Contexte

C'est une crypto-monnaie lancer en 2014 par 7 créateurs dont 5 anonymes (d'après certaine théorie, Satoshi Nakamoto ferai parti d'un de ces 5 créateurs anonymes). Monero a été créer de base pour effectuer des transactions sur le Darknet, mais la communauté a très vite aperçu son potentiel. Son objectif est de conserver l'anonymat et la confidentialité des transactions.

Monero

Principes et buts

C'est une blockchain décentralisé utilisant le Proof-of-Work pour valider ces blocs. Le Monero est un fork du Bytecoin, cela signifie qu'on as créer une crypto-monnaie à partir du code source d'une autre crypto-monnaie. Son jeton natif de gouvernance est le XMR. Il utilise la preuve de travail pour valider les blocs, avec une particularité qui dissuade l'exploitation minière par ASIC en faveur de CPU et GPU, favorisant ainsi une décentralisation optimal étant donner que les grosses fermes de minage ne peuvent pas en miner en trop grande quantité. Monero utilise l'algorithme de hachage RandomX, en plus de la technologie des Ring Signatures pour un anonymat renforcé. Les Ring Signatures mélange l'adresse de l'expéditeur avec d'autres adresses, rendant difficile le traçage. La fongibilité est une caractéristique clé, permettant à Monero d'être échangé sans qu'aucun enregistrement ne puisse révéler son historique.

Réalisation et futur

Cela fait quasiment 10 ans que ce projet existe, il y à une grosse communauté derrière. Son évolution a été marquée par des améliorations techniques telles que l'introduction de l'algorithme de dissimulation Ring Signatures et l'algorithme de hachage RandomX pour essayer d'atteindre le plus de décentralisation possible.

En chiffres

Offre en circulation	18 319 522
Offre maximum	∞
Date de création	En 2014

FORMATOM