

Cours Blockchain

Module 1 : Introduction, Concepts & Fondements



1

COMPRENDRE LA BLOCKCHAIN

Comprendre et anticiper le potentiel de disruption de la Blockchain



2

1. Contexte & genèse de la Blockchain
2. La Blockchain
3. Concepts de Blockchain
4. Glossaire de Blockchain
5. Annexes et Sources



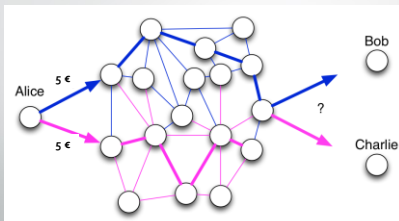
3

1 - CONTEXTE

DISRUPTION

4

Qu'est-ce que la Blockchain ?



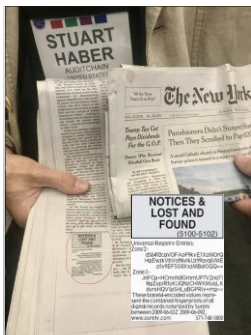
Consulty

5

Qu'est-ce que la Blockchain ?

- Blockchain est un système composé de..
 - Transactions
 - Registres immuables
 - Pairs décentralisés
 - Processus de cryptage
 - Mécanismes de consensus
 - Contrats intelligents optionnels

6



Histoire de la blockchain

- 1991** : Initialement un système d'horodatage et de certification de documents (Stuart Haber and Stornetta)
- 1995** : Le NY Times met en place la première blockchain qui est toujours active et qui est la plus longue de l'histoire (logiciel surety)
- 1994-2008** : Nick Szabo développe les concepts de base, et lance Bitgold, précurseur de Bitcoin
- 2008** : Satoshi Nakamoto (Szabo ou un collectif ou un inconnu) publie un article qui pose les bases de Bitcoin
- 2013-2015** : Vitalik Buterin va développer Ethereum qui est à la fois une monnaie cryptographique et une plateforme applicative distribuée.
- L'air du temps** : le croisement big-data (cloud), blockchain (intégrité référentielle) et IA (deep learning, machine learning): Deep Brain Chain, Cortex Virtual Machine,...

7

Une brève histoire de la Blockchain

- Le 31 octobre 2008, Satoshi Nakamoto a publié le Livre blanc Bitcoin décrivant un système électronique de transfert d'actifs/espèces numériques purement peer to peer. Il s'agit de la première mise en œuvre populaire de la Blockchain et est attribué comme la naissance de l'industrie blockchain d'aujourd'hui. Depuis lors, d'autres Blockchains ont été popularisés, Ethereum, diverses solutions de projet Hyperledger, ainsi que de nombreuses autres, y compris des solutions « Blockchain like » telles que les produits KSI de GuardTime

8

Immuable

- Comme pour les bases de données existantes, blockchain conserve les données via les transactions
- La différence est qu'une fois écrit à la chaîne, les blocs peuvent être changés, mais il est extrêmement difficile de le faire. Nécessitant une refonte sur tous les blocs ultérieurs et le consensus de chacun.
- La transaction est immuable ou indélébile
- En termes DBA, blockchains sont écrire et lire seulement
- Comme un grand livre écrit à l'encre, une erreur serait résolue avec une autre entrée

9

Pairs décentralisés

- Plutôt que le type centralisé de réseau « Hub and Spoke », blockchain est un réseau décentralisé peer to peer
- Chaque NOEUD a une copie du grand livre.

Legacy Network Blockchain Network

DB centralisée



Registres distribués



10

Domaines d'utilisation de la blockchain

- Secteur banque & finance
 - Portefeuilles électroniques
 - Transaction entre particuliers, professionnels & entre banques
 - Certification de documents
 - Permis de conduire, état civil, diplômes
 - Protection des droits d'auteurs, protection industrielle
- Logistique et distribution
 - Suivi du transport
 - Sécurité et traçabilité alimentaire (couplage avec IOT)
- Santé
 - Applications encore très peu développées

<http://www.bortzmeyer.org/a-quoi-sert-blockchain.html>



11

Transactions

- Comme pour les transactions d'entreprise d'aujourd'hui, la Blockchain est une archive historique des décisions et des actions des décisions et des mesures prises
- Preuve de l'historique, fournit la provenance

Exemples de cas notables d'utilisation des transactions

| |
|--|
| Enregistrement foncier – Remplacement des exigences relatives à la recherche sur les actes (Enregistrement foncier en Suède) |
| Identification personnelle – Remplacement des certificats de naissance/bébé, permis de conduire, cartes de sécurité sociale (Estonie) |
| Transport – Factures de chargement, suivi, certificats d'origine, formulaires internationaux (Maersk/BM) |
| Services bancaires – Stockage de documents, efficacité accrue des back-office (UBS, Sberbank en Russie) |
| Fabrication – Documentation du berceau à la tombe pour tout assemblage ou sous-assemblage |
| Distribution alimentaire – Fournir l'emplacement, le lot, la date de récolte Les supermarchés peuvent épingler les aliments problématiques (Walmart) |
| Audits – En raison de la nature décentralisée et immuable de la Blockchain, les audits changeront fondamentalement. |

- Demo : <https://andersbrownworth.com/blockchain>

12

ÉLÉMENTS DE CONTEXTE

- Dans un contexte de crise économique (2008-2009), de scandales financiers et monétaires, de perte de confiance en les institutions bancaires, un groupe de *hackers* a créé une crypto-monnaie émise par un système d'échange entre pairs et dénué de tout système de contrôle centralisé. C'est ainsi que **Satoshi Nakamoto** pose les principes fondateurs de Bitcoin dans en 2009
- Blockchain est l'architecture et le paradigme sous-jacent au Bitcoin.
 - Bitcoin est le **use-case** monétaire de Blockchain (et accessoirement le use-case le plus connu)
- Blockchain est souvent victime de préjugés négatifs et de l'amalgame avec Bitcoin
 - Origine nébuleuse de Bitcoin
 - Satoshi Nakamoto (Craig Wright de son vrai nom) est-il une personne physique? Est-ce un groupe de hackers? Pour qui agissent-ils? Qui maîtrise les nœuds du réseau?...
 - Quelques scandales : Achats illégaux, blanchiment d'argent et vols
 - En 2014, vol de l'équivalent de 400 M\$ en bitcoin à Mt. Gox
 - En 2015, BitPay
 - Découverte régulière de malwares



13

Origine de la Block...Chain

La première Blockchain est apparue en 2009 avec la monnaie numérique **Bitcoin**, développée par un inconnu se présentant sous le pseudonyme Satoshi Nakamoto. Elle en est l'architecture sous-jacente.

Si Blockchain et Bitcoin ont été construits ensemble, aujourd'hui de nombreux acteurs (entreprises, gouvernements, etc) envisagent l'utilisation de la technologie blockchain pour d'autres cas que la monnaie numérique.



14

Terminologie Blockchain



- **Bitcoin**
 - La cryptomonnaie Bitcoin est le premier actif basé sur la technologie Blockchain
 - Utilisée pour la vente en ligne de drogues et armes illégales, ainsi que les *ransomware* (rançongiciel)
 - Utilisée pour réaliser des transferts de fonds, de la spéculation, et en tant que réserve de valeur

"Ce dont on a besoin est un système de paiement électronique basé sur des preuves cryptographiques et non sur la confiance, qui permettrait à deux parties de réaliser des transactions directement entre elles, sans avoir besoin de tierce partie de confiance."

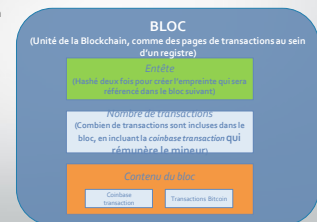
Satoshi Nakamoto – 31 Oct. 2008

15

Terminologie Blockchain



- **Bitcoin**
 - À l'intérieur de la blockchain Bitcoin



16

17

Terminologie Blockchain



Bitcoin

- À l'intérieur de la blockchain Bitcoin
 - Entête du bloc : contient des données techniques, le hash du bloc précédent, racine de Merkle, horodatage, difficulté, nonce
- Voici un exemple :

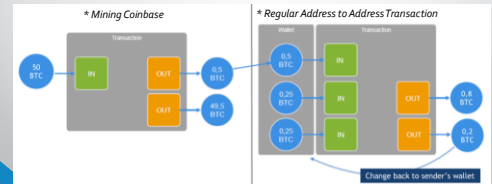
[illegible]

18

Terminologie Blockchain



- **Bitcoin**
 - À l'intérieur de la blockchain Bitcoin
 - Contenu du bloc : Flux de transactions



19

Terminologie Blockchain



- **Bitcoin**
 - À l'intérieur de la blockchain Bitcoin
 - Exemple de transactions d'un bloc

[illegible]

20

Contrats intelligents

- Code informatique
- Fournit la couche logique d'entreprise avant la soumission de bloc

| Blockchain | SmartContracts? | Language | |
|-------------|-----------------|----------|---------------------------|
| Bitcoin | Non | | |
| Ethereum | Oui | Solidity | |
| Hyperledger | Oui | Divers | GoLang, C++, etc, depends |
| Others | Depends | Depends | |

Terminologie Blockchain

• Ethereum

- Proposé fin 2013 par Vitalik Buterin (chercheur et programmeur dans le domaine des cryptomonnaies)
- Financement participative par vente d'Ether contre des bitcoin, durant l'été 2014
- Bitcoin gonflé aux stéroïdes !

"Une blockchain est un ordinateur magique sur lequel tout le monde peut télécharger des programmes, et les faire s'auto-exécuter, où l'état présent ainsi que l'historique des états de tous les programmes sont toujours visibles publiquement, et qui intègre une garantie crypto-économique très forte que ces programmes continueront de s'exécuter exactement de la manière spécifiée par le protocole de la blockchain."

Vitalik Buterin

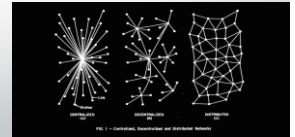


21

Terminologie Blockchain

• Ethereum

- Plateforme d'applications décentralisées (appelées Dapps)
- Registre de transactions et de contrats intelligents
- Basé sur l'Ethereum Virtual Machine (EVM), machine virtuelle d'Ethereum
- Intègre une cryptomonnaie, appelée Ether (ETH)



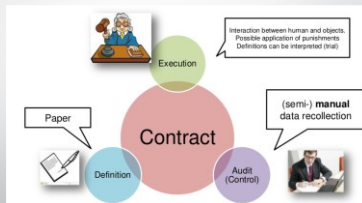
22

Terminologie Blockchain

• Ethereum

- Contrat intelligent

Comment un contrat "traditionnel" fonctionne



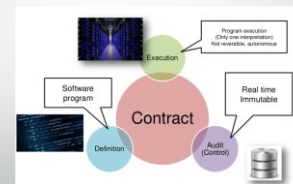
23

Terminologie Blockchain

• Ethereum

- Contrat intelligent

Comment un contrat "intelligent" fonctionne



24

Capacités blockchain

Une technologie de grand livre partagée permettant à tout participant au réseau d'affaires de voir le système d'enregistrement (grand livre)

Assurer une visibilité appropriée; transactions sont sécurisées, authentifiées et vérifiables

Toutes les parties conviennent de réseauter les transactions vérifiées.

Termes d'affaires intégrés dans la base de données des transactions et exécutés avec des transactions

Résumé de la Blockchain

Un problème d'affaires à résoudre
Cela ne peut pas être résolu avec des technologies plus matures.

Un réseau d'affaires identifiable
Avec les participants, les actifs et des transactions

Un besoin de confiance
Consensus, immutabilité, finalité ou provenance

Indicateurs négatifs, anti-modèles

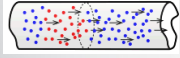
Besoin de transactions haute performance (milliseconde)
Petite organisation (pas de réseau d'affaires)
Vous cherchez un remplacement de base de données
À la recherche d'un remplacement de messagerie
Vous cherchez le remplacement du traitement des transactions
Les processus et les mesures ne sont pas clairs au sein de l'écosystème
La valeur, la vitesse et/ou la variabilité ne sont pas présentes

Consulty

25


A l'instar de l'électricité, la blockchain donne naissance à d'autres technologies...

Electricité



- les lampes à incandescence
- les moteurs électriques
- l'électroménager
- le transistor
- les ordinateurs
- ☐ ...

Blockchain

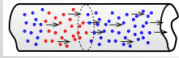


- les crypto-monnaies
- les Tokens
- les Smart Contract
- les DApps (Decentralized Applications)
- ☐ ...

26


... et à de nouveaux produits et services !

Electricité



- La lampe à incandescence
- Le congélateur
- Le Smart Phone
- La calculatrice
- ☐ ...

Blockchain



- Le Bitcoin : une devise anti-inflationniste
- Les micro-paiements dans les pays non bancarisés
- Le stockage de données décentralisé et résilient
- La traçabilité publique des produits
- ☐ ...

27



28

La promesse du blockchain : **DISRUPTION** remplacer les tiers de confiance.

Blockchain étape 1 : Gestion des actifs, l'exemple de Bitcoin.

Blockchain étape 2 : Gestion des contrats, l'exemple d'Ethereum.

Blockchain étape 3 : Gestion des agents économiques autonomes.



29

La Blockchain en tant que structure de données

• Différents types de blockchains

Il y a trois principaux types de Blockchain, qui ont émergés après l'apparition de Bitcoin.

✓ Blockchain publique :

Personne ne dirige le réseau, n'importe qui peut participer en lisant, écrivant, ou en auditant la blockchain (i.e. Bitcoin, Litecoin, etc.)

✓ Blockchain privée :

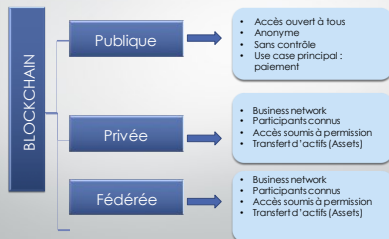
La propriété privée d'un individu ou d'une organisation, où une entité dirige l'écriture / la lecture ou bien les droits d'accès à l'écriture / à la lecture (i.e. Bankchain)

✓ Blockchain fédérée / consortium :

Plusieurs personnes dirigent le réseau. Un groupe d'entreprise ou d'individus représentant prennent des décisions communes au profit du réseau (i.e. r3, EWF)

30

Les types de BLOCKCHAIN



31

Les types de BLOCKCHAIN - **Publique**

- Sans permission
- Anonyme
- Transparente

Quiconque peut rejoindre le réseau

- Participer au processus de vérification des bloc (consensus)
- Créer des contrats intelligents
- Générer des transactions

▶ BITCOIN !



32

Les types de BLOCKCHAIN - Privée

- ▶ Accès par autorisation
- ▣ Identité des participants connue et vérifiée
- ▶ Le principe de consensus est vérifié par un nombre limité et prédéfini de participants.
- ▣ **Blockchain de consortium**
- ▣ Regroupe plusieurs acteurs qui possèdent des droits.
- ▣ Les décisions sont prises par la majorité des acteurs.

BLOCKCHAIN FOR BUSINESS



Conzultly

33

La promesse blockchain

DISRUPTION

La blockchain est une technologie qui permet de gérer un registre infalsifiable sans organe central de contrôle.
Avec la blockchain, la confiance est établie par des pairs et non plus par des tiers.
Elle permet de réaliser des transactions sans avoir à passer par des intermédiaires.

Conzultly

34

Réseau Peer to peer

Chaque nœud du réseau contient une copie de la base de données. Chaque utilisateur réalise des transactions via un nœud du réseau. Il effectue ses transactions à l'aide d'un portefeuille électronique.

Conzultly

35

Modèles en trois couches

Les systèmes de blockchain peuvent naturellement être divisés en trois couches, la couche réseau, consensus et incitations.

- Couche réseau
- Couche de consensus
- Couche des incitations

Conzultly

36

Modèles en trois couches Couche réseau

contient :

- les nœuds du réseau
- leurs emplacements géographiques
- la connectivité entre eux.

Elle définit quelles informations doivent être propagées ainsi que le mécanisme pour propager ces informations.



37

Modèles en trois couches Couche de consensus

- définit les algorithmes et les règles pour parvenir à un accord sur l'état de la blockchain entre les nœuds du réseau
- Ces règles spécifient :
 - quel nœud est éligible pour générer et ajouter le bloc suivant au grand livre de la blockchain,
 - à quelle fréquence les blocs sont générés
 - comment résoudre les conflits



38

Modèles en trois couches Couche Incitation

- utilise la crypto-monnaie de la blockchain pour établir une structure d'incitation,
- distribue des récompenses entre les mineurs participants qui gèrent le registre de la blockchain
- Les incitations protègent également le système de blockchain contre diverses attaques (par exemple, les attaques DDoS dans Ethereum, [Buterin, 2016](#)) et contre les comportements malveillants des nœuds (par exemple, stratégies d'extraction égoïstes, [Eyal et Sirer, 2018](#)).



39

Blockchain étape 1 : Gestion des actifs, l'exemple de Bitcoin.

- *"Une chose qui manque est un système de paiement sécurisé qui permettra de transférer des fonds d'une personne A à une personne B sans qu'ils se connaissent, de la même façon que je vous tends un billet de 20\$."*

citation de Milton Friedman

- C'est exactement, ça, Bitcoin est une sorte de porte monnaie avec un système de téléportation.



40

Les promesses du bitcoin

- Première devise monétaire électronique décentralisée.
- Transactions quasi instantanées de personnes à personnes.
- Aucun ou peu de frais.
- Pas de notions de pays, de conditions préalables ou de limites arbitraires.
- Votre "compte" ne peut être bloqué ou confisqué.
- Relatif Anonymat.



41

L'arrivée de l'email

Avant l'email, avec la poste

- La poste doit connaître le destinataire et vous devez suivre les processus établis.
- Frais "importants" et variables en fonction de la destination.
- Le transport du courrier peut prendre un temps variable en fonction de la destination.
- Tous les individus ne sont pas accessibles via ce système.

Avec l'email

- Le destinataire a juste besoin d'avoir une adresse email.
- Le coût d'envoi d'un email est proche de zéro.
- L'envoi et la réception sont quasi instantanés.
- Toute personne ayant un accès à internet peut recevoir un email.



42

BLOCKCHAIN : BITCOIN

- Analogie Bitcoin / Mail :



43

L'arrivée du Bitcoin

Avant le bitcoin, avec le système bancaire

- Il faut que vous soyez enregistré auprès d'une banque qui va vous octroyer votre "adresse" (IBAN).
- Vous devez utiliser les normes du système bancaire.
- Il peut y avoir des frais en fonction des banques et en fonction des pays où vous envoyez de l'argent.
- Un virement peut prendre un temps très variable, surtout si vous le faites vers l'étranger.
- La moitié de la population mondiale n'a pas accès à un compte bancaire.

Avec le bitcoin

- Vous pouvez vous même créer un "compte" pour recevoir/envoyer des bitcoins sans avoir besoin de faire appel à une autorité centrale et sans conditions préalables.
- Vous pouvez envoyer instantanément des bitcoins à n'importe qui, peu importe où il se trouve et pour un coût proche de zéro.
- Toute personne ayant un accès à internet peut se créer un "compte", ça ne coûte rien, c'est instantané et vous n'avez pas à vous enregistrer auprès de qui que ce soit.



44

Avant de poursuivre, deux choses à savoir...



Conzultly

45

a) Bitcoin fonctionne en P2P

Le réseau Bitcoin est un réseau de machines en peer to peer (P2P), ce qui signifie que toutes les machines qui y participent ne sont pas plus importantes les unes que les autres.



Conzultly

46

Un des Fondamentaux Technologiques pour le « Transport » et les « Transactions » Numériques

- Le Protocole TCP / IP pour le transport de Paquets codés (infrastructure de données, ce communication et de calcul)
- > Blockchain pour le transport de Blocs codés ...et + (s'appuyant par ailleurs sur le réseau TCP IP)

47

b) La blockchain est un registre public

- Le réseau Bitcoin maintient un fichier qui est un registre global de toutes les transactions : La blockchain.
- Ce fichier permet à tout le monde de savoir qui a combien de bitcoins mais le "qui" n'est pas relié à une personne physique ou morale !

Conzultly

48

Les smart contracts

- Aujourd'hui, les contrats "s'exécutent" dans des programmes qui se trouvent sur des serveurs centralisés (banques, assurances, mutuelles...). Si un contrat est déployé sur un serveur centralisé, alors une panne, une faillite ou une attaque peuvent bloquer son exécution.
- Un smart contract (ou contrat autonome) est un programme qui s'exécute sans qu'un tiers puisse l'empêcher ou le modifier.



53

Ethereum

- Bitcoin ne gère que des contrats extrêmement simples.
- Vitalik Buterin, après avoir contribué aux projets Bitcoin, Name Coin et Colored Coin a construit une blockchain spécifiquement "orientée contrat" : **Ethereum**.



54

Comment cela fonctionne

- De la même façon que les bitcoins sont "stockés" dans la blockchain bitcoin, les programmes (contrats) que l'on va écrire vont être stockés sur la blockchain ethereum et ils vont être exécutés par celui-ci.
- Vous pouvez imaginer ethereum comme une sorte d'ordinateur global qui exécutera votre contrat de manière impartiale.

Mais nous y reviendrons plus tard...



55

Blockchain étape 3 : Gestion des agents économiques autonomes.

- Les DAO (organisations autonomes), DAC (entreprises décentralisées), et DAS (sociétés décentralisées) sont de nouveaux concepts que l'on peut imaginer grâce à la technologie Blockchain.



56

Exemple DAO

- Une DAO (Decentralized Autonomous Organization) est une organisation fonctionnant grâce à un programme informatique qui fixe les règles de gouvernance à une communauté.
- Ces règles sont transparentes et immuables car inscrites dans la blockchain.
- Trois choses importantes :
 - Une DAO ne peut pas être arrêtée ou fermée.
 - Aucune personne ou organisation ne peut contrôler l'entité.
 - Tout y est transparent et auditable.

<https://www.stateofthedapps.com/fr/rankings/category/property?page=2>



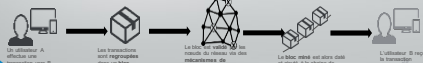
57

3 – Concepts de la Blockchain

58

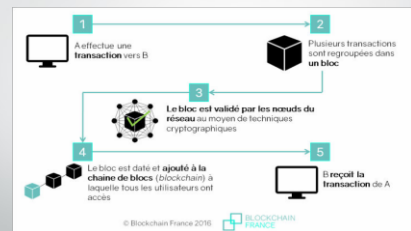
Comment « ça marche » précisément ?

- Toute blockchain publique fonctionne nécessairement avec une **monnaie** ou un **token (jeton)** programmable. Bitcoin est un exemple de monnaie programmable.
- Les transactions effectuées entre les utilisateurs du réseau (les pairs aussi appelés **nœuds** du réseau) sont regroupées par blocs.
- Chaque **bloc** est validé via un mécanisme de consensus par les **nœuds** du réseau appelés les **"mineurs"**, selon des techniques qui dépendent du type de blockchain. Dans la blockchain du bitcoin cette technique est appelée le **"Proof-of-Work"**, preuve de travail, et consiste en la résolution de problèmes algorithmiques.
 - Concrètement, le premier nœud qui **mine** le bloc s'attribue la **Proof-of-Work** et, est donc rétribué.
 - Des mécanismes de consensus permettent de gérer les doubles minages et d'arriver à un consensus rapidement (mise en compétition des **miners** qui augmente la puissance de calcul du réseau)
- Une fois le bloc validé, il est horodaté et ajouté à la chaîne de blocs.
- La transaction est alors visible pour le récepteur ainsi que l'ensemble du réseau.



59

En Résumé...

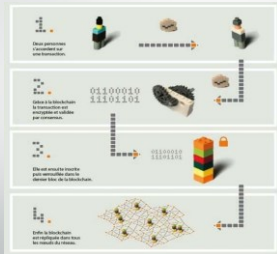


© Blockchain France 2016

BLOCKCHAIN FRANCE

60

Définition – Fonctionnement



61

Définition – Fonctionnement

La blockchain est une chaîne de blocs, 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 (registre). 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.



62

Définition – Fonctionnement

Il existe des blockchains publiques, ouvertes à tous, et des blockchains privées, dont l'accès et l'utilisation sont limitées à un certain nombre d'acteurs.

Une blockchain publique peut donc être assimilée à un **grand livre comptable public, anonyme et infalsifiable**. Comme l'écrit le mathématicien Jean-Paul Delahaye, il faut s'imaginer « un très grand cahier, que tout le monde peut lire librement et gratuitement, sur lequel tout le monde peut écrire, mais qui est impossible à effacer et indestructible. » (Blockchain France)

MODÈLE CENTRALISÉ ET RÔLE DU TIERS DE CONFIANCE

Quelques exemples de systèmes centralisés :

- Le système bancaire
- Le système notarial
- Le système de vote
- Une base de données standard
- Guinness Book des records

Les limites de ce système :

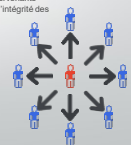
- Forte dépendance au tiers de confiance
- Le tiers de confiance constitue un point de défaillance potentiel (anti-pattern : single point of failure)
- Nécessite la confiance en le tiers de confiance
- Ajout de processus supplémentaires et donc d'un surcoût économique
- Limitant en terme de passage à l'échelle

Principe :

Dans un modèle centralisé, un tiers de confiance (middle man) joue le rôle d'intermédiaire dans les échanges entre les différents intervenants du système

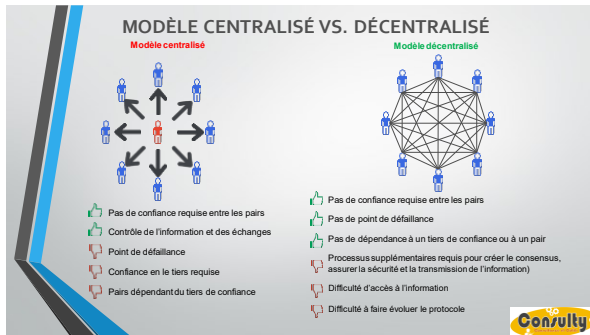
Quel rôle joue le tiers de confiance ?

- Il facilite les échanges entre les intervenants
- Il est le garant de la sécurité et de l'intégrité des échanges

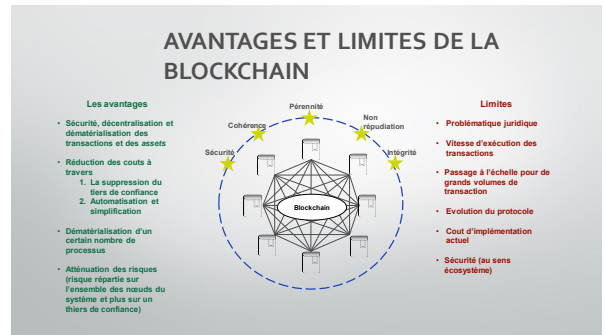


63

64



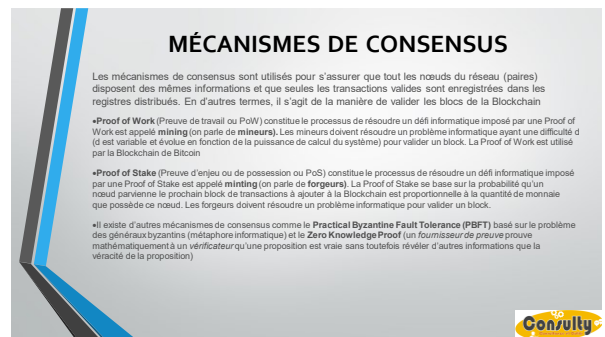
65



66



67



68

Conclusion

- La technologie blockchain apporte pour la première fois une solution à un problème que l'humanité a toujours résolu par l'administration.
- Pour la première fois, on peut transférer un titre de propriété digital à un autre utilisateur de manière simple, sécurisée, connue de tous et non répudiable.
- Nous pourrions voir l'avènement de systèmes qui gèrent des transactions (humain / humain, humain / machine ou machine / machine) et qui pourront remplacer certaines structures humaines existantes (banques, notaires, cadastres...).



69

4 – Glossaire

70

LEXIQUE DE LA BLOCKCHAIN

A compléter

- **Altcoin** : Abréviation de l'expression « Alternative Coin ». Une altcoin est une cryptomonnaie autre que le bitcoin (e.g. Litecoin, ether, amazcoin...)
- **Bitcoin (BTC)** : Cryptomonnaie électronique décentralisée conçue en 2009 par Satoshi Nakamoto
- **Blockchain** : ou « Chaine de bloc » est un paradigme de stockage décentralisé et de transmission d'informations à coût réduit, sécurisé et transparent. Blockchain peut être assimilée à une base de données sécurisée et distribuée et à un grand livre comptable public, anonyme et théoriquement infalsifiable
- **Fonction de Hachage** : On nomme fonction de hachage une fonction particulière qui, à partir d'une donnée fournie en entrée, calcule une empreinte servant à identifier rapidement, bien qu'incomplètement, la donnée initiale. Les fonctions de hachage sont utilisées en informatique et en cryptographie
- **Hash** : Résultat que produit une fonction de Hachage
- **Ledger** : Registre dans lequel sont enregistrés les transactions d'un système
- **Mining** : utilisation de la puissance de calcul informatique afin de traiter des transactions, sécuriser le réseau et permettre à tous les utilisateurs du système de rester synchronisés
- **Noeud** : ordinateur relié au réseau et utilisant un programme relayant les transactions
- **UTXO** : Etat du système à un instant t ou encore un « collection d'outputs de transactions non dépensées



71

5 – sources (liste partielle)

72

A compléter

Livres :

- Blockchain, Blueprint for new economy, Melanie SWAN – O'Reilly

Blogs et sites web :

- Principes fondateurs de Bitcoin de Satoshi Nakamoto - <https://bitcoin.org/bitcoin.pdf>
- Blockchaincafe - <http://blogchaincafe.com/> - David TERRUZI
- Finyear - <http://www.finyear.com/>
- Blockchain France - <https://blockchainfrance.net/>
- Practical Byzantine Fault Tolerance (PBFT) - <http://pmg.csail.mit.edu/papers/osdi99.pdf>

Whitepapers :

- Bitcoin : A Peer-to-Peer Electronic Cash System
- Comprendre la Blockchain – éditée par U – plateforme de transformation digitale

73

Ressources supplémentaires

- [Bitcoin White Paper](#) – Satoshi Nakamoto
- [Blockchain Demo](#) – Anders Brownworth
 - [Videos](#)
- [Blockchain for Business - An Introduction to Hyperledger Technologies](#) - edX.org
- [Ethereum White Paper](#)
- [Guardtime](#) – Blockchain like official site
- [Hyperledger official site](#) - Linux Foundation
- [IBM Blockchain for Business](#) – IBM Dev Center
- [IBM Blockchain Essentials Course](#) – IBM Dev Center
- [IBM Blockchain Foundation Developer](#) – IBM Dev Center
- <https://www.bitcoinsimulator.tk/blockchain?chain=public> – Bitcoin Simulator

Et beaucoup d'autres et les pages changent constamment...

74