# Blockchain, énergie, smart*

*Laurent Signac* – CC-BY-SA – 02-03-20 1110 f7ea1ec2e7105f6b3218

Quelques sites Web pour vous aider à comprendre le fonctionnement technique de la blockchain :

- Visualiser les blocs de la blockchain bitcoin ou Ethereum : https://www.blockchain.com/fr/explorer
- Voir une blockchain factice avec les explications : https://blockchaindemo.io/
- Démo blockchain : https://andersbrownworth.com/blockchain

## 1 Objectif et domaines d'utilisation

L'objectif principal de la blockchain est de proposer une «base de données» non centralisée infalsifiable. Le côté non-centralisé permet de se passer du tiers de confiance, et l'exploit est que la base de donnée distribuée soit néanmoins infalsifiable.

Dans le cas des bitcoins, la blockchain stocke des transactions entre comptes. Dans le cas d'Éthereum, elle stocke des *smart contracts* c'est à dire des programmes dont on peut garantir qu'ils ne seront pas falsifiés et seront exécutés par le réseau lorsque certaines conditions seront réunies. Une blockchain peut aussi stocker n'importe quel *document preuve* : telle personne a eu tel diplôme, telle personne a déposé tel brevet, ou a été la première à écrire tel texte etc…

## 2 Principe de fonctionnement

L'idée générale est de réunir quelques transactions (qui peuvent être de natures diverses) dans un bloc (de données). Puis, ce bloc doit être ajouté à l'ensemble des blocs déjà présents qui constituent la blockchain.

La possibilité d'ajouter est soumise à condition. Dans le cas des bitcoins, un nouveau bloc est ajouté, si lorsqu'on concatène le *Nonce* calculé, les données du bloc, et le hash du précédent bloc, on obtient un bloc dont le hash respecte certains critères (par exemple, commence par dix-neuf 0) : https://andersbrownworth.com/blockchain.

Le calcul du *Nonce* qui permet d'arriver à ce résultat est complexe (il faut essayer énormément de valeurs), et il constitue l'activité de minage *proof of work* (il existe d'autres systèmes a priori moins consommateurs en énergie).

Dans le cas des bitcoins, le mineur vérifie aussi que les transactions présentes dans le bloc sont valides (que l'argent dépensé existe), sans quoi son bloc serait de toutes façons rejeté, et il aurait réalisé un calcul inutile (pour lequel il ne serait pas rémunéré).

Si un nœud du réseau présente un bloc correct, les autres nœuds ajoutent ce bloc à leur copie de la blockchain (cela peut prendre un peu de temps), qui converge vers une blockchain unique.

## 3 Utilisation dans le cadre des smartgrids

Actuellement, un producteur local d'énergie revend à EDF (qui fixe le prix). Cette énergie est réinjectée dans le réseau et redistribuée.

La blockchain peut être utilisée pour qu'un producteur soit directement rémunéré pour l'énergie qu'il fournit et qu'un consommateur puisse acheter cette énergie précisément (cela se soldera par une transaction sur la blockchain). Le prix n'est plus alors fixé par un intermédiaire, mais par le marché et la blockchain est utilisée comme support aux transactions.

## 4 Utilisation dans le cadre de l'IOT

La multiplication des capteurs pourrait permettre à chacun de revendre les données ainsi produites (qui ont une valeur, et sont bien localisées). La gestion d'un tel marché reste cependant complexe et coûteux

en maintenance. La blockchain peut être utilisée comme support technique à la revente de ces données, supprimant le rôle de la plate forme intermédiaire.