Introduction à la Technologie Blockchain

Eugène C. Ezin & Nelson Saho

1er février 2023

Contenu

Contenu

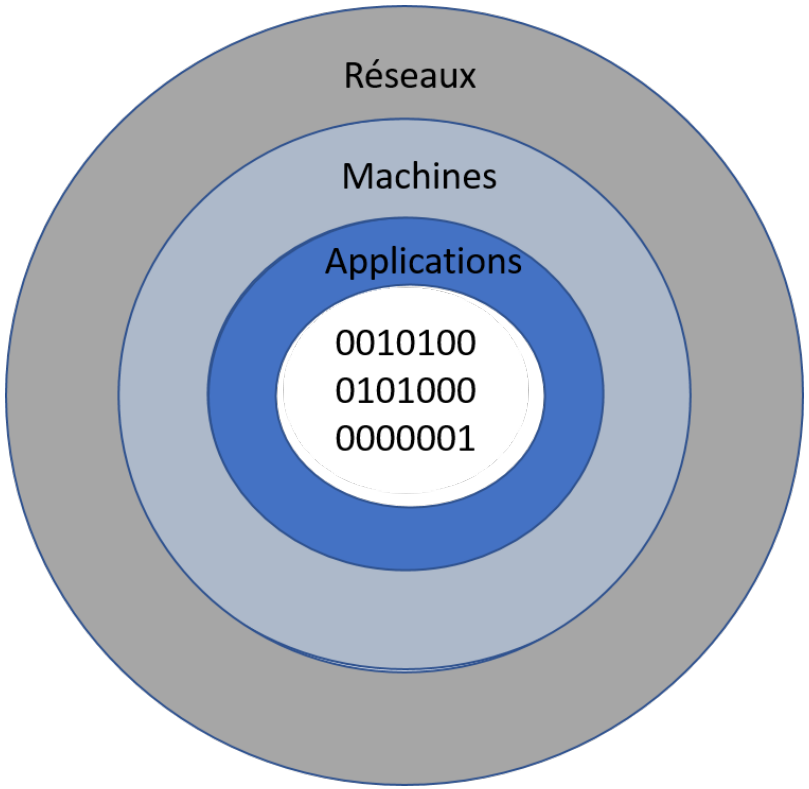
Les niveaux de sécurité

D'une manière générale, la sécurité est présente à plusieurs niveaux à savoir :

- au niveau physique (les locaux) ;
- au niveau des réseaux ;
- au niveau des machines ;
- au niveau des applications ; et
- au niveau des données ;

Les niveaux de sécurité (suite)

Cette figure illustre les différents niveaux de la sécurité d'un Système d'information.



Les types de menaces

Les menaces peuvent être vues comme des violations potentielles de la sécurité qui existent en raison des vulnérabilités du système. Les menaces envers un système informatique comprennent les éléments suivants :

- Destruction d'information et /ou d'autres ressources ;
- Corruption ou modification d'informations ;
- Vol, suppression ou perte d'informations et /ou d'autres ressources ;
- Divulgation d'informations ; et
- Interruption de service.

Les types de menaces (suite)

Avec la populatirité des réseaux, des échanges de données, et les transmissions entre individus, de nombreuses menaces émergent. En catégorisant les différentes menaces possibles, On peut citer :

- les menaces accidentelles ;
- les menaces intentionnelles ;
- les menaces passives ; et
- les menaces actives.

Les menaces accidentelles ou menaces intentionnelles peuvent être actives ou passives.

Les types de menaces : menaces accidentelles

Les menaces accidentelles sont celles qui existent sans qu'il y ait préméditation. Des exemples de menaces accidentelles sont :

- les bugs de logiciels ;
- les pannes matériels ;
- les défaillances incontrôlables.

Les types de menaces : menaces intentionnelles

- Elles reposent sur l'action d'un tiers désirant s'introduire et relever des informations.
- On parle ici d'attaque de système informatique. D'où la notion d'attaquant. Les menaces intentionnelles peuvent aller de l'examen fortuit, utilisant des outils de contrôle facilement disponibles, aux attaques sophistiquées, utilisant une connaissance spéciale du système.
- Les menaces intentionnelles peuvent être passives ou actives. Par exemple
  - les virus comme les chevaux de troie ;
  - les hackers.

Les types de menaces : menaces passives

- Dans le cas d'une menace passive, l'intrus tente de dérober les informations par audit du système d'information sans modifier les fichiers et les éléments de ce système.
- Les menaces passives sont celles qui, si elles se concrétisent, ne produiraient aucune modification d'informations contenues dans le(s) système(s) et avec lesquelles ni le fonctionnement, ni l'état du système ne changent.
- Il est très difficile de détecter ce type de menaces car elles sont inoffensives par rapport aux fonctions normales du système.
- L'utilisation de branchements clandestins passifs pour observer des informations transmises via une ligne de communication (surveillance de réseau) est une concrétisation d'une menace passive.

Les types de menaces : menaces actives

- Les menaces actives ou attaques envers un système comprennent l'altération d'informations contenues dans ce système, ou des modifications de l'état ou du fonctionnement du système.
- Les menaces actives sont, contrairement aux menaces passives, plus faciles à détecter si des précautions appropriées ont été prises au préalable.
- Les exemples d'attaques sont la destruction, la modification, la fabrication, l'interruption ou l'interception de données.
- Le résultat d'une attaque est soit une divulgation de l'information : violation de la confidentialité de l'objet, soit une modification des objets : violation de l'intégrité de l'objet, soit un déni de service : violation de la disponibilité.

Les types de menaces : menaces actives

On distingue donc quatre catégories de menaces actives :

- **Interruption** - il s'agit d'un problème lié à la disponibilité des données.
- **Interception** - il s'agit d'un problème lié à la confidentialité des données.
- **Modification** - il s'agit d'un problème lié à l'authenticité des données.
- **Fabrication** - provoque des attaques de déni de service (DOS) dans lesquelles l'attaquant s'efforce d'empêcher les utilisateurs d'accéder à certains services, auxquels ils sont autorisés ou, en termes simples, l'attaquant accède au réseau, puis verrouille l'utilisateur autorisé.

Contenu

Les modèles de sécurité

Il existe plusieurs modèles de sécurité notamment :

- le triangle CIA
- le protocole AAA
- le pentagone de confiance
- le modèle de Donn Parker
- le cube de McCumber

Les modèles de sécurité : Le triangle CIA

Il s'agit d'un modèle de sécurité introduit en 1987 qui définit les grands axes de la sécurité à savoir :

- la confidentialité (*Confidentiality*) - l'information n'est connue que des entitiés communicantes.
- l'intégrité (*Integrity*) - l'information n'a pas été modifiée entre sa création et son traitement et même pendant son transfert.
- la disponibilité (*Availability*) - l'information est toujours accessible et ne peut être perdue ni bloquée.

Le triangle CIA sert de base à la plupart des autres modèles.

Les modèles de sécurité : protocole AAA

Le contrôle d'accès (encore appelé le protocole AAA) se fait en quatre étapes :

- l'Identification - qui êtes-vous ?
- l'Authentification - prouvez-le !
- l'Autorisation - Avez-vous les droits requis ?
- Accounting/audit : Qu'avez-vous fait ?

On parle de protocole AAA simplement parce que les deux premières étapes sont fusionnées. Dans certains cas, la quatrième étape est scindée.

Les modèles de sécurité : protocole AAA

On parle d'accounting lorsque le fait de comptabiliser des faits sera demandé.

On parle d'audit lorsque des résultats plus globaux devront être étudiés.

L'authentification visant à prouver l'identité peut se faire de plusieurs manières(mot de passe, code PIN, carte magnétique, lecteur de carte, empreintes digitales, réseau rétinien, etc.)

Les modèles de sécurité : pentagone de confiance

Ce modèle a été défini par Piscitello en 2006 et précise la notion d'accès à un système. Ce modèle précise aussi la confiance que peut/doit avoir l'utilisateur en présence d'un système informatisé. Les cinq étapes de ce modèle de confiance sont :

- l'authentification (*Authentification*)
- l'autorisation (*Authorization*)
- la disponibilité (*Availability*)
- l'admissibilité (*Admissibility*)
- l'intégrité (*Authenticity - Integrity*)

La confiance se traduit par l'admissibilité. De façon plus précise, la machine sur laquelle nous travaillons, à laquelle nous nous connectons est-elle fiable ? Peut-on faire confiance à la machine cible ?

Les modèles de sécurité : Modèle de Donn Parker

Le modèle de Donn Parker encore appelé Parkerian Hexad est introduit en 1998 comporte la notion d'utilité en plus des notions de

- confidentialité ;
- intégrité ;
- disponibilité ;
- authentification ;
- contrôle ou possession.

Une information chiffrée pour laquelle on a perdu la clé de déchiffrement n'est plus d'aucune utilité bien que l'utilisateur y est accès, que cette information soit confidentielle, disponible et intègre.

Les modèles de sécurité : Modèle de Donn Parker

Figure 2 – Le modèle Parkerian Hexad [1]

Les modèles de sécurité : Le cube de McCumber

Le cube de McCumber est introduit en 1991 et inclut deux autres dimensions en plus des trois piliers de la sécurité (CIA). Les deux autres dimensions sont :

- l'état des données : le stockage, la transmission, l'exécution ;
- les méthodes : les principes et règles à adopter pour atteindre le niveau de sécurité souhaité.

Les modèles de sécurité : Le cube de McCumber

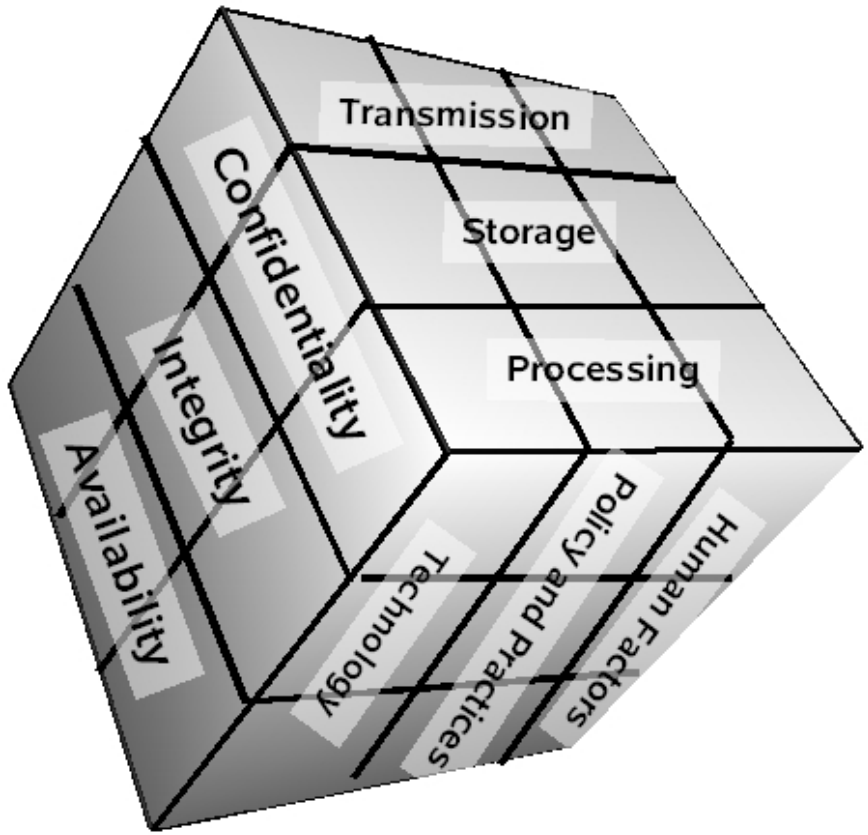


Figure 3 – Le cube de McCumber [2]

Notion de sécurité parallèle

On parle de sécurité en parallèle lorsque plusieurs mécanismes de sécurité protégeant un système possèdent le même rôle. Dans ce cas, le niveau de protection du système est équivalent à celui du mécanisme le moins sûr.
Comme exemple, on peut considérer un ordinateur portable que l'on peut déverrouiller par mot de passe, ou empreinte digitale.

Notion de sécurité en série

On parle de sécurité en série ou de défense en profondeur lorsque plusieurs mécanismes de sécurité protègent un système et ont des rôles différents.
Par exemple, le réseau d'une entreprise comportant un firewall hardware, les différentes machines équipées de firewall logiciel, les ordinateurs comportent des logiciels accessibles par mot de passe, etc.
Le niveau global de sécurité des systèmes d'information est défini par le niveau de sécurité du maillon le plus faible. Les précautions et contre-mesures doivent être envisagées en fonction des vulnérabilités propres au contexte auquel le système d'information est censé apporter service et appui.

Contenu

Les objectifs de la sécurité informatique

Les principaux objectifs de la sécurité informatique sont :

- la disponibilité ;
- l'intégrité ;
- la confidentialité des infrastructures informatiques (données, services, systèmes).

Les mesures de sécurité

Il existe plusieurs mesures de sécurité pour atteindre les objectifs de la sécurité informatique. Parmi elles, nous pouvons citer :

- le contrôle d'accès
- **le chiffrement des données ou mieux la cryptographie**
- la gestion des incidents ;
- la gestion des erreurs ;
- la gestion des dysfonctionnements ;
- la gestion des intrusions ;
- le cloisonnement d'environnements ;
- etc.

Vocabulaire

- **sûreté :** protection contre les actions non intentionnelles
- **sécurité :** protection contre les actions intentionnelles malveillantes
- **menace :** moyen potentiel par lequel un attaquant peut attaquer un système
- **risque :** prise en compte à la fois la probabilité d'une menace et de sa gravité si elle réussit

Cryptographie et sécurité informatique

La cryptographie est un outil fondamental de la sécurité informatique. En effet :

- la mise en oeuvre de la cryptographie permet de réaliser des services de confidentialité des données transmises ou stockées ;
- la mise en oeuvre de la cryptographie permet les services de contrôle et d'intégrité de données ;
- la mise en oeuvre de la cryptographie permet l'authentification d'une entité lors des transactions ou opérations.

Cryptographie et sécurité informatique

De par l'utilisation d'une clef, il existe deux branches en cryptographie : les cryptographie symétrique et la cryptographie asymétrique. Et c'est justement la sécurité de cette clef qui constitue la plupart du temps la faille des cryptosystèmes symétriques et asymétriques :

- Avec les cryptosystèmes symétriques, la sécurité autour de la clé secrète est un souci.
- Avec les cryptosystèmes asymétriques, la sécurité autour de la clé privée ne se pose pas tellement mais il y a insécurité tout de même.
- etc.

La clé est un souci majeur pour les cryptosystèmes. Une alternative est la technologie Blockchain.

Merci pour votre attention.
Commentaires ? Questions ?

Contenu

Généralités sur la Blockchain

- 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 chaînes 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 chaîne de bloc et l'a implémenté en 2009 - d'où le bitcoin - première monnaie virtuelle.

Généralités sur la Blockchain

Définition de la Blockchain

- La blockchain est une technologie de stockage et de transmission d'informations, *transparente*, *sécurisée*, et *fonctionnant sans organe central de contrôle* (définition de Blockchain France).
- Il s'agit d'une technologie de stockage et de transmission d'information sans organe de contrôle. C'est-à-dire 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 chaîne.

Généralités sur la Blockchain

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 distribuées c'est-à-dire que les données ne se trouvent pas sur la même machine.

Les différents modes de stockage des données sont :

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

Schéma d'une base de données distribuée

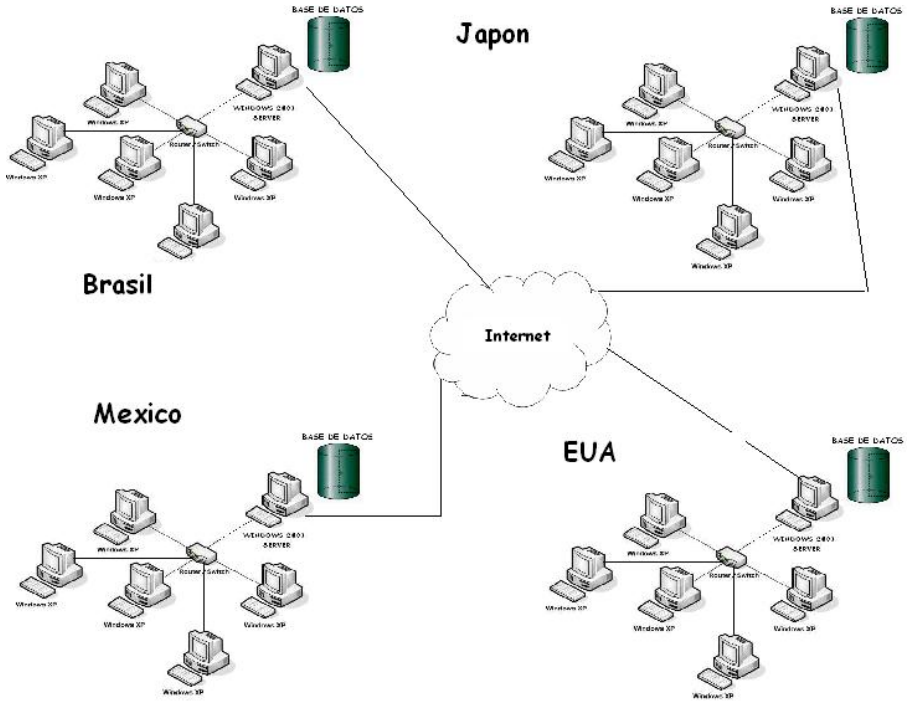


Figure 4 – Une base de données distribuée.

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

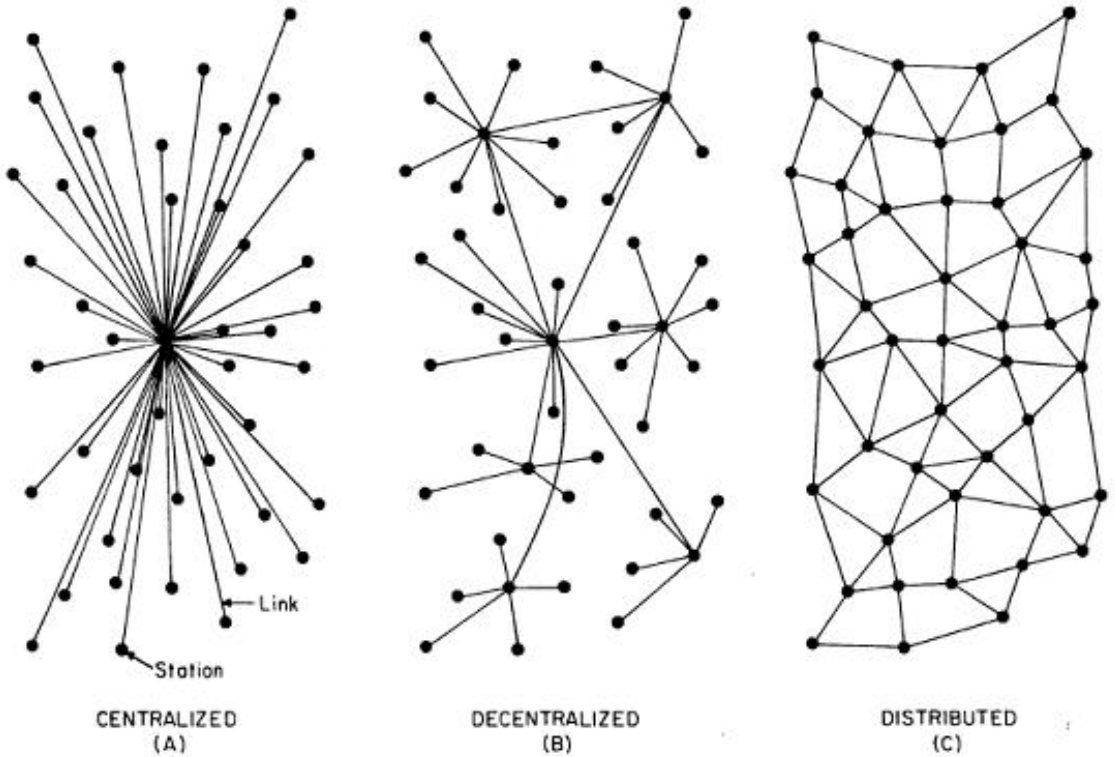


Figure 5 – Architectures centralisées - décentralisées et distribuées

Propriétés fondamentales

Les trois propriétés fondamentales d'une Blockchain sont les suivantes :

- la désintermédiation ;
- la sécurité dont l'horodatage ; et
- 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 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 infalsifiables.
- Le système est protégé contre la fraude de la double-dépense [3].

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

Illustration de la double dépense

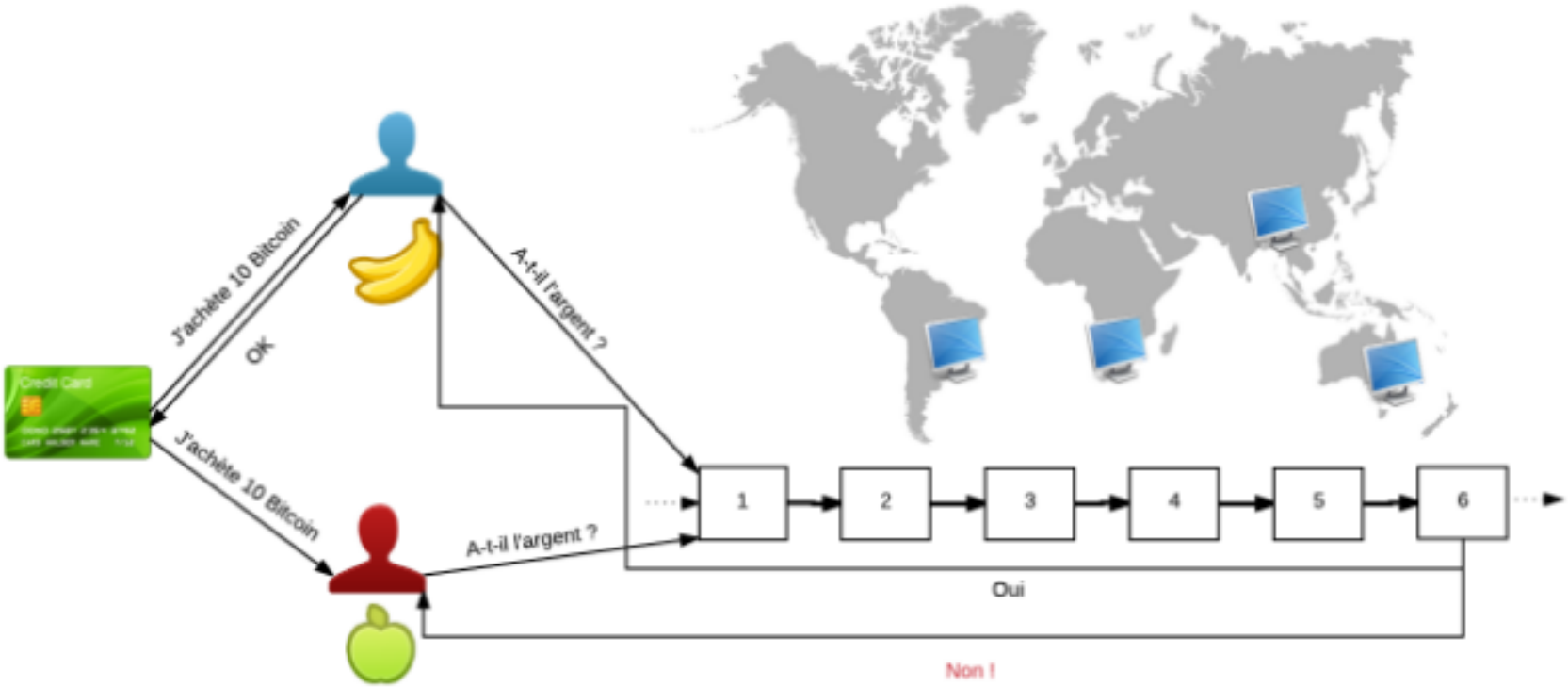


Figure 6 – Un exemple pour illustrer la double-dépense.

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.
- 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 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.

Vocabulaire de la Blockchain

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 de la Blockchain

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 de la Blockchain

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 de la Blockchain

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

Vocabulaire de la Blockchain

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'une 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 cryptomonnaie. Ce qui génère une compétition entre les mineurs et les pousse à acquérir du matériel plus puissant.

Vocabulaire de la Blockchain

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.

Vocabulaire de la Blockchain

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.

Vocabulaire de la Blockchain

Proof of stake

- 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 cryptomonnaie.

Comme exemples de monnaies PoS on a :

- Peercoin,
- NeuCoin, etc.

Vocabulaire de la Blockchain

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 de la Blockchain

Transaction

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

Genenis 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.

Vocabulaire de la 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.

Contenu

Les catégories de blockchains

Il existe deux différentes catégories de blockchains :

- les blockchains publiques ;
- les blockchains privées.

Blockchains publiques

Définition

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 révéler son identité ou correspondre à des critères déterminés.
- Par exemple, les membres du réseau bitcoin téléchargent le protocole Bitcoin par l'intermédiaire 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 Blockchains privées

Dans la catégorie des blockchains privées on peut citer :

- Hyperledger
- IOTA
- Litecoin

Nous étudierons essentiellement les deux premiers.

Blockchains publiques VS 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.

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

Bitcoin : Son fonctionnement

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.
- Génération 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).

Blockchain publique : Bitcoin

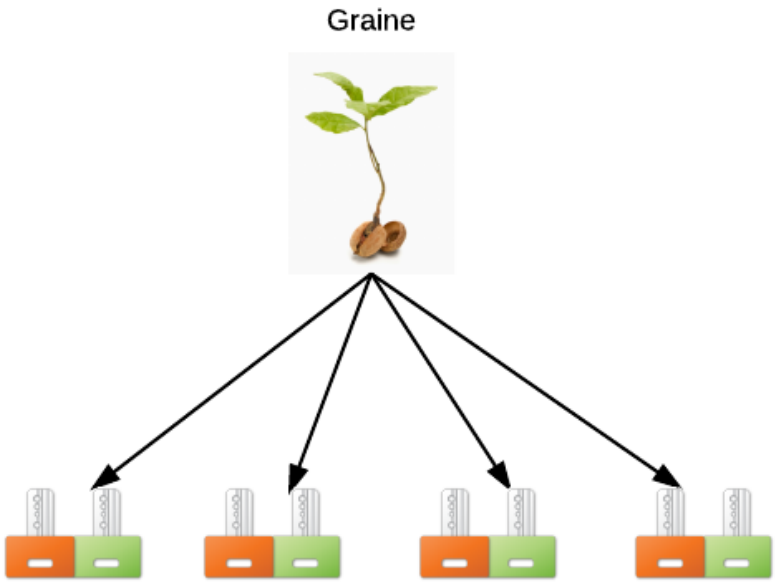


Figure 7 – Génération de clés

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

Blockchain publique : Bitcoin

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. Accélération possible du processus en payant des frais.

Blockchain publique : Bitcoin

Minage des transactions

- C'est un processus par lequel les nouvelles transactions sont validées et ajoutées au blockchain.
- Cela exige du matériel d'exploitation dédié. Les nœuds qui participent au processus sont connus sous le nom de mineurs.
- 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.

Blockchain publique : Bitcoin

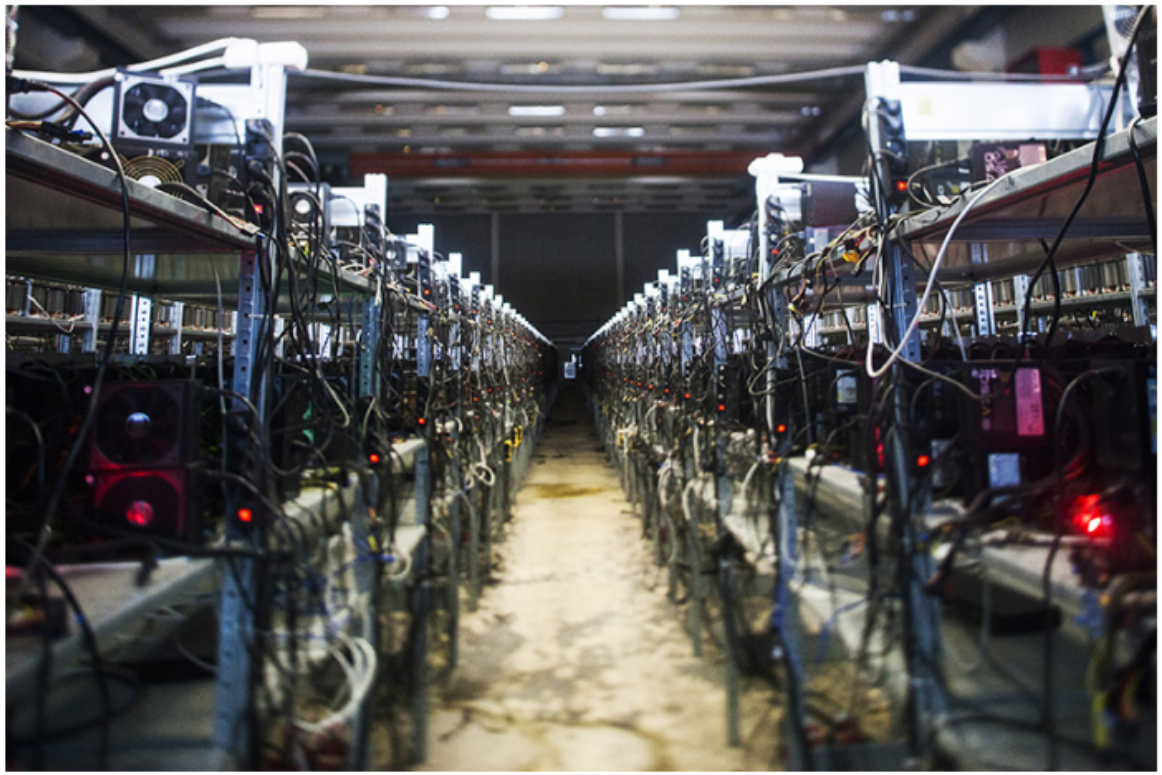


Figure 8 – Vue partielle d'un mineur en Europe du nord

Blockchain publique : Bitcoin

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 6,25 BTC mais sera de 3,125 C en 2024. Elle est divisée par deux tous les 210 000 blocs ou environ tous les 4 ans.

Blockchain publique : Bitcoin

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.

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.

Blockchain publique : Ethereum

Dans la technologie Ethereum, de nombreux réseaux coexistent :

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

Blockchain publique : Ethereum

Les types d'utilisateurs

- 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.

Blockchain publique : Ethereum

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.

Blockchain publique : Ethereum

Decentralized Applications

- 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.

Blockchain publique : Ethereum

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.

Blockchain publique : Ethereum

Les composants d'Ethereum

- 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.

Blockchain publique : Ethereum

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 Ethereum à des fins de développement ou d'exploitation.
  - **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.

Blockchain publique : Ethereum

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.

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 dans la blockchain.

- Iroha
- Fabric
- Sawtooth
- Burrow
- Indy

Blockchain privée : Hyperledger

Caractéristiques	Bitcoin	Ethereum	Hyperledger
Cryptocurrency	Bitcoin	Ether	Non
Smart Contract	Non	Oui	Oui
Type de Blockchain	Publique	Publique	Privée
Consensus	PoW	PoW	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
  - Smart contract services

Blockchain privée : Hyperledger

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 privée : Hyperledger

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 Chaincodes.

Blockchain privée : Hyperledger

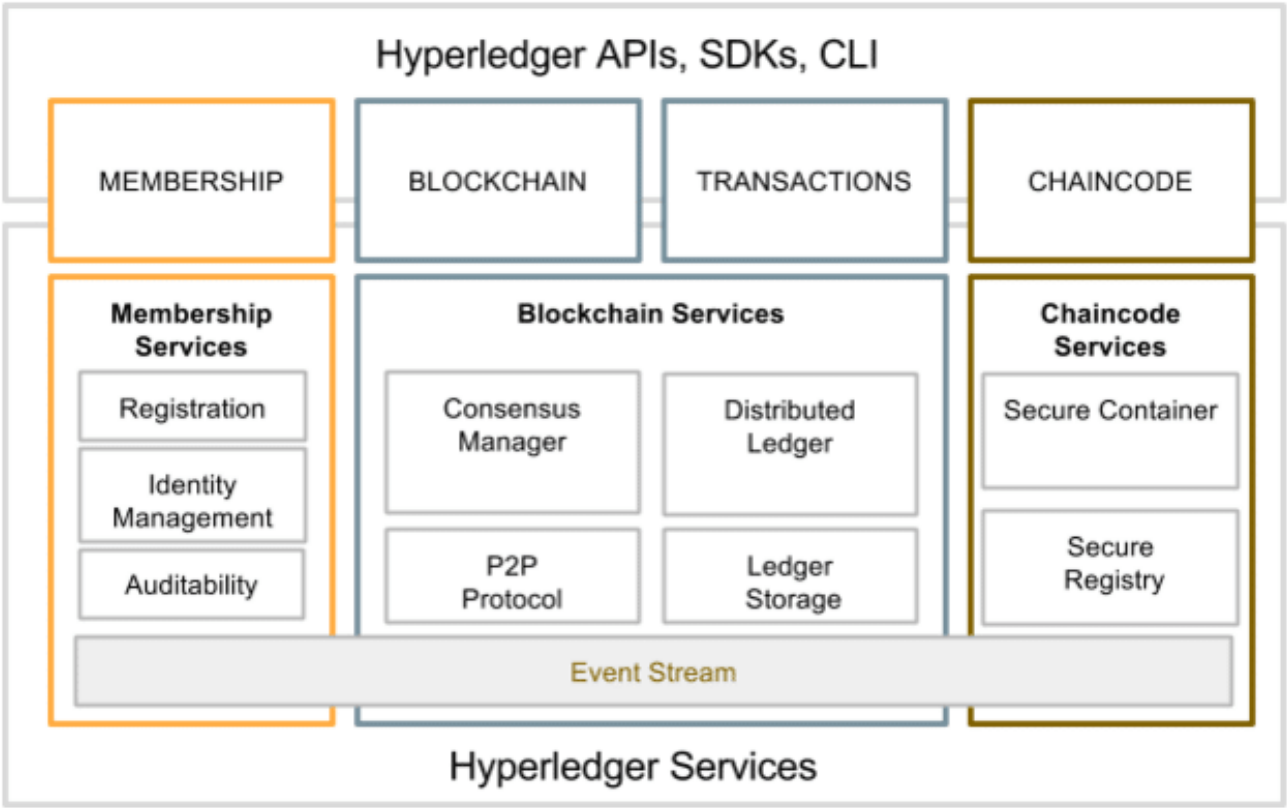


Figure 9 – Architecture générale de Hyperledger

Blockchain privée : Hyperledger

- 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.

Blockchain privée : Hyperledger

- **Hyperledger explorer** : conçu pour créer une application Webconviviale, 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.

Composantes Hyperledger Fabric : Membre

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.

Composantes Hyperledger Fabric : Actif

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.

Composantes Hyperledger Fabric : Chaincode

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.

Composantes Hyperledger Fabric : Ledger

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.

Composantes Hyperledger Fabric : Channel

Définition

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.

Composantes Hyperledger Fabric : Membership

Définition

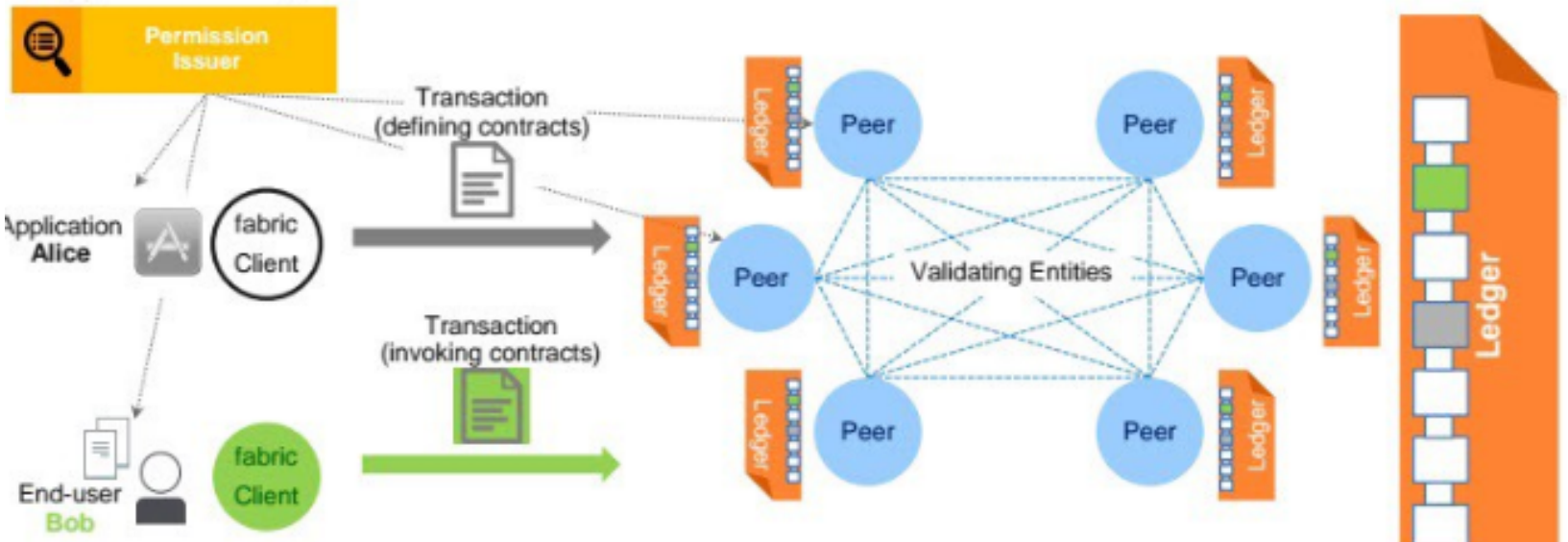
- A la différence des blockchains publiques qui sont ouverts à tous comme Bitcoin, les blockchains utilisées par Hyperledger sont privées et impliquent donc que l'identité de tous les membres soit connue.
- L'identité des *Peer Nodes*, des Client Applications, des *Business Entities* et des Administrateurs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

Composantes Hyperledger Fabric : Consensus method

Définition

- Technique utilisée par les membres du réseau pour décider quel bloc 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, etc.

Blockchain privée : Hyperledger



- **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 10 – Modèle de Hyperledger Fabric

Merci pour votre attention.
Commentaires ? Questions ?

Contenu

Exemple

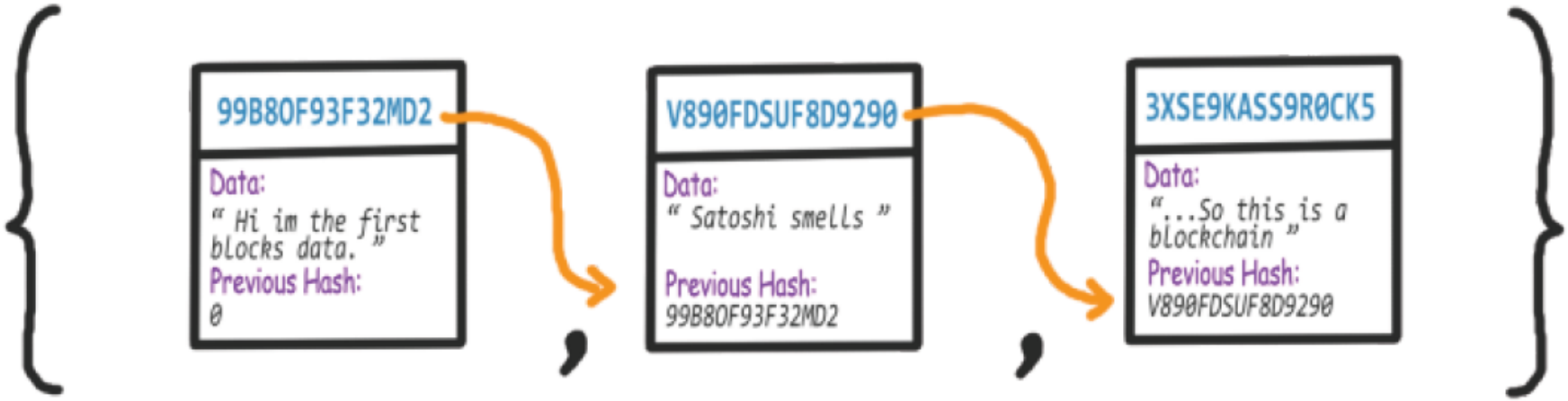


Figure 11 – Exemple de blocs

Caractéristiques d'un bloc

Un bloc ?

Un bloc peut-il être considéré comme une classe ?

Un bloc au vue de l'exemple est caractérisé par :

- *Hash* : string
- *previousHash* : string
- *data* : string
- *timeStamp* : Long

Le constructeur

- Quel devra être le ou les paramètres du constructeur ?

Le constructeur

- Quel devra être le ou les paramètres du constructeur ? Le *previousHash* et les données.
- Intégrer le calcul des *Hash* en se servant de l'utilitaire *StringUtil* à votre disposition.

Le constructeur

- Quel devra être le ou les paramètres du constructeur ?
  Le *previousHash* et les données.
- Intégrer le calcul des *Hash* en se servant de l'utilitaire *StringUtil* à votre disposition.
- Tester le bon fonctionnement de la classe Bloc dans un main.
  - Créer par exemple trois différents blocs et afficher-les

Le constructeur

- Quel devra être le ou les paramètres du constructeur ?
  Le *previousHash* et les données.
- Intégrer le calcul des *Hash* en se servant de l'utilitaire *StringUtil* à votre disposition.
- Tester le bon fonctionnement de la classe Bloc dans un main.
  - Créer par exemple trois différents blocs et afficher-les
  - On peut rassembler ces blocs dans un réseau ! *public static ArrayList<Block> blockchain = new ArrayList<Block>()*
  - Intégrer le fichier Jar Gson pour l'affichage. *GsonBuilder().setPrettyPrinting().create().toJson()*
- Écrire la fonction *isChainValid()* pour vérifier l'intégrité de la chaîne. Elle retourne un *boolean*.

Le Minage ! ! !

- C'est quoi le minage est quelle est son utilité ?

Le Minage ! ! !

- C'est quoi le minage est quelle est son utilité ?
- Ici la difficulté à introduire est de s'assurer que tout hash commence par un nombre indiqué de 0.

Le Minage ! ! !

- C'est quoi le minage est quelle est son utilité ?
- Ici la difficulté à introduire est de s'assurer que tout hash commence par un nombre indiqué de 0.
  String target = new String(new char[difficulty]).replace('\0', '0');
- Ajouter le nonce.
- Revoir le calcul du hash
- Écrire la fonction du minage
- S'assurer de miner avant d'ajouter dans la chaîne

Validité du bloc

Avec le minage réalisé, le contenu de la fonction *isChainValid()* devra connaître des modifications.

Validité du bloc

Avec le minage réalisé, le contenu de la fonction *isChainValid()* devra connaître des modifications.

- Vérifier le *hash* calculé
- Vérifier si le niveau de difficulté est respecté
- Le hash précédent figurant dans un bloc i est-il égal au hash du bloc $i - 1$
- etc.

Contenu

Ajout de portefeuille

- Créer la classe *Wallet* pour implémenter les portefeuilles.
- Un portefeuille est caractérisé par quoi ?

Ajout de portefeuille

- Créer la classe *Wallet* pour implémenter les portefeuilles.
- Un portefeuille est caractérisé par quoi ?
  - Une adresse publique public *PublicKey*
  - Une adresse privée *PrivateKey*
- Dans son constructeur sans paramètre, il suffira de générer les deux clés. On vous donnera la fonction *generateKeyPair()* qui permet de générer les clés.

Transactions et signature

Une transaction est caractérisée par :

- Sa clé *TransactionId*
- L'adresse publique de celui qui envoie les fonds (*sender*)
- L'adresse publique de celui qui reçoit (*receiver*)
- Le montant envoyé
- Les transactions *inputs* ayant permis au *sender* d'envoyer, preuve que le *sender* a suffisamment de fonds : collection de *TransactionInput*

Transactions et signature

- *Outputs*, qui montrent le montant reçu par le *receiver* et le reliquat éventuel du *sender* : collection de *TransactionOutput*
- Une signature, qui prouve que le propriétaire de l'adresse est celui qui envoie cette transaction
- Pour distinguer une transaction à l'autre ajouter soit un *timestamp* pour chacune ou ajouter une séquence (un entier) pour les décompter

TransactionInput et TransactionOutput

- Pour TransactionInput : C'est une *transaction output* qui devient une *transaction intput*.
- La notion de UTXO : *Unspent Transaction*
- Une TransactionOutput sera caractérisé par :
  - Son identifiant *id*
  - L'adresse du *reciepient*
  - Sa valeur
  - L'identifiant de la translation qui lui a donné naissance : *parentTransactionId*

TransactionInput et TransactionOutput

- Pour TransactionInput : C'est une *transaction output* qui devient une *transaction intput*.
- La notion de UTXO : *Unspent Transaction*
- Une TransactionOutput sera caractérisé par :
  - Son identifiant *id*
  - L'adresse du *reciepient*
  - Sa valeur
  - L'identifiant de la translation qui lui a donné naissance : *parentTransactionId*
- Son constructeur : *reciepient*, *value*, *parentTransactionId*. *id = StringUtil.applySha256(StringUtil.getStringFromKey(reciepient)+Float.toStr*

Traiter une transaction

- Ecrire la fonction *calulateHash()* pour le calcul de l'identiifiant.
- Se servir de *StringUtil* pour écrire les fonctions *generateSignature* et *verifySignature*.
- Tester pour l'instant dans le *main* les *wallet* et les signatures.

Traiter une transaction

- Ecrire la fonction *calulateHash()* pour le calcul de l'identiifiant.
- Se servir de *StringUtil* pour écrire les fonctions *generateSignature* et *verifySignature*.
- Tester pour l'instant dans le *main* les *wallet* et les signatures.
- Si tout marche essayer à présent de traiter une transaction : *processTransaction()* retourne un *boolean*.
- Changer la structure des blocs, ajouter les transactions aux blocs.
- Simuler votre blockchain avec deux portefeuilles au moins.

Merci pour votre attention.
Commentaires ? Questions ?