Partie 9 - Minage

Le minage de bitcoins est un **aspect central** du réseau, permettant à la fois d'émettre des nouveaux bitcoin et de protéger le réseau des attaques diverses.

Il existe plusieurs façon d'attaquer le réseau bitcoin, mais elles sont tous protégés par le minage:

- Bannir le minage lui-même: Étant décentralisé géographiquement, il faudrait que **tous les pays** s'entendent sur cette loi. De plus, comme le minage est assez lucratif, un pays avec des surplus d'énergies serait enclin à inviter les compagnies de minage à s'installer chez lui, **rapportant des taxes et ajoutant des emplois**.
- Faire un transaction à double dépense: Réussir une telle transaction nécessiterait le contrôle de 51% du minage pendant plusieurs jours, ce qui coûterait **+10M$ par jour**. En plus, si cette transaction était réussie et profitable, tous les acteurs et utilisateurs de bitcoin perdraient instantanément confiance au réseau, **faisant fondre sa valeur**.
- Créer un « nouveau bitcoin »: Une nouvelle monnaie décentralisée utilisant d'autres principes cryptographiques nécessiterait de **changer tout le parc de machines de minage**, ce qu'aucun opérateur de mine ne fera. À l'inverse, si la nouvelle monnaie est compatible avec les même machines, elle risque d'être **attaquée par l'immense puissance de calcul** que possède le réseau Bitcoin.