

SECURITE DES BASES DE DONNEES (O7CYASBD)



Introduction

Présentation du cours

- Prof intervenant : Marwane Ayaida
 - Professeur au Département Electronique de l'INSA HdF
 - Membre de l'IEMN
- Module O7CYASBD : SECURITE DES BASES DE DONNEES
 - 10 H de CM :
 - Définition et problématique de la Blockchain
 - Notions du consensus et du distribué
 - Fonctionnement des Smart Contracts
 - Plateforme Ethereum
 - 4 H de TD :
 - Tests de la plateforme Ethereum
 - Exemples de Codes en Solidity
 - 6 H de TP :
 - Smart Contrats à developper et à tester
 - Contrôle continu :
 - Compte-rendu de TP
 - DS



sommaire

- Introduction à la Blockchain
- Les bases de la Blockchain
- La structure de la Blockchain
- Les opérations de base de la Blockchain
- Au-delà du Bitcoin

Introduction à la Blockchain

Que pouvez vous dire sur... ?

- Système distribué?
- Consensus?
- Bitcoin?
- Blockchain?
- Ethereum?
- Smart Contracts?
- Sécurisation des échanges (Clés, Hashage, etc.)



Introduction à la Blockchain

Introduction à la Blockchain ?

- Questions légitimes :
 - C'est quoi la Blockchain ?
 - Pourquoi s'en soucier?
- Blockchain :
 - Permet le transfert en peer to peer d'actifs numériques sans aucun intermédiaire
 - Créée à l'origine pour soutenir la Crypto-monnaie Bitcoin
 - Avance depuis indépendamment du Bitcoin
- Domaines de la Blockchain :
 - Finance
 - Santé
 - Gouvernement
 - Production
 - Distribution
 - Etc.



Source: <https://medium.com/m/global-identity/redirectUrl=https%3A%2F%2Fbetterprogramming.pub%2Funderstand-how-a-blockchain-peer-to-peer-network-works-565ecd34c6d2>



Introduction à la Blockchain

Applications de la Blockchain

- Permet d'innover et de transformer un large éventail d'applications :
 - Transfert de médias numériques : ventes d'oeuvre d'art
 - Prestation de services à distance : voyages et tourisme
 - Plateforme décentralisée pour le business : le déplacement du calcul vers des sources de données
 - L'intelligence distribuée : l'obtention des diplômes d'éducation
 - Utilisation des ressources distribuées : production et distribution d'énergie
 - Crowd funding : collecte de fonds de démarrage
 - Crowd operations : vote électronique
 - Gestion des identités : un identifiant pour toutes les fonctions de votre vie
 - Mise à disposition des documents publics du gouvernement : gouvernement ouvert
 - Etc.
- Aller vers une économie plus inclusive :
 - Participer à un processus démocratique quand on est dans un coin reculé dans le monde
- Les possibilités d'applications innovantes sont infinies :
 - Un besoin grandissant pour les concepteurs et développeurs pour concevoir et créer de nouveaux modèles d'application pour la blockchain pour que cela bénéficie au monde entier.

Les bases de la Blockchain

Focus sur le Bitcoin



- Deux innovations majeures sont à mettre sur le compte du Bitcoin :
 - C'est un système de monnaie numérique disponible d'une façon continu
 - C'est le premier modèle de mise en oeuvre de la technologie d'application décentralisée autonome qui est la Blockchain.
- Bitcoin est une des applications de la Blockchain.
- Un peu d'historique :
 - L'avènement d'Internet a transformé tous les aspects de notre vie
 - Fonctionnement des marchés boursiers
 - Explosion des technologies Web 2.0 et de l'e-commerce
 - En 2008-2009 : crise financière et des subprimes
 - Le confiance dans les institutions et les marchés s'est effondrée.
 - Satoshi Nakamoto a introduit une nouvelle monnaie numérique, une crypto-monnaie, appelée Bitcoin.
- Le Bitcoin a permis de mettre en oeuvre une plate-forme innovante pour le transfert de valeur de pair à pair sans aucune autorité centrale.

Les bases de la Blockchain

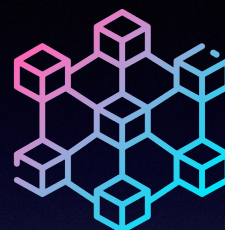
Fonctionnement du Bitcoin



- Sans autorité centrale, comment le Bitcoin permet-il de garantir la confiance et la sécurité ?
 - La mise en oeuvre de logiciels pour la validation, la vérification et le consensus dans une nouvelle infrastructure appelée Blockchain.
 - À partir de 2012-2013, des éléments de calcul ont été rajoutés à cette Blockchain
 - Ceci a ouvert la porte à de nouvelles applications autres que juste le transfert d'argent
- ==> Généralisation vers la Blockchain

Les bases de la Blockchain

Qu'est-ce que la Blockchain ?



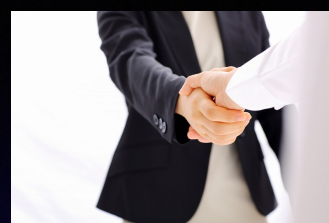
- La Blockchain est un système d'équipements qui sert à :
 - activer les transactions de pair à pair dans un réseau décentralisé
 - établir la confiance entre pairs inconnus
 - enregistrer les transactions dans un livre distribué immuable (appelé immutable Ledger).

Les bases de la Blockchain

Centralisé Vs. Décentralisé

- Essayons de comprendre la différence entre « centralisé » et « décentralisé » avec un scénario simple :
 - Scénario : un client veut acheter un bien avec sa carte de crédit
 - Fonctionnement centralisé :
 - Les intermédiaires :
 - L'agence de carte de crédits (Visa, Mastercard, etc.)
 - La banque du client
 - Un échange et un transfert d'argent
 - La banque du marchand
 - Le marchand
 - Fonctionnement décentralisé :
 - Sans intermédiaire
 - Les paires (noeuds) traitent directement ensemble quelque soit l'endroit où ils se trouvent
 - Les fonctions réalisées par les intermédiaires sont déplacées vers la périphérie et donc vers les participants dans l'infrastructure Blockchain
 - Les pairs ne sont pas nécessairement connus les uns des autres

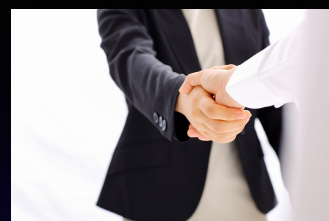
Les bases de la Blockchain



Confiance dans un système décentralisé

- Comment est mise en place cette confiance ?
 - Mise en place d'un processus pour la :
 - validation des transactions
 - vérification des transactions
 - confirmation des transactions
 - Enregistrement de la transaction dans le Livre (Ledger)
 - Création d'un enregistrement inviolable des blocs
 - Rajout à la chaîne ces blocs en utilisant un algorithme de consensus
 - Pour résumer : la validation, la vérification, le consensus et l'enregistrement immuable conduisent à la confiance et à la sécurité de la Blockchain.

Les bases de la Blockchain



Exemple de scénario dans un système décentralisé



Emilie



Martin



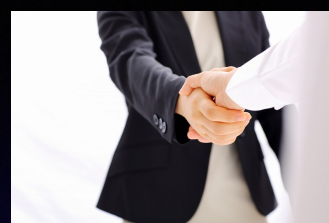
Lina



Kevin



Les bases de la Blockchain

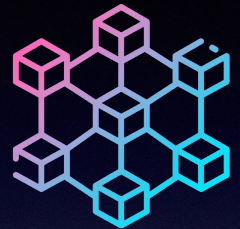


Extension du scénario dans un système décentralisé

- Le scénario précédent présente le concept de base d'un Ledger distribué immuable défini dans un processus de Blockchain.
- Dans ce scénario, tout le monde se connaît et sont physiquement dans le même endroit :
 - Quid d'une transaction en ligne avec quelqu'un d'inconnu?
 - Quid de 10 000 transaction, voire 1M de transactions?
- Martin doit être capable de traiter aussi facilement qu'avec Lina, Emilie ou Kevin, même en ligne.
- Il est demandé à la Blockchain de supporter les mêmes fonctionnalités qu'avec un système centralisé :
 - Kevin doit valider la transaction précédente de 10€, s'il trouve 8€, il refuse la transaction
 - Donc, les mécanismes de validation, puis de vérification conçus par la Blockchain et mises en œuvre par les noeuds fournissent la confiance nécessaire dans un système décentralisé

Les bases de la Blockchain

Résumé de la Blockchain



- La Blockchain est une technologie qui permet de mettre en oeuvre les fonctionnalités nécessaires à un système peer-to-peer décentralisé, telles qu'un modèle de confiance collectif et un registre immuable distribué des enregistrements de transactions.

Les bases de la Blockchain

Quizz I

Le Bitcoin est-il un système centralisé ou décentralisé d'échange de valeur ?

- 1. Centralisé
- 2. Décentralisé 

Les bases de la Blockchain

Quizz 2

La validation, la vérification, l'enregistrement immuable et _____ conduisent à la confiance et à la sécurité.

- 1. Les algorithmes
- 2. Les jetons
- 3. La monnaie
- 4. Le consensus ✅

Les bases de la Blockchain

Quizz 3

Qui a introduit la crypto-monnaie numérique en ligne connue sous le nom de Bitcoin ?

1. Hal Finney
2. Wei Dai
3. Satoshi Nakamoto 
4. Nick Szabo

Les bases de la Blockchain

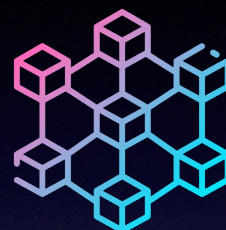
Quizz 4

Une Blockchain permet le transfert peer-to-peer de monnaie numérique sans aucun intermédiaire tel qu'une banque.

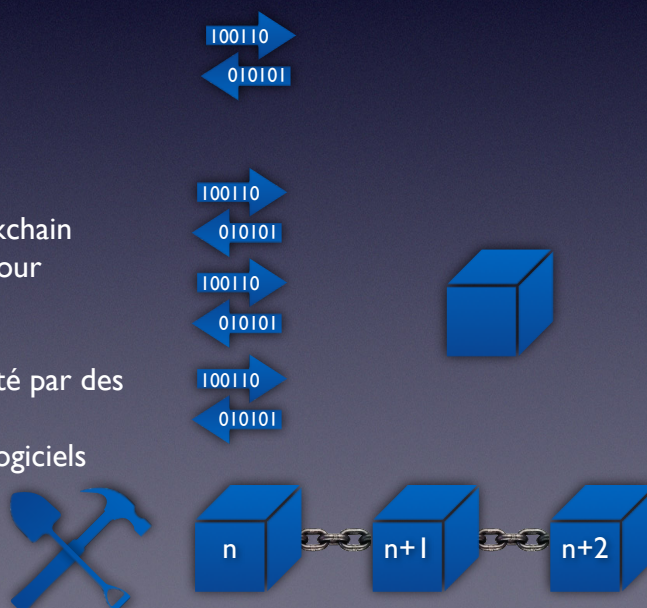
- 1. Vrai 
- 2. Faux

La structure de la Blockchain

Structure de la Blockchain



- La transaction est l'élément de base d'une Blockchain
 - Ces transactions sont validées et diffusées
- Un ensemble de transactions forme un bloc
- Les blocs sont chaînés ensemble pour former la Blockchain
- Les noeuds font appel à un processus de consensus pour sélectionner le bloc suivant qui sera ajouté à la chaîne
- Le bloc choisi est vérifié et ajouté à la chaîne actuelle
- Le processus de validation et de consensus est exécuté par des noeuds homologues spéciaux appelés mineurs :
 - Ce sont des ordinateurs puissants exécutant des logiciels définis par le protocole de la Blockchain

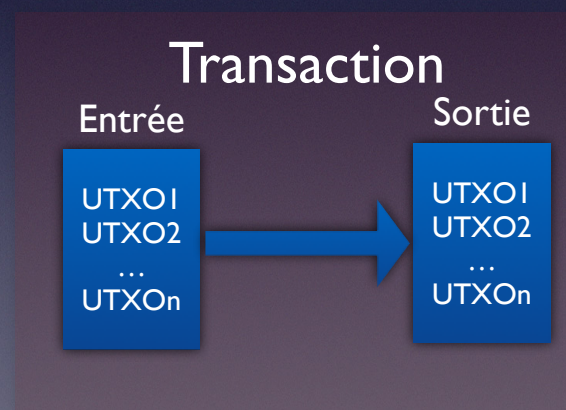


La structure de la Blockchain

La transaction dans le Bitcoin



- Un concept fondamental du réseau Bitcoin est la sortie de la transaction non dépensée (Unspent Transaction Output), également connu sous le nom UTXO
- L'ensemble de tous les UTXOs dans un réseau Bitcoin définit collectivement l'état de la Blockchain Bitcoin
- Les UTXOs sont référencés comme entrées dans une transaction.
- Les UTXOs sont également des sorties générées par une transaction
- Tous ces UTXOs sont stockés par les nœuds participants dans une base de données

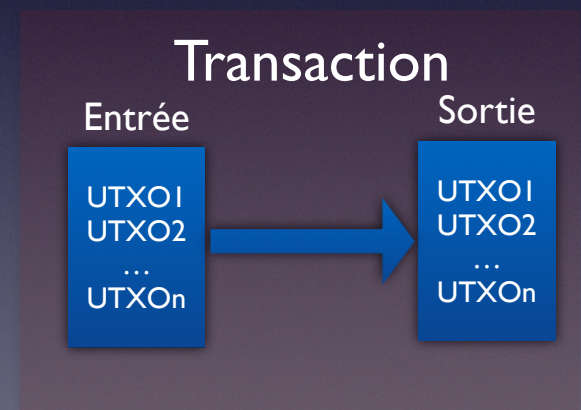




La structure de la Blockchain

La validation d'une transaction dans le Bitcoin

- Les participants peuvent valider le contenu de la transaction :
 - La référence de l'UTXO d'entrée existe-t-elle dans l'état actuel du réseau ?
 - Ces UTXOs sont-ils valides?
 - Ex : Emilie qui vérifie le registre de Martin
 - Il existe plusieurs autres critères de validation...





La structure de la Blockchain


Exploration de la Blockchain Bitcoin

- Explorons maintenant une transaction : <https://www.blockchain.com/btc/tx/22bb5dd2a88f9c5183df59aef20a44b8bce4a4056562b5d9cfff20a0ae2ffc1a>
- Explorons un Bloc (Genesis Block) : <https://www.blockchain.com/explorer/blocks/btc/0>
- Explorons un autre Bloc : <https://www.blockchain.com/explorer/blocks/btc/428808>
- Considérons maintenant la chaîne de trois blocs :
 - 488867 : <https://www.blockchain.com/explorer/blocks/btc/488867>
 - 488868 : <https://www.blockchain.com/explorer/blocks/btc/488868>
 - 488869 : <https://www.blockchain.com/explorer/blocks/btc/488869>
- Pour résumer :
 - La transaction entraîne un transfert de valeur dans la Blockchain Bitcoin
 - Le concept d'UTXO définit les entrées et les sorties d'une telle transaction
 - Une fois qu'un bloc est vérifié en utilisant un algorithme prédéfini par les mineurs, il est ajouté à la chaîne de blocs, à savoir la Blockchain.

La structure de la Blockchain

Quizz 5


Un bloc dans une Blockchain a une en-tête et des _____.

- 1. Ledger numérique
- 2. Bitcoins
- 3. Transactions 
- 4. Entrées

La structure de la Blockchain

Quizz 6

Que signifie UTXO ?

- 1. Unspent Trade Offer
- 2. Unspent Transaction Output 
- 3. Unique Transaction Offer
- 4. Unsent Transaction Output

La structure de la Blockchain

Quizz 7


Une transaction génère de nouveaux UTXOs pour transférer le montant spécifié dans les UTXOs d'entrée.

- 1. Vrai 
- 2. Faux

La structure de la Blockchain

Quizz 8

Les mineurs sont des ordinateurs qui exécutent les _____.

1. opérations définies par des transactions
2. opérations définies par les utilisateurs
3. opérations définies par le protocole blockchain 

Les opérations de base de la Blockchain

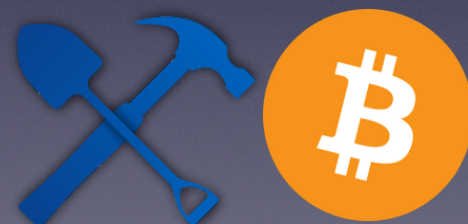
La définition des opérations

- Les opérations dans le réseau décentralisé sont sous la responsabilité des noeuds participants et de leurs capacités de calcul
 - Ex : ordinateurs fixes, ordinateurs portables, serveurs, etc.
- Ces opérations sont principalement :
 - La validation des transactions
 - La collecte des transactions pour un bloc
 - La diffusion des transactions valides ainsi que les blocs
 - L'exécution du consensus pour la création du prochain bloc
 - L'enchaînement des blocs ensemble pour former l'enregistrement immuable

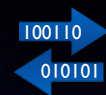
Les opérations de base de la Blockchain

Les participants à la Blockchain

- Les participants à la Blockchain sont principalement :
 - Les noeuds initiateurs du transfert d'une valeur en créant une transaction
 - D'autres noeuds supplémentaires, appelés aussi mineurs, qui choisissent de prendre un travail supplémentaire qui permet de :
 - Vérifier les transactions
 - Diffuser les transactions
 - Entrer en concurrence pour revendiquer le droit de créer un bloc
 - Travailler avec les autres pour parvenir à un consensus en validant le bloc
 - Diffuser le bloc nouvellement créé
 - Confirmer ou infirmer les transactions
- Nombre de mineurs : change mais plus de 1M de mineurs (compte individuels)
- Pourquoi ces mineurs font ce travail?
 - ==> Ils sont rétribués en Bitcoin pour leurs efforts de maintenance!

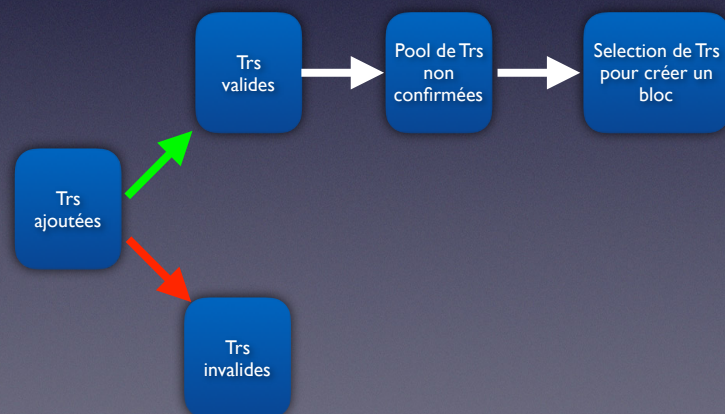


Les opérations de base de la Blockchain



La validation d'une transaction dans la Blockchain

- Ce processus implique la validation de plus de 20 critères :
 - La taille,
 - La Syntaxe,
 - La validité des UTXOs d'entrée,
 - La validité des UTXOs de sortie,
 - Le montant de référence de l'entrée et celui de sortie correspondent bien,
 - Etc.
- Les transactions non valides sont rejetées et ne sont pas diffusées
- Toutes les transactions valides sont ajoutées à un pool de transactions
- Les mineurs sélectionnent un ensemble de transactions dans ce pool pour créer un bloc

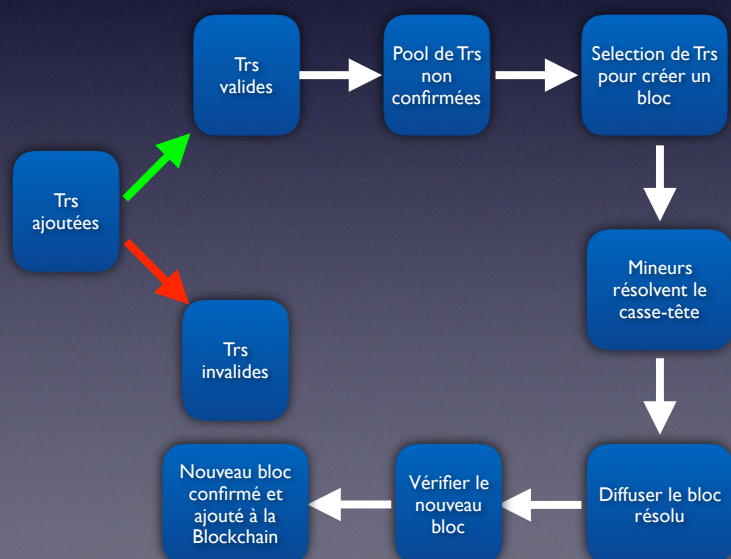


Les opérations de base de la Blockchain

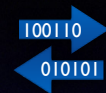


La création d'un bloc dans la Blockchain

- Ce mode de création présente un challenge :
 - Qu'est-ce qui se passe si chaque mineur crée son propre bloc?
 - ==> Il y aura plusieurs branches de la chaîne et donc un état incohérent entre les noeuds.
 - Rappel : La Blockchain est une unique chaîne de blocs liés et doit rester cohérente
 - La Solution est :
 - Les mineurs rivalisent pour résoudre un casse-tête pour déterminer qui gagne le droit de créer le bloc suivant
 - Dans le Bitcoin : c'est un puzzle qui nécessite un calcul intensif en termes de CPU
 - Une fois qu'un mineur a résolu le puzzle, l'annonce est diffusée sur le réseau et le bloc est également diffusé
 - Les autres participants vérifient le nouveau bloc
 - Si les participants parviennent à un consensus, ils ajoutent ce nouveau bloc à la chaîne
 - L'ensemble des transactions sont sauvegardées
- ==> Algorithme utilisé : Proof of Work!



Les opérations de base de la Blockchain




La transaction 0 dans un bloc

- La transaction zéro à l'indice zéro du bloc confirmé est créée par le mineur du bloc d'une façon unilatérale
- Elle a un UTXO spécial qui ne correspond pas à un UTXO d'entrée.
- Elle est appelée aussi la transaction « Coinbase » qui génère les frais du mineur pour la création de ce bloc.
- Actuellement, les frais du mineur sont de 6,25 BTC pour le Bitcoin :
 - 50 BTC par bloc en 2009
 - Réduite de moitié tous les 210 000 blocs : environ 4 ans
 - Devrait tendre vers 0 en 2140 (sans changement de protocole)
 - Les mineurs seront payés seulement en frais de validation de transactions
- C'est ainsi que les nouvelles pièces sont fabriquées dans le Bitcoin.

Les opérations de base de la Blockchain

Quizz 9

L'algorithme de consensus dans la blockchain Bitcoin est appelé protocole _____.

1. Proof of Work 
2. Proof of Worth
3. Proof of Stake
4. Proof of Elapsed Time

Les opérations de base de la Blockchain

Quizz 10

La confirmation de la transaction est effectuée indépendamment par tous les nœuds mineurs.

1. Vrai 
2. Faux

Les opérations de base de la Blockchain

Quizz I I

La transaction 0 dans chaque bloc de la blockchain bitcoin
_____.

1. est utilisée pour payer les frais de mineur.
2. n'a pas d'UTXO d'entrée.
3. s'appelle la transaction Coinbase.
4. tout ce qui précède. ✅

Au-delà du Bitcoin



Les types de Blockchain

- La Blockchain Bitcoin :
 - Open-source et le code entier est disponible sur le GitHub : <https://github.com/bitcoin/bitcoin>.
 - Plus de 300 crypto-monnaies se sont inspirées de ce code pour introduire leurs propres monnaies depuis 2009.
 - Le Bitcoin propose une fonctionnalité facultative appelée « scripts » pour le transfert conditionnel de valeurs.
- La Blockchain Ethereum a étendu cette fonctionnalité de « scripts » pour un framework complet d'exécution de code appelé « Smart Contracts ».
 - Un « Smart Contract » fournit une capacité très puissante d'exécution de code pour intégrer la logique métier sur la Blockchain (# au Bitcoin)
- Selon ces capacités, il y a eu trois grandes familles de Blockchains :
 - Type 1 - Crypto-monnaies : gère seulement le transfert de crypto-monnaies
 - —> Ex : Bitcoin
 - Type 2 - Crypto-monnaies + Logique Business : gère non seulement le transfert de crypto-monnaies, mais intègre aussi la logique métier grâce à une couche supplémentaire qui permet l'exécution de codes
 - —> Ex : Ethereum
 - Type 3 - Logique Business : n'implique pas de transfert de devise, mais prend en charge l'exécution de logiciels pour la logique métier
 - —> Hyperledger de la Fondation Linux

Au-delà du Bitcoin



Les catégories de Blockchain

- Avec l'ajout de l'exécution de codes, vient la considération de l'accès public ou non à la Blockchain
- Donc, cela a donné trois catégories :
 - Catégorie 1 - Blockchain publique :
 - N'importe qui peut rejoindre et partir comme il le souhaite.
 - Les blocs de transaction et la Blockchain sont observables publiquement même si les participants sont anonymes.
 - Elle est open-source.
 - Cette restriction aide à simplifier les opérations normales tel que la création de blocs.
 - Catégorie 2 - Blockchain privée :
 - L'accès à la Blockchain est limité aux participants sélectionnés
 - Par exemple : les collaborateurs au sein d'une organisation.
 - Catégorie 3 - Blockchain autorisée : également appelée Blockchain consortium.
 - Elle est destinée à un consortium de parties collaboratrices pour initier des transactions dans une Blockchain afin de faciliter la gouvernance, la provenance et la responsabilité
 - Par exemple : un consortium de toutes les entreprises automobiles ou organisations de soins de santé.
 - La blockchain autorisée a les avantages d'une Blockchain publique en permettant uniquement aux utilisateurs autorisés de collaborer et d'effectuer des transactions

Au-delà du Bitcoin

Quizz 12

Dans une blockchain publique, un participant peut rejoindre et quitter la blockchain comme et quand il le souhaite?

- 1. Vrai 
- 2. Faux

Les bases de la Blockchain

Post-it

- La Blockchain est un système d'équipements qui sert à activer les transactions de pair à pair dans un réseau décentralisé, à établir la confiance entre pairs inconnus et à enregistrer les transactions dans un livre distribué immuable (immutable Ledger).
- La transaction entraîne un transfert de valeur dans la Blockchain Bitcoin.
- Le concept d'UTXO définit les entrées et les sorties d'une telle transaction.
- Une fois qu'un bloc est vérifié en utilisant un algorithme prédéfini par les mineurs, il est ajouté à la chaîne de blocs (la Blockchain).
- Dans le Bitcoin, il y a des nœuds initiateurs de transactions et des mineurs.
- Il y a trois types de Blockchains représentés par le Bitcoin, Ethereum et Hyperledger
- Il y a trois catégories de Blockchains : publique, privée et autorisée.
- Par la suite, on s'intéressera d'un peu plus près à la Blockchain Ethereum.