Introduction à la Technologie Blockchain

Eugène C. Ezin[1] & Nelson Saho[2]

[1]Institut de Formation et de Recherche en Informatique
& Institut de Mathématiques et de Sciences Physiques
[2]Doctorant en Sciences de l'Ingérieur
Université d'Abomey-Calavi

Contenu

Contenu

Historique

- En 1991, Stuart Haber et Scott Stometta ont mis en application un système où les documents horodatés ne pouvaient être falsifiés ou antidatés. Ce qui a conduit à la première étude sur les chaines de blocs.

Historique

- En 1991, Stuart Haber et Scott Stometta ont mis en application un système où les documents horodatés ne pouvaient être falsifiés ou antidatés. Ce qui a conduit à la première étude sur les chaines de blocs.
- En 1992, Bayer, Haber et Stometta ont incorporé le concept d'arbre de Merkle au système pour amélioration dans le souci d'avoir d'avoir plusieurs documents en un seul bloc.

Historique

- En 1991, Stuart Haber et Scott Stometta ont mis en application un système où les documents horodatés ne pouvaient être falsifiés ou antidatés. Ce qui a conduit à la première étude sur les chaines de blocs.
- En 1992, Bayer, Haber et Stometta ont incorporé le concept d'arbre de Merkle au système pour amélioration dans le souci d'avoir d'avoir plusieurs documents en un seul bloc.
- En 2008, Satoshi Nakamoto a conceptualisé la première chaine de bloc et l'a implémenté en 2009 - d'où le bitcoin - première monnaie virtuelle.

Définition

Définition

Il s'agit d'une technologie de stockage et de transmission d'information sans organe de contrôle. Il s'agit donc d'une base de données distribuée dont les informations envoyées par les utilisateurs et les liens internes à la base sont vérifiés et groupés à intervalle de temps régulier en des blocs liés formant ainsi une chaine. Source wikipedia.

Base de données distribuée

Définition

Une base de données distribuée est une base de données dont la gestion est traitée par un réseau d'ordinateurs interconnectés qui stockent des données de manière ditribuée i.e. les données ne se trouvent pas sur la même machine. Source Wikipedia

Les différents modes de stockage des données sont:

- Le stockage peut être partitionné entre différents noeuds du réseau

Base de données distribuée

Définition

Une base de données distribuée est une base de données dont la gestion est traitée par un réseau d'ordinateurs interconnectés qui stockent des données de manière ditribuée i.e. les données ne se trouvent pas sur la même machine. Source Wikipedia

Les différents modes de stockage des données sont:

- Le stockage peut être partitionné entre différents noeuds du réseau
- Le stockage peut être répliqué entièrement sur chacun des noeuds

Base de données distribuée

Définition

Une base de données distribuée est une base de données dont la gestion est traitée par un réseau d'ordinateurs interconnectés qui stockent des données de manière ditribuée i.e. les données ne se trouvent pas sur la même machine. Source Wikipedia

Les différents modes de stockage des données sont:

- Le stockage peut être partitionné entre différents noeuds du réseau
- Le stockage peut être répliqué entièrement sur chacun des noeuds
- Le stockage peut être organisé de façon hybride.

Schéma d'une base de données distribuée

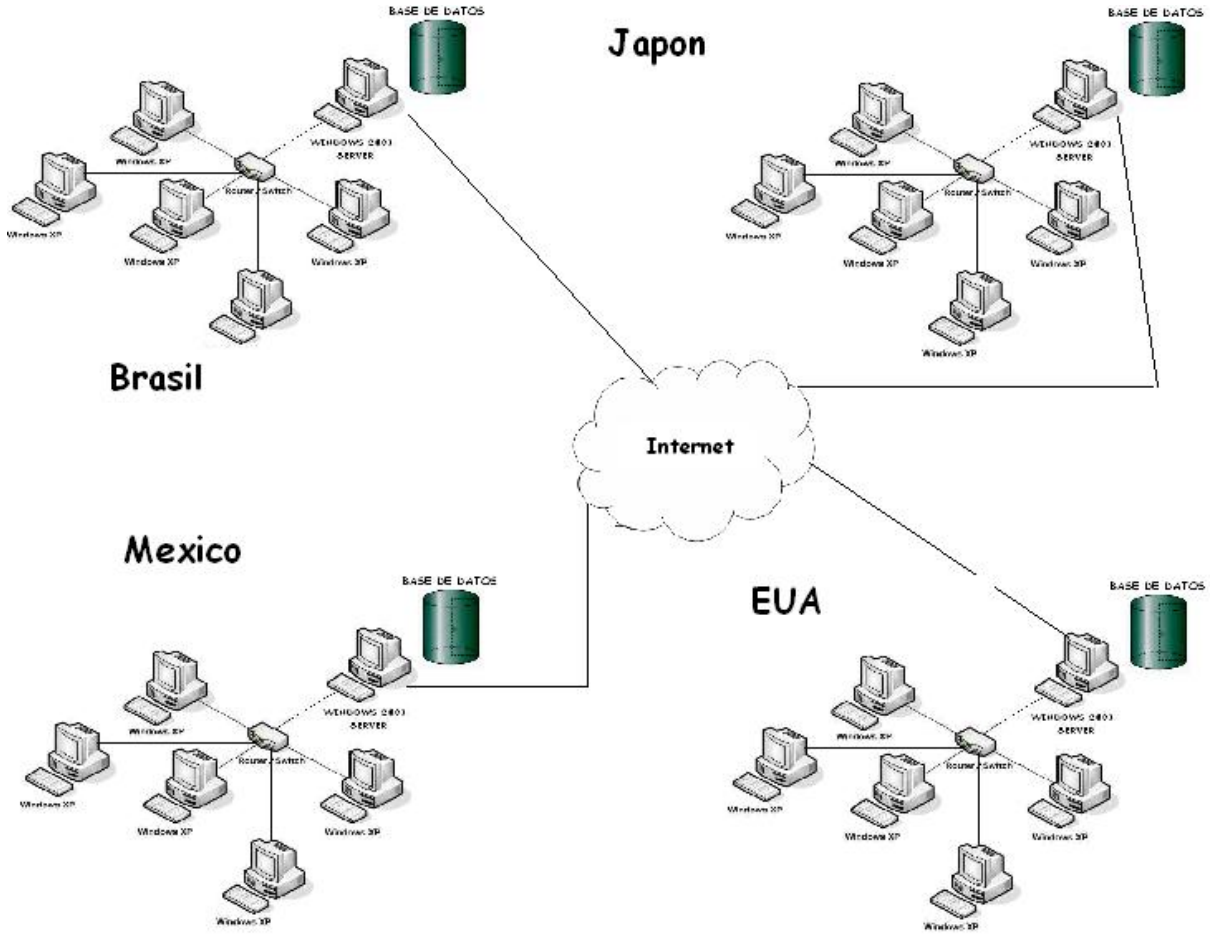


Figure: Schéma d'une base de données distibuée.

Blockchain : réseau P2P

- La chaîne de blocs est un réseau P2P dans lequel tous les noeuds sont égaux entre eux donnant comme résultat un système distribué.

Blockchain : réseau P2P

- La chaîne de blocs est un réseau P2P dans lequel tous les noeuds sont égaux entre eux donnant comme résultat un système distribué.
- La blockchain est un réseau P2P qui résiste aux attaques informatiques, des fautes ou des falsifications.

Blockchain : réseau P2P

- La chaîne de blocs est un réseau P2P dans lequel tous les noeuds sont égaux entre eux donnant comme résultat un système distribué.
- La blockchain est un réseau P2P qui résiste aux attaques informatiques, des fautes ou des falsifications.
- Dans la blockchain, même si un noeud manque, on peut se rendre à ces autres qui sont connectés par des voies alternatives. Ce qui n'est pas possible dans un système décentralisé.

Blockchain : réseau P2P - illustration

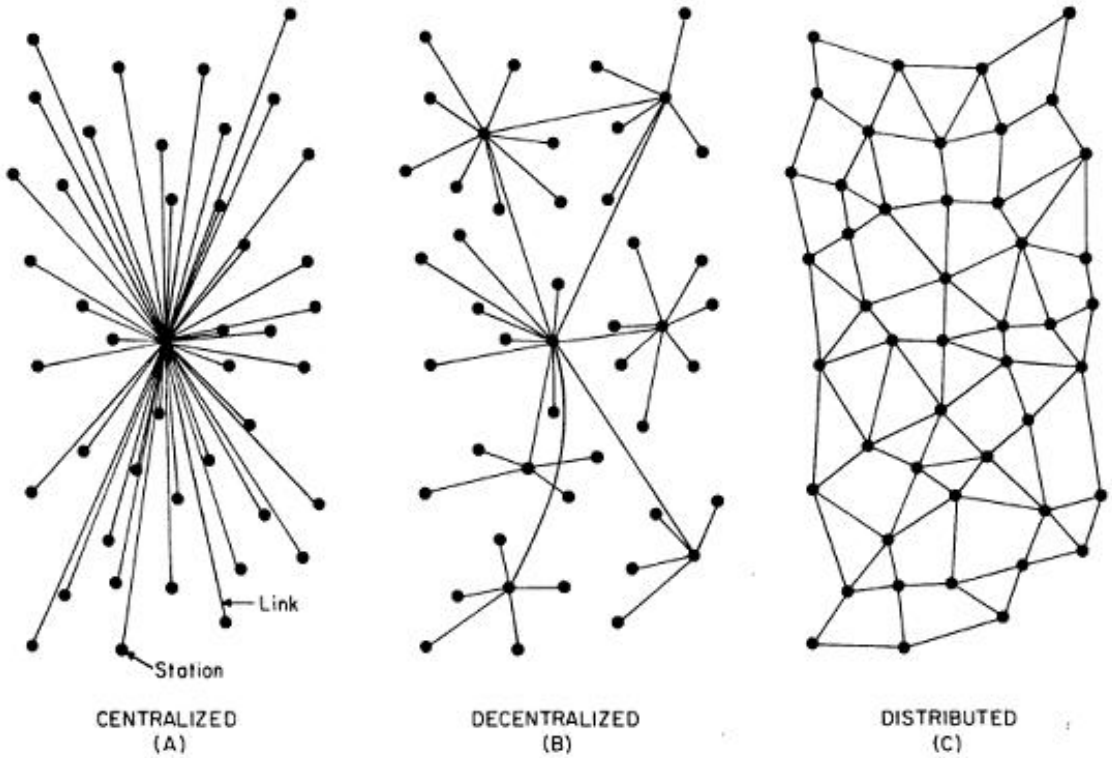


Figure: Comparaison des architectures centralisées - décentralisées et distribuées

Contenu

Propriétés de la Blockchain

Les trois propriétés de la blockchain sont:

- la désintermédiation ou la tansparence;

Propriétés de la Blockchain

Les trois propriétés de la blockchain sont:

- la désintermédiation ou la tansparence;
- la sécurité dont l'horodatage;

Propriétés de la Blockchain

Les trois propriétés de la blockchain sont:

- la désintermédiation ou la tansparence;
- la sécurité dont l'horodatage;
- l'autonomie.

La désintermédiation

Définition

La désintermédiation dans les blockchains est la suppression du rôle des intermédiaires au profit des communications directes entre un client et un fournisseur.

- Les transactions permettent un paiement sans tiers de confiance

La désintermédiation

Définition

La désintermédiation dans les blockchains est la suppression du rôle des intermédiaires au profit des communications directes entre un client et un fournisseur.

- Les transactions permettent un paiement sans tiers de confiance
- La monnaie est créée sans autorité de contrôle.

La sécurité

Définition

La sécurité dans les blockchains est la combinaison entre consensus et immutabilité.

- Les transactions sont infalsiafiables

[1]La double-dépense consiste à émettre deux transactions qui dépensnet le même avoir: la première transaction est émise pour payer un premier destinataire, la seconde trasaction est émise pour payer un complice ou le pirate lui-même, afin de récupérer la somme dépensée.

La sécurité

Définition

La sécurité dans les blockchains est la combinaison entre consensus et immutabilité.

- Les transactions sont infalsiafiables
- Le système est protégé contre la fraude de la double-dépense[1]

[1] La double-dépense consiste à émettre deux transactions qui dépensnet le même avoir: la première transaction est émise pour payer un premier destinataire, la seconde trasaction est émise pour payer un complice ou le pirate lui-même, afin de récupérer la somme dépensée.

Illustration de la double-dépense

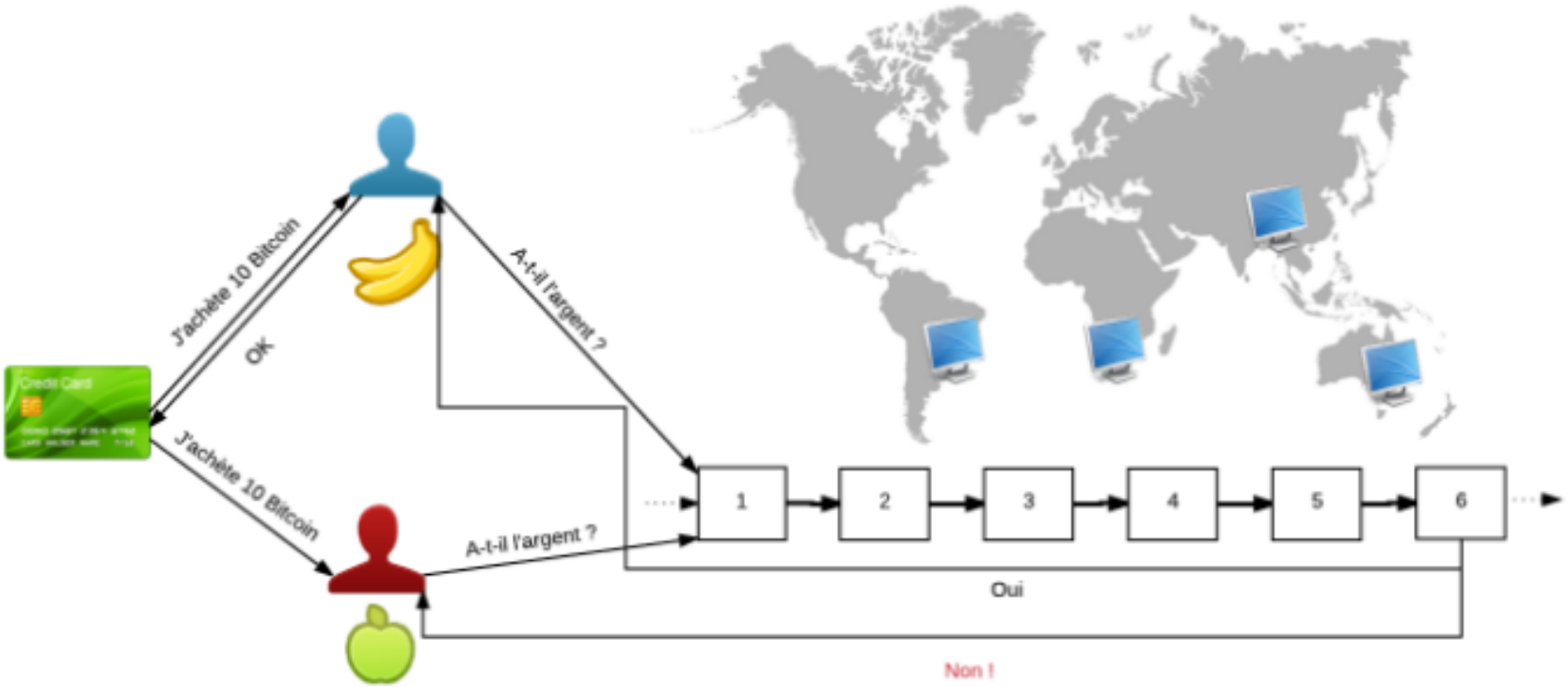


Figure: Un exemple pour illustrer la double-dépense.

L'autonomie

Définition

L'autonomie dans les blockchains se traduit par le fait que chaque noeud est à la fois un client et un serveur c'est à dire la puissance de calcul et l'espace d'hébergement sont fournis par les noeuds du réseau eux-mêmes.

- Le réseau pair à pair utilisé par les blockchains vise à s'affranchir d'un tiers de confiance pour les paiements.

L'autonomie

Définition

L'autonomie dans les blockchains se traduit par le fait que chaque noeud est à la fois un client et un serveur c'est à dire la puissance de calcul et l'espace d'hébergement sont fournis par les noeuds du réseau eux-mêmes.

- Le réseau pair à pair utilisé par les blockchains vise à s'affranchir d'un tiers de confiance pour les paiements.
- Tous les participants du réseau ont le même statut: aucun participant ne peut se prévaloir d'une quelconque légitimité supérieur i.e. chaque participant est considéré comme un pair vis à vis des autres.

Les objectifs de la blockchain

Les choix de conception de la blockchain visent à répondre aux exigences suivantes :

- Les transactions enregistrées sont irréversibles, on ne peut les effacer du registre.

Les objectifs de la blockchain

Les choix de conception de la blockchain visent à répondre aux exigences suivantes :

- Les transactions enregistrées sont irréversibles, on ne peut les effacer du registre.
- Les transactions sont infalsifiables.

Les objectifs de la blockchain

Les choix de conception de la blockchain visent à répondre aux exigences suivantes :

- Les transactions enregistrées sont irréversibles, on ne peut les effacer du registre.
- Les transactions sont infalsifiables.
- Les transactions permettent un paiement sans tiers de confiance.

Les objectifs de la blockchain

Les choix de conception de la blockchain visent à répondre aux exigences suivantes :

- Les transactions enregistrées sont irréversibles, on ne peut les effacer du registre.
- Les transactions sont infalsifiables.
- Les transactions permettent un paiement sans tiers de confiance.
- La monnaie est créée sans autorité de contrôle.

Les objectifs de la blockchain

Les choix de conception de la blockchain visent à répondre aux exigences suivantes :

- Les transactions enregistrées sont irréversibles, on ne peut les effacer du registre.
- Les transactions sont infalsifiables.
- Les transactions permettent un paiement sans tiers de confiance.
- La monnaie est créée sans autorité de contrôle.
- Les transactions sont publiques et vérifiables par tous, mais sont anonymes.

Les objectifs de la blockchain

Les choix de conception de la blockchain visent à répondre aux exigences suivantes :

- Les transactions enregistrées sont irréversibles, on ne peut les effacer du registre.
- Les transactions sont infalsifiables.
- Les transactions permettent un paiement sans tiers de confiance.
- La monnaie est créée sans autorité de contrôle.
- Les transactions sont publiques et vérifiables par tous, mais sont anonymes.
- Le système est protégé contre la fraude de la double-dépense.

Les objectifs de la blockchain

Les choix de conception de la blockchain visent à répondre aux exigences suivantes :

- Les transactions enregistrées sont irréversibles, on ne peut les effacer du registre.
- Les transactions sont infalsifiables.
- Les transactions permettent un paiement sans tiers de confiance.
- La monnaie est créée sans autorité de contrôle.
- Les transactions sont publiques et vérifiables par tous, mais sont anonymes.
- Le système est protégé contre la fraude de la double-dépense.
- Le système vise le commerce électronique sur internet.

Contenu

Vocabulaire des blockchains

Bitcoin

Le Bitcoin est un système de monnaie électronique entièrement de personne à personne permettant d'effectuer des paiements en ligne sans passer par une institution financière.

- Bitcoin est la première application développée sur une blockchain et, à ce jour, la plus massive.
- Le bitcoin est un logiciel open-source dont le code est visible et modifiable par tous.

Vocabulaire des blockchains

Mining

Le mining (minage en français), est l'action de validation des informations inscrites sur une blockchain. C'est aussi l'acte de création monétaire.

Vocabulaire des blockchains

Mining

Le mining (minage en français), est l'action de validation des informations inscrites sur une blockchain. C'est aussi l'acte de création monétaire.

D'après cette définition deux points caratérisent le mining:

- Le minage est l'activité de résolution de problèmes cryptographiques qui permettent la validation des blocs. Effectué par certains noeuds du réseau, c'est l'instrument qui remplace la vérification d'un office unique par un travail décentralisé. Cette opération collective produit un consensus sur la validité ou non d'une transaction.

Vocabulaire des blockchains

Mining

Le mining (minage en français), est l'action de validation des informations inscrites sur une blockchain. C'est aussi l'acte de création monétaire.

D'après cette définition deux points caratérisent le mining:

- Le minage est l'activité de résolution de problèmes cryptographiques qui permettent la validation des blocs. Effectué par certains noeuds du réseau, c'est l'instrument qui remplace la vérification d'un office unique par un travail décentralisé. Cette opération collective produit un consensus sur la validité ou non d'une transaction.

- Chaque validation est rémunérée par quelques milli-centimes de crypto-monnaie : c'est le mécanisme de création monétaire des cryptomonnaies sur une blockchain.

Vocabulaire des blockchains (suite)

Miner

Un miner (mineur en français) est un noeud du réseau qui valide les transactions et alimente la puissance de calcul de la blockchain. C'est un noeud du réseau qui opère la validation des transactions à la place d'u'ne instance centrale.

- Les miners peuvent être des individus ou des organisations qui apportent le matériel informatique nécessaire pour résoudre des problèmes cryptographiques en temps réel.

Vocabulaire des blockchains (suite)

Miner

Un miner (mineur en français) est un noeud du réseau qui valide les transactions et alimente la puissance de calcul de la blockchain. C'est un noeud du réseau qui opère la validation des transactions à la place d'u'ne instance centrale.

- Les miners peuvent être des individus ou des organisations qui apportent le matériel informatique nécessaire pour résoudre des problèmes cryptographiques en temps réel.
- Le premier des miners 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.

Vocabulaire des blockchains (suite)

Proof of work ou Proof of activity

La Proof of Work (PoW -preuve de travail) est le résultat du problème cryptographique à résoudre pour qu'une nouvelle information soit ajoutée dans un bloc. Ce résultat est difficile à obtenir et nécessite beaucoup de puissance informatique. En revanche, sa vérification est peu consommatrice de ressources.

Comme exemples de monnaies PoW on a:

- Bitcoin,
- Litecoin,
- Verge, etc.

Proof of stake

Proof of stake

La Proof-of-Stake (PoS - preuve d'intérêt) est une autre méthode de validation des blocs. Celle-ci est basée sur les avoirs (ainsi que leur temps de conservation) de la personne et se définit généralement par un pourcentage de création monétaire. C'est une méthode parallèle pour atteindre un consensus décentralisé et qui a l'avantage de consommer peu d'énergie. En d'autres termes, la proof of stake est une méthode pour atteindre le consensus distribué dans un réseau blockchain qui ne demande pas aux utilisateurs d'utiliser leur puissance de calcul, mais de prouver la propriété d'un certain montant de crypto-monnaie.

Comme exemples de monnaies PoS on a:

- Peercoin,
- NeuCoin, etc.

Vocabulaire des blockchains

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
- Le token de la blockchain bitcoin est le Bitcoin.
- Les tokens sont l'unité transactionnelle et informationnelle sur une blockchain.

Vocabulaire des blockchains

Transaction

Les transactions représentent les échanges entre les utilisateurs, qui sont stockés au sein des blocs de la chaîne de blocs.

Vocabulaire des blockchains

Genesis block

On appelle genesis block ou bloc de genèse, le tout premier bloc de la transaction d'une blockchain.

Token

Un token est un actif numérique émis et échangeable sur une blockchain. Un peut être transféré sur Internet sans duplication en pair-à-pair.

Les éléments d'une blockchain

Chaque bloc de la blockchain est constitué des éléments suivants:

- plusieurs transactions ;
- une somme de contrôle appelée *hash*, utilisée comme identifiant ;
- la somme de contrôle du bloc précédent (à l'exception du premier bloc de la chaîne, appelé bloc de genèse) ;
- une mesure de la quantité de travail qui a été nécessaire pour produire le bloc. Celle-ci est définie par la méthode de consensus utilisée au sein de la chaîne, telle que la *preuve de travail*, etc.

Merci pour votre attention.
Commentaires ? Questions ?

Introduction à la Technologie Blockchain

Eugène C. Ezin[1] & Nelson Saho[2]

[1]Institut de Formation et de Recherche en Informatique
& Institut de Mathématiques et de Sciences Physiques
[2]Doctorant en Sciences de l'Ingérieur
Université d'Abomey-Calavi

Contenu

Contenu

Les deux catégories des blockchains

Il existe deux différentes catégories de blockchains :

- les blockchains publiques
- les blockchains privées

Blockchains publiques

Definition

Une blockchain est publique lorsque n'importe qui peut devenir membre du réseau sans condition d'admission.

- Quiconque souhaite utiliser le service proposé par le réseau peut télécharger le protocole localement sans réveler son identité ou correspondre à des critères déterminés.
- Par exemple, les membres du réseau bitcoin téléchargent le protocole Bitcoin par l'intermédiare de leur wallet pour prendre part au réseau et échanger des bitcoins à condition de disposer de la connexion Internet.

Exemples de blockchains publiques

Dans la catégorie des blockchains publiques on peut citer

- Bitcoin
- Ethereum
- Litecoin

Nous étudierons essentiellement les deux premiers.

Blockchains privées

Définition

Une blockchain est privée lorsque les membres du réseau sont sélectionnés avant de pouvoir télécharger le protocole et utiliser le service proposé par le réseau.

- Un réseau reposant sur une blockchain privée n'est pas décentralisée.
- Les capacités de minage et le système de consensus dans son ensemble sont centralisés au sein d'une même entité.

Exemples de blockchain privées

Dans la catégorie des blockchains privées on distingue

- Hyperledger.
- IOTA
- Corda

Nous étudierons essentiellement les deux premiers

Contenu

Brève comparaison des blockchains publiques aux blockchains privées

Les différences entre les types de blockchain reposent sur les niveaux de confiance entre les membres et les niveaux de sécurité qui en découlent.

- Plus le niveau de confiance entre les membres du réseau est élevé, plus le mécanisme de consensus peut-être léger.
- Il n'y a aucune confiance entre les membres d'une blockchain publique
- On note une confiance beaucoup plus forte dans les blockchains privées puisque les membres sont pré-sélectionnés.
- Dans les réseaux reposant sur les blockchains, le niveau de confiance entre les membres impacte donc directement la structure et les mécanismes mis en place.

Contenu

Blockchain publique : Bitcoin

- Bitcoin est la première crypto-monnaie et la première implémentation de blockchain dans le monde
- Satoshi Nakamoto a introduit le bitcoin en 2009
- Blockchain typique avec un réseau partagé P2P

Fonctionnement de la technologie Bitcoin

Les différentes étapes suivantes sont nécessaires pour le fonctionnement de la Bitcoin:

- Créer un compte dans Bitcoin en créant un porte monnaie électronique (*digital wallet*). Des fournieurs à l'instar de *Coinbase* ou *Bitcore* ou d'autres permettent d'y parvenir.
- Généreration d'une graine de laquelle seront générées des paires de clés. Les clés publiques serviront d'identifiant c'est-à-dire de pseudonyme (c'est pourquoi on dit que Bitcoin est pseudo anonyme).

Bitcoin (suite)

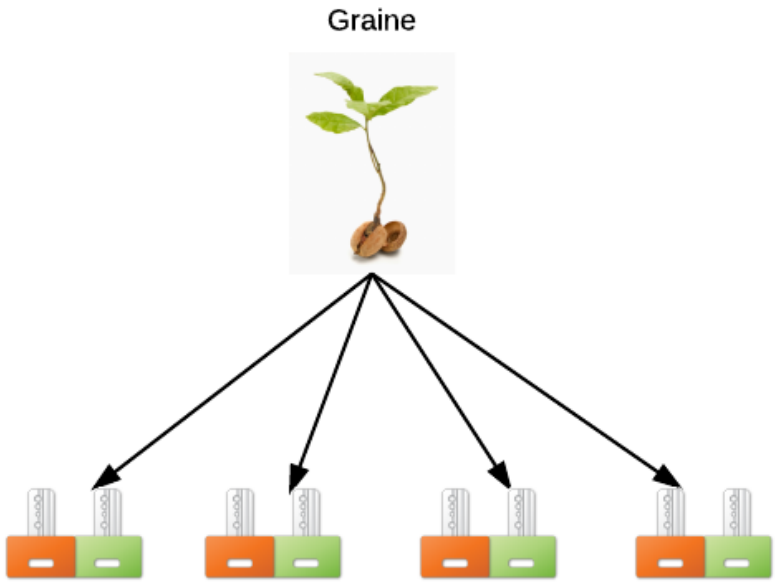


Figure: Génération de clés

La graine (liste de mots) est donc ce qu'il y a de plus précieux. Toutes les paires de clés en dérivent.

Bitcoin (suite)

Transactions

- L'envoi de bitcoins d'un compte à un autre à travers les portefeuilles.
- Les transactions sont vérifiées par les mineurs avant leur ajout dans un bloc.
- Une transaction est gratuite et le temps de validation est de 10 minutes en moyenne. Accélaration possible du processus en payant des frais

Minage des transactions

- Le sujet le plus important et plus intéressant de la technologie Bitcoin.
- C'est un processus par lequel les nouvelles transactions sont validées et ajoutées au blockchain.
- Cela exige du matériel d'exploitation dédié et par conséquent, les nœuds sont impliqués dans le minage.
- Les nœuds qui participent au processus sont connus sous le nom de mineurs

Bitcoin (suite)

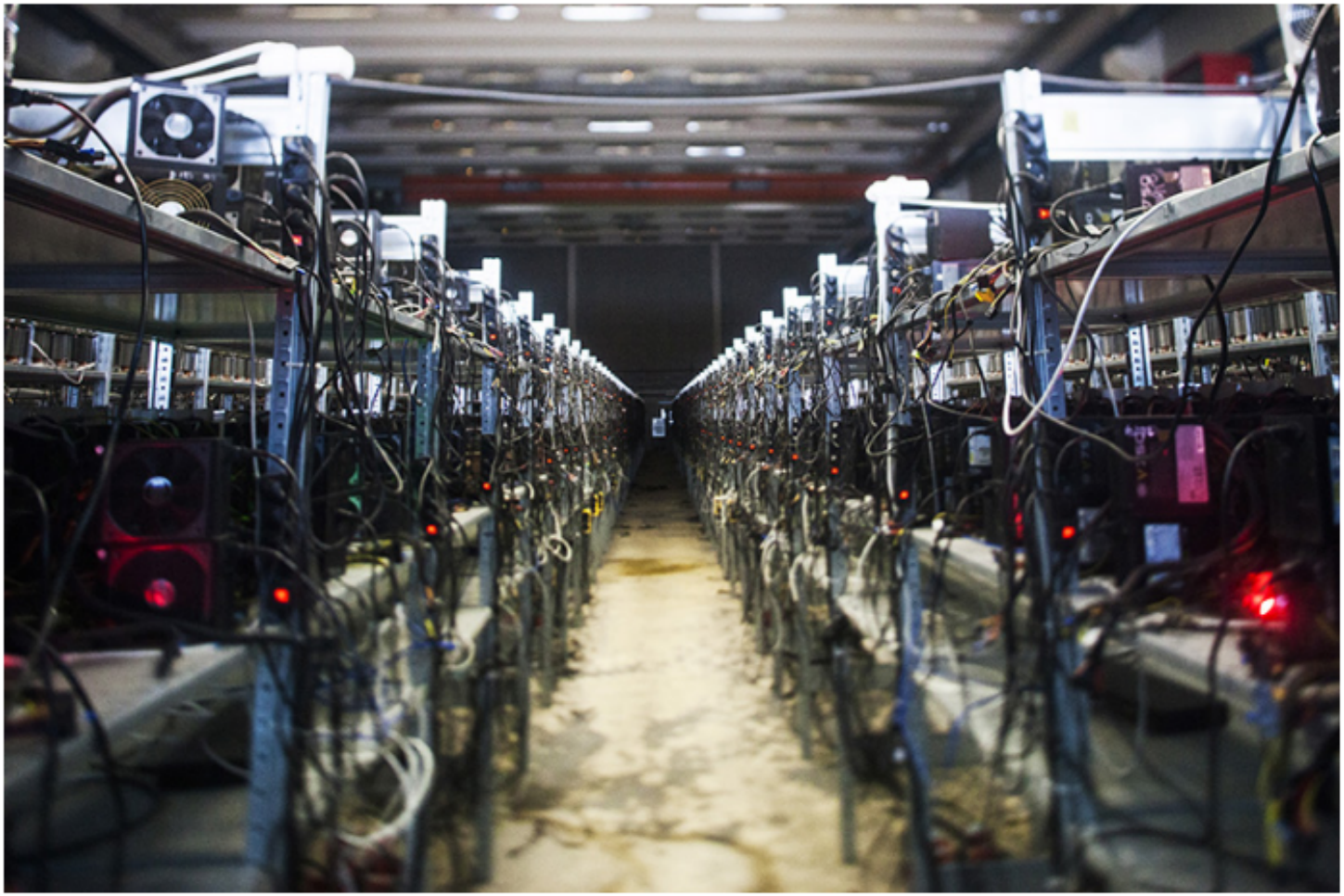


Figure: Vue partielle d'un mineur en Europe du nord

Bitcoin (suite)

Minage des transactions

- La naissance de toute nouvelle transaction est diffusé dans tout le réseau
- Les mineurs écoutent cette émission et s'engagent dans une activité de vérification
- Une fois les transactions vérifiées, elles sont ajoutées à un bloc

Activités des mineurs

- La mission est de trouver une valeur de hachage pour le nouveau bloc
- Le mineur qui trouve que la valeur de hachage est récompensée en premier par des bitcoins appelés récompense de blocs *block reward*. Maintenant, il est 12,5 BTC mais sera de 6,25 BTC en 2020. Elle est divisée par deux tous les 210 000 blocs ou environ tous les 4 ans

Bitcoin (suite)

Activités des mineurs

- Le niveau de difficulté est spécifié en termes de nombre de zéros qui début chaque hash
- Le nœud qui a équipé avec du matériel dédié et haute la puissance de calcul a une plus grande chance de gagner ce jeux et d'obtenir la récompense de bloc . Ceux qui trouveront le hash en premier diffuseront le résultat
- En recevant cela, les autres cessent de solutionner et valident si le hachage reçu satisfait le niveau de difficulté spécifié. Si oui, les nœuds montrent leur acceptation en l'ajoutant à la blockchain.

Bitcoin (suite)

Sommaire	
Nombre de transactions	2275
Somme des outputs	3,215.32828762 BTC
Volume estimé des transactions	254.17359807 BTC
Frais des transactions	0.36551962 BTC
Hauteur	586236 (Chaîne principale)
Date (timestamp)	2019-07-20 16:23:48
Date de réception	2019-07-20 16:23:48
Relayé par	Unknown
Difficulté	9,064,159,826,491.41
Morceaux	387911067
Taille	1162.417 kB
Poids	3992.686 kWU
Version	0x20000000
nonce	1821208781
Récompense du bloc	12.5 BTC

Hashes	
Hash	0000000000000000000156bebd1f399d83e506c5d1ef1305a92e1db944efc6e47
Bloc précédent	00000000000000000000064829f4eb5dabb71f734a471f4d611120cd5590ce508c
Bloc(s) suivant(s)	000000000000000000052c28b26236315feeb1a52411f52af87f7bb94739c57b
Racine de Merkle	38f67a881d8b6291849fc5606beaf7d195293a5247d15b5e83fe009e86cdffd3

Figure: Caractéristiques du Bloc #586236

Contenu

Blockchain publique : Ethereum

- Ethereum est une blockchain *open source* créé par Vitalik Buterrin, qui permet le développement et le déploiement des applications basées sur la technologie Blockchain.
- La technologie Ethereum incorpore toutes les fonctionnalités de la technologie Blockchain dans un seul réseau et évitant la création des blockchains individuels pour chaque objectif.
- La technologie Ethereum a ouvert les possibilités de la technologie Blockchain à d'autres domaines d'applications tels que les jetons, les portefeuilles, les applications sociales, etc.

Ethereum (suite)

Dans la technologie Ethereum, de nombreux réseaux coexistent :

- private network;
- public test network;
- main Ethereum network.

Ethereum (suite)

Les types d'utilisateurs de Ethereum

- Il existe deux types d'utilisateurs dans la blockchain Ethereum : ceux qui créent les applications décentralisées (*Decentralized Application or Smart contract*) et d'autres qui participent au contrat.
- Chaque utilisateur crée un compte appelé *Externally Owned Accounts (EOA)*. Chaque DApps possède aussi une adresse de compte appelé *Contract Account*.
- La transaction de l'utilisateur est associée à ces uniques comptes. Les utilisateurs peuvent effectuer des transactions avec les autres EOA ainsi que les *Contract Account*.

Ethereum (suite)

Decentralized Applications

- Il s'agit des applications tournant sur la blockchain sans aucun contrôle centralisé.
  Exemple : bitcoin est une application décentralisée de la blockchain Bitcoin.
- On utilise le grand livre partagé au lieu d'un serveur pour enregistrer toutes les transactions. Dans Ethereum, des codes en arrière-plan contiendront le contrat intelligent et l'interface frontale fournira une interface utilisateur permettant à l'utilisateur d'interagir avec la blockchain. Une fois que les contrats intelligents sont déployés sur la blockchain, le DApp deviendra accessible.
- Les DApps peuvent être développés pour tous les cas d'utilisation. Toute application qui en cours d'exécution sur le modèle client-serveur peut être implémentée en tant que DApp. Quelques exemples de Ethereum DApp: Green Ether Project, splitcoin, the immortals, etc.

Ethereum (suite)

Les composants d'Ethereum

- **Smart contracts :** Les contrats intelligents sont le coeur de la structure d'Ethereum. Toutes les opérations sont contrôlées avec des contrats intelligents. Bien sûr, ce sont des lignes de codes et il est utilisé pour échanger tout ce qui a de la valeur de manière plus sécurisée et transparente. Dans Ethereum, ces contrats intelligents sont écrits avec le langage **solidity**. Le contrat intelligent assurera l'exécution directe du contrat entre l'expéditeur et le destinataire sans intermédiaire.
  - Tout d'abord un compte de contrat est créé dans la blockchain. Le contrat aura des règles spécifiques et des actions basées sur ces règles.
  - Le contrat est ensuite codé.
  - Le contrat codé est déployé dans le réseau Ethereum. Il a une adresse de clé publique unique, l'adresse étant utilisée pour accéder au contrat dans le réseau. Une fois le contrat déployé, il ne peut plus être modifié, même par l'émetteur.

Ethereum (suite)

Les composants d'Ethereum

- **Ether :** Ether est la crypto-monnaie du réseau Ethereum, donc ainsi que l'épine dorsale des transactions dans Ethereum
- **Ethereum clients :** Les outils utilisés pour se connecter à la blockchain Ethereum à des fins de développement ou d'exploitation. Voici quelques uns :
  - **Geth :** un client Ethereum travaillant dans le langage GO. Geth dispose d'un outil d'interface de ligne de commande (CLI) qui communique avec le réseau Ethereum et joue le rôle de lien entre les différents nœuds du réseau.
  - **Eth :** Tournant en C ++ Eth est un puissant client Ethereum attire davantage les mineurs.
  - **Pyethapp :** ce client est utile pour le développement DApp en utilisant python.
  - **Pythapp :** également un excellent choix pour les recherches académiques ou non dans Ethereum blockchain.

Ethereum (suite)

Les composants d'Ethereum

- **EVM :** Moteur de toute la blockchain Ethereum, les contrats intelligents sont exécutés sur la machine virtuelle Ethereum (EVM).
- **Etherscripter :**Outil visuel de création de contrat intelligent développé par Ethereum. Il fournit une interface graphique pour la création de contrats intelligents en étapes simples. Etherscripter fournit une interface simple de glisser-déposer où les codes en arrière-plan sont générés dans le langage *Serpent, LLL et XML*. En utilisant Etherscripter, même un non-programmeur peut créer des contrats intelligents.

Contenu

Blockchain privée : Hyperledger

Définition

Hyperledger est une plateforme *open source* de développement de blockchain. Ce projet a été initié en décembre 2015 par la fondation Linux. Le développement s'y fait essentiellement en langage Go. Elle regroupe différents frameworks permettant de développer des contrats intelligents ou des applications décentralisées dans la blockchain, à destination des entreprises.

- Iroha
- Fabric
- Sawtooth
- Burrow
- Indy

Hyperledger (suite)

Tableau comparatif

Caractéristiques	**Bitcoin**	**Ethereum**	**Hyperledger**
Cryptocurrency	Bitcoin	Ether	Non
Smart Contract	Non	Oui (Smart contracts)	Oui (Chain code
Type de Blockchain	Publique	Publique	Privée
Méthode de consensus	Proof of Work	Proof of Work	Méthodes variées

Les services d'Hyperledger Fabric

- Une des principales caractéristiques d'Hyperledger Fabric est sa flexibilité. Son objectif est de permettre le plus d'interaction entre les membres d'Hyperledger tout en étant au plus proche de leurs besoins opérationnels.
- Hyperledger offre quatre types de services :
  - Identity services
  - Policy services
  - Blockchain services and
  - Smart contract services.

Hyperledger (suite)

Identity services

Assure la gestion de l'identité des parties membres du réseau.

Policy services

Gère les questions d'accès au réseau, la confidentialité, les règles du consortium ainsi que les règles de consensus.

Blockchain services

Gère les questions liées au protocol de communication peer to peer, l'état de la blockchain, l'algorithme de consensus utilisé par le mécanisme de consensus.

Smart contract services

Offre l'environnement d'exécution pour les Chaincode.

Architecture générale de Hyperledger

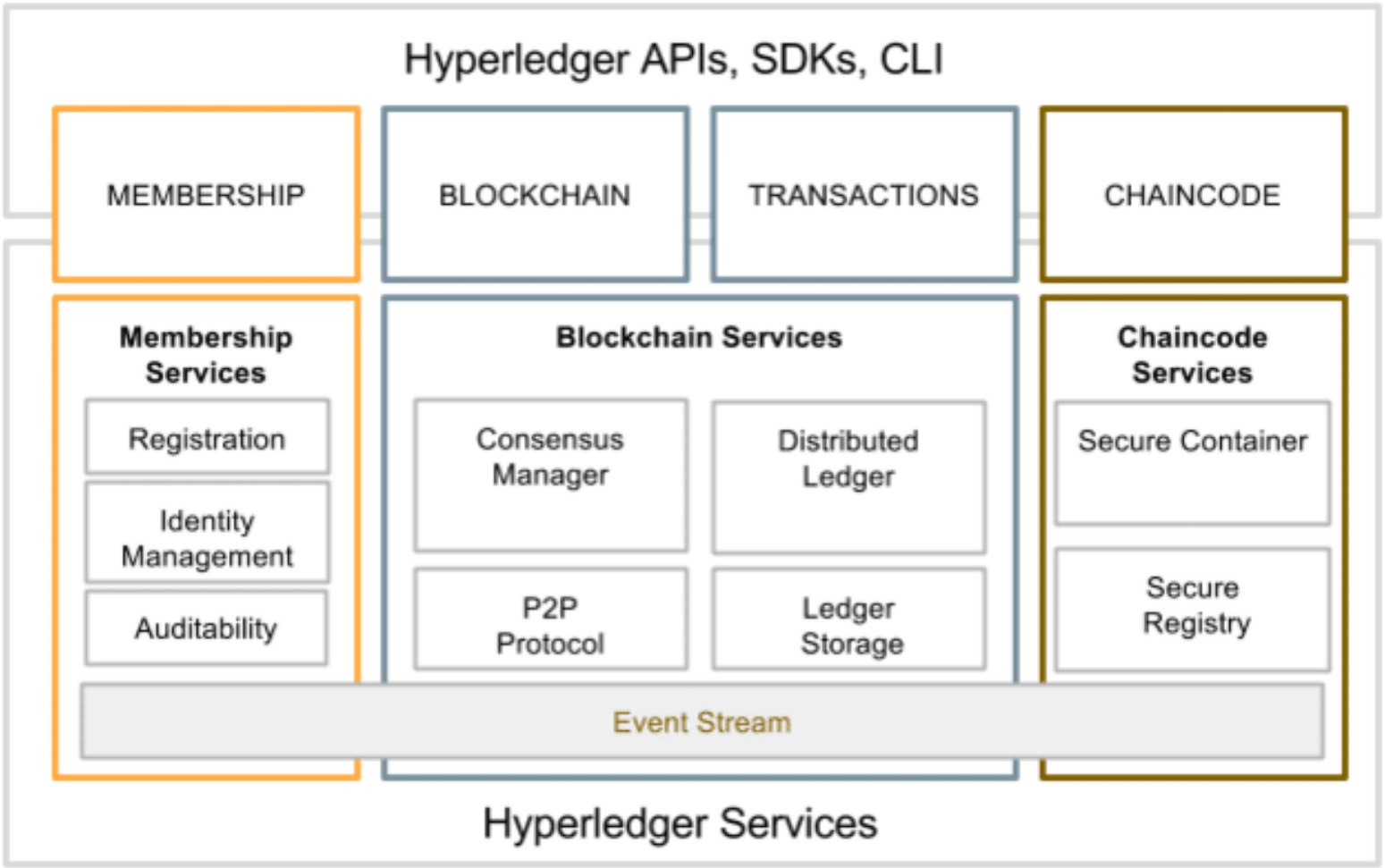


Figure: Architecture générale de Hyperledger

Hyperledger (suite)

- Les applications communiquent avec chacun de ses services à travers des API. CLI est une interface utilisée pour invoquer ces API.
- Quatre différents outils facilitent le développement des applications :
  - **Hyperledger cello :** initialement fourni par IBM, avec des sponsors de Soramitsu, Huawei et Intel, aide les utilisateurs à utiliser et gérer les chaînes de blocs de manière plus efficace.
  - **Hyperledger composer :** Ensemble d'outils de collaboration permettant de créer des réseaux d'entreprise blockchain, qui permettent aux propriétaires et développeurs de créer facilement des contrats intelligents et des applications blockchain pour résoudre les problèmes de l'entreprise.

Hyperledger (suite)

- **Hyperledger explorer :** conçu pour créer une application Web conviviale, Hyperledger Explorer peut afficher, appeler, déployer ou interroger des blocs, des transactions et des données associées, des informations réseau (nom, statut, liste de nœuds), des chaînes de code et des familles de transactions, ainsi que tout autre type de réseau.
- **Hyperledger quilt :** offre une interopérabilité entre les systèmes de grand livre en implémentant le protocole Interledger (également appelé ILP), qui est principalement un protocole de paiement et est conçu pour transférer de la valeur entre des grands livres distribués et des grands livres non distribués.

Composantes du modèle Hyperledger Fabric

Le modèle d'Hyperledger Fabric est constitué de nombreux éléments dont:

- les membres (*peers*);
- les assets;
- les chaincodes;
- les ledgers;
- les channels;
- les memberships
- la méthode de consensus.

Les membres

Définition

Encore appelés peers, les membres du réseau sont ceux qui initient les transactions et tiennent à jour l'état de la blochchain.

Il existe trois types de membres à savoir:

- **Endorsing peers** : recevoir, valider et signer qu'ils reçoivent et les retourner à l'application qui les a créées.
- **Ordering services** : Collecter les transactions qui ont été validées, les ajouter dans les blocks et les envoyer au *Commiting Peers*.
- **Committing Peers** : Verifient que les transactions n'ont pas été réalisées plusieurs fois et les ajoutent à la blockchain.

les actifs

Définition

Encore appelés assets, les actifs représentent les biens tangibles ou intangibles qui sont représentés sur la blockchain et échangés sur le réseau. Ces biens sont formalisés en *key.value* dans un Json file.

les chaincodes

Définition

Les chaincodes sont des contrats intelligents encore appelés *smart contracts*. Leur fonction est de définir les actifs (assets) en organisant leur stockage, ainsi que les fonctions qui permettent d'agir sur ces actifs et changer leur état.

Les ledgers

Définition

La Blockchain utilisée par Hyperledger est la même que les autres blockchains, c'est un registre qui marque dans le temps les changements de transactions ou d'état de la blockchain. Les changements d'état sur le blockchain sont initiés par les fonctions des Chaincode, elles-mêmes actionnées par des transactions envoyées par les membres du réseau. Ce fonctionnement n'est pas très différent de celui utilisé par Ethereum. Une **key-value** est attachée à chaque transaction ce qui fait de la blockchain un registre de stockage des key-value.

Les channels

Channels

Les canaux (*channels*) offrent la possibilité d'utiliser Blockchain Fabric de manière privative et confidentielle, c'est-à-dire uniquement par les membres qui auront été présélectionnés et sur une blockchain privée.

Membership

Définition

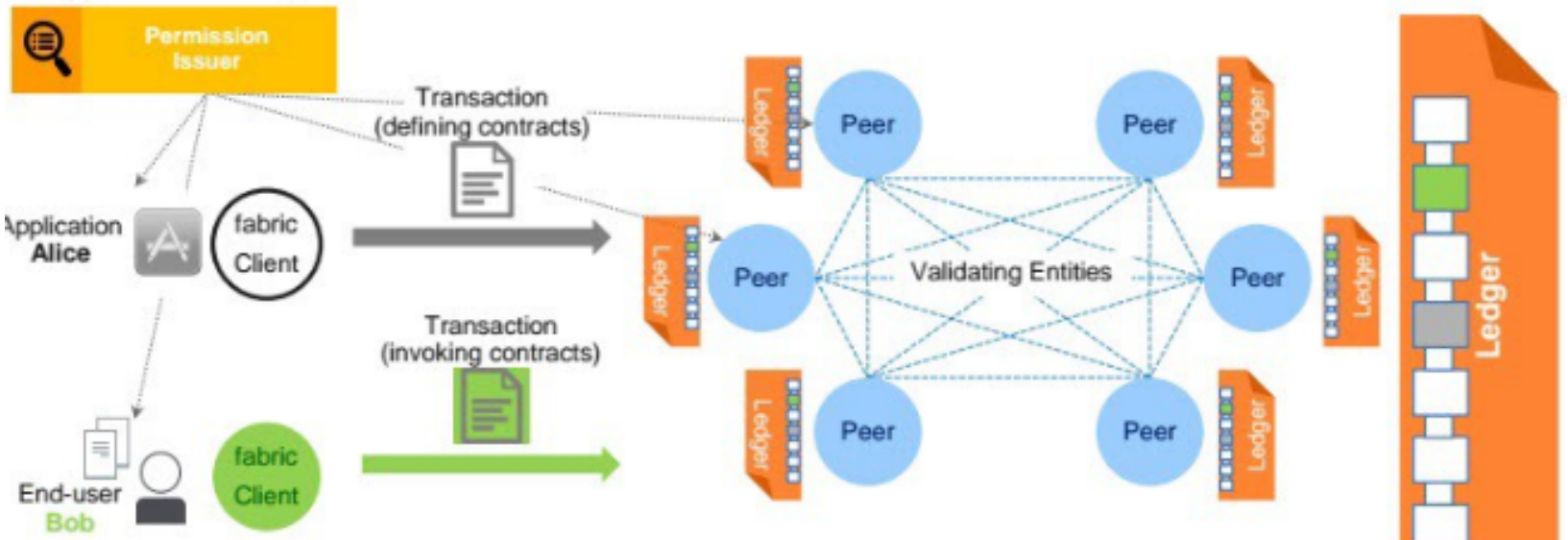
A la différence des blockchains publiques qui sont ouverts à tous comme Bitcoin, les blockchains utilisées par Hyperledger sont privées et impliquent donc que l'identité de tous les membres soit connue. L'identité des *Peer Nodes*, des *Client Applications*, des *Business Entities* et des *Administrateurs* est établie digitalement à travers un cerficat *X.509*. Ces cerficat contiennet le rôle de chacune des entités et leur niveau d'accès aux informations contenues sur le blockchain.

Hyperledger : Fabric

Consensus method

Technique utilisée par les membres du réseau pour décider quel bock de transmission sera le prochain à être ajouté à la blockchain et par quel membre. Le vérification de l'ordre et de la validité des transactions fait parti du mécanisme de consensus.
L'avantage comparatif de Hyperledger réside dans le fait que les membres du réseau peuvent choisir entre différentes méthodes de consensus
Plus il y a de confiance dans le réseau, plus le mode de consensus peut être léger. Plusieurs mécanismes peuvent être utilisés comme le PoW, le *round robin policy*, le *Simple Consensus*.

Hyperledger : Fabric



- **Permissioned** system; strong **identity management**
- Distinct roles of **users**, and **validators**
- Users **deploy** new pieces of code (chaincodes) and **invoke** them through **deploy & invoke** transactions
- Validators evaluate the effect of a transaction and reach consensus over the new version of the **ledger**
- **Ledger** = total order of transactions + hash (global state)
- **Pluggable consensus** protocol, currently PBFT & Sieve

Figure: Modèle de Hyperledger Fabric