La blockchain fonctionne sans organe central, elle adopte le peer to peer qui signifie que l’échange se fait directement d’un internaute à un autre et ne passe donc pas par un intermédiaire quelconque. Elle a pour but est de stocker des données numériques de manière durable, infalsifiable et en architecture distribué, ce qui veut dire que tout le monde communique avec tout le monde. La première blockchain est parut en 2008 avec le bitcoin et a été développé par un inconnu se nommant sous le pseudodyme de « Satoshi Nakamoto »

Il existe des blockchain publique ouverte à tous et des blockchain privées qui elles sont restreintes à un certain publique. La blockchain publique est comme l’a dit Comme Jean-Paul Delahaye « un très grand cahier, que tout le monde peut lire librement et gratuitement, sur lequel tout le monde peut écrire, mais qui est impossible à effacer et indestructible. »

Aujourd’hui, beaucoup d’entreprise/gouvernement ou autre, envisage d’utiliser la technologie blockchain dans un autre cadre que la monnaie numérique comme Berkshire Hathaway ou apple qui étudient cette technologie.

Toutes blockchain publique fonctionnent avec une monnaie ou un token programmable. (ex: bitcoin)

Un token est un actif numérique émis et échangeable sur une blockchain. Il peut être crée par n’importe qui, peut être échangé comme une crypto-monnaie

Les transactions effectuées entre les utilisateurs sont regroupées par blocs. Chaque bloc est validés par les “mineurs”, ils sont qualifié de « nœud du réseau » et sont chargés d’assurer la validité d’un bloc selon des techniques qui dépendent du type de blockchain sur lequel nous somme. Par exemple, dans la blockchain du bitcoin, cette technique est appeler le « Proof to work » qui consiste à changer le hash du bloc pour le rendre valide. Une fois le bloc validé, il est visible par tout le monde et, selon les blockchain il devient in-modifiable, et de ce fait infalsifiable ce qui est le cas pour le Bitcoin.

Un nouveau bloc est composé du hash du bloc précédent, des données du bloc, cela peut être n’importe quoi comme par exemple des transactions, du texte etc. Un bloc est aussi composé de la signature de l’auteur. Celle-ci est basée sur la cryptographie asymétrique. Comment ça marche ? L’empreinte est chiffrée en utilisant la clef privée du signataire et ne peut se déchiffrer uniquement en utilisant la clef publique du même signataire. Le bloc est ensuite soumis au proof to work , le proof to work (preuve de travail) est utilisé dans la blockchain du bitcoin mais pas forcément dans une autre, il consiste à changer le hash du bloc pour qu’il réponde aux conditions de création du prochain bloc par exemple si la condition est : « le hash devra commencé avec 12 zéros » le proof to work consistera à rajouter du texte pour que le hash de change et commence par 12 zéros pour finir le bloc se verra attribué sont hash.

