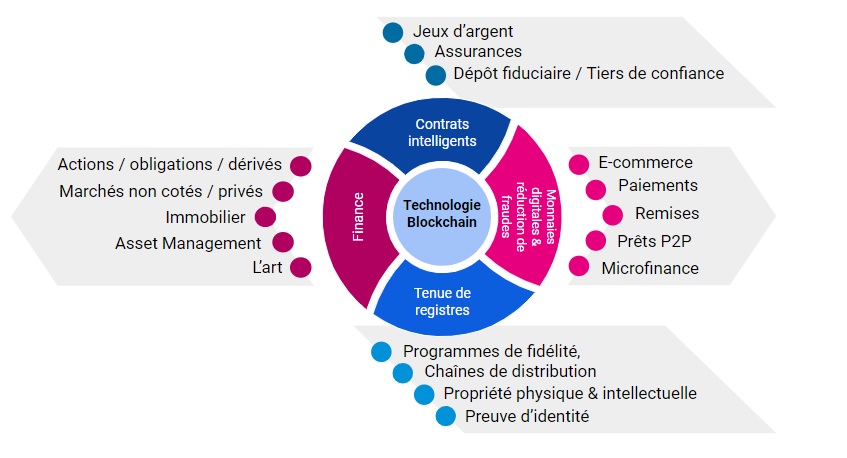
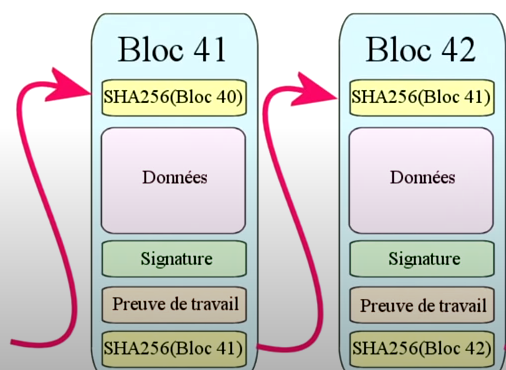
Block Chain

* Les banques cherchent même a exploité cette technologie
* Théorème FLP (théorème d’impossibilité du consensus)
* Pour les cryptomonnaies ils existent aussi un autre système, les forgeurs : Proof of Stake (PoS)
* On peut suivre de façon gratuite et publique les transactions de cryptomonnaie : <https://www.blockchain.com/explorer>
* Il n’y a pas le droit à l’erreur dans la blockchain car rien ne peut être effacer ou modifier dans le « cahier »
* Fonction de hachage importante au sein de la block Chain (cf tp2 d’intro système info) pour déterminer l’identifiant du futur block
* Réseau p2p



1. Fonctionnement

* Stockage de l’information décentralisé avec un grand nombre de contributeur
* La sécurité de la blockchain de dépend d’aucune entité
* Ralentissement des contributions grâce à un système de block (chaque block récapitule chaque évènement qui a eu lieu)
* Cumule de consensus partiel qui avec le temps et grande probabilité entraine un consensus essentiellement unanime (phénome du fork)
* Il peut avoir un phénomène : le fork, où un contributeur créer 2 block valide simultanément (possible que ce phénomène existe que pour les cryptomonnaie)
* A la fin de chaque, il y a une suite de bit permettant de lier chaque block : c’est un NONCE (Sha-256 (block-1))
* Utilisation de hashage entre chaque block et NONCE (comme Sha-256, …) => Le ralentissement de la mise à jour de la block Chain et donc validé son principe
* Cryptographie asymétrique : la signature se fait grâce à une clé publique de déchiffrement et une clé privé chiffrement (prouvant bien l’auteur du block)



1. Bitcoin

* Le minage (pour le bitcoin) est une spécificité pas nécessaire à la blockchain : c’est le proof of work (PoW)
* Le minage sert à résoudre les 2 principes majeurs de la block Chain : Contribution par block et concernant les consensus
* Le minage à pour contribution le bitcoin et permet de résoudre l’équation de cryptage du block
* Le fait que les mineurs cherchent à miner la branche la plus longue, cela permet d’augmenter le nombre de mineur sur la branche la plus longue et donc de résoudre le problème de consensus
* Or le minage consomme beaucoup d’énergie et il existe des alternatives
* Depuis 10 ans, la blockchain du bitcoin n’a jamais connu de panne

1. Fonction de hachage

* Doit résister aux collisions (or on n’a pas de preuve mathématique prouvant le fait qu’il ne risque de pas avoir de collision)