BCH - Bitcoin Cash

Introduction à Bitcoin Cash (BCH)

Bitcoin Cash (BCH) est né en août 2017 d'une divergence au sein de la communauté Bitcoin concernant la manière de faire évoluer le réseau pour répondre à une demande croissante. Le cœur du désaccord portait sur la scalabilité : certains souhaitaient augmenter la taille des blocs pour permettre plus de transactions, tandis que d'autres préféraient des solutions de seconde couche ou une approche plus conservatrice. Cette divergence a conduit à un "hard fork", créant Bitcoin Cash comme une nouvelle blockchain distincte, partageant une histoire commune avec Bitcoin jusqu'au moment de la scission.

Objectif et Proposition de Valeur

L'objectif fondamental de Bitcoin Cash est de réaliser la vision originale de Satoshi Nakamoto d'un "système de paiement électronique de pair à pair" (peer-to-peer electronic cash system). Cela se traduit par une priorité donnée aux transactions rapides, fiables et à très faibles coûts, le rendant ainsi adapté aux paiements quotidiens, aux microtransactions et aux transferts de fonds internationaux. Contrairement à Bitcoin, qui est souvent perçu comme une "réserve de valeur" (digital gold), BCH se positionne comme de l'argent numérique facile à dépenser.

Technologie et Fonctionnement

- **Augmentation de la Taille des Blocs :** C'est la différence technique la plus significative par rapport à Bitcoin. La limite de taille des blocs de BCH est passée de 1 Mo (pour BTC) à 8 Mo lors de sa création, puis a été augmentée à 32 Mo. Cela permet de traiter un volume de transactions beaucoup plus important dans chaque bloc, ce qui contribue à réduire la congestion du réseau et à maintenir des frais de transaction bas.
- **Vitesse de Transaction :** Grâce à sa capacité accrue, les transactions sur le réseau Bitcoin Cash sont généralement confirmées plus rapidement qu'avec Bitcoin. Les confirmations sont souvent mesurées en secondes ou minutes plutôt qu'en dizaines de

minutes.

- **Frais de Transaction :** Les frais sont typiquement très bas, souvent une fraction de centime, ce qui rend les micro-paiements économiquement viables.
- **Mécanisme de Consensus :** BCH utilise le même mécanisme de consensus que Bitcoin : la "Proof of Work" (Preuve de Travail) avec l'algorithme SHA-256. Cela signifie que les mineurs valident les transactions et créent de nouveaux blocs en résolvant des problèmes mathématiques complexes.
- **Offre Limitée :** Comme Bitcoin, l'offre maximale de BCH est plafonnée à 21 millions de pièces, garantissant une rareté programmée.
- **Mises à Jour Protocolaires :** Au fil du temps, Bitcoin Cash a introduit plusieurs améliorations, telles que les signatures Schnorr, un nouveau système d'ajustement de difficulté (ASERT), et plus récemment les "CashTokens" qui étendent ses capacités pour l'émission de jetons et des applications de type "smart contract" (contrats intelligents) via des "covenants" (clauses restrictives).

Cas d'Usage et Utilité

- **Paiements Quotidiens :** BCH est conçu pour être utilisé dans les magasins physiques et en ligne pour l'achat de biens et de services. De nombreux commerçants et plateformes de paiement acceptent BCH.
- **Microtransactions :** Les frais très bas rendent BCH idéal pour de petites transactions, comme des pourboires en ligne ou de petits achats.
- **Rémittances Internationales :** La rapidité et le faible coût des transactions en font une solution attrayante pour envoyer de l'argent à l'étranger.
- **Stockage de Valeur (secondaire) :** Bien que son objectif principal soit les paiements, sa rareté et sa similarité avec Bitcoin lui confèrent également un potentiel de stockage de valeur pour certains utilisateurs.
- **Développement d'Écosystème :** Avec l'introduction des CashTokens et des améliorations pour les smart contracts, BCH vise à supporter des applications décentralisées (dApps) et des jetons, élargissant ainsi son utilité au-delà des simples paiements.

Tokenomics et Gouvernance

- **Tokenomics :** La politique monétaire de BCH est identique à celle de Bitcoin, avec une offre maximale de 21 millions de BCH. L'émission se fait via des récompenses de bloc pour les mineurs, qui sont divisées par deux tous les 210 000 blocs (environ tous les quatre ans), un événement connu sous le nom de "halving". La majorité de l'offre est déjà en circulation.
- **Gouvernance :** La gouvernance de Bitcoin Cash est décentralisée, reposant principalement sur le consensus des mineurs (hash rate) et sur les discussions au sein de la communauté. Cependant, cette approche a également mené à des divisions, y compris une autre scission majeure de Bitcoin Cash en Bitcoin ABC et Bitcoin SV en 2018, illustrant les défis de la coordination décentralisée.

Avantages et Limites

Avantages :

- Transactions rapides et à faible coût.
- Scalabilité on-chain (sur la chaîne principale) accrue.
- Rareté et politique monétaire prévisible (21 millions de pièces).
- Compatibilité avec une grande partie de l'écosystème Bitcoin existant (portefeuilles, outils).
- Potentiel d'innovation avec les CashTokens et les améliorations de smart contracts.

Limites :

- Adoption et activité de chaîne inférieures à celles de Bitcoin.
- Concurrence féroce d'autres blockchains rapides et spécialisées.
- Historique de divisions communautaires qui a pu nuire à sa perception et à sa force collective.
- Sécurité du réseau (mesurée par le hashrate) généralement inférieure à celle de Bitcoin, ce qui peut le rendre plus vulnérable aux attaques.
- La perception publique est parfois entachée par des personnalités influentes et des

stratégies marketing controversées.

Conclusion

Bitcoin Cash s'est positionné comme une alternative à Bitcoin, privilégiant la fonctionnalité de "cash numérique" grâce à des transactions plus rapides et moins chères. Bien qu'il ait démontré sa capacité à innover avec des mises à jour technologiques et à étendre ses cas d'usage vers les contrats intelligents et la tokenisation, son succès dépendra de sa capacité à gagner une adoption massive, à se différencier de la concurrence et à maintenir une communauté unie et dynamique. Il représente une tentative continue de réaliser la vision d'une monnaie numérique décentralisée pour les transactions quotidiennes.