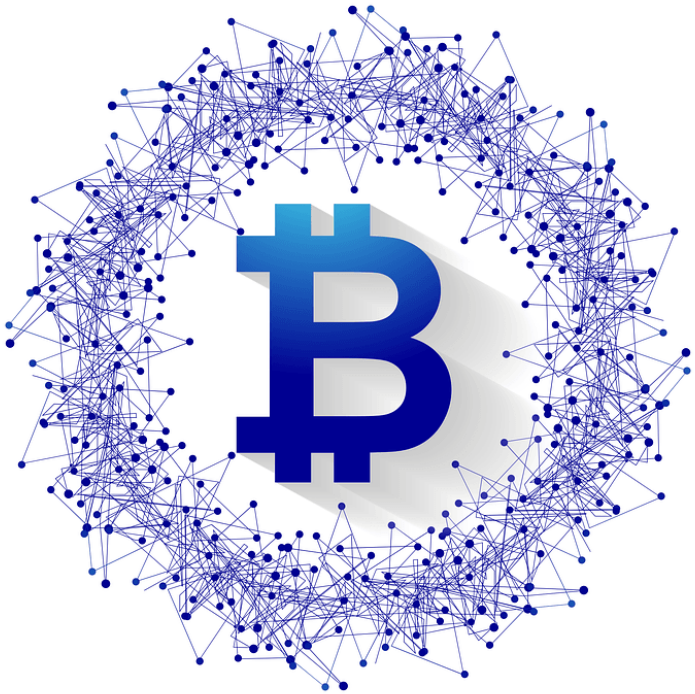


thenextweb.com

Principes et propriétés de la Blockchain

Présenté par
Christian Adja

Sommaire

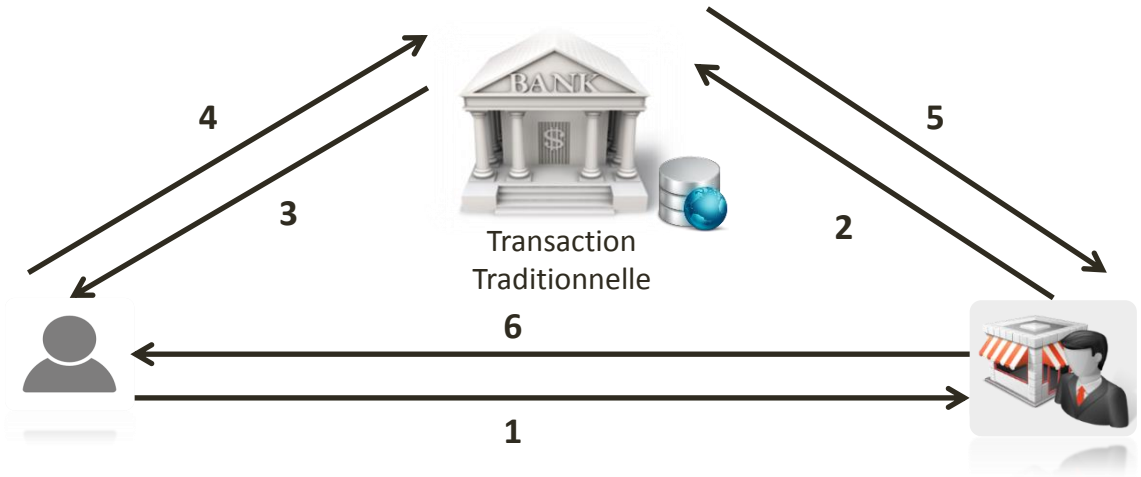
- **Vue Globale**
  - Qu'est-ce que c'est?
  - Premiers objectifs
- **La Chaine de Block**
  - Structure des blocks
  - Transactions
- **Blockchain privée et publique**
- **Le Réseau**
  - Les nœuds
- **Le Consensus**
  - Le problème des généraux Byzantins
  - Algorithmes de consensus
- **Les applications**
- **La fork**
- **L'évolution de la Blockchain**
- **ICO**

Besoins

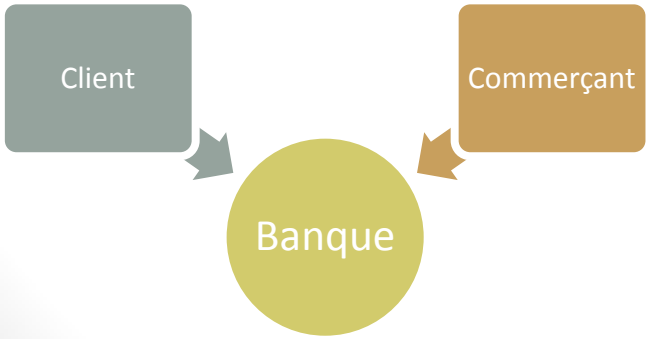
- Crise financière de 2008: Faillite de la LEHMAN BROTHERS
  - Le système peut s'effondrer

- Nécessité d'un système de paiement électronique libre et fiable
  - Qui s'affranchir de toutes autorités de confiance
  - Dénationalisation de la monnaie
  - Réduire les couts de transaction

Besoins



Modèle de confiance

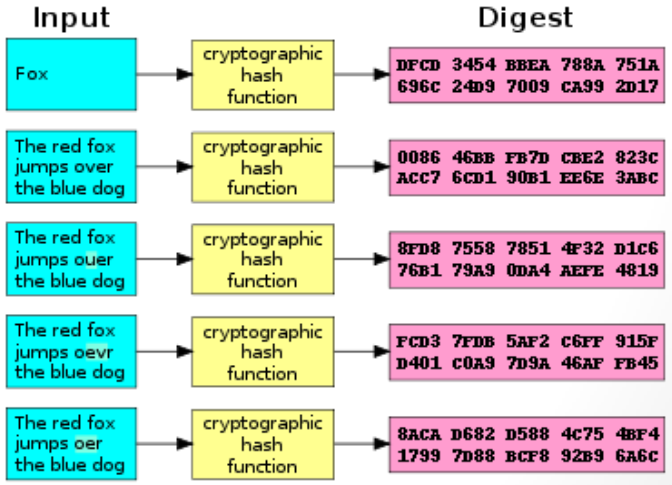


- Banque
  - Assure la sécurité des transactions et données utilisateurs
  - Vérifie les identités
- Client et commerçant
  - Utilisateurs du système

Que savons nous faire?

- Garantir l'intégrité des données numériques
  - Grace au fonctions d'hachages

Les cryptologues Whitfiel Diffie et Martin E. Hellman publient en 1976 un article consacré aux "nouvelles directions en cryptographie" dans lequel ils identifient la nécessité d'une fonction de hachage unilatérale (one-way hash function) pour la signature électronique.



Wikipedia

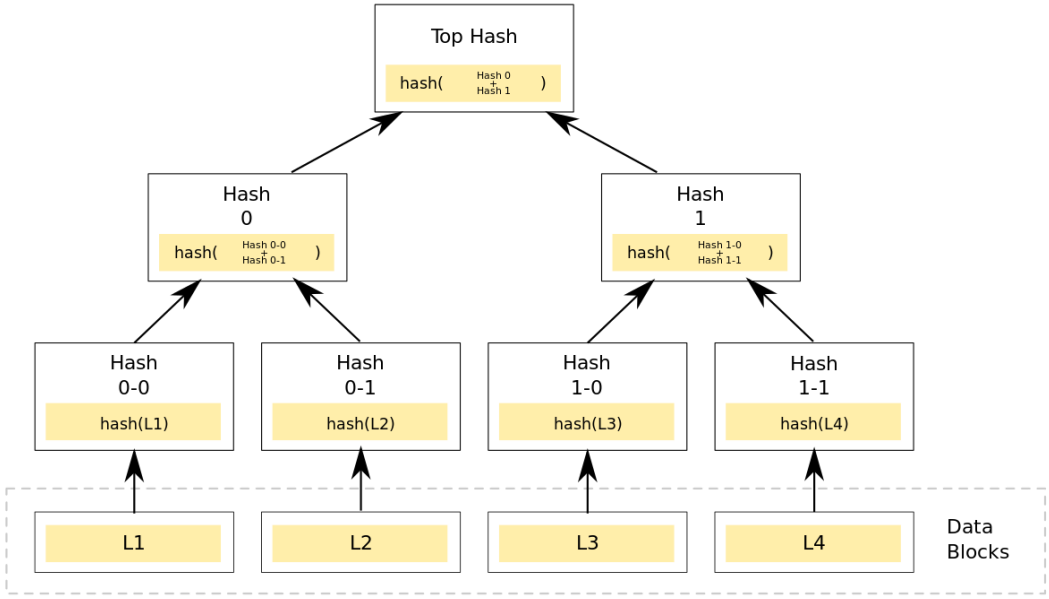
Que savons nous faire? (suite)

- Le système:
  - Est composé d'une entrée « la donnée » et d'une sortie « l'emprunte »
  - La fonction d'hachage est:
    - Caractérisé par la dimension de l'empreinte
    - Elle est a un seul sens

Results	
Original text	orsys
Original bytes	6f:72:73:79:73 (length=5)
Adler32	06b60241
CRC32	7d304ba6
Haval	a69a0ae950546d25e502ff78e6115b3c
MD2	1078641c1187311591b33d52729e5834
MD4	51557b3151dc848fbca40107603e33c1
MD5	7ab59e1100930763c1c4a37809bb285c
RipeMD128	6c290c9b231b57d1abe8aa3813072e1a
RipeMD160	3f3f8bc13ed9be465387c316f790564fd5905ff1
SHA-1	76936b357b5d95c4f53590a16e4b16dccab2efc0
SHA-256	333b3b4679fdb98911a11c47a434cbbd9e9146af9d049108de53ceaaa5becac7
SHA-384	69a1aba770af4b20f0edb36e364520b07f56cee95f9f2763891f8664d49678df4f54c6fd623007cca622e0768419e143
SHA-512	ea9c10f7c6a6353773d8d18bece12623ad9e120e18a648bac806ef2471edded42599d45aac73f1cd15cac66bb7218d6d1e52df7e045cea22a5ea1eda478836b9
Tiger	aca18cf5f3664b59946bbe3751a7aaedefcf6b88d6516046
Whirlpool	534b77b6a9a042fafce42d5ebe18febeedb3653e709a58070e05e81d34f8b558ebeb44bd839e50bb180a23ddd428200915c14698cab920f3f4e36225fd4d4235

Que savons nous faire? (suite)

- L'arbre de merkle (Merkle tree)
  - Ralph C. Merkle publie en 1979 la description d'une méthode de certification des signatures numériques et introduit une arborescence (tree signature).



Que savons nous faire? (suite)

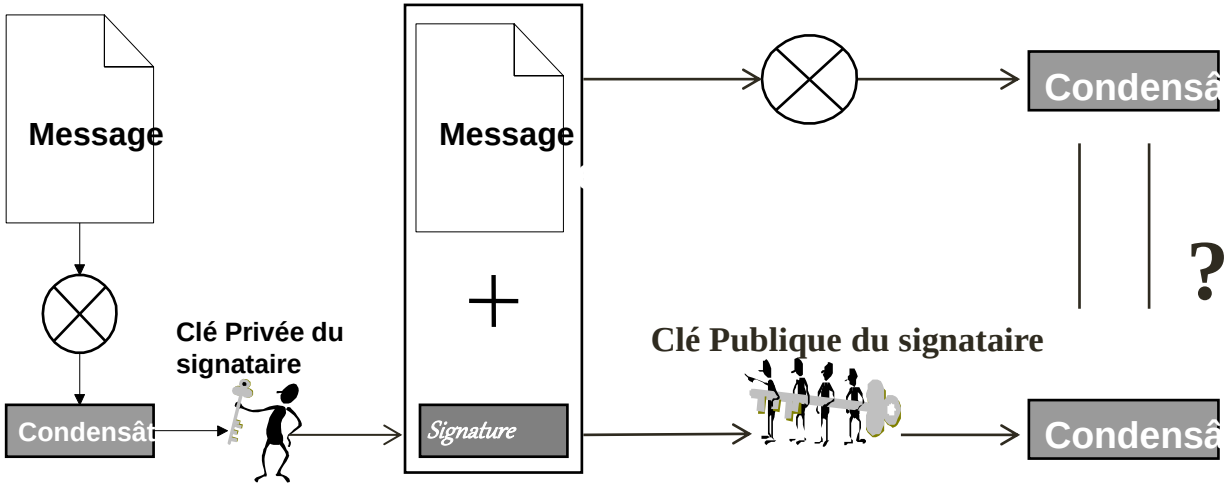
- Crypto Asymétrique
  - Notion de pair clé de clé publique/privée inventé par Ron L. Rivest, Adi Shamir et Leonard Adleman (1977) à travers le chiffrement RSA
  - Fournit un service de confidentialité et non-repudiation

Que savons nous faire? (suite)

- Plusieurs algorithmes de chiffrement asymétrique existant:
  - RSA
  - Diffie-Hellman
  - El Gamal
  - etc

Que savons nous faire? (suite)

- La signature numérique
  - Le cocktail des fonctions de hachage et de la crypto asymétrique assure un service de non répudiation



Que savons nous faire? (suite)

- **1990**: David Chaum invente DigiCash
  - Première monnaie a usage purement électronique
  - Pour:
    - Anonymat relatif des utilisateurs
    - Dénationalisation de la monnaie
  - Contre:
    - Présence d'un tiers de confiance
    - Trop de surcout

Que savons nous faire? (suite)

- **1991**: Wakefield Scott Stornetta énonce pour la première fois la Block-chain (Block-chain system)
  - La Blockchain comme system hiérarchique pour horodater les documents digitaux
    - Le transactions sont ordonnancé grâce à une estampille temporelle
    - Pour fournir un service de preuve de dépôt
  - Accessible ici

Que savons nous faire? (suite)

- **1992**: Publication de l'article « Pricing via Processing or combatting Junk Mail » par Cynthia Dwork, Moni Naor.
  - Naissance du proof-of-work dans l'objectif de combattre les mails indésirable et/ou contrôler l'accès au ressources partagées

Que savons nous faire? (suite)

- **1994**: L'informaticien et cryptographe Nick Szabo invente le mot smart contract.
  - Il définit le smart-contract comme le contrat intelligent comme « un protocole de transaction informatique qui exécute les termes d'un contrat. La conception d'un tel contrat a pour principaux objectifs de satisfaire les conditions contractuelles courantes, de minimiser les exceptions tant malveillantes qu'accidentelles ou le besoin d'intermédiaire de confiance. Les buts économiques associés incluent la réduction des coûts de fraude, d'arbitrage, de mise en application, et autres coûts de transaction »

Traduction de Jérôme Pons

Que savons nous faire? (suite)

- 1998: L'informaticien Wei Dai publie: « b-money, an anonymous, distributed electronic cash system".
  - Introduit la notion de minage
    - L'argent est crée à terme de la résolution d'un problème cryptographique
    - Une fois que la solution est vérifié, le pair ajoute une certaine somme au solde de celui qui a trouvé la solution
  - Notion de registre distribué

Que savons nous faire? (suite)

- 1999: Naissance du réseau pair –à- pair
  - Shawn Fanning lance Napster
    - Encore à architecture centralisé
  - Présence d'un goulot d'etranglement
- 2000: Naissance de Gnutella
  - Architecture totalement distribué

Résumé

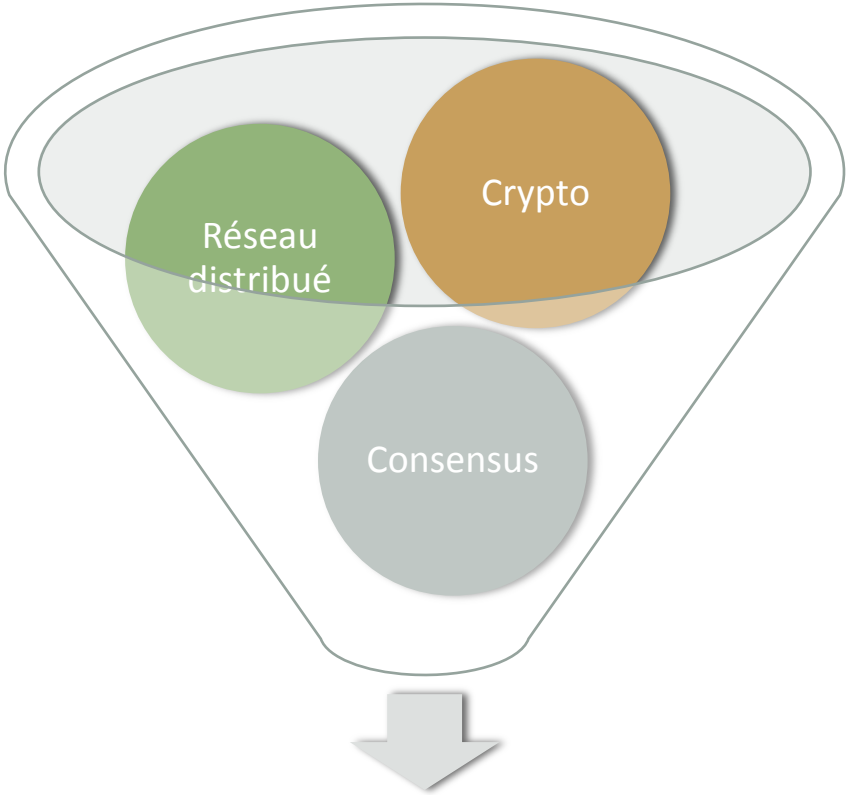
Nous savons faire

- Garantir l'intégrité des données
- Garantir la confidentialité des données
- La signature électronique
- Le contrôle d'accès sur des ressources partagées
- Décentraliser et distribuer un réseau

Ce qui reste

- Un modèle de confiance distribué
- Répartition des charges entre utilisateurs inconnus
- Distribution de la gestion d'identité entre utilisateurs
- Le consensus dans un environnement distribué

La Blockchain



Genèse

- Inventé en 2008 par Satoshi Nakamoto
  - Satoshi Nakamoto “Bitcoin: A Peer-to-Peer Electronic Cash System”
  - Encore inconnu
- C’est le résultat de la superposition de technos existantes.
- Elle est la technologie de base pour plus de 90% des crypto-monnaies actuelles

Définitions

- **Blockchain France**
  - La Blockchain est une technologie de stockage et de transmission d'informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle. Par extension, une Blockchain constitue une base de données qui contient l'historique de tous les échanges effectués entre ses utilisateurs depuis sa création. Cette base de données est sécurisée et distribuée : elle est partagée par ses différents utilisateurs, sans intermédiaire, ce qui permet à chacun de vérifier la validité de la chaîne.
- **Banque de France, (**ABC de l'Economie**)**
  - La Blockchain, ou chaîne de blocs, est une technologie de stockage et de transmission d'informations. Par extension, ce mot désigne une base de données numérique décentralisée. Souvent assimilée à un registre, cette base regroupe un historique de transactions électroniques.
- **Commission européenne**
  - La technologie Blockchain est un réseau qui stocke des blocs d'information qui sont identiques à travers le réseau. L'information stockée sur une Blockchain est partagée, vérifiable, publique et accessible.

Les preuves de la Blockchain

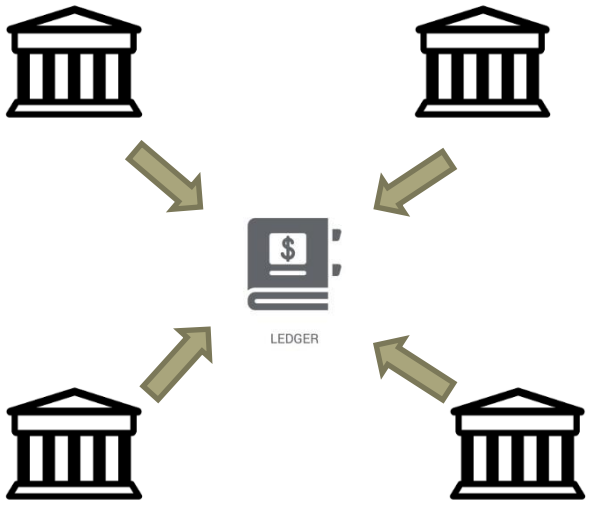
- *"The usage of a third-party Blockchain platform that is reliable without conflict of interests provides the legal ground for proving the intellectual infringement."* ***Hangzhou Internet Court (China)***

- *"Blockchain legislation pending or passed in at least 18 US states."* ***National Conference of State Legislatures***

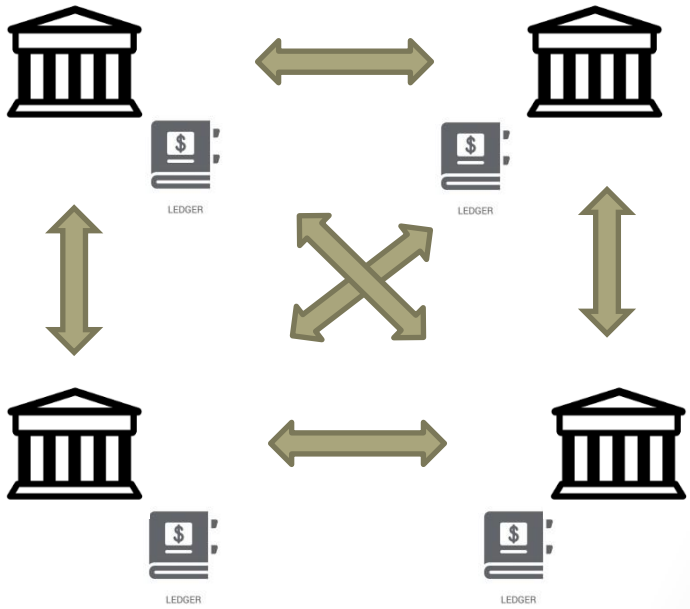
- *"A signature that is secured through Blockchain technology is considered to be in an electronic form and to be an electronic signature."* ***Arizona Bill HB2603***

Que est ce que c'est que la Blockchain?

- C'est une Distributed Ledger Technologie (DLT)
  - Livret comptable dont tous les membres détiennent une copie
  - Actualisé seulement après accord de tous les membres du réseau



Centralized Ledger



Distributed Ledger

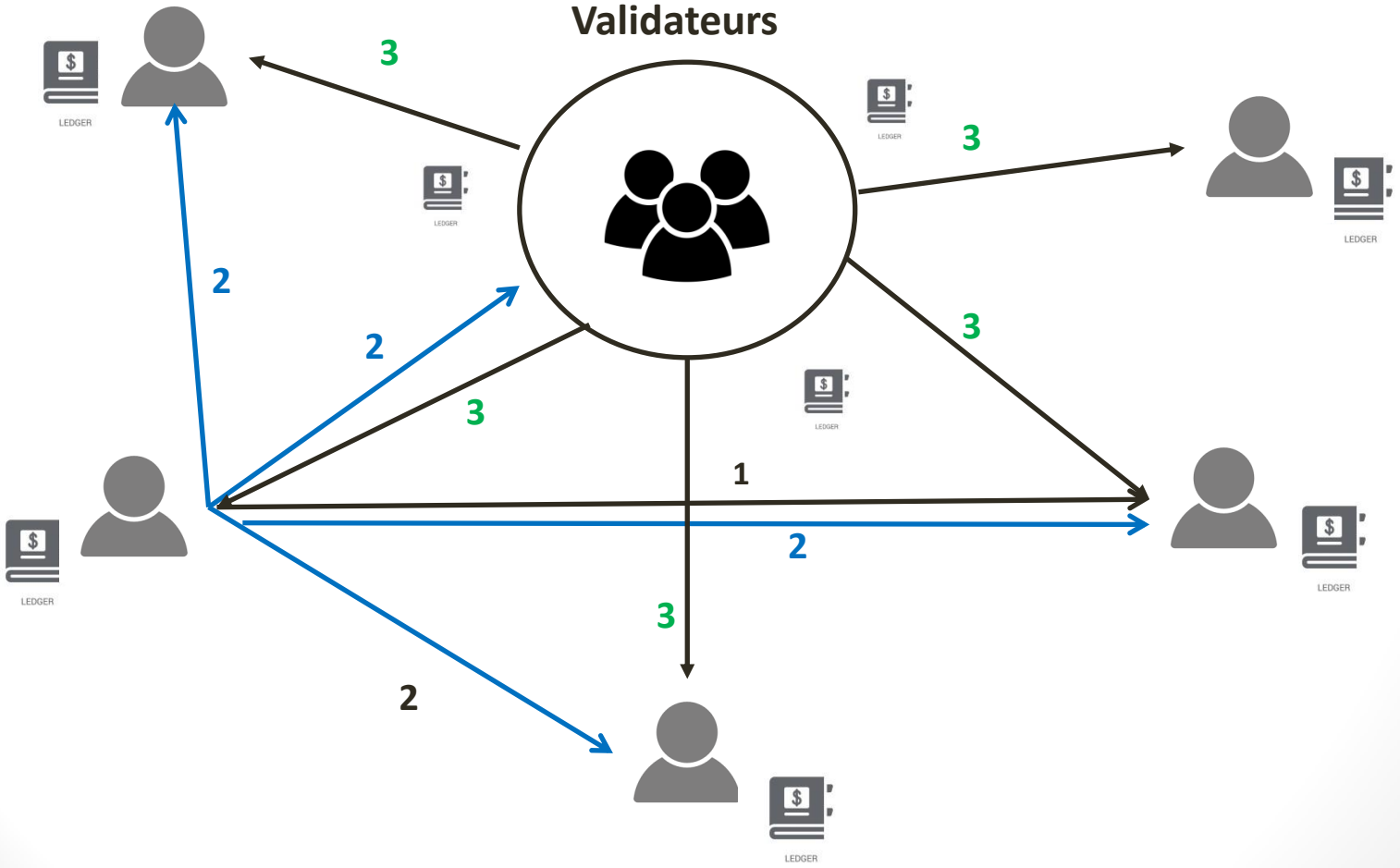
Que est ce que c'est que la Blockchain?

- Une infrastructure
  - Soutenue et gouverné par un réseau de pairs
- Un réseau
  - Sans architecture
  - Un réseau de pairs pseudo-anonyme
  - Dont la robustesse dépend de la grandeur du réseau
- Une Base de donnée
  - Distribué
  - Asymétrique
  - Accessible a tous

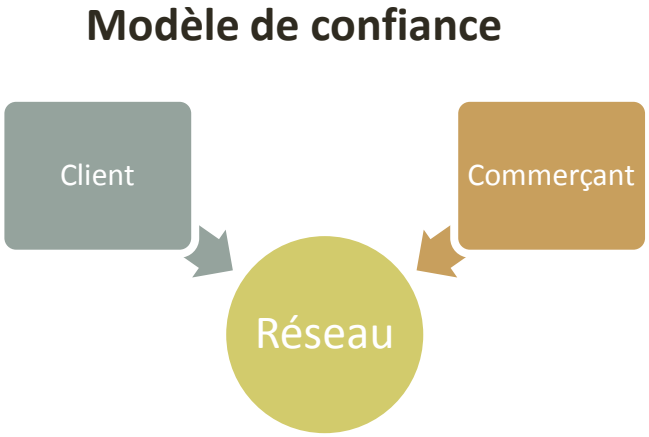
Que est ce que c'est que la Blockchain? (suite)

- C'est une sorte de livret comptable dont des informations ne peuvent être ajoutées sans l'accord des parties prenantes
  - Accessible à tous pour garantir la transparence des données
  - Avec une gouvernance démocratique
  - Aucune confidentialité
  - Assure un service d'intégrité et de non répudiation sur toutes données y contenus
- Complètement modulable

Transaction selon la Blockchain



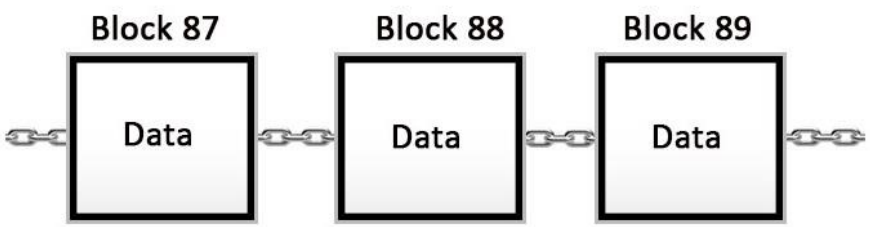
La Blockchain



- **Le réseau**
  - Assure la sécurité des transactions
  - Vérifie les comptes bancaires
- **Client et commerçant**
  - S'occupe de la gestion des propres identités
  - S'occupe de la gestion de son compte
  - S'occupe de la gestion de ses transactions

La chaine de blocs

- Une suite de Blocs liés les une au autres
  - A travers des algorithmes cryptographiques
  - Qui assure l'inviolabilité
- Les blocks sont:
  - Des conteneurs de transactions
  - Des structures de données qui dépendent de l'application qui s'y pose
    - Du consensus



Bloc: Structure Générale

<table>
<tr><td>Spécifique</td><td rowspan="5">Header</td><td rowspan="2">Dépendant de l’application et du consensus</td></tr>
<tr><td>Contrôle intégrité</td></tr>
<tr><td>Contrôle non répudiation</td></tr>
<tr><td>Consensus et preuves</td></tr>
<tr><td>horodatage</td><td rowspan="4">Commun</td></tr>
<tr><td>Transaction</td><td rowspan="3">Transactions</td></tr>
<tr><td>…</td></tr>
<tr><td>Transaction</td></tr>
</table>

Transactions

- Moyen de transport des échanges
  - Pièce fondamentale
  - Les échanges d'actifs dans le réseau sont effectués a travers les transactions.
- Structure
  - Informations sur le destinataire
  - Informations sur l'envoyeur
  - Quantité d'actif ou somme à transférer
- Accessibilité
  - Privée ou publique
- L'émission d'une transaction n'est pas forcement gratuit

Transactions

Structure générale

Emetteur	**Commun**
Destinateur	
Actif ou coin	Selon l'application
Données	

Le champs données contient des informations additifs qui dépendent de l'application

Database VS Blockchain

La Base de données

- Existait bien avant la Blockchain
  - A beaucoup évoluer dans ces dernières années
- Se base sur le principe CRUD
  - Create-Read-Update-Delete
  - Peut être modifié à tous moments par l'administrateur
  - Aucune assurance sur l'intégrité des données
- Utilise un organisation logique des données
  - Les données peuvent être facilement retrouvées
- Facile à mettre en place
  - Il existe beaucoup de compétences sur le sujet
- Largement utilisé

La Blockchain

- Assez récente (2008)
- Se base sur le principe append-only
  - On ne peut effacer aucune donnée
  - Les actualisations s'y ajoute sans effacer les données précédente
- Intégrité sur les données est garanti
  - Personne n'a le droit d'ajouter des données sans l'accord de la communauté.
- On ne peut pas y stocker toutes sortes de données
  - Seule les transactions sont stockées

La Blockchain

- Les donnée ne suivent pas un vrai organisation structuré
  - Le donnée sont insérer en ordre FIFO
  - Recherche difficile.
- Synchronisation lente
- Technologie encore méconnu

Projets combinés

- Certains projet exploite les deux technologie
  - La Base de donnée pour stocker les données
  - La Blockchain pour garantir l'intégrité sur la base de données et les données.
  - Ex: Hyperledger Fabric, ProvenDB

Classification

- On peut classer les Blockchains en fonction
  - De l'accessibilité à la Blockchain
  - La gouvernance
  - Des services

L’accessibilité

- Il existe trois types de Blockchain selon l’accessibilité
  - La Blockchain Publique
  - La Blockchain Privée
  - La Blockchain à permission

Blockchain privée ou publique

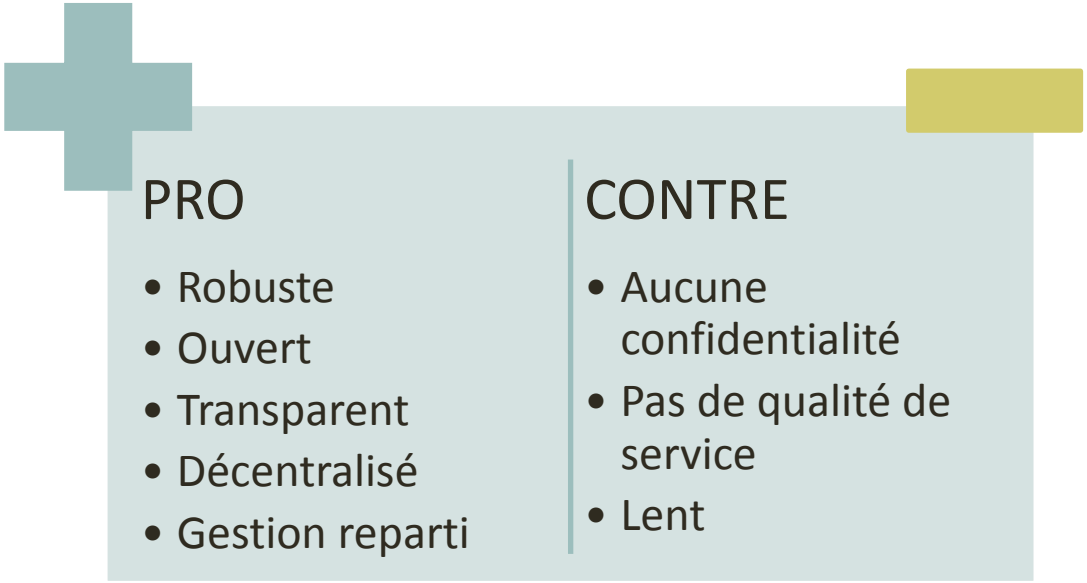
- La limite entre la Blockchain privée ou publique est encore controversé
- Selon Vitalik Buterin co-fondateur d'Ethereum:
  - Public Blockchain : "Public blockchain is a blockchain that anyone in the world can read, anyone in the world can send transactions to … and anyone in the world can participate in the consensus process…"
  - Fully private blockchains: "A fully private blockchain is a blockchain where write permissions are kept centralized to one organization. Read permissions may be public or restricted to an arbitrary extent …"

Blockchain publique

- La Blockchain est défini publique
  - Si tous le monde peut lire, écrire dans la Blockchain
  - Toutes les données présentes dans la Blockchain sont accessible à tous
  - Si tous ceux qui ont les moyens peuvent valider et ajouter des Blocks
  - Si le validateurs sont récompensés pour leurs tâche.

Blockchain publique

- La Blockchain publique s'adapte mieux
  - Ouvert
  - À un réseau dont la dimension et le nombre de nœuds sont inconnus
  - À des utilisateurs qui ne se connaissent et qui ne se font pas confiance.



Blockchain à permission

- Une Blockchain est définit à permission:
  - Si il existe une ou plusieurs autorités délivrant les droits d'accés, de lecture, d'écriture ou de validation.
- La Blockchain publique s'adapte mieux
  - À un environnement cloisonner
  - À un réseau de taille moyenne
  - À des utilisateurs qui ne sont connus
  - Aux collaborations entre entreprise (consortium)

Blockchain à permission

TELECOM ParisTech

PRO

- Rapide
- QoS
- Confidentialité (possible)

CONTRE

- Couteux
- Risque centralisation
- Ne passe pas à l'échelle

Blockchain Privée

- Une Blockchain est définit privée s'il existe une ou une élite d'entités qui détiennent de pouvoir absolu
  - de validation et d'écriture.
- La Blockchain publique s'adapte mieux
  - À un environnement cloisonner
  - À un réseau de petite ou à un réseau interne
  - À des utilisateurs qui sont connus

Blockchain Privée

PRO

- Rapide
- QoS
- Confidentialité (possible)

CONTRE

- Couteux
- Centralisé
- Ne passe pas à l'échelle

Gouvernance

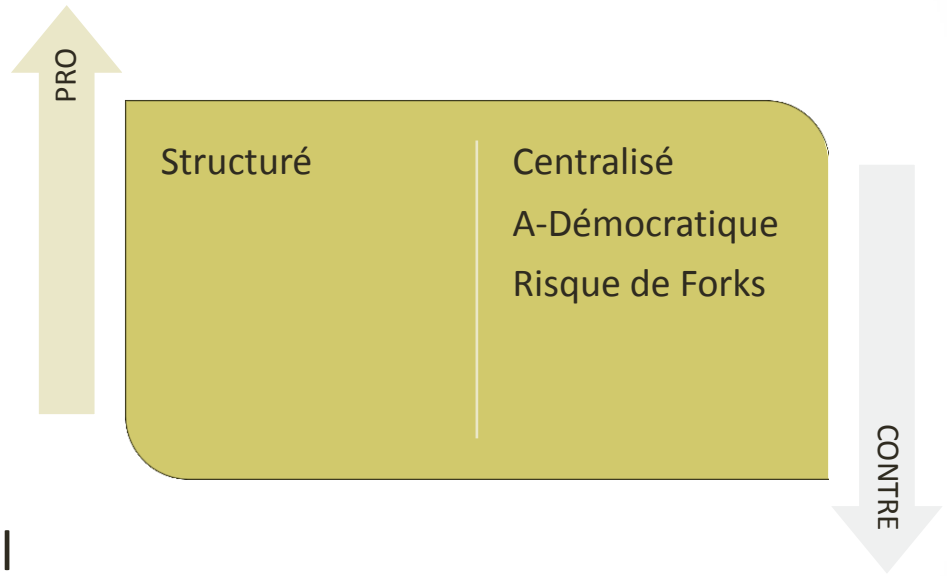
- Système traditionnel
  - Hiérarchique
  - Pouvoir détenu par une entité (une institution)
    - Une poignée de personnes
    - Qui soumettent et approuvent les lois

Gouvernance

- La Blockchain est sensé être gouverné démocratiquement (idéalement)
  - Par tous les utilisateur du réseau
  - sans un pouvoir centrale
- Deux types de gouvernance
  - On-chain
  - Off-chain

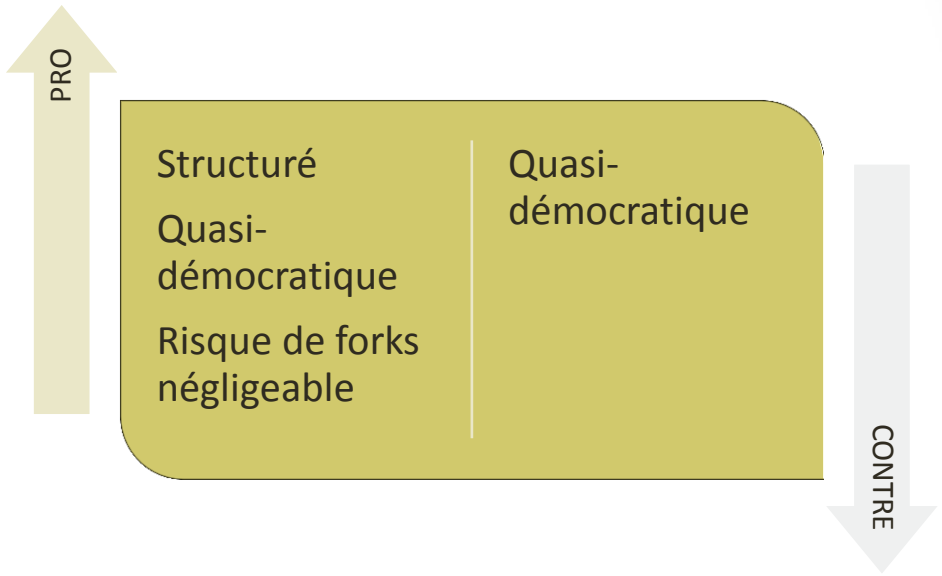
Gouvernance Off-chain

- Le pouvoir de modification ou changement des règles détenu par une ou une élite de personne
- Les décisions se prennent loin des réflecteurs
- Les membres de la communauté ont le seul pouvoir d'accepter ou de refuser

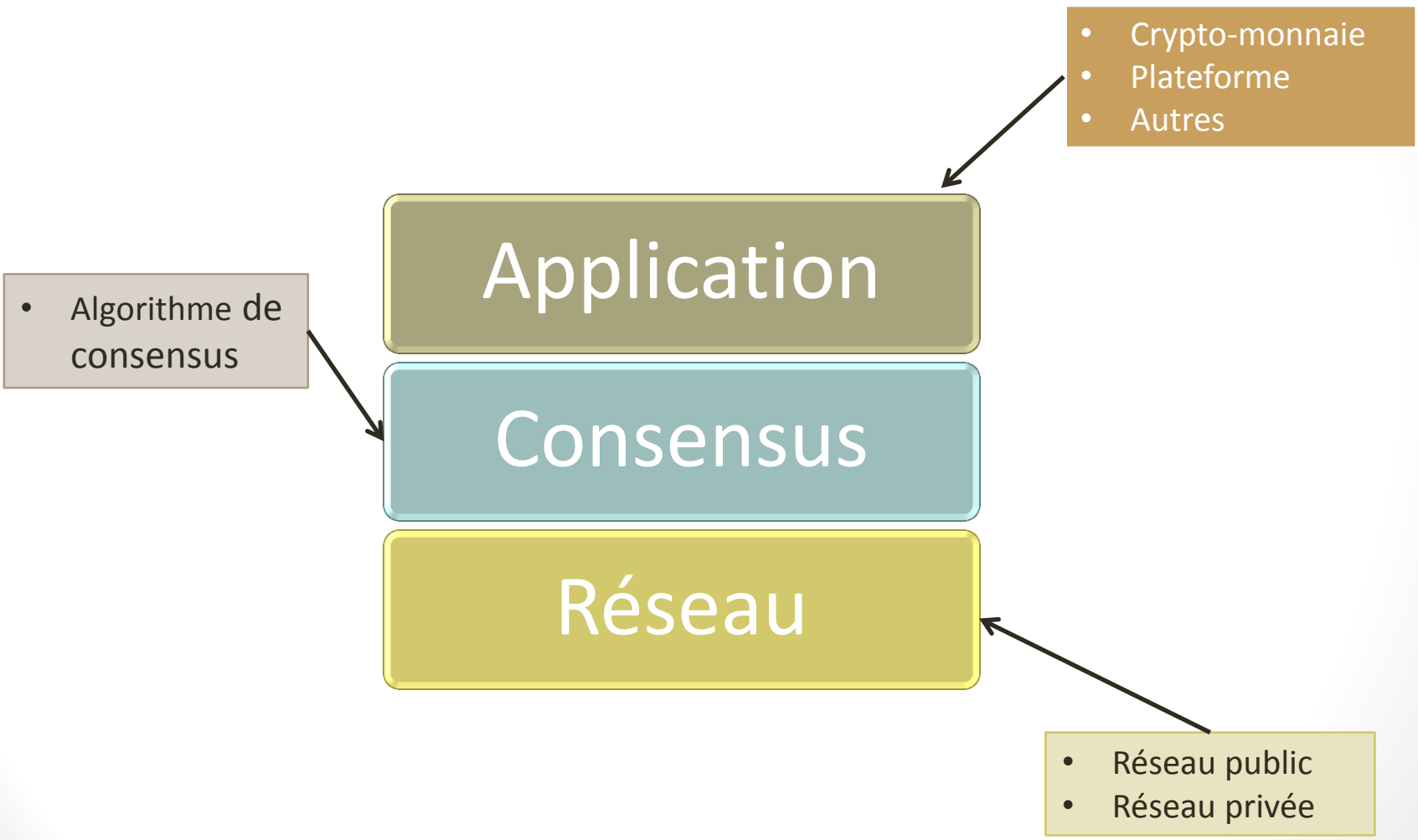


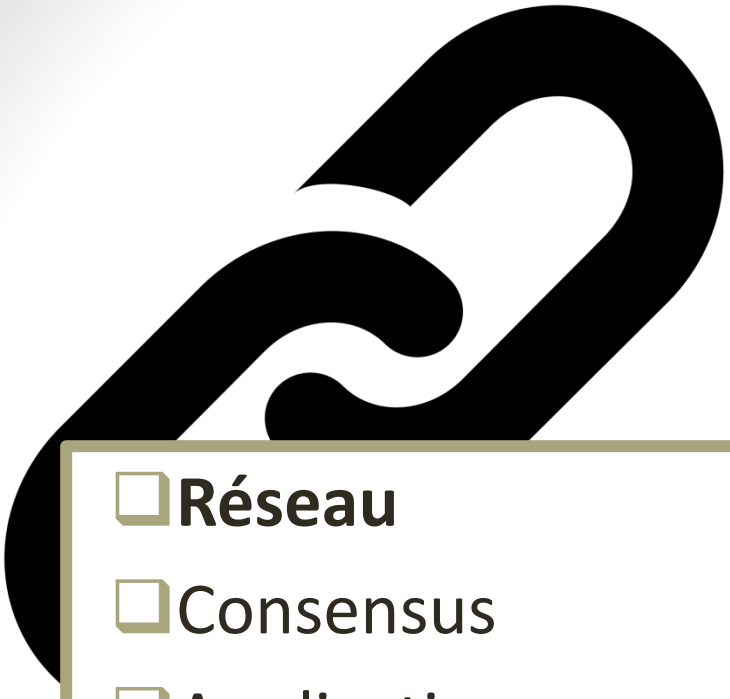
Gouvernance On-chain

- Proche du régime démocratique
- Tous le monde peut faire de suggestions ou des proposition
- Les décisions sur le protocole se prennent de manière transparente dans la Blockchain
- Les membres de la communauté ont le pouvoir d'accepter ou de refuser



Le stack de la Blockchain





- **Réseau**
- Consensus
- Application

Réseau Blockchain

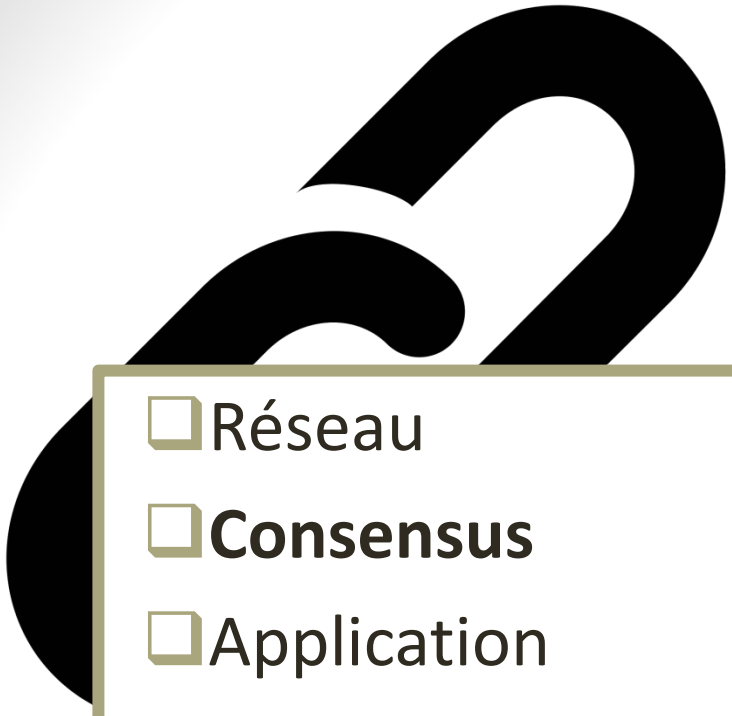
- La Blockchain s'appuie sur un réseau d'utilisateurs
- Les membres du réseau peuvent se connaitre ou non
  - En fonction type de Blockchain
  - Du type de consensus
- Le pairs communiquent au niveau transport à travers des connections TCP (la plupart du temps)
  - Fiable
  - Ordonné
  - Résistant au erreurs
  - Non sécurisé, pas de confidentialité
- Aucune authentification entre pair
  - Dans le cas des Blockchain publiques
- Difficile évaluer l'étendu du réseau

Deux types de nœuds

- **Deux grand groupes de nœuds**

  Tous Identifiés par une pair de clés

  - **Validateurs**: Les utilisateurs qui veillent au respect des normes du protocole et qui valident les blocs et transactions.
    - Quand rémunérés on les appellent (Mineurs)
    - Peuvent émettre des transactions
  - **Simple**: Les utilisateurs qui ne font que usage des services proposés par la Blockchain.



- Réseau
- **Consensus**
- Application

Le problème du consensus

- Comment plusieurs nœuds peuvent détenir des copies cohérentes de la Blockchain.
  - Des nœuds distants!
  - Des nœuds qui ne se font absolument pas confiance!
  - Des nœuds qui ne se connaissent pas
- Qui et quand peut-on ajouter un block à la chaine?
- Ce qui nous conduit problème des généraux byzantins!

Problème des généraux byzantins

- Definit par L. Lamport, R. shotak et M. Pease en 1982 « The byzantine Generals Problem »
  - Un système bien défini doit être capable de gérer les composants défaillants qui donne de fausses a différentes parties du système.
- Un exemple pour clarifier:
  - Des généraux byzantins, chacun avec son armée se trouvent autour d'une ville ennemie. La ville à de bonne défense donc pour gagner tous les généraux doivent attaquer ensemble. Les généraux ne peuvent communiquer que par des messagers.
    - Comment assurer une communication, sachant que certains généraux ont été corrompu par l'ennemi?
    - Les messagers peuvent être intercepté en route ou même être aussi corrompus?

Le consensus

- Les nœuds doivent trouver une manière de s'accorder même s'ils ne se font pas confiance.
- L'algorithme du consensus vas fortement dépendre du type privée ou publique.
- En effet il en existe plusieurs

Algorithmes de consensus

- **Proof-of-Work (Preuve de travail)**
  - Bitcoin, BitcoinCash, Ethereum, Litecoin, Monero, Zcash, etc.
- **Proof-of-Stake(PoS)**
  - Neo, Bitshares, Dash, Nxt etc.
- **Hybrid** (Proof-of-Work / Proof-of-Stake)
  - Peercoin
- **Pratical Byzantine Fault Tolerance (PBFT)**
  - Hyperledger, stellar, Ripple
- **Consensus propriétaire**
  - Iota, Hashgraph,

Proof-of-Work (PoW)

TELECOM ParisTech

❑ Que-est-ce que le proof of work?

- Aussi appelé preuve de travaille
- Pour pouvoir acquérir un droit, l'utilisateur doit travailler.
  - Fournir une preuve de son travail
- En générale le travaille est difficile à effectuer
  - Mais très facile à vérifier.
- La preuve de travaille est une solution couteuse et non écologique.
- Une sorte de meritocratie

PoW

En pratique …

- Le principe est de trouvé une solution à un problème cryptographique qui é difficile à trouver mais facile à vérifier.
- Il s'agit de calculer sur des données un hash dont la valeur serait inferieur à un seuil appelé Target

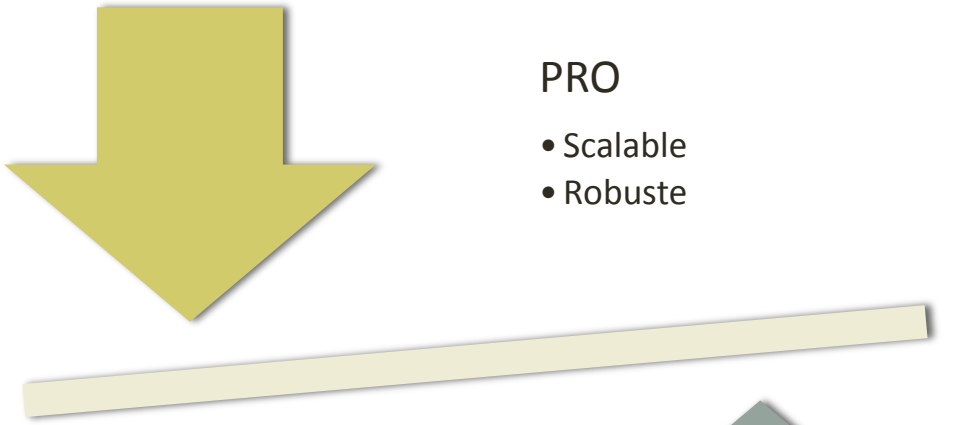
((hash)(data + Nonce))<Target

Data=Données

Hash=fonction de hachage générique

- Comment nous savons bien le hash est un entier aléatoire
  - Il faudrait plusieurs tentatives pour y arriver
- Le bon Nonce sera notre preuve de travail!

Proof-of-Work (PoW)



PRO

- Scalable
- Robuste

CONTRE

- Couteux
- Energivore
- Injuste envers les pauvres
- Lent

Proof-of-Stake (PoS)

❑ Qu'est-ce-que le Proof-of-Stake?

- Couramment appelé preuve d'enjeu
- Pour pouvoir acquérir un droit l'utilisateur doit avoir un capital enjeu.
  - Il faudra fournir une preuve d'enjeu
- Plus élevé est ton capital enjeu, plus de probabilité as-tu de valider
- C'est un concurrent du proof-of-work
- La version de base n'est quasi jamais utilisé, plutôt présent sur le marché sous plusieurs variantes
  - Proof of use (PoU)
  - Proof of hold (PoH)
  - Proof of stake/time (PoST) –(Coinage)
  - Proof o minimum aged stake (POMAS)
  - Delegated Proof of stake (DPOS) – Ethereum /Bitshares

Proof-of-Stake (PoS)

- Delegated Proof of stake (DPOS) – Ethereum (bientot) /Bitshares /EOS
  - La charge de la validation des blocks est au main d'un groupe de témoin
  - Chaque témoin valide à son tour dans un determiné timeslot
  - Les utilisateurs votent les temoins qui vont les representés
  - Le nombre de temoin indique le dégré de décentralisation

- Proof of Stake Velocity (PoSV) –Reddcoin
- Proof of Importance (POI) – NEM

Proof-of-Stake (PoS)

- **<u>En pratique …</u>**

- L'utilisateur doit toujours trouver un hash inferieur à un seuil dénommé Target, mais d'autre variable s'ajoutent à l'equation

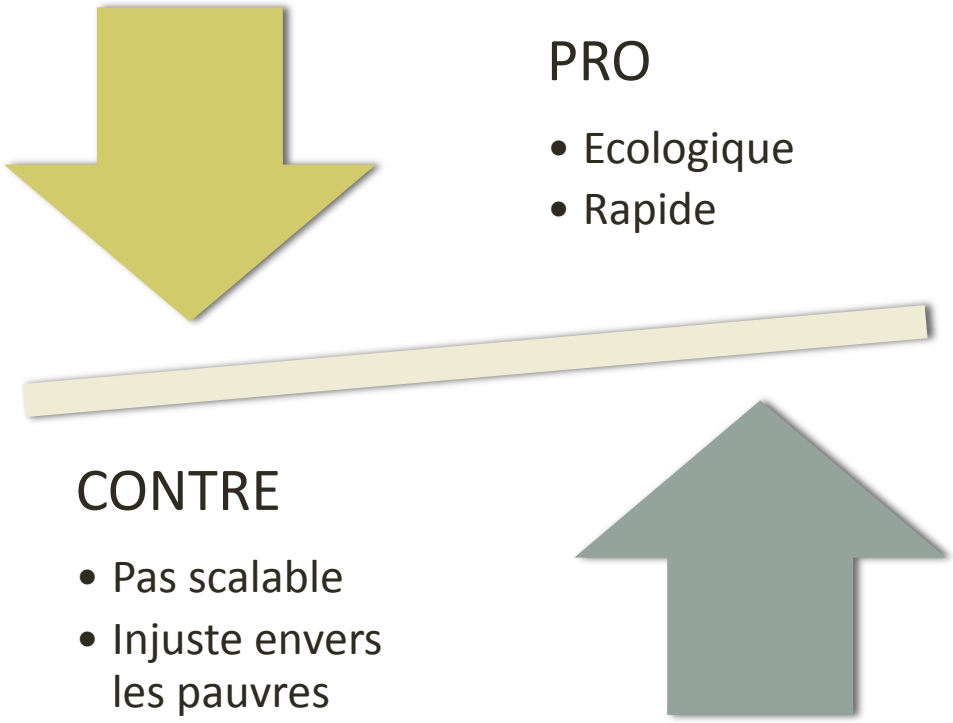
((hash)(data))<Target *α

Data=Données

Hash=fonction de hachage générique

α = Facteur déterminant les variantes

Proof-of-Stake (PoW)



PRO

- Ecologique
- Rapide

CONTRE

- Pas scalable
- Injuste envers les pauvres

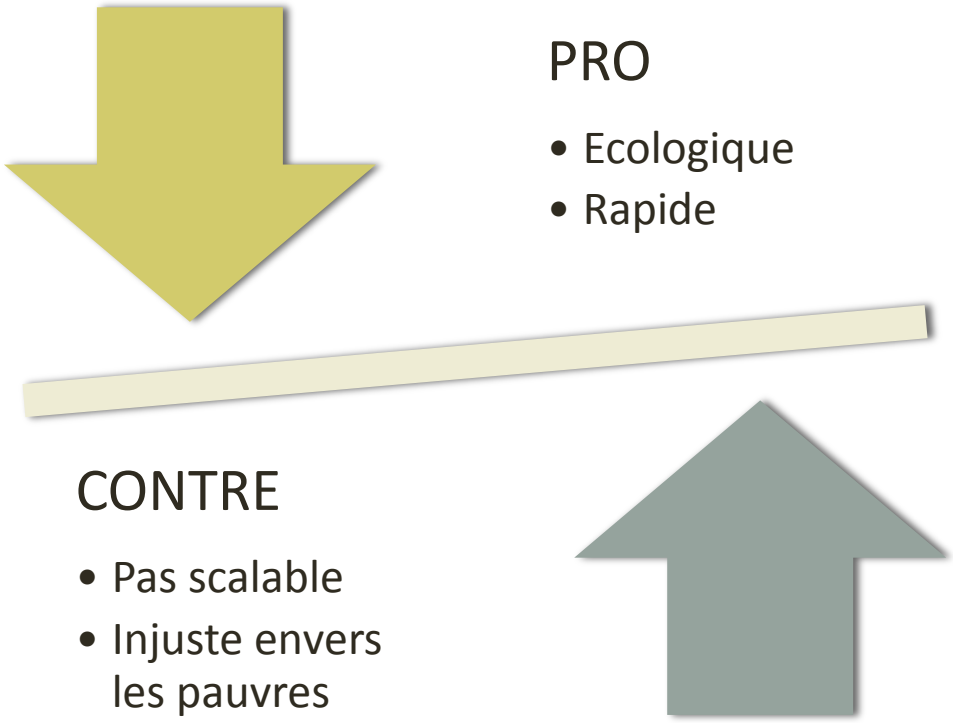
PoW Vs PoS (Resumé)

Criteres	PoW	PoS
Type de Blockchain	Orienté Blockchain publique	Orienté Blockchain Privée
Scalabilité	>100K	Efficacité inversement proportionnelle au nombre de nœuds
Compromis 51% attack	Déterminé selon la puissance de calcul des nœuds	Déterminé selon la quantité d'enjeu
Difficulté du minage	Directement proportionnelle à la quantité de mineur	N'est pas corrélé au nombre de mineur
Energie	Besoin de quantité d'énergie extraordinaire	Normal

Pratical Byzantine Fault Tolerance (PBFT)

- Idéalement conçu en 1998 pour faire face au pannes byzantine puis réadapté à la Blockchain.
- N'est pas distribué mains plutôt décentralisé
  - Le droit de ce voit attribuer à un certain nombre de nœud
  - Qui s'accordent pour en choisir leader
- Le PBFT se voit plus appliqué au Blockchain Privées ou à permission

PBFT

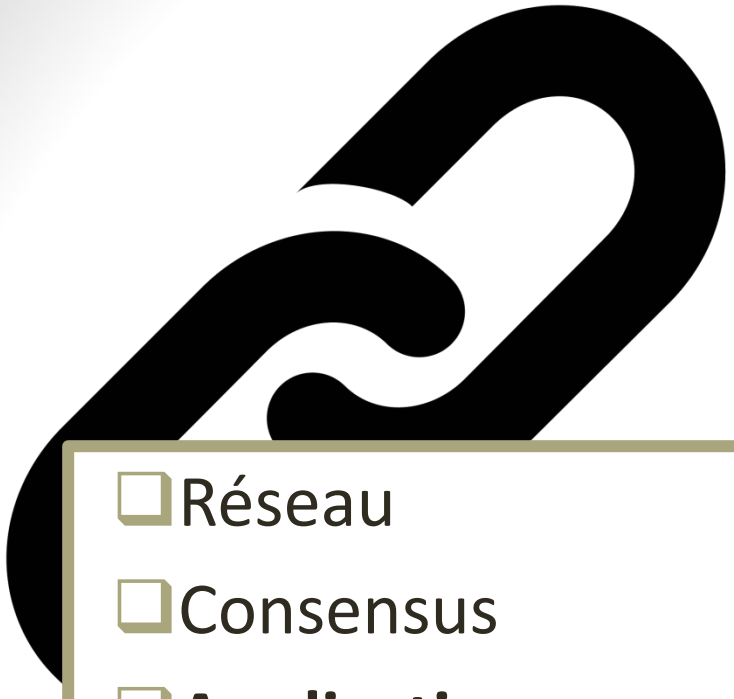


PRO

- Ecologique
- Rapide

CONTRE

- Pas scalable
- Injuste envers les pauvres



- Réseau
- Consensus
- **Application**

Applications

- **Deux grands groupes de Blockchains**
  - Blockchains orientés crypto-monnaies
    - Gestion des systèmes de paiement
  - Blockchains orientés smart-contract
    - Gestions des digital assets et smart properties

Blockchains orientés crypto-monnaies

- **Exploités pour:**
  - Crée des monnaies virtuelles
  - Des systèmes de paiement électroniques
  - Pour gérer des contrats élémentaux

Blockchains orientés crypto-monnaies

- **LINTERNAUTE**
  - La crypto-monnaie désigne une monnaie virtuelle intégrant l'utilisateur dans le processus de règlement des transactions qu'il effectue. La crypto-monnaie, et notamment le bitcoin, n'est pas une monnaie légale
- **WIKI**
  - Une cryptomonnaie, dite aussi cryptoactif, cryptodevise, monnaie cryptographique ou encore cybermonnaie est une monnaie émise de pair à pair, sans nécessité de banque centrale, utilisable au moyen d'un réseau informatique décentralisé. Elle utilise les principes de la cryptographie et associe l'utilisateur aux processus d'émission et de règlement des transactions
- **Le petit larousse**
  - Moyen de paiement virtuel, utilisable essentiellement sur Internet, s'appuyant sur la cryptographie pour sécuriser les transactions et la création d'unités et échappant à tout contrôle des régulateurs et des banques centrales.

Certains exemples

https://coinmarketcap.com/

Blockchains orientés smart-contract

- **Exploités pour:**
  - Fournir des plateformes pour l'exécution des smart-contracts
  - Pour la gestion des actifs et smart-properties

Blockchains orientés smart-contract

- **Smart-contract**

  “A smart contract is a computerized transaction protocol that executes the terms of a contract. The general objectives of smart contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitration and enforcement costs, and other transaction costs”. **Nick Szabo, 1994**

Blockchains orientés smart-contract

- **Smart-contract**
  - C'est une solution logiciel, utilisé pour exécuter les termes d'un contrat automatiquement, quand certaines conditions établie sont vérifiés.
  - Peut être aussi vu comme la dématérialisation du contrat papier

- **Pourquoi les smart-contracts sont utilisés?**
  - Principalement pour la gestions d'actifs digitaux (digital asset)
  - Pour la gestion des smart-properties

Blockchains orientés smart-contract

- **Smart property**

Smart property is property whose ownership is controlled via the Bitcoin blockchain, using contracts. Examples could include physical property such as cars, phones or houses. Smart property also includes non-physical property like shares in a company or access rights to a remote computer. ***(Bitcoin Wiki)***

- **Pourquoi est-il utile rendre smart une propriété privée?**
  - Pour faciliter la vente ou la location en toute sécurité
  - Pour réduire les intermédiaires et les couts de transactions

Blockchains orientés smart-contract

- **Examples**
  - Louer sa maison à des inconnus sans passer par Airbnb
  - Louer sa voiture sans passer par Drivy ou Ouicar ou etc.
  - Vendre des objets entre particulier sans passer par Ebay
  - Ecc.

Blockchains orientés smart-contract

- **Digital Asset**

A digital asset, in essence, is anything that exists in a binary format and comes with the right to use. Data that do not possess that right are not considered assets. Digital assets include but are not exclusive to: digital documents, audible content, motion picture, and other relevant digital data that are currently in circulation or are, or will be stored on digital appliances such as: personal computers, laptops, portable media players, tablets, storage devices, telecommunication devices, and any and all apparatuses which are, or will be in existence once technology progresses to accommodate for the conception of new modalities which would be able to carry digital assets. (Wikipedia)

Blockchains orientés smart-contract

- **Pourquoi gérer un actif sur la Blockchain?**
  - Pour assurer la paternité.
  - Pour résoudre les litiges.
  - Pour vendre et louer se passant des intermédiaires.
  - Pour le stocker en toute sécurité
  - Ecc.

Plateforme pour smart-contract

Assurance

FIZZY

- Il propose à ses souscripteurs d'être indemnisés directement et automatiquement en cas de retard de leur vol. Si votre avion a plus de deux heures de retard ou à été annulé, fizzy vous rembourse automatiquement.
  - Se base sur la Blockchain d'Ethereum

Processus électoral

- **2018**: La Sierra Leone devient le premier pays à utiliser la Blockchain dans son processus électoral.
  - Blockchain de type à permission développé par l'entreprise suisse Agora
  - Objectifs:
    - Donner de la transparence aux données
    - Empêcher la modification non autorisé
    - Avoir les résultats en temps réel

Gestion d'identité

- IBM Blockchain Trusted Identity
  - Gestion d'identité à travers la blockchain

- Blockchain orienté à la gestion d'dentité.

- Civic est une compagnie qui offre un système permettant au utilisateur d'avoir le contrôle sur les informations personnels partagées

Chaine de distribution

- Carrefour lance sa Blockchain pour garantir au consommateur la traçabilité de ses produits

- Alipay en collaboration avec la ville la ville chinoise de Wuchang utilise la Blockchain pour assurer la traçabilité de son riz « premium »

Chaine de distribution

2017: Nestlé, Unilever, Walmart, Dole, Driscoll's, Golden State Foods, Kroger, McCormick and Company, McLane Company et Tyson Foods décident de s'appuyer sur la Blockchain pour travailler sur la traçabilité des denrées périssables.

Objectifs:

- Cibler le conditionnement et le mouvement des denrées alimentaires périssables.
- Accélérer l'accès à des informations fiables.
- Plateforme visée: Hyperledger Fabric et composer d'IBM

Droit d'Auteur et droits patrimoniaux

MONEGRAPH

- Système basée Blockchain pour assurer a paternité d'une œuvre en cas de litige

https://monegraph.com/

- Système basée Blockchain pour certifiée l'authenticité d'un diplôme

https://www.bcdiploma.com/

Energie

- Electric-chain est une Blockchain pour tracer en temps réel la production de 7 million de panneaux solaires
- SolarCOIN à été crée pour récompenser les producteurs d'energie Verte
- 2016: Le Français lumo rejoint le réseau

Audio

- AudioCoin est une cryptomonnaie comme Bitcoin, qui s'acquiert par l'achat ou le partage d'une œuvre musicale.

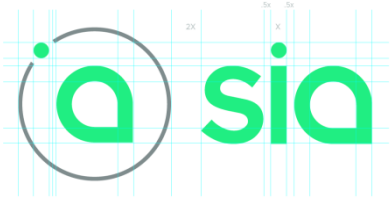
- Start-up basée Blockchain, rachetée par Spotify pour donner plus de transparence rétribution des revenus qui découlent de l'exploitation de certains titres sur leur plateforme.

- Plateforme d'echange sans intermédiaire entre artistes et consommateur.

Stockage

- Réseau d'échange, de partage et de vente d'espace de stockage entre utilisateur;

https://storj.io/



- https://sia.tech/

- https://filecoin.io/

Vidéo

- Plateforme de production et distribution d’œuvre artistique visuel.

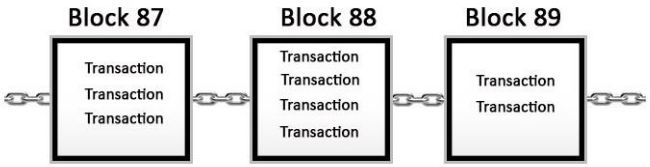
Colored Coin

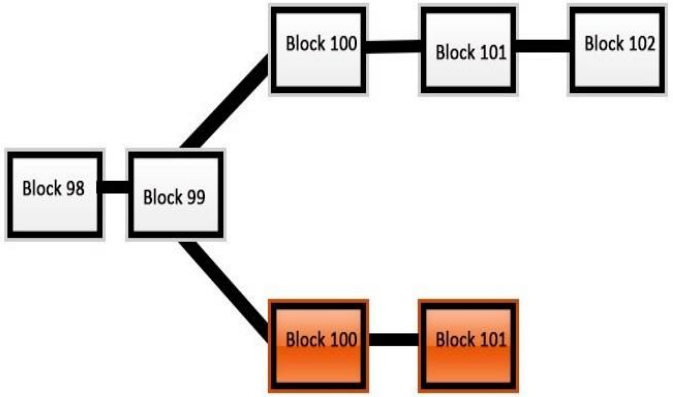
- **Gestion d'actifs**
  - CoinSpark, OpenAssets, Omni Layer, CounterParty
- **Gestion de droits Patrimoniaux**
  - Proof of existence, Stampery, Blocksign, BitProof, Diploma, LaPreuve, Stampd, etc
- **Gestion droits d'auteur**
  - Monegraph, Ascribe, Blockai, etc
- **Applications à venir**…

LA FORK

La Fork

- Division de la Blockchain en deux branches





- Conséquences directe d'un désaccord dans la communauté régissant la Blockchain.
  - Suite à un changement de règles dans le protocole
- Conséquence d'une attaque

La Fork

- La Fork Conséquence d'un désaccord
  - Suite à un changement ou maintien de règles non partagées.
  - Suite à une modification logiciel.
- La Fork conséquence d'une attaque
  - Suite à l'action d'un utilisateur malveillant
- Deux types de fork
  - Soft Fork
  - Hard Fork

- La fork exprime l'indépendance des utilisateurs

La Fork

- Soft Fork
  - Changement de règles mineur dans la politique de la crypto-monnaie
    - Segwit, Bomb factor
- Hard Fork
  - Changement majeur
    - Tel que la dimension des blocks
    - Le type de consensus
    - Peut provoquer la division du réseau

Hard Fork

- Presque toujours une hard fork conduit à la création d'une nouvelle crypto-monnaie.

- Les deux cryptos résultantes peuvent partager le même historique
  - BitcoinCash, BitcoinGold, Ethereum Classic
- Les deux cryptos résultantes peuvent ne pas partager le même historique
  - Litecoin, dogecoin, etc

Evolution Blockchain

- **Blockchain 1.0**
  - Bitcoin, Litecoin, Namecoin
- **Blockchain 2.0**
  - Ethereum
  - Hyperledger
- **Blockchain 3.0**
  - Iota, Hashgraph

Blockchain ICO

- La plus part des nouvelles Cryptocurrency débute par un Initial Coin Offering (ICO)
  - Comme l'IPO mais spécifique à la crypto-monnaie.
  - Aucune part du projet n'est mis en jeu
  - L'ICO peut débuté sous présentation d'un simple « whitepaper »
- Une quantité de monnaie (Token) est pré-miné et distribué
  - Avec l'ambition que le projet prendra valeur

Blockchain ICO

- Différemment des IPOs
  - Les start-Ups n'ont pour le moment aucune obligation légale
    - Ne sont pas régulé
  - Se fait en ligne et tous le monde peut y participer
    - Il suffit d'etre en possession d'une crypto monnaie (Ether, Bitcoin)
    - Se fait avant la mise en marché du projet
  - Appelé aussi crowd-sales

ICO

- Toutes une liste de ICO ouvertes sur https://www.coinschedule.com/
- C’est un marché colossal

Historique ICO

- **Tezos** é l'ICO ayant levé plus d'argent
  - Une somme de 232 millions de dollars.
  - Tezos une ambitieuse plateforme pour les contrats intelligent comme Ethereum.
- **EOS** à levé à l'ICO 200 millions de dollars
  - ICO encore en cours
- **Storj** est un service de stockage cloud décentralisé
  - Elle possède une monnaie appelé Storjcoin
  - Storjcoin à levé 30 millions

Questions ?

Elloh.adja@telecom-paristech.fr

Notes bibliographiques

- http://solidity.readthedocs.io/en/develop/assembly.html
- A Survey on Security and Privacy Issues of Bitcoin, Mauro Conti, Senior Member, IEEE, Sandeep Kumar E, Member, IEEE, Chhagan Lal, Member, IEEE, Sushmita Ruj, Senior Member, IEE
- https://www.developpez.com/actu/194082/La-Sierra-Leone-devient-le-premier-pays-a-s-appuyer-sur-la-blockchain-dans-son-processus-electoral-technologie-developpee-par-le-Suisse-Agora/
- https://www.developpez.com/actu/156443/Blockchain-Nestle-Unilever-et-d-autres-grands-noms-du-secteur-agroalimentaire-se-tournent-vers-IBM-pour-la-tracabilite-des-denrees-perissables/
- https://www.businessinsider.fr/sierra-leone-premier-pays-voter-blockchain/