

Partie 8 - Sécurité

Le Bitcoin est un réseau complètement décentralisé, dont la sécurité repose sur la **vérification et non sur la confiance**. Comme les transactions sont effectuées de pair à pair et sont irréversibles, on ne court pas le risque d'un chèque sans provision ou d'une fraude par carte de crédit.

Tous les acteurs du réseau ont un intérêt à le maintenir décentralisé et à ne pas changer les règles du jeu :

- Les **nœuds** vérifient rapidement et facilement que les transactions ne sont pas frauduleuses. Ces vérifications reposent sur les règles établies et adoptées par toutes les nœuds, formant un consensus. C'est donc dans leur intérêt que les **règles ne changent pas**.
- Les **mineurs** dépensent beaucoup d'énergie et d'argent pour construire les blocs de transactions (qui seront vérifiés par les nœuds). Étant récompensés par l'émission de nouveaux bitcoins, ils ont donc intérêt à ne pas inclure de **transactions frauduleuses**, qui seront rejetées rapidement.
- Les développeurs **ne sont pas payés** par une compagnie mais ont, pour la plupart, amassé de bonnes sommes de bitcoins. C'est donc à leur avantage si le bitcoin prend de la valeur. Il prendra de la valeur s'il est **fiable** et qu'il ne change pas constamment.

