**BLOCK CHAIN**

La Block Chain est une technologie de stockage et de transmission d’informations.

Avantage réseau distribuer :

* Performant
* Robuste

Désavantage réseau distribuer :

* Surcharge réseau

Principes :

* Partager le registre entre plusieurs Opérateurs
* Chaque participant à la transaction à accès au Registre (traçage)
* Une transaction enregistrée ne peut être modifiée, elle doit être « annulée » si nécessaire auquel cas cette opération est une transaction aussi

Qu’est-ce que la Block Chain :

* Basée sur la répartition des « risques » (R.O.)
* Basée sur l’accès à l’information(blocks) tous les membres du réseau
* Basée sur Internet (P2P)
* Interdit la redondance des informations
* Interdit la modification, suppression de l’information enregistrée.
* Basée sur le cryptage

Validation d’une transaction : Principes :

* Accord de tous les participants
* Traçage du « bien » et des participants
* Transaction enregistrée de façon « immuable »
* Enregistrement dans UN registre unique partagé, accessible aux participants à la transaction entre autres.

Cryptographie :

* Encoder des informations de façon que seuls les Emetteurs et Destinataires qui sont « propriétaire » de ces informations puissent en disposer.
* C’est-à-dire : Ecrire, Lire, Modifier, Supprimer selon de Règles partagées et acceptées.
* La principale technologie utilisée est : la crypto Asymétrique (dite à clé publique) par opposition à la crypto Symétrique.

Clé symétrique :

Même clé pour chiffrer et déchiffrer.

Clé asymétrique :

Si vous voulez recevoir un message crypté ‘un destinataire, pour le crypter il lui faudra votre clé publique, **pour déchiffrer le message vous utiliserez une deuxième clé dite « privée ».**

Chainage de blocks contenant :

* Des pointeurs « précédent-suivant » (liste chaînée restrictive)
* Des transactions

Principes chainage de blocks contenant :

* Hash code => pointeur et ID unique
* Pas de possibilité de casser ce pointeur ou d’insérer un autre block entre deux blocks
* Les Hash Code sont des témoins d’intégrité !
* Rappel : Un block contient des transactions.

Composants Block Chain :

Les Nœuds légers ou complets : infrastructure

* Réseau d’ordinateurs, de serveurs donc interconnectés
* Contiennent une copie de la BC si nœud complet
* Se synchronisent (Ordinateur éteint) entre eux (Maj BC)

Les mineurs : acteurs + infrastructure :

* Qui mettent à disposition une puissance de calcul (Nœud)
* **Sont motivés financièrement**
* Sont contrôlés (« proof of stake », « proof of work »)

Les mineurs :

* Outre leur fonction de Nœuds ils créent des blocks
* Chaque mineur est différentiable : les blocks qu’il crée sont identifiables et propre à chaque mineur
* La création d’un nouveau Block doit être validée par le « réseau » d’où un gap temporel

Composants : dynamique du système :

* Avant de créer un nouveau Block, le mineur doit récupérer les Transactions qui ne sont pas encore incluses dans un Block
* Puis créer ce nouveau Block le Mineur doit résoudre un puzzle « cryptographique ». Le mineur le plus rapide gagne et peut donc l’inscrire dans la BC (Registre collectif)

Contrôle :

* Le Mineur le plus rapide pour solutionner le Puzzle transmet sur le Réseau et sa solution et son Block.
* Le Réseau (tous les nœuds) Vérifie que la solution est bonne et accepte l’inscription du nouveau Bloc

Puzzle :

* Composition : un Hash est une valeur numérique issue d’une fonction de ‘hashage’.
* Cette fonction est faite pour qu’il soit très, très difficile de retrouver sa valeur en calcul ‘brute’ [style tous les cas possibles]
* En B.C. ce code sert à :
* Vérifier que le Block n’a pas été modifié
* Lier ce block au suivant

Le Hash prend en variable les Transactions, qui ont leur propre Hash, le Hash du Block précédent etc…

* Rajoutons un nouveau champs appelé ‘Nonce’ [Number used Once], dans le Block donc le Hash change.
* Contraintes sur le Hash
* Trouver le Nonce qui donnera ce nouveau Hash.. C’est le minage
* Le Nonce est une contrainte créée à la création de la BC :
* Le Nonce est une chaine de ‘0000’ ou < 1000

**Contrôle des mineurs :**

Probleme : DeadLock : Fork

Deux blocks créés en même temps (TimeStamp)

Si 80% des Mineurs recevant le block A avant le Block très identique B, et si ces même Mineurs utilisent cette chaine alors c’est A qui l’emporte et B est «destroyed»

Proof of stake (PoS) :

**Validateur : système de ‘validation des Blocks’ concurrent ou complémentaire du PoW**

Rappel la Block Chain est basée aussi sur la théorie des jeux

Les Validateurs sont des utilisateurs qui parient qu’ils vont être élus pour Forger des Blocks.

Ils envoient des fonds dans le Pool des Validateurs ou ils sont bloqués tant que le Validateur n’a pas rempli son contrat, à savoir : Forger des Blocks

La validation d’un Block consiste à justifier d’un montant d’unité des biens propre à la BC concernée

Consensus :

Lors de la création d’un nouveau Block, tous les nœuds l’enregistrent. Mais il y a un pb de ‘Timestamp’ au niveau mondial. Il faut donc resynchroniser l’ensemble : consensus sur la genèse des écritures.