La blockchain la plus connu est Bitcoin et elle fonctionne avec sa propre crypto monnaie : elle porte le même nom que la chaine donc le Bitcoin (BTC).

Dans cette blockchain, les nœuds de stockage sont appelés des mineurs, leur action de miner veut dire d’utiliser la puissance des calculs des machines pour la résolution de problème mathématique pour générer un nouveau bloc.

Pour faire une transaction entre 2 personnes dans cette blockchain, l’émetteur transmet l’information de transaction a l’ensemble du réseau, et chaque mineur de la blockchain doivent vérifier que l’ordre émane bien du bon émetteur et les informations de la transaction sont conformes.

Pour prouver l’auteur d’une transaction on utilise la signature électronique, ce principe a pour but de prouver l’authentification de l’auteur.

L’auteur possède une clé privée avec laquelle il va chiffrer en hash un message tel que : « Je donne 10 BTC à Kevin » et les autres personnes du réseau vont appliquer la clé publique de ce même auteur sur son message afin de le déchiffrer. Cette méthode permet bien de prouver l’auteur car seul lui peut chiffrer de cette manière avec sa propre clé privée.

Pour effectuer la transaction, la notion de « Proof to work » rentre en jeu, preuve de travail en français. Les mineurs du réseau récupèrent les transactions à valider et se mettent à chercher le hash de ces transactions.

Mais ce n’est pas si simple, car en effet, on aurait pu trouver le hash de ce fichier simplement à l’aide de site internet qui peuvent calculer cela. De ce fait des conditions rentrent en jeu.

Une condition qui entre en jeu est un « Nonce » qui va changer le résultat du hashage du fichier. On impose donc une condition sur le résultat. Il faut donc trouver un nonce qui va faire en sorte que le résultat du hashage est conforme à la condition initiale.

Lorsqu’un mineur réussit à trouver le bon hash conforme aux conditions, celui-ci la propose aux autres mineurs du réseaux. La blockchain étant un organisme décentralisé la notion de consensus est très importante, ainsi pour qu’un bloc soit validé, il faut qu’il y ait un consensus entre les mineurs et donc pour générer ce bloc il faut qu’il y ait un vote majoritaire pour ce bloc.

Si ce bloc est accepté par tous alors chaque nœud du réseau s’aligne sur la nouvelle blockchain.

Mais on peut observer un nouveau problème. Imaginons que deux mineurs proposent leurs blocs en même temps. Pour éviter cela, Bitcoin a mis un intervalle de 10 minutes, qui à peu près le temps que le bloc fasse le tour du monde, afin de valider un bloc, mais même avec ces précautions il y a quand même un risque que cela se produise.

De ce fait lorsque ça se produit, une nouvelle chaine de blocs se créer en parallèle de la première.

Chacune d’elle va avancer à son rythme mais rapidement une chaine va être plus longue que l’autre et donc les autres nœuds s’aligneront tous sur la chaine la plus longue.