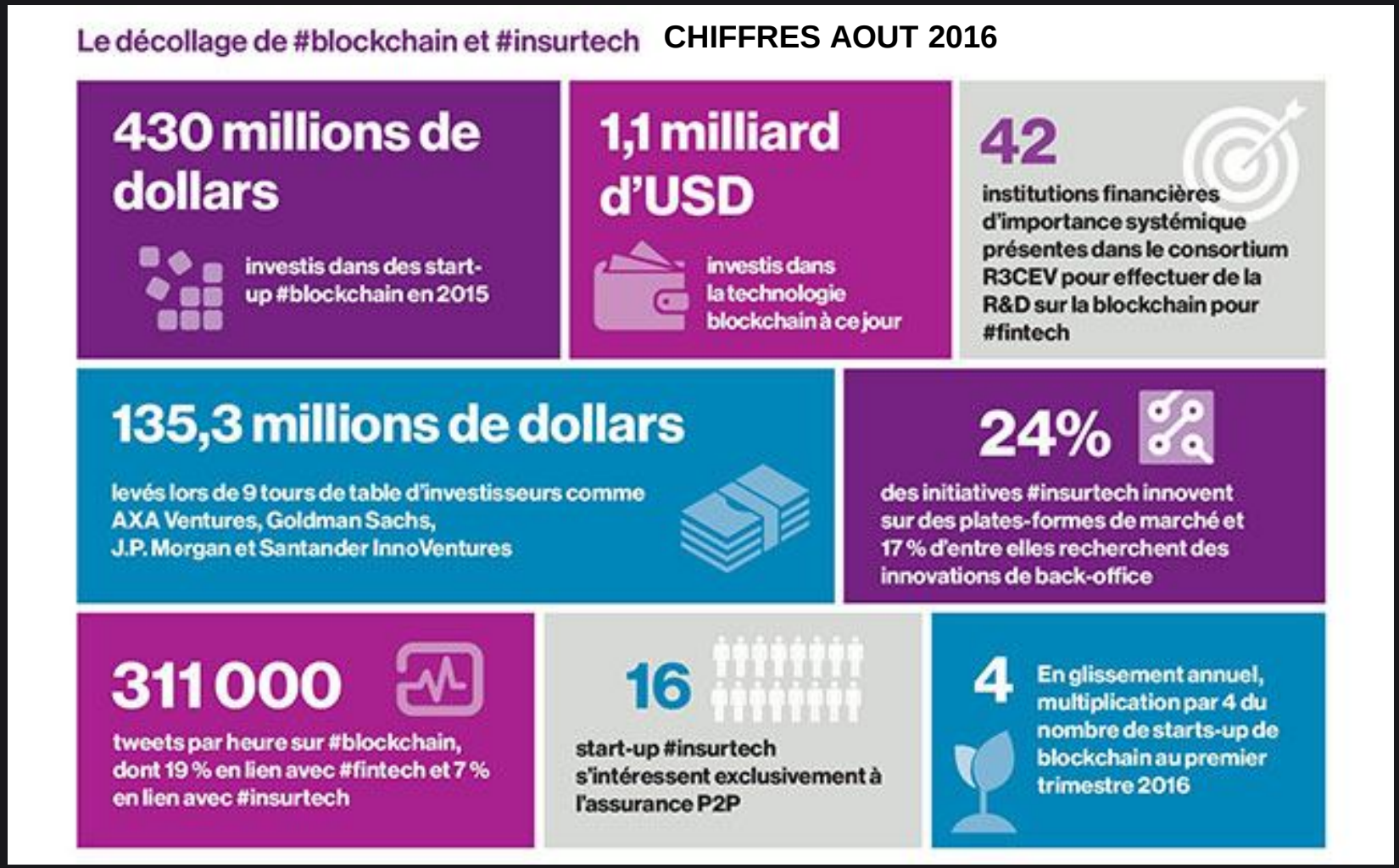
Lisk est la première solution décentralisée d'application écrite entièrement en Node.js. Il travaille donc de manière asynchrone et permet de traiter sans retard (apparent) les taches, comme les transactions réseau. La base de données utilise SQLite pour permettre l'utilisation et l'exécution de query complexes. Lisk se base sur HTML5 et CSS3 pour le frontend.

Plus d'infos : http://blogchaincafe.com/lisk-le-concurrent-dethereum

8. Blockchain Applications

Blockchain Applications | Finance

Blockchain Applications | assurances



Blockchain Applications | assurances

Six manières dont blockchain pourrait perturber le secteur de l'assurance

Blockchain Applications | assurances

EVERLEDGER : société qui utilise la blockchain pour combattre la fraude dans le domaine du luxe

Le premier marché auquel s'est attaqué Everledger est celui du diamant où la fraude coûte près de 50Md$ par an aux assureurs. Il n'existerait pas, en effet, de base de données centralisée fiable qui permette de tracer l'origine des diamants et la suite des transactions.
La start-up Everledger propose d'utiliser la blockchain pour bâtir un livre ouvert de transactions qui relève l'ensemble des données qui identifient correctement le diamant (les 4 C's – color, clarity, cut, carat – mais aussi les 40 meta-points qui le caractérisent spécifiquement).

IoT et ASSURANCE

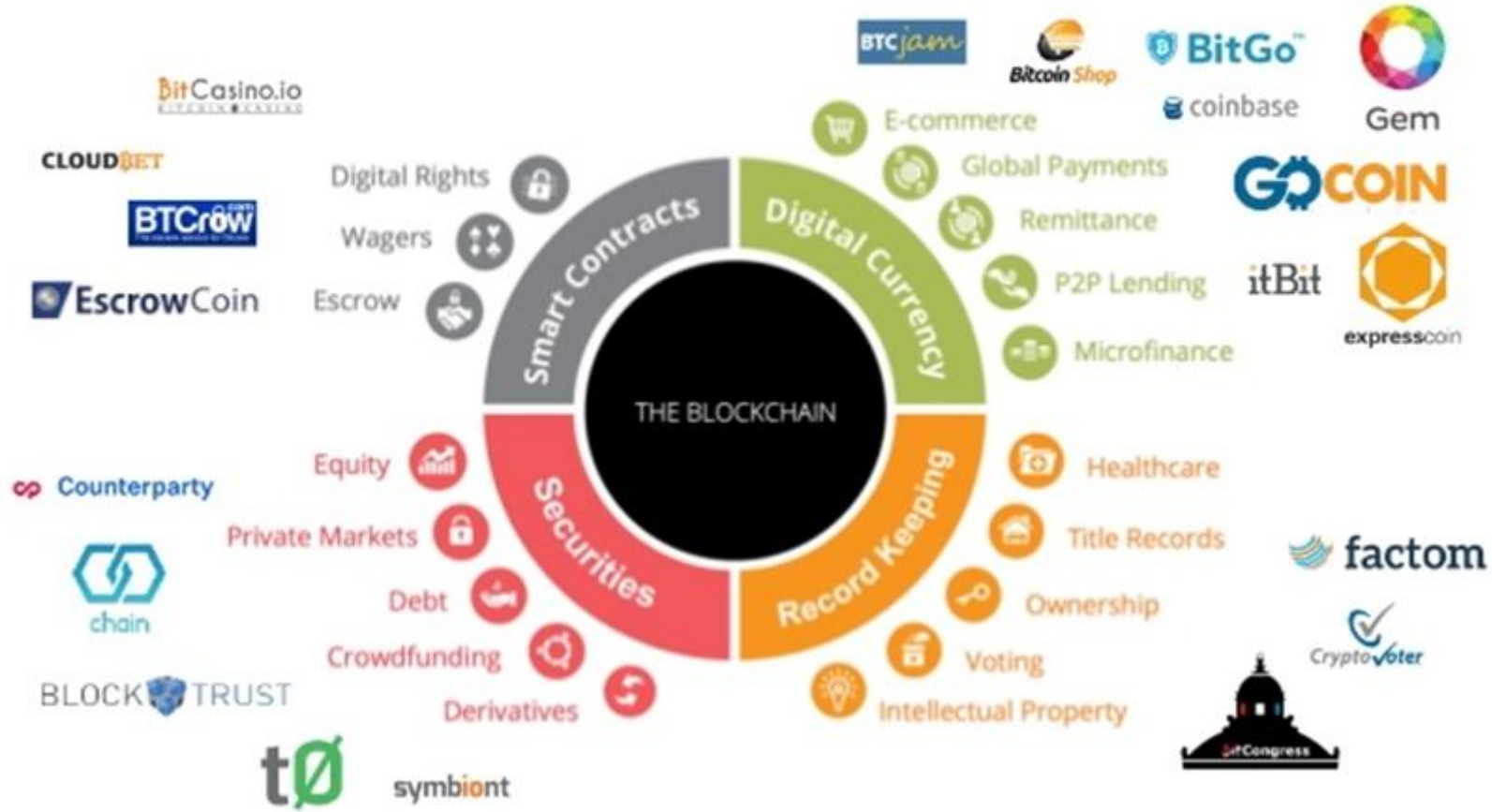
Coupler objets connectés et contrats d'assurance (habitation, automobile, etc…).
Les objets connectés produiront d'ici 2020 plus de 50% du total des données disponibles dans le monde.
Dans son livre blanc sur la transformation numérique de l'assurance, le Conseil National du Numérique affirmait que l'assurance pourrait même constituer le modèle économique de l'Internet des Objets (comme la publicité l'a été pour Internet).

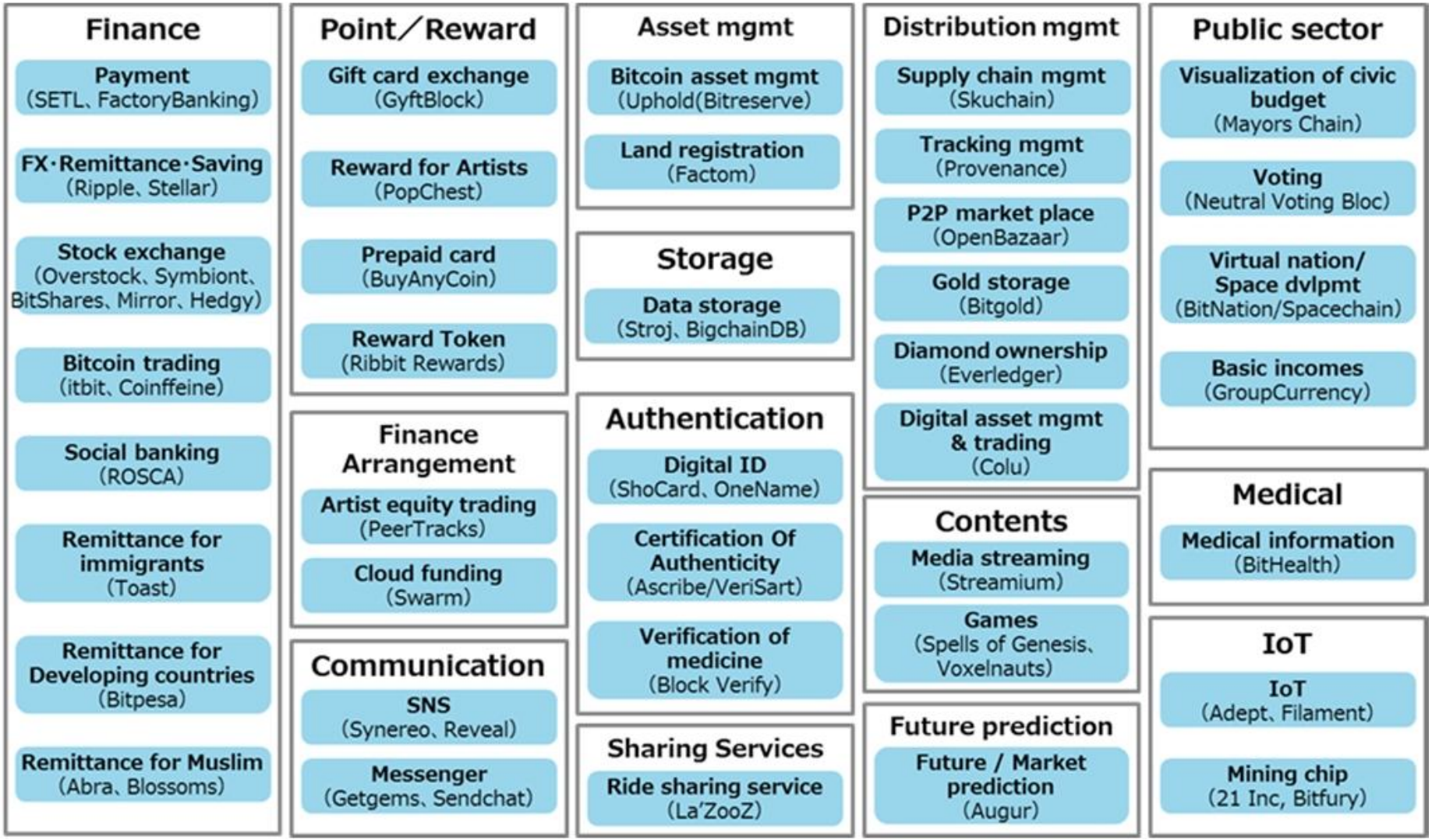
Nous pouvons également citer les startups : Friendsurance, Guevara, TongJuBao ou Lemonade.
Pour plus d'infos :
www.friendsurance.com : économie de partage
www.dynamisapp.com : assurance peer-to-peer

Blockchain Potential Applications & Disruption

The blockchain is radically changing the future of transaction based industries

BTCS powers the ecosystem and touches every blockchain transaction




Finance
Payment (SETL、FactoryBanking)
FX・Remittance・Saving (Ripple、Stellar)
Stock exchange (Overstock、Symbiont、BitShares、Mirror、Hedgy)
Bitcoin trading (itbit、Coinffeine)
Social banking (ROSCA)
Remittance for immigrants (Toast)
Remittance for Developing countries (Bitpesa)
Remittance for Muslim (Abra、Blossoms)
Point／Reward
Gift card exchange (GyftBlock)
Reward for Artists (PopChest)
Prepaid card (BuyAnyCoin)
Reward Token (Ribbit Rewards)
Finance Arrangement
Artist equity trading (PeerTracks)
Cloud funding (Swarm)
Communication
SNS (Synereo、Reveal)
Messenger (Getgems、Sendchat)
Asset mgmt
Bitcoin asset mgmt (Uphold(Bitreserve)
Land registration (Factom)
Storage
Data storage (Stroj、BigchainDB)
Authentication
Digital ID (ShoCard、OneName)
Certification Of Authenticity (Ascribe/VeriSart)
Verification of medicine (Block Verify)
Sharing Services
Ride sharing service (La'ZooZ)
Distribution mgmt
Supply chain mgmt (Skuchain)
Tracking mgmt (Provenance)
P2P market place (OpenBazaar)
Gold storage (Bitgold)
Diamond ownership (Everledger)
Digital asset mgmt & trading (Colu)
Contents
Media streaming (Streamium)
Games (Spells of Genesis、Voxelnauts)
Future prediction
Future / Market prediction (Augur)
Public sector
Visualization of civic budget (Mayors Chain)
Voting (Neutral Voting Bloc)
Virtual nation/ Space dvlpmt (BitNation/Spacechain)
Basic incomes (GroupCurrency)
Medical
Medical information (BitHealth)
IoT
IoT (Adept、Filament)
Mining chip (21 Inc, Bitfury)

2016 The Blockchain Ecosystem

Market Insight • Proposition Development • Customer Engagement • Product Launch

FirstPartner

Introduction

The blockchain combines cryptography & distributed computing to deliver secure, direct peer to peer transactions without the need for a central party. At its heart is the Distributed Ledger. This is a tamper proof, public, network-hosted, record of all consensus verifiedtransactions.

Initially realised via Bitcoin & similar "cryptocurrencies", focus & investment is now shifting to the potential of blockchain technology to revolutionise the infrastructure & processes of established Financial Institutions & other enterprises.

This Map summarises the key principles behind the blockchain & the emerging ecosystem addressing payments, banking & other potential use cases.

Blockchain numbers

$921million Cumulative VC investment in Bitcoin & blockchain companies to Oct 2015. $462 million of this in 2015 alone.

$121million Largest cumulative funding total - raised by Bitcoin computer developer 21inc. [1]

805 Number of early stage Bitcoin & blockchain companies identified by Venture Scanner [2]

30+ Banks & Financial Institutions known to be testing, analysing or investing in the blockchain technologies [3]

11m Number of registered Bitcoin wallets in Sept 2015 - up from 6.6m in Sept 2014 [4]

106,000 Number of merchants who accept Bitcoin [4]

$4.9bn Bitcoin capitalisation Nov 2015. Bitcoin accounts for around 90% of the capital value of all cryptocurrencies [5]

$2.7bn value of Bitcoin trading in Sept 2015 [6]

475 Bitcoin ATMs installed worldwide [7]

Sources:
1 CoinDesk & Crunchbase
2 Venturescanner.com reviewed Nov 2015
3 FirstPartner research
4 CoinDesk State of Bitcoin Report Q3 2015
5 Blockchain.info checked 16th Nov 2015
6 Bitcoinity.org
7 Coin ATM Radar checked Oct 2015

Author | Richard Warren
rwarren@firstpartner.net

Like what you see?
Contact us for in-depth insight into your target markets!

Contacts | hello@firstpartner.net
+44 (0) 870 874 8700
@firstpartner
www.firstpartner.net

Payment Use Cases

Retailing | Person 2 Person | Remittances | Financial Inclusion | Interbank Clearing | Forex | Resilience | Trading & Markets

The Cryptocurrency Ecosystem

Specialist companies facilitating transaction validation, currency exchange, storage & payment on existing cryptocurrency newtworks (primarily Bitcoin)

Users | Merchants

Wallets: Blockchain, Xapo, Armory, bitreserve, case

Bitcoin Debit Cards: WageCan, ANXPRO

BitCoin ATM: Lamassu, genesiscoin, BitAccess

International Remittance: ABRA, BitPesa, RebitR

Merchant Payment Processing: PEY, DC POS

Bitcoin PoS: Bitnet, GoCoin, bitpay

Risk & Fraud Management: vogogo

PSPs Supporting Bitcoin: PayPal, adyen, Braintree, stripe

Exchanges: Bitfinex, kraken, LocalBitcoins.com, Bitstamp, HUOBI.com, BTC-e

Multiservice Companies (Mining | Exchange | Wallet | Processing): coinbase, Circle, BitX, BTCC, Gamium

Mining

Mining Technology & Commercial Operations: 21 INC, KnCMiner, BitFury, spondooliestech, HASHRABBIT, BTCS

Mining Pools: - Ghash.io - F2Pool - AntPool - Slush'spool

Established Financial Ecosystem

Regulated financial institutions & platform vendors exploring blockchain technology as an alternative to centralised & correspondent payment processing

Money Transfer Operators: Western Union

Market Makers: Nasdaq

Securities Markets: Nasdaq

Retail & Commercial Banks: Barclays, Deutsche Bank, Bank of America, BNP Paribas, BBVA, fidor Bank, HSBC, citi, ING, J.P.Morgan, UBS, RBS, Santander

Central Banks & Initiatives

Liquidity Provision | National Clearing | Complaince | Policy

The following major central banks have undertaken assesments or issued statements on regulation, potential risks to financial systems and/or benefits but none yet has a definitive policy stance.

- Bank of England
- Banque de France
- Deutsche Bundesbank
- European Central Bank
- The Federal Reserve
- Monetary Authority of Singapore
- People's Bank of China
- Reserve Bank of India

Card Schemes: VISA, MasterCard, American Express

Interbank Networks: SWIFT, earthport

Enabling the Financial Services Blockchain

Commercial platforms & services targeting Financial Institutions

Securities & Derivatives & Asset Trading Platforms

Smart contracts & blockchain for transparent trading & post trade settlement: Mirror, symbiont, clearmatics, HEDGY, SETL

The R3 Consortium

Technology led initiative of 30+ banks to design & apply distributed ledger technology to global financial markets

Institutional Investment: TradeBlock, itBit, SolidX

Financial Infrastructure & APIs

Enable implementation of private Blockchains/ sidechains &/or the development & securing of financial applications

BLOCKCYPHER, eris INDUSTRIES, Gem, ripple, Digital Asset Holdings, Chain, Blockstack.io

Bitcoin Based Cryptocurrencies

Bitcoin
Created as an alternative to central bank controlled fiat currencies. Bitcoin was the first working Cryptocurrency. It remains dominant but lack of scalability and other inherent flaws will likely prevent mass adoption.
Validation: Proof of Work
Latency: 10 minutes
Currency: BTC - on and off-network
Issuance: Mining Reward. 21M Limit

Litecoin
Consensus: Proof of Work
Latency: 2.5 minutes
Currency: LTC - on and off-network
Issuance: Mining Reward. 84M Limit

Dogecoin
Consensus: Proof of Work
Latency: 1 minute
Currency: Doge - on & off-network
Issuance: Mining Reward. Unlimited

Open Protocols for Institutions

Ripple
Consensus based protocol designed specifically for existing financial institutions. Supplementing existing processes & directly suporting fiat currencies, lead use cases are international paymemts & inter Financial institution settlement
Validation: Distributed consensus
Latency: 3 seconds
Currency: XRP on-network only
Issuance: At inception -100 BN units created.

Ethereum
Smart contract & distributed app focus
Validation: Proof of Work
Latency: 12 seconds
Currency: ETH on-network only
Issuance: Mining Reward.

Stellar
Ripple derivative. Financial focus
Validation: Distributed consensus
Latency: 2-5 seconds
Currency: Lumens on-network only
Issuance: 100 BN then 1% issued PA

Blockchain

Distributed P2P Networks

The Distributed Ledger

Anatomy of a Transaction

1 Initiation — Transaction Instruction -prior transaction(s) -recipient address -value & conditions -digital signature — sender

2 Verification — the network — nodes or miners: -propogate -group into "candidate blocks" -validate signatures -verify through "consensus"

3 Completion — Verified Block — "Value" — recipient — Blockchain

Protocol Components

The Currency
The medium for transaction settlement within the newtork & rewarding miners. Cryptographically generated, protocol rules detremine issuance & destruction. May be tradeable "off the newtork" (e.g. Bitcoin) or only exist on network (e.g. XRP)

The Ledger
AKA the Blockchain. A Public record of all transactions - stored across a distributed P2P network of servers. Verified transactions are added in "blocks" and the history provides proof of value or assets "owned".

Consensus
Prevents "double spend" or validation of fraudulent transactions:
Proof of work: miners compete to validate blocks by solving highly processor/RAM intensive cryptographic problems for reward
Distributed consensus: majority validation by trusted subnetworks of peer nodes within the network. Used by Ripple & Stellar
Proof of stake: achieves distributed consensus by network users proving their ownership of currency. Used by Peercoin & Bitshares

Crypto 2.0 - Building on the Bockchain

Smart Contracts

Encode & validate "conditions" for a transaction between parties. Potentially facilate legally binding transactions over the blockchain

consensys, CLEARINGHOUSE, Counterparty, CODIUS

Colored Coins & Open Assets

Bitcoins altered to represent an asset. Exchanged via the Open Assets Protocol. Allows trading of physical & other assets

colu, ChromaWay, Omni, coinprism

Core Blockchain Protocols

bitcoin, stellar, ripple, DASH, ethereum, Peercoin, VIACOIN

Enabling Layers
Protocols, platforms & SDKs that build on top of core blockchain protocols to enable additional transaction types & services

Ripple: facilitating multiple Financial Institutions focussing on payment solutions

Protocol Commercialisation
Consensys: building an Ethereum based ecosystem & partnered with Microsoft for Ethereum Blockchain as a Service

FILAMENT, IBM, SAMSUNG, factom, MaidSafe, STORJ.IO, ShoCard, stampery, Bitproof.io

lighthouse, OpenBazaar, La'Zooz, BLOCKPARTY, ALEXANDRIA, BISANTYUM

IoT — Registering and validating connected devices

Data — Distributed storage of and access to business data

e-Identity — Registering and validating individual identity

Legal — Executing smart legal contracts

Crowd Funding — Raising finance & distributing equity

Market Places — Trading & sharing of physical & digital assets & services

Publishing — Digital asset rights management, distribution & payment

Proof of Ownership — Tamper proof registration & "stamping" of physical & digital assets

Other Use Cases

Data & Analytics: COINALYTICS, BLOCKCORP, blockr, KAIKO, bitcoin charts

Key Security/HSMs: gemalto, THALES

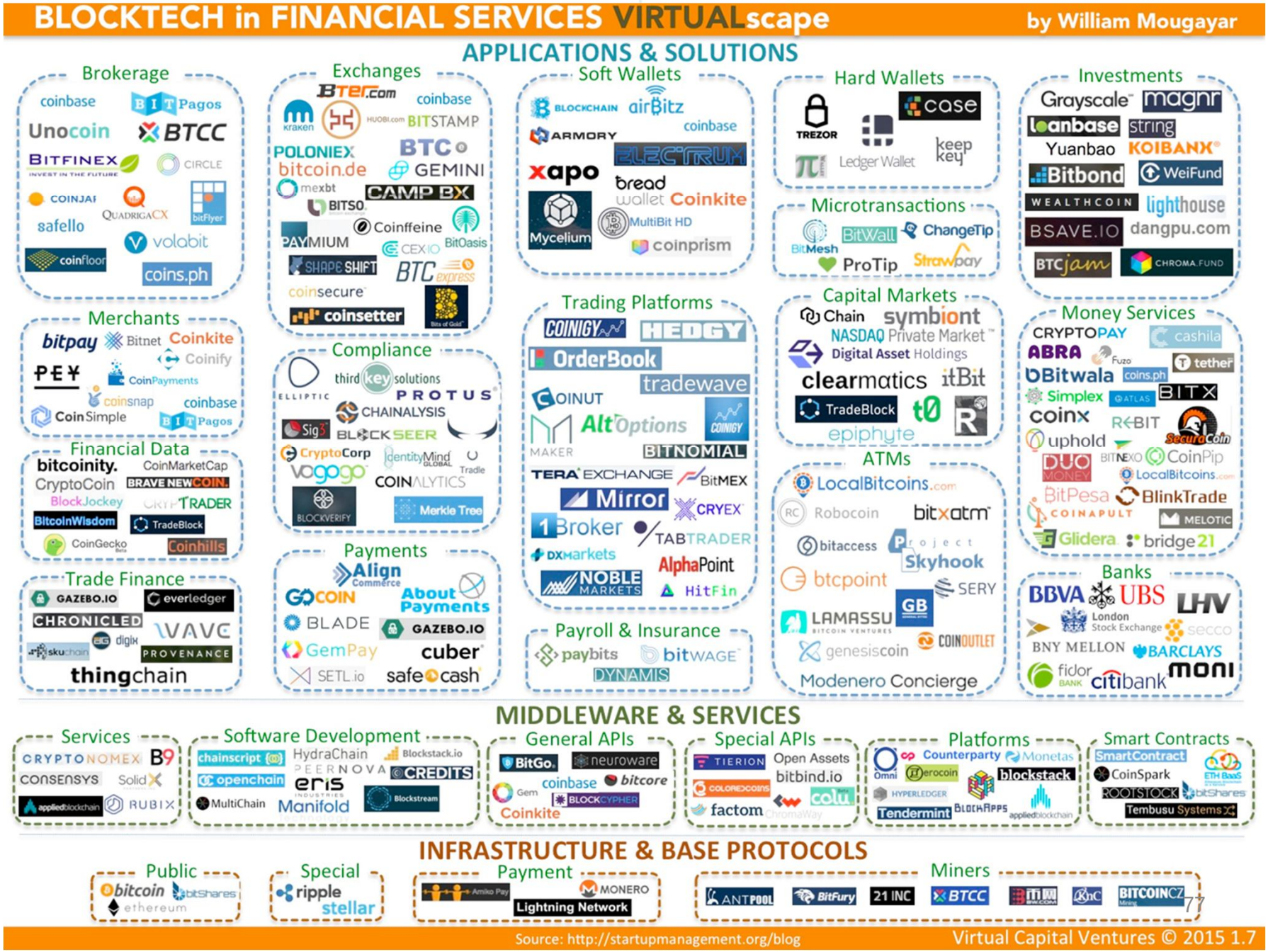
Balancingthe Benefits

Blockchain Benefits
- Ecosystem simplification
- Faster interbank clearing & settlement
- Lower transaction costs
- Reduced counterparty risk
- Transaparency & auditability
- Ease of software development/integration

Vs.

Risks
- Unproven technology
- Untested capacity/scalabilitty
- Low transaction speed
- Possible concensus protocol flaws
- Cryptocurrency price volatility
- Uncertain regulatory status

Investors: ANDREESSEN HOROWITZ, BLOCKCHAIN CAPITAL, overstock, Google ventures, LIGHTSPEED VENTURE PARTNERS, AME CLOUD VENTURES, DIGITAL CURRENCY GROUP, PANTERA


BLOCKTECH in FINANCIAL SERVICES VIRTUALscape
by William Mougayar
APPLICATIONS & SOLUTIONS
Brokerage
coinbase
BitPagos
Unocoin
BTCC
BITFINEX
CIRCLE
COINJAR
QUADRIGACX
bitFlyer
safello
volabit
coinfloor
coins.ph
Exchanges
BTer.com
coinbase
kraken
HUOBI.com
BITSTAMP
POLONIEX
BTC
bitcoin.de
GEMINI
mexbt
CAMP BX
BITSO
Coinffeine
PAYMIUM
CEX.IO
BitOasis
SHAPE SHIFT
BTC express
coinsecure
coinsetter
Bits of Gold
Soft Wallets
BLOCKCHAIN
airBitz
ARMORY
coinbase
ELECTRUM
xapo
bread
wallet
Coinkite
Mycelium
MultiBit HD
coinprism
Hard Wallets
TREZOR
case
Ledger Wallet
keep key
Investments
Grayscale
magnr
Loanbase
string
Yuanbao
KOIBANX
Bitbond
WeiFund
WEALTHCOIN
lighthouse
BSAVE.IO
dangpu.com
BTCjam
CHROMA FUND
Microtransactions
BitMesh
BitWall
ChangeTip
ProTip
Strawpay
Merchants
bitpay
Bitnet
Coinkite
Coinify
PEY
CoinPayments
coinsnap
coinbase
CoinSimple
BitPagos
Compliance
third key solutions
ELLIPTIC
PROTUS
CHAINALYSIS
Sig3
BLOCKSEER
CryptoCorp
IdentityMind GLOBAL
Tradle
vogogo
COINALYTICS
BLOCKVERIFY
Merkle Tree
Trading Platforms
COINIGY
HEDGY
OrderBook
tradewave
COINUT
AltOptions
COINIGY
MAKER
BITNOMIAL
TERA EXCHANGE
BitMEX
Mirror
CRYEX
1Broker
TABTRADER
DXmarkets
NOBLE MARKETS
AlphaPoint
HitFin
Capital Markets
Chain
symbiont
NASDAQ Private Market
Digital Asset Holdings
clearmatics
itBit
TradeBlock
t0
R
epiphyte
Money Services
CRYPTOPAY
cashila
ABRA
Fuzo
tether
BBitwala
coins.ph
Simplex
ATLAS
BITX
coinx
REBIT
SecuraCoin
uphold
BITNEXO
CoinPip
DUO MONEY
LocalBitcoins.com
BitPesa
BlinkTrade
COINAPULT
MELOTIC
Glidera
bridge21
Financial Data
bitcoinity.
CoinMarketCap
CryptoCoin
BRAVE NEW COIN
BlockJockey
CRYPTOTRADER
BitcoinWisdom
TradeBlock
CoinGecko
Coinhills
ATMs
LocalBitcoins.com
Robocoin
bitxatm
bitaccess
Project Skyhook
btcpoint
SERY
LAMASSU
GB
genesiscoin
COINOUTLET
Modenero Concierge
Payments
Align Commerce
GOCOIN
About Payments
BLADE
GAZEBO.IO
GemPay
cuber
SETL.io
safecash
Payroll & Insurance
paybits
bitWAGE
DYNAMIS
Banks
BBVA
UBS
LHV
London Stock Exchange
secco
BNY MELLON
BARCLAYS
fidor BANK
citibank
moni
Trade Finance
GAZEBO.IO
everledger
CHRONICLED
VAVE
skuchain
digix
PROVENANCE
thingchain
MIDDLEWARE & SERVICES
Services
CRYPTONOMEX
B9
CONSENSYS
Solid
applied blockchain
RUBIX
Software Development
chainscript
HydraChain
Blockstack.io
PEERNOVA
CREDITS
openchain
eris INDUSTRIES
MultiChain
Manifold
Blockstream
General APIs
BitGo
neuroware
coinbase
bitcore
Gem
BLOCKCYPHER
Coinkite
Special APIs
TIERION
Open Assets
bitbind.io
COLOREDCOINS
factom
Platforms
Omni
Counterparty
Monetas
erocoin
blockstack
HYPERLEDGER
Tendermint
BLOCKAPPS
applied blockchain
Smart Contracts
SmartContract
CoinSpark
ETH BaaS
ROOTSTOCK
bitShares
Tembusu Systems
INFRASTRUCTURE & BASE PROTOCOLS
Public
bitcoin
bitShares
ethereum
Special
ripple
stellar
Payment
Amiko Pay
MONERO
Lightning Network
Miners
ANTPOOL
BitFury
21 INC
BTCC
BITCOINCZ
Source: http://startupmanagement.org/blog
Virtual Capital Ventures © 2015 1.7


coin
cryptography
network
technology
concept
data
symbol
business
payments
Blockchain
electronic
currency
exchange
digital
finance
financial
virtual
transaction
market
currency
electronic
payments
money
Blockchain
crypto
exchange
cryptocurrency
cryptography
money
contract
business
internet
transaction
cash
payments
finance
market
internet
business
data
network
technology

9. Lexique

Lexique

Adresses
Les adresses (adresses crypto-monnaies) sont utilisées pour envoyer et recevoir des transactions sur le réseau. Une adresse est une chaîne de caractères alphanumériques, mais elle peut également être représentée par un QR Code analysable.

ASIC
ASIC est un acronyme pour "Application Specific Integrated Circuit". Les ASIC sont des puces de silicium spécialement conçus pour faire une seule tâche. Dans le cas de Bitcoin, ils sont conçus pour traiter SHA-256 problèmes de hachage aux nouveaux bitcoins minés.

Block ou bloc
Un groupe de transactions.

Blockchain
Une blockchain est un type de livre distribué, composé des données immuables, enregistrées numériquement en paquets appelés blocs (un peu comme rassemblés sur une seule feuille de papier). Chaque bloc est ensuite «enchaîné» au bloc suivant, en utilisant une signature cryptographique. Cela permet à des chaînes de blocs d'être utilisés comme un livre, qui peut être partagé et accessible à tous avec les autorisations appropriées.

Lexique (suite)

Bloc récompense ou Block Reward
La récompense accordée à un mineur qui a haché avec succès un bloc de transaction. La récompense de bloc peut être un mélange de pièces de monnaie et des frais de transaction, en fonction de la stratégie utilisée par la crypto-monnaie en question, et si toutes les pièces ont déjà été exploités avec succès. La récompense du bloc courant pour le réseau Bitcoin est 25 bitcoins pour chaque bloc (voir présentation bitcoin plus haut)

Clef publique/privée
Le jeu de clef publique/privée est le mécanisme d'identification de la Blockchain. Cette innovation décisive provient de travaux sur la cryptographie asymétrique dans les années 70. Les deux clefs sont liées mathématiquement de sorte que la clef publique (connue de tous) permet de coder un message tandis que la clef privée (connue par l'utilisateur seul) permet de le décoder. En somme, une clef privée permet de calculer la clef publique mais l'inverse est impossible.

Crypto-monnaie
Une forme de monnaie numérique basée sur les mathématiques, où les techniques de cryptage sont utilisés pour réguler la production d'unités de la monnaie et vérifier le transfert de fonds. En outre, les crypto-monnaies fonctionnent indépendamment d'une banque centrale.

Lexique (suite)

Distributed Ledger
Les livres distribués sont un type de base de données qui sont réparties sur plusieurs sites, des pays ou des institutions. Les enregistrements sont stockés les uns après les autres dans un registre continu, les données du grand livre distribué peuvent être soit «Permissioned» ou «UnPermissioned» afin de contrôler qui peut voir.

Genesis Block
Le premier bloc d'une chaîne de blocs

Hash Rate
Le nombre de tables de hachage qui peuvent être réalisées par un mineur Bitcoin dans une période de temps donnée (généralement une seconde).

Lexique (suite)

Hash Cryptographique et contrôle de l'authenticité
L'algorithme permettant de relier les blocs entre eux est un hash cryptographique (de son petit nom intime SHA256). Il va mélanger les données arrivant afin de sortir un nombre. La complication vient du fait que ce mélange est irréversible : il est impossible de partir du nombre d'arrivée pour remonter aux données d'arrivée sans faire énormément de suppositions aléatoires. Or, c'est exactement ce que font les mineurs : insérer dans cette fonction de nombreux chiffres de sortie jusqu'à ce que le chiffre d'entrée corresponde à certains critères. Après cet aspect aléatoire, les mineurs peuvent ajouter un block du pool d'attente au dernier bloc de la chaine. Chaque nœud du réseau, appelé node, représente un ordinateur connecté via son wallet, qui dispose une copie complète de la blockchain.
Sur la base des technologies mathématiques de pointe présentées ci-dessus, les transactions sont vérifiées par les mineurs, qui veillent à la fiabilité et l'exactitude du ledger. Les principes mathématiques permettent également aux nodes de vérifier continuellement et automatiquement la légitimité et la véracité de l'état actuel du ledger et de chaque transaction ayant lieu. En effet, chaque transaction dispose d'une signature mathématique spécifique et unique. Si une tentative de fraude à lieu, les nodes ne pourront pas arriver à un consensus, et la transaction ne sera pas acceptée dans la blockchain.

Pour résumer, chaque transaction est publique et des milliers de nodes acceptent unanimement qu'une transaction a eu lieu à telle heure, telle date. C'est presque comme si ce réseau permettait de valider chaque transaction par un notaire.

Lexique (suite)

Miners
Les miners, ou mineurs en français, sont les nœuds du réseau qui valident les transactions et alimentent la puissance de calcul de la Blockchain. Ce sont eux qui opèrent la validation des transactions à la place d'une instance centrale. Ce sont des individus ou des organisations qui apportent le matériel informatique nécessaire pour résoudre des problèmes cryptographiques en temps réel. Le premier des mineurs à trouver cette solution est rémunéré en crypto-monnaie, ce qui génère une compétition entre les mineurs et les pousse à acquérir du matériel plus puissant [voir Proof-of-Work].
Une carte en temps réel des miners de la blockchain Bitcoin est disponible sur https://bitnodes.21.co.

Mining ou Minage
Le processus par lequel les transactions sont vérifiées et ajoutées à une blockchain. Ce processus de résolution des problèmes de cryptographie utilisant du matériel informatique déclenche également la libération de crypto-monnaies.

Multi Signature
Multi-signature (multisig) sont des adresses permettent à de multiples parties d'exiger plus d'une clé pour autoriser une transaction. Le nombre nécessaire de signatures est convenu lors de la création de l'adresse. Plusieurs adresses de signature ont une bien plus grande résistance au vol.

Lexique (suite)

P2P
Peer-to-peer se réfère aux interactions décentralisées qui se produisent entre au moins deux parties dans un réseau fortement interconnecté. Le participant P2P traitent directement avec l'autre à travers un point de médiation unique.

Permissioned Ledgers
Les Permissioned Ledgers peuvent avoir un ou plusieurs propriétaires. Quand un nouvel enregistrement est ajouté, l'intégrité du livre est vérifié par un processus de consensus limité. Ceci est réalisé par des acteurs de confiance - des ministères ou des banques, par exemple - ce qui rend la tenue d'un registre partagé beaucoup plus simple que le processus de consensus utilisé par les grands livres unpermissioned.
Les Permissioned Blockchains fournissent des ensembles de données très vérifiables car le processus de consensus crée une signature numérique, qui peut être vue par toutes les parties. Un grand livre «Permissioned» est généralement plus rapide qu'un livre «unpermissioned».

Proof of Stake ou Preuve de participation
Une alternative à la preuve du travail, dans lequel votre jeu existant dans un crypto-monnaie (le montant de cette monnaie que vous détenez) est utilisé pour calculer le montant de cette monnaie que vous pouvez miner.

Lexique (suite)

Proof of Work ou Preuve de travail
Un système qui lie la capacité du minage à la puissance de calcul. Les blocs doivent être hachés, ce qui est en soi un processus de calcul facile, mais une variable supplémentaire est ajoutée au processus de hachage pour le rendre plus difficile. Quand un bloc est haché avec succès, le hachage doit avoir pris un peu de temps et d'effort de calcul. Ainsi, un bloc haché est considéré comme une preuve de travail.

Smart Contracts
Les contrats intelligents sont des contrats dont les termes sont enregistrés dans une langue à la place de la langue juridique de l'ordinateur. Les contrats intelligents peuvent être automatiquement exécuté par un système informatique, tel qu'un système de référentiel distribué approprié (distributed ledger system)

Ripple (Ondulation)
Un réseau de paiement intégré sur les grands livres distribués qui peuvent être utilisés pour transférer des devises. Le réseau se compose de nœuds de paiement et de passerelles exploités par les autorités. Les paiements sont effectués en utilisant une série de reconnaissances de dettes, et le réseau est basé sur des relations de confiance.

Scrypt
Une alternative «Preuve de travail» au SHA-256, conçu pour être particulièrement convivial pour les mineurs de CPU et GPU, tout en offrant peu d'avantages aux mineurs ASIC.

Lexique (suite)

SHA 256
La fonction cryptographique utilisée comme base pour la Preuve de travail de Bitcoin.

Secret key (clé privée)
Il s'agit d'un numéro que vous devez garder secret et qui permet de gérer les bitcoins envoyés à l'adresse publique.

Token
Le token (jeton en anglais) est l'unité de base d'une blockchain. C'est cette unité transférable qui devient donc une preuve de propriété : le token est possédé sur un compte, une adresse au sein du système (par exemple, le token de la blockchain bitcoin est le Bitcoin). De plus, il est possible d'adosser des informations à des tokens et de les utiliser au-delà d'application monétaires : un titre de propriété, un bulletin de vote, une preuve d'antériorité…
Un moyen d'affecter une valeur spécifique à un token est la coloration de coins : des tokens taggés (colorés) qui seront comme un sous-sytème monétaire au sein d'une blockchain. Cela peut servir à émettre et gérer des actions pour un moindre coût, le site Coinprism permet de tester cette fonction assez facilement.
Les tokens sont l'unité transactionnelle et informationnelle sur une blockchain.

Lexique (suite & fin)

Transaction
Le wallet comporte la clé privée, et permet la création de signatures. Pour créer une signature, la clé privée et le texte issu d'une transaction sont introduits dans une fonction cryptographique (basée sur l'arithmétique principalement, cette fonction permet de préserver la confidentialité des données, mais aussi à assurer leur intégralité et leur authenticité). Une autre fonction permet aux autres personnes de pouvoir vérifier cette signature, afin de vérifier qu'elle a bien été créée par le compte en question. Ainsi, ces signatures ne peuvent être copiées et réutilisées. Elles sont uniques à chaque transaction.

Unpermissioned Ledgers
Les Unpermissioned Ledgers tels que Bitcoin n'ont pas de propriétaire unique - en fait, ils ne peuvent pas faire l'objet d'une propriété. Le but d'un livre unpermissioned est de permettre à quiconque de fournir des données au livre et pour chaque partie en possession du livre d'avoir des copies identiques.
Cela crée une résistance à la censure, ce qui signifie qu'aucun acteur ne peut empêcher une transaction d'être ajouté à la comptabilité. Les participants maintiennent l'intégrité du livre pour parvenir à un consensus à propos de son état.

Wallet
C'est le logiciel qui contient vos adresses bitcoin publique et vos clés publiques / privées.