# MWC - MimbleWimbleCoin

MimbleWimbleCoin (MWC) est une cryptomonnaie qui met en œuvre le protocole MimbleWimble, un protocole de blockchain conçu pour améliorer la confidentialité et la scalabilité des transactions. Le nom MimbleWimble provient d'un sort du monde de Harry Potter, utilisé pour empêcher quelqu'un de lancer des sorts ou de parler. Dans le contexte des cryptomonnaies, il s'agit d'un protocole qui assure la confidentialité.

**Fonctionnement et Technologie :**

Le protocole MimbleWimble permet des transactions confidentielles, ce qui signifie que les montants des transactions sont chiffrés et ne sont pas visibles publiquement. Seul l'expéditeur et le destinataire connaissent les montants échangés. Contrairement à Bitcoin, MimbleWimble ne nécessite pas de vérifier l'historique complet des coins pour valider une transaction, réduisant ainsi considérablement la taille de la blockchain. Il utilise des techniques comme 'cut-through' au niveau des transactions et des blocs pour agréger plusieurs transactions en une seule, en supprimant les données intermédiaires et en ne conservant que les entrées et sorties nettes. Cela optimise l'espace de stockage sur la blockchain et améliore l'efficacité. Le réseau MWC utilise un algorithme de preuve de travail (Proof of Work) en deux variantes : Cuckaroo (résistant aux ASIC) et Cuckatoo (ciblant les ASIC). Les transactions sur la couche de base utilisent CoinJoin et des transactions confidentielles (CTs) avec agrégation de signatures.

**Utilité et Cas d'Usage :**

L'objectif principal de MWC est de servir de monnaie numérique privée et fongible. Les cas d'usage incluent :

- **Transactions privées :** MWC s'adresse aux utilisateurs et aux services financiers qui exigent une confidentialité élevée pour leurs transactions. Il rend les transactions difficiles à tracer pour les observateurs externes.
- **Récompense pour les Mineurs :** Le token MWC est utilisé pour récompenser les mineurs qui valident les transactions et sécurisent le réseau.
- **Fongibilité :** Grâce à la confidentialité des transactions, chaque MWC est considéré comme fongible, c'est-à-dire qu'il peut remplacer une autre unité de la même monnaie

sans distinction, car il n'a pas d'historique de transaction unique et traçable.

- **Programme HODL :** MWC propose un programme HODL qui récompense les adresses conservant leurs jetons sans mouvement pendant une période prédéterminée, encourageant ainsi la conservation à long terme.

**Tokenomics :**

MWC a une offre maximale fixe de 20 millions de jetons, ce qui le rend intrinsèquement rare et anti-inflationniste. La récompense de bloc diminue avec le temps, et les frais de transaction sont basés sur le nombre d'outputs créés/détruits et la taille totale de la transaction. L'offre en circulation est d'environ 11 millions de MWC.

**Avantages et Limites :**

**Avantages :**

- **Confidentialité améliorée :** Le protocole MimbleWimble masque les détails des transactions.
- **Scalabilité accrue :** La réduction des données sur la blockchain permet des transactions plus rapides et plus efficaces.
- **Fongibilité :** Les transactions privées rendent la monnaie plus interchangeable.
- **Rareté :** L'offre maximale limitée contribue à la rareté.

**Limites :**

- **Défis réglementaires :** La confidentialité accrue peut soulever des préoccupations réglementaires.
- **Complexité d'intégration :** L'adoption dans les marchés grand public peut être compliquée.
- **Liquidité :** Comme beaucoup de cryptomonnaies moins établies, MWC peut présenter moins de pipelines de liquidité par rapport à Bitcoin.

**Perspectives :**

Le développement de MWC vise à innover technologiquement et économiquement pour maximiser les bénéfices du protocole MimbleWimble. L'équipe a développé un portefeuille GUI fonctionnel, une méthode de stockage à froid sécurisée, et a réalisé des échanges atomiques MWC/BTC. Des recherches sont en cours pour le développement de

transactions multi-signatures et du Lightning Network. Les futurs développements seront guidés par les besoins du marché, avec une priorité donnée aux demandes bénéficiant aux utilisateurs finaux.