



كلية العلوم ببنزرت
FACULTÉ DES SCIENCES DE BIZERTE



Ministère de l'Enseignement Supérieur
et de la Recherche Scientifique
Université de Carthage

Blockchain

Fondements de la technologie Blockchain

Plan

- ▶ Du registre au DLT (Distributed Ledger Technologies)
- ▶ Caractéristiques d'un système de Blockchain
- ▶ Cas d'utilisation : chaîne d'approvisionnement alimentaire
- ▶ Réseau Blockchain
- ▶ Limites générales de la Blockchain publique
- ▶ Réseau de découverte et maintenance de la topologie dans la Blockchain
- ▶ Diffusion dans le réseau Blockchain
- ▶ Utilisateurs/Nœuds dans le réseau Blockchain
- ▶ Couches de la Blockchain
- ▶ Séquence de fonctionnement général de la Blockchain

Du registre au DLT (Distributed Ledger Technologies)

▶ Registre :

- ▶ Recueil qui regroupe un ensemble d'informations homogènes (registre du commerce, registre des biens fonciers, registre des présences des classes...)
- ▶ Tenu manuellement
- ▶ Risque de fraude, d'usure, ...

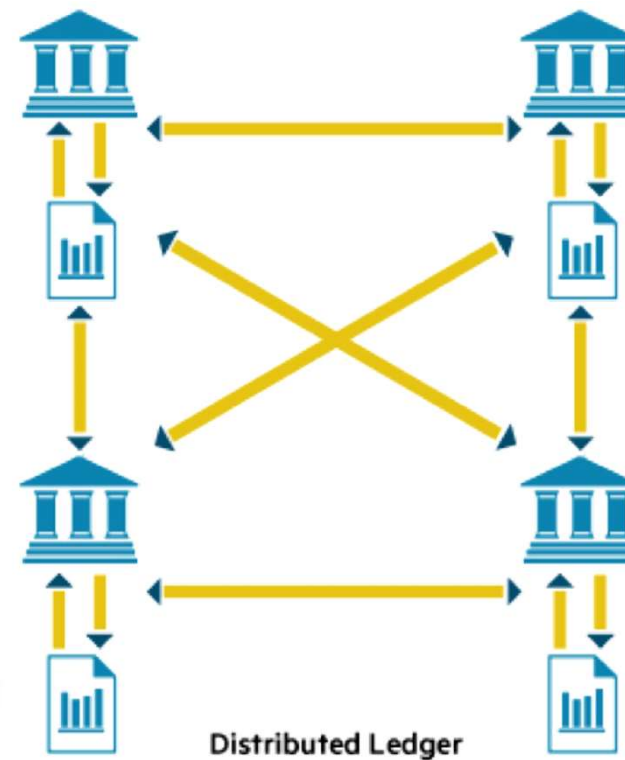
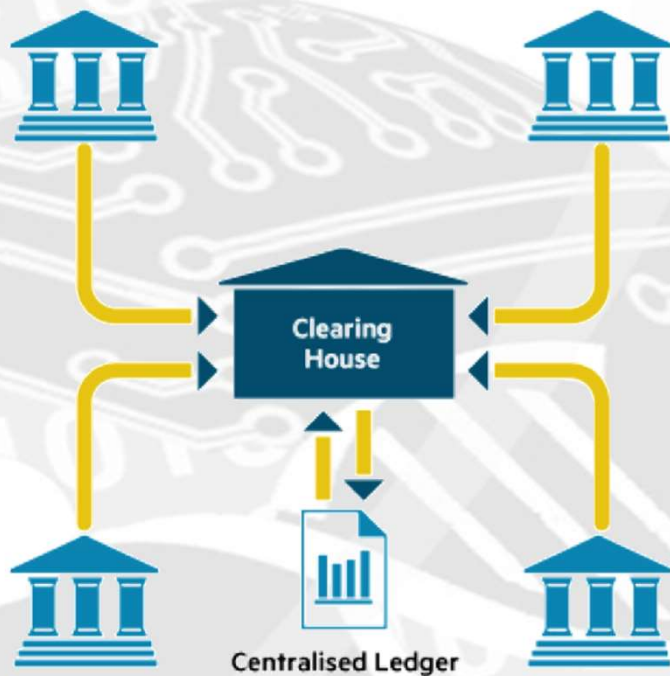
▶ DLT : registre numérisé distribué et décentralisé

Du registre au DLT (Distributed Ledger Technologies)

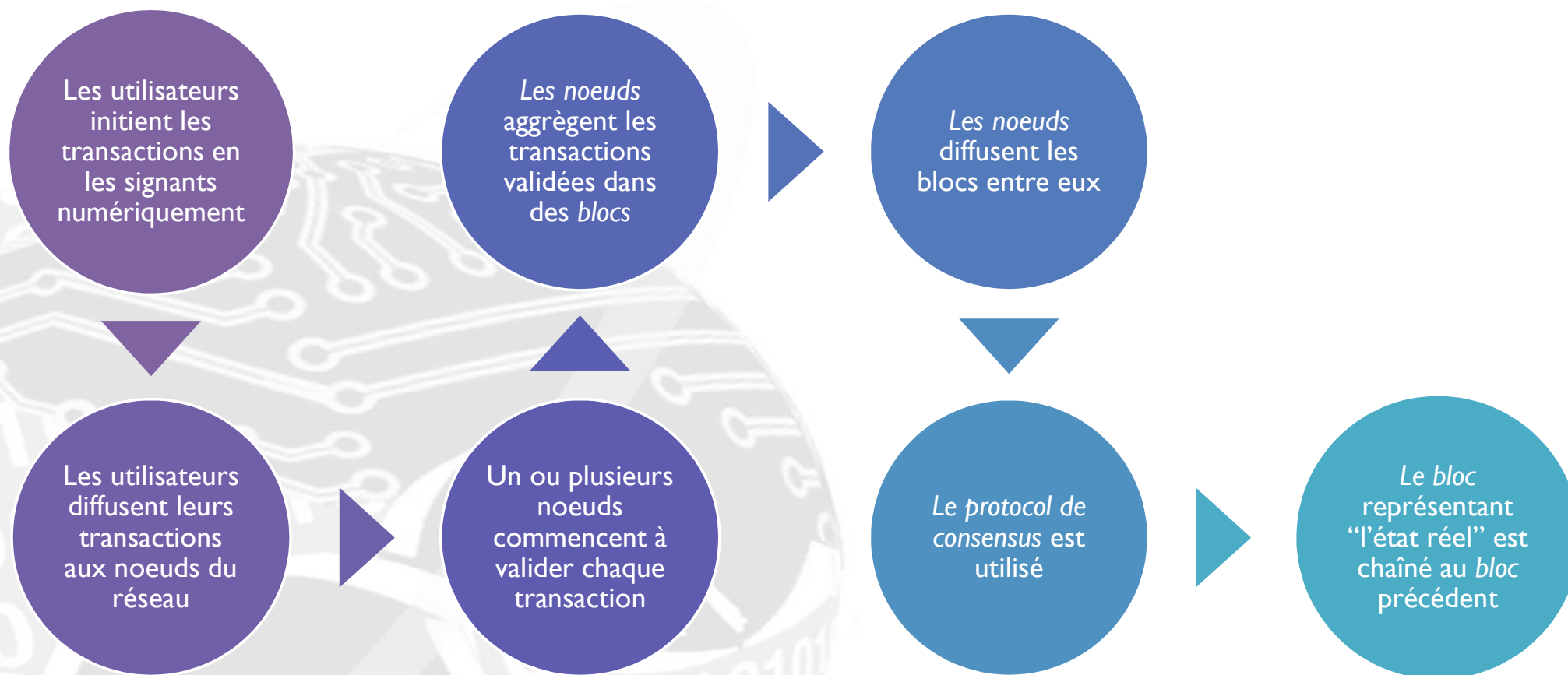
Technologie	Description
Registre	Enregistrements conservés sur les registres et les livres imprimés et gérés manuellement
Registre numérique	Enregistrements conservés sur ordinateur à l'aide de logiciels tels sous forme de traitement de texte ou de tableurs
Registre numérique distribué	Enregistrements conservés sur plusieurs ordinateurs, mais un central l'entité les gère
Registre numérique distribué décentralisé	Enregistrements conservés sur plusieurs ordinateurs mais gérés de manière décentralisée. Ceci est également connu que la technologie blockchain

Du registre au DLT (Distributed Ledger Technologies)

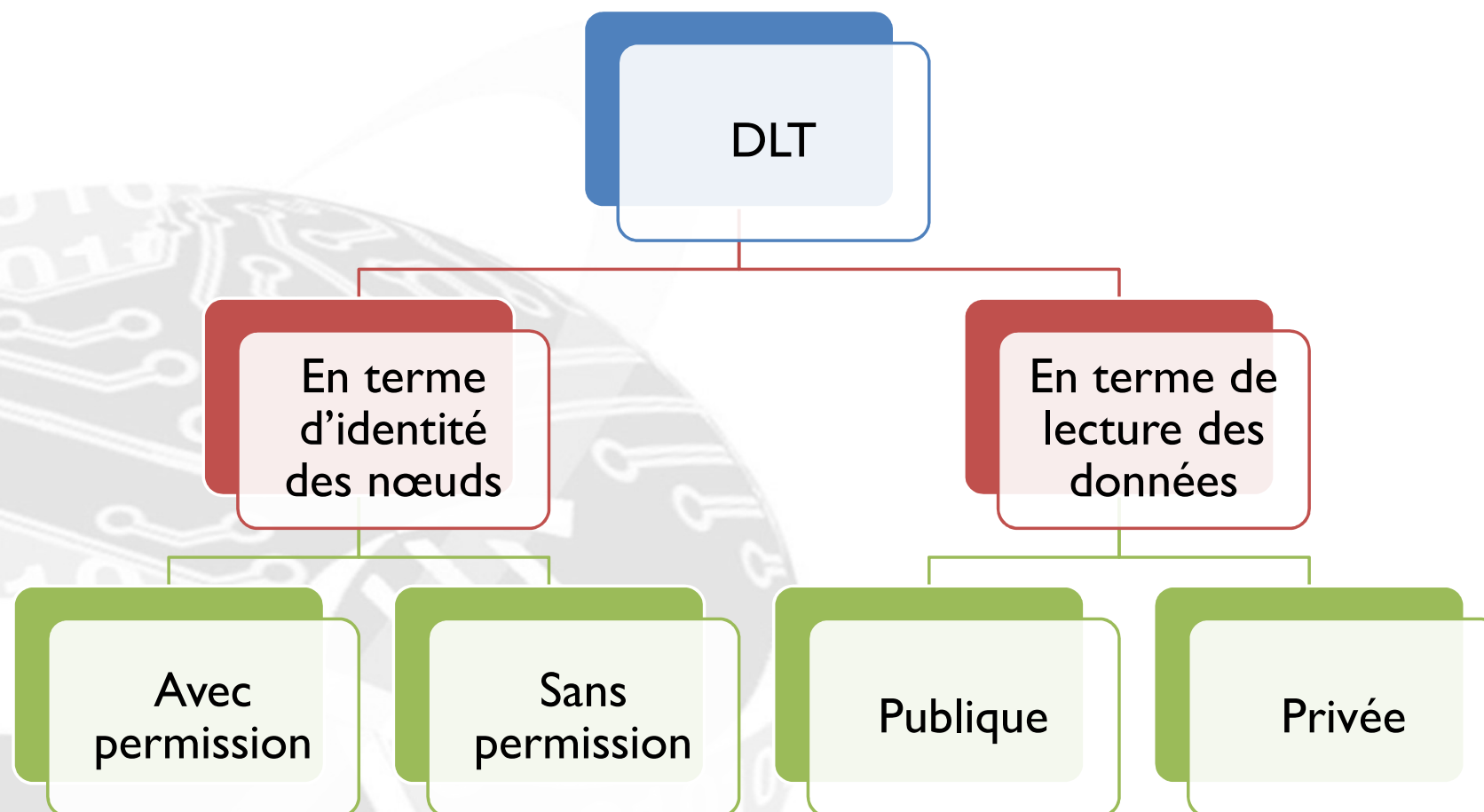
- Un ledger distribué – qu'est ce que c'est ?



Du registre au DLT (Distributed Ledger Technologies)

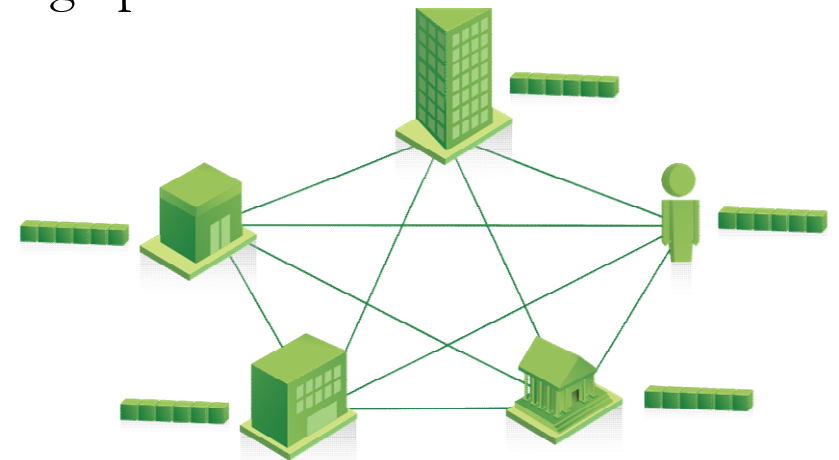


Du registre au DLT (Distributed Ledger Technologies)



Du registre au DLT (Distributed Ledger Technologies)

- ▶ Une Blockchain – Qu'est ce que c'est ?
- ▶ Technologiquement, c'est :
 - ▶ Une base de données distribuée – un registre public (il est possible d'insérer ou de rechercher des données, mais pas de les mettre à jour ou les supprimer)
 - ▶ Un ordinateur distribué – qui exécute des contrats intelligents
 - ▶ Basé sur les technologies P2P (pair-à-pair), la cryptographie et des API



Définition de Blockchain

- ▶ En fait, les blockchains forment plus qu'une technologie, elles :
 - ▶ Contiennent habituellement des transactions financières
 - ▶ Sont répliquées à travers un grand nombre de systèmes en quasi-temps réel
 - ▶ Utilisent la cryptographie et les signatures numériques pour prouver l'identité des acteurs, l'authenticité des transactions, et faire respecter les droits d'accès en lecture/écriture
 - ▶ Peuvent être accédées en écriture par un certain nombre de participants
 - ▶ Peuvent être lues par les participants, habituellement un cercle plus large que pour les droits en écriture
 - ▶ Possèdent des mécanismes pour rendre difficile le changement des données historiques, ou du moins rendent facile la détection d'une tentative de le faire



Caractéristiques d'un système de Blockchain

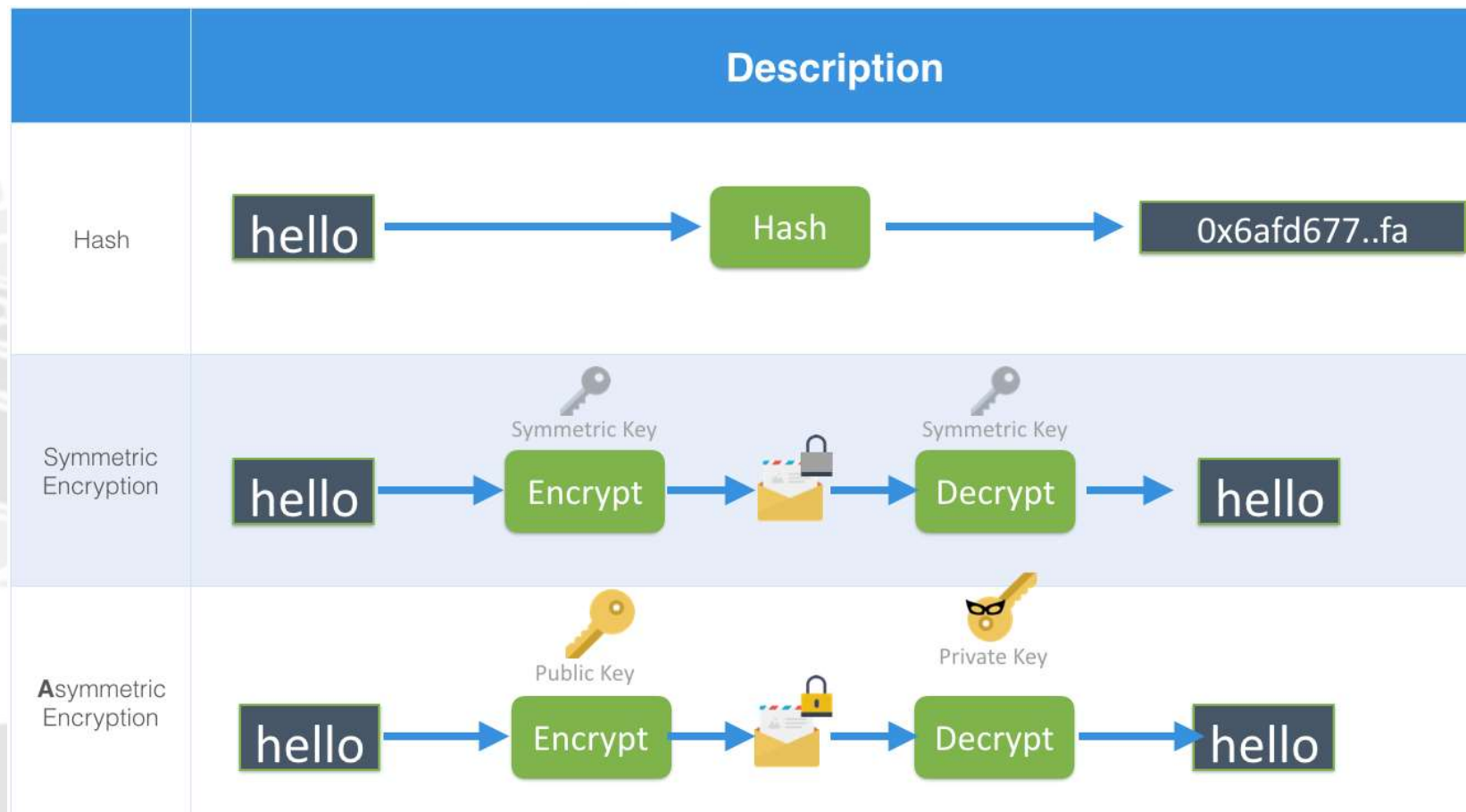
- ▶ Décentralisation
- ▶ Transparence
- ▶ Immuabilité
- ▶ Disponibilité
- ▶ Pseudonimité
- ▶ Sécurité
- ▶ Non-Répudiation
- ▶ Auditable
- ▶ Détection de falsification de données

Éléments de fonctionnement

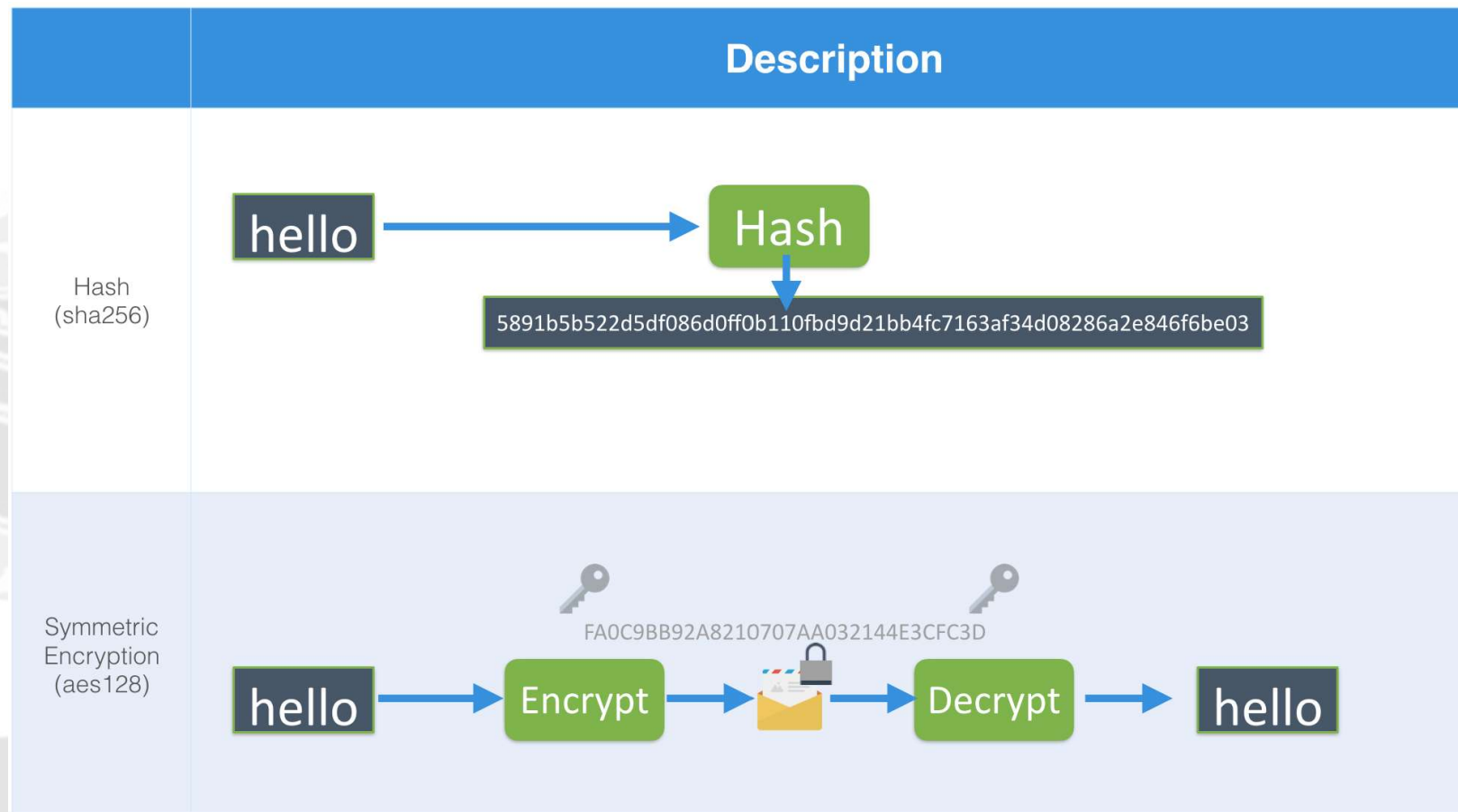
- ▶ Cryptographie: Le chiffrement et déchiffrement des données
- ▶ 2 concepts principaux de cryptographie utilisée dans la technologie Blockchain :
 - ▶ Les fonctions de hashage
 - ▶ Les signatures numériques
- ▶ Il existe 3 formes de chiffrement largement utilisées :

Cryptography symétrique	Cryptography asymétrique	Hashage
Le même mot de passe sert à chiffrer et déchiffrer les données	Un mot de passe sert à chiffrer les données, un autre à les déchiffrer	Projette vers un espace de dimension fixe
Fonction bidirectionnelle	Les mots de passe vont par pair (clé publique / clé privée)	Fonction monodirectionnelle


Éléments de fonctionnement



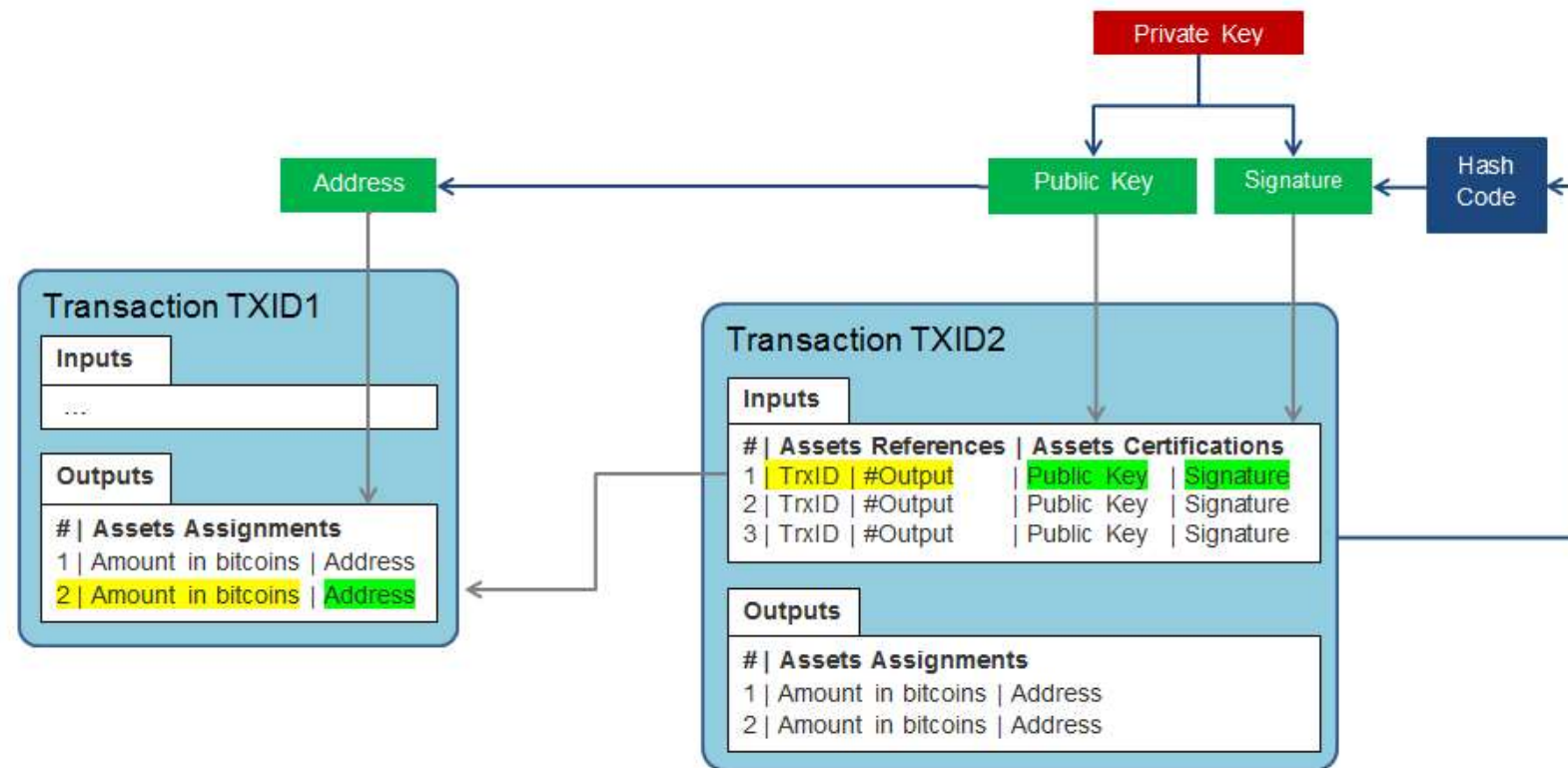
Éléments de fonctionnement



Eléments de fonctionnement

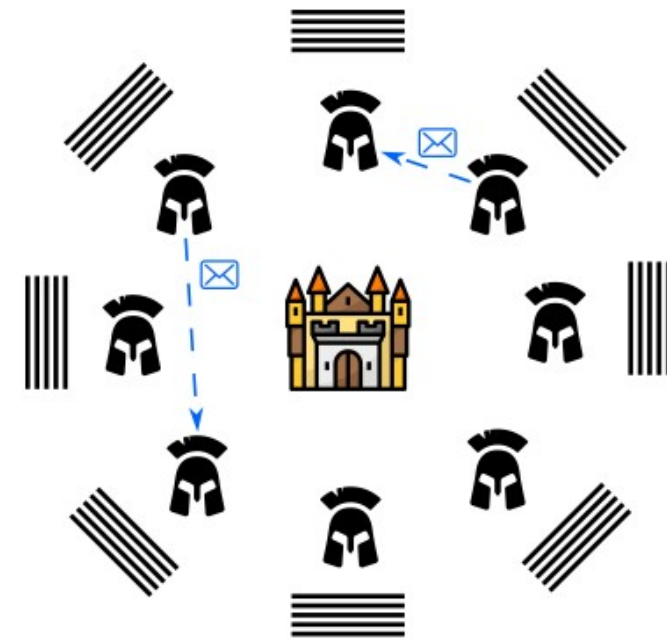
	Description	
Asymmetric Encryption	 <pre> graph LR A[hello] --> B[Encrypt] B --> C[Locked Box] C --> D[Decrypt] D --> E[hello] PK[Public Key] --> B PRK[Private Key] --> D </pre>	
Asymmetric Encryption (RSA 1024)	<pre> -----BEGIN RSA PRIVATE KEY----- MIICXQIBAAKBgQCISSbEbdh3GzlrF4OFCApMvZzTWBYucKkjs18XQ9B7peqtXj 9CejXQTTXfpRjDKM+k6TCDrlyRhfrN7zAq5SmfFreIYHa37VE8XFZP5UOylv3W bwHJXGp0AAKHx3bokh3SgJ4RFBdVvIBIFvumapQLn70ze0KE37Je3Kf2QIDAQAB AoGAluorocX7dz/DUxRyby+ElcQFGNisopHq5lBldIA96+IP6PKQys3gVx3ex5sa pktqzhVnjcMc+4LRu0Hs94oks03aKlG248vODjZPYTKINKLCHG5HmLUbsK8uCl GRl+Hxd1AGH7IoyDcfseRhMltjQY1D5GGkg6sA1nIs/AQECQQDAIJCzzV4xLWz onV45V0gTkt4wUhlvZcheWfpZoy7yW1L00zbH3XfCjbsXKagnY/vqQaA99uU6cO 8tBrOt5hAkeAtaUR8Zr+isCspb7WZ7Dv0t5yffBfkeAOCT7QI7hptJA+66KUUC KV58oUXHBGAfYrgGm+aKevePXZUm3yEeQJBALV+ThRtUuXWHRRS5nXSAYfdx17 BRXcjKnggahlwUb7+56EcAGZBvFRVnq8gv1qKPEAAppl1a4ggRstJyXvGECQClk BvIZ7Nl8T+yRo+lj+8ZFVRLUscXxRHqW7R05xks0NchoPAkE2K0BIFNu8qR6+U b9I9+UoxlIFMSolckbEQCQvIn3KbC8lBeretn5mOR8CvUmxU42vk4E0Elzy8q eWxZmTdgLWfcgm1M3dLIQCdbk15GDNKYsywdZxbF05Zz -----END RSA PRIVATE KEY----- </pre>	<pre> -----BEGIN PUBLIC KEY----- MIGfMA0GCQsGSIb3DQEBAQUAA4GNADCBiQKBgQCISSbEbdh3GzlrF4OFCApMvZz TWBYucKkjs18XQ9B7peqtXj9CejXQTTXfpRjDKM+k6TCDrlyRhfrN7zAq5SmfF reIYHa37VE8XFZP5UOylv3WbwHJXGp0AAKHx3bokh3SgJ4RFBdVvIBIFvumapQ Ln70ze0KE37Je3Kf2QIDAQAB -----END PUBLIC KEY----- </pre>
Asymmetric Encryption (secp256k1)	<pre> 8ab2da1ed39fad3491ceb556b6bf2e124822614f6987056e073452b068a12fb </pre>	<pre> 04e17e467d8f78110bea2ae18c8fa1a6963202d8ee9845c86080cb8ae5b5a 558ad279ae57e0b56259470f92021a2dccb0f7ceb68c88f25b13bce9f2c0e9c8adb8c </pre>

Eléments de fonctionnement



Problème des généraux byzantins

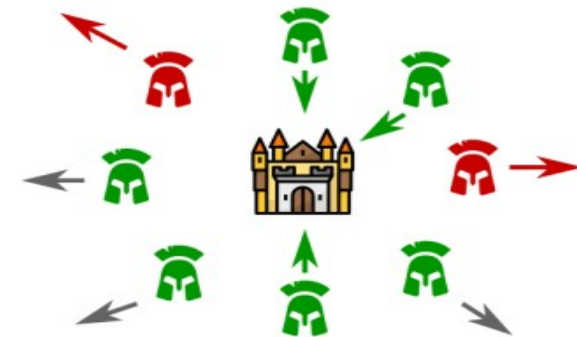
- ▶ Problème d'informatique distribuée
- ▶ Formalisé par *Leslie Lamport*, *Robert Shostak* et *Marshall Pease* en 1982
- ▶ Enoncé du problème :
 - ▶ Des généraux de l'armée byzantine campent autour d'une cité ennemie avec leurs unités et souhaitent l'attaquer
 - ▶ Ils ne peuvent communiquer qu'à l'aide de messagers oraux et doivent établir un plan de bataille commun
 - ▶ L'idée est de coordonner une attaque à un moment précis, disons à l'aube
 - ▶ Les généraux partagent ce qu'ils vont faire en envoyant le message « **attaque** » pour confirmer l'assaut, et « **retraite** » pour l'annuler.



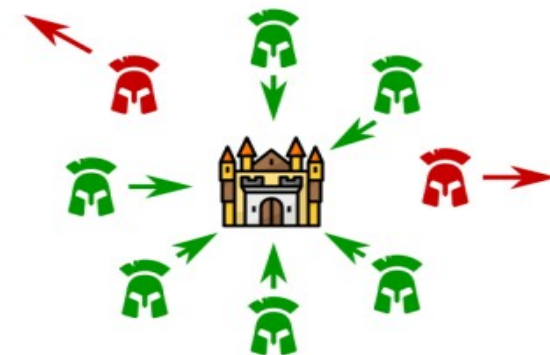
Problème des généraux byzantins

- ▶ Cependant, un certain nombre de ces généraux peuvent s'avérer être des traîtres qui essaient de semer la confusion au sein de l'armée. Ainsi, ils envoient le message « **retraite** », pour convaincre certains généraux loyaux de battre en retraite au moment de l'assaut et pour causer une défaite certaine.
- ▶ Le problème est de trouver un algorithme pour s'assurer que *tous les généraux loyaux arrivent à se mettre d'accord sur un plan de bataille*. Les traîtres trahiront tout de même en battant en retraite, mais puisque leur nombre est supposé être restreint, l'attaque sera un succès.
- ▶ Même en désignant des commandants auxquels des généraux subordonnés obéiront, *la situation fait qu'il est très difficile de parvenir à un consensus* car le commandant peut également être un traître.

Défaite



Victoire



Problème des généraux byzantins

- ▶ Objectif :
 - ▶ parvenir à un consensus
 - ▶ tolérance aux pannes byzantines (« *byzantine fault tolerance* », BFT)
- ▶ Il a été montré que le problème des généraux byzantins peut être résolu de manière absolue si et seulement si les généraux loyaux représentent strictement ***plus des deux tiers*** de l'ensemble des généraux.
- ▶ Solution :
 - ▶ Algorithme de consensus PBFT (« Practical Byzantine Fault Tolerance »), par Miguel Castro et Barbara Liskov en 1999.
 - ▶ Il permet à un nombre donné de participants de se mettre d'accord en gérant des milliers de requêtes par seconde avec une latence de moins d'une milliseconde.

Problème des généraux byzantins

► Limites des solutions classiques :

- Pas assez robustes
- Besoin de sélectionner préalablement les nœuds ayant le droit de participer au consensus : cela peut se faire par **preuve d'autorité** (« *proof-of-authority* »), via une liste blanche de nœuds, ou par **preuve d'enjeu déléguée**.
- Dans les deux cas, le système est relativement fermé et vulnérable aux attaques extérieures, puisque les nœuds validateurs sont connus de tous et donc soumis aux menaces.

Problème des généraux byzantins

► Nouvelle solution :

- nouvel algorithme de consensus qui apparaît : l'algorithme de consensus de Nakamoto par preuve de travail.
- Celui-ci met en jeu des blocs de transactions, qui sont ajoutés à une chaîne par le biais d'une dépense d'énergie électrique (d'où le terme de preuve de travail), et c'est la chaîne qui accumule le plus d'énergie (« la chaîne la plus longue ») qui est considérée valide.
- S'il peut y avoir des divergences ponctuelles dans le consensus (embranchements), ce n'est très souvent pas le cas en raison des incitations économiques du protocole : les validateurs, appelés mineurs, utilisent leur puissance de calcul en l'échange d'une récompense en bitcoins, et n'ont pas de réel intérêt à œuvrer contre le bon fonctionnement du système.

Cas d'utilisation : chaîne d'approvisionnement alimentaire

- ▶ Traçabilité et provenance dans la chaîne d'approvisionnement alimentaire
- ▶ Identification et élimination des aliments contaminés
- ▶ Blockchain pour la chaîne d'approvisionnement alimentaire

Réseau Blockchain

- ▶ Réseau Blockchain publique – Sans permission
- ▶ Réseau Blockchain privé – Avec permission
- ▶ Réseau Blockchain à consortium – Avec permission

Limites générales de la Blockchain publique

- ▶ Transactions limitées
- ▶ Mise à l'échelle
- ▶ Pseudonymité
- ▶ Taille des Block
- ▶ Consommation d'énergie

Utilisateurs/Nœuds dans le réseau Blockchain

► Type :

- Nœuds Blockchain complets
- Nœuds Blockchain légers
- Nœuds mineurs

► Comportement :

- Nœuds de la Blockchain comme leaders et validateurs
- Nœuds de la Blockchain comme émetteurs et récepteurs

Nœuds complets

► Fonctionnement :

- prennent en charge et assurent la sécurité du réseau
- téléchargent tout l'historique d'une blockchain pour observer et appliquer ses règles.

► Sous type : Super-nœud

- complet visible publiquement
- communique avec tout nœud qui décide d'établir une connexion avec lui
- fonctionne généralement tout le temps, transmettant l'historique de la blockchain et les données de transaction à plusieurs nœuds
- *De nombreux bénévoles gèrent des nœuds Bitcoin complets dans le but d'aider l'écosystème Bitcoin. À l'heure actuelle, environ 47 000 nœuds publics fonctionnent sur le réseau Bitcoin.*
- *Outre les nœuds publics, il existe de nombreux nœuds cachés (nœuds sans écoute). Ces nœuds s'exécutent généralement derrière un pare-feu.*

Nœuds légers

► Fonctionnement :

- tout utilisateur du réseau est un nœud léger
- doit se connecter à un nœud complet pour pouvoir participer.

Nœuds mineurs



► Rôle :

- vérifier les transactions et opérations effectuées par les utilisateurs sur le réseau. Il les inscrit ensuite sur la blockchain.
- la vérification des transactions requiert de la puissance de calcul.
- comme la blockchain est *open-source*, devenir mineur est ouvert à tous.

► Type :

- Mineur solo : mineur peut travailler seul, utilise son propre nœud complet
- Mineur en pool : en groupe, seul l'administrateur peut jouer le rôle d'un nœud complet, appelé nœud complet d'un mineur de pool.

Travail du mineur

- ▶ L'action de "miner" une crypto-monnaie pourrait se résumer ainsi :
 1. Le mineur reçoit en temps réel toutes les transactions émises par les utilisateurs sur le réseau.
 2. Le mineur vérifie si la signature électronique apposée par l'émetteur de la transaction est valide.
 3. Le mineur vérifie si l'adresse de l'envoyeur est bien en possession des fonds qu'elle prétend vouloir transférer sur une autre adresse.
 4. Le mineur rassemble toutes les transactions validées dans un bloc.

Travail du mineur

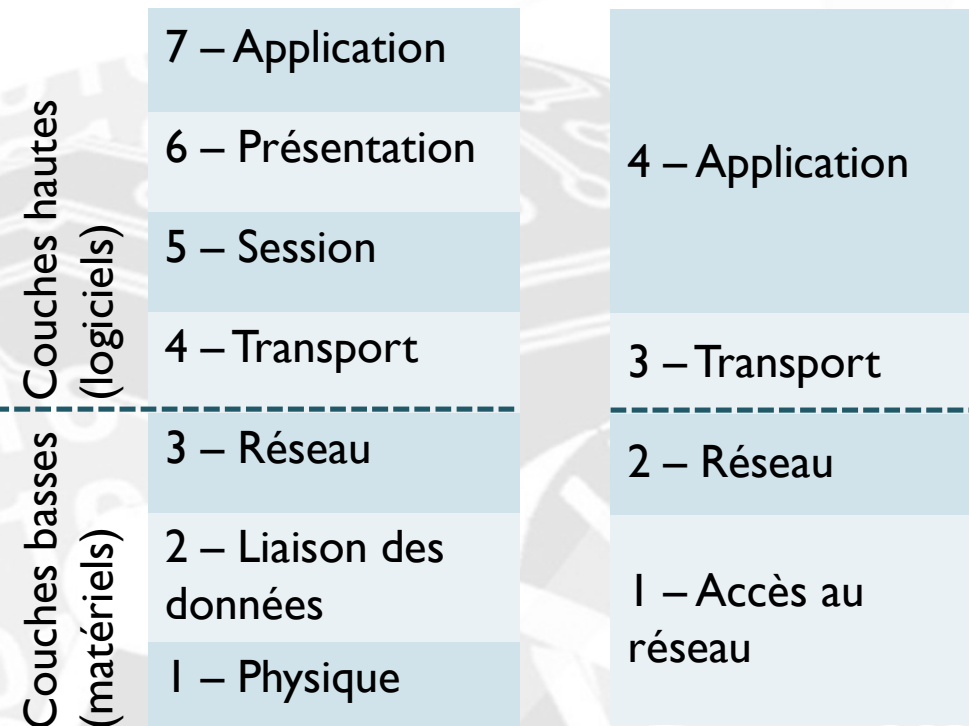
- ▶ Les tâches de minage sont réalisées par tous les mineurs du réseau.
- ▶ Dans la mesure où chacun ne reçoit pas les transactions au même moment (situation géographique, vitesse de connexion...), les blocs générés ne sont pas tous identiques
- ▶ Il est ensuite nécessaire de décider quel mineur aura le droit d'ajouter son propre bloc à la seule et unique chaîne de blocs. C'est ici que les règles de consensus interviennent. Les règles de consensus désignent le protocole selon lequel un mineur sera choisi pour ajouter son bloc au registre. Ce sont les règles de consensus qui assurent la sécurité du réseau et dissuadent les mineurs de falsifier leurs blocs. Dans le cas de la blockchain Bitcoin, on parle d'un consensus de type Proof of Work (preuve de travail) ; il s'agit de trouver la solution à un problème mathématique complexe. Le premier à résoudre le problème n'a plus qu'à en diffuser la preuve : c'est la preuve de travail. Le minage à proprement parler correspond à cette étape gourmande en énergie et en temps.

Incitation au minage

- ▶ Afin d'être récompensés pour le temps et la puissance de calcul investis, les mineurs reçoivent :
 - ▶ les frais de transactions payés par les utilisateurs (fees). L'émetteur d'une transaction peut également adjoindre un "pourboire" destiné aux mineurs. Ces derniers sont naturellement incités à sélectionner les transactions associées à des récompenses les plus élevées.
 - ▶ la récompense de minage associée à la création d'un nouveau bloc sur la blockchain : c'est de cette manière que la crypto-monnaie est créée

Couches de la Blockchain

Mise en réseau des systèmes informatiques



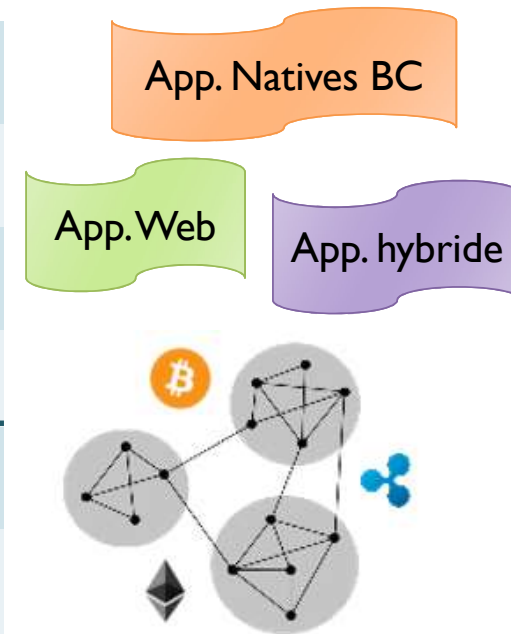
Le Modèle OSI, 1978

Le Modèle TCP/IP, 1983

Réseau et applications décentralisées



Le Modèle Bitcoin, 2009



Couches de la Blockchain

- ▶ Couche accès réseau :
 - ▶ Fonction de la couche physique et des liaisons de données
- ▶ Couche réseau :
 - ▶ Fonction d'organisation des données et des topologies
- ▶ Couche Blockchain
 - ▶ Fonctions de réseau et SE
 - ▶ L'infrastructure blockchain proprement dite, qui pose les bases de sécurité, de redondance et la logique d'assemblage des blocs
- ▶ Couche protocole
 - ▶ Fonction de consensus
 - ▶ Embarque le langage de développement des applications
- ▶ Couche jeton
 - ▶ Fonctions de virtualisation et gestion des Smart Contracts
 - ▶ Fonctions de transfert de valeur (unités de comptes d'une cryptomonnaie)
- ▶ Couche application :
 - ▶ Applications natives blockchain, appelées Dapps (Decentralized applications)