CKBTC - Chain-key Bitcoin

Le ckBTC, ou Chain-key Bitcoin, est une cryptomonnaie développée sur la blockchain Internet Computer (ICP) qui agit comme un jumeau synthétique du Bitcoin (BTC). Il est conçu pour être conforme aux standards de tokens ICRC-1 et ICRC-2, assurant une interopérabilité et une intégration fluides au sein de l'écosystème ICP. La caractéristique fondamentale du ckBTC est qu'il est soutenu à 1:1 par du Bitcoin réel, ce qui signifie qu'un ckBTC peut toujours être échangé contre un BTC et vice versa. Cette parité de valeur est maintenue sans recourir à des ponts centralisés, qui sont souvent des points de vulnérabilité pour la sécurité. Au lieu de cela, le ckBTC utilise la cryptographie avancée de la "chain-key" et des contrats intelligents (canisters) sur l'ICP pour gérer directement le Bitcoin brut.

L'architecture du ckBTC repose sur l'intégration native du réseau Bitcoin par l'Internet Computer. Cela permet aux canisters de l'ICP d'obtenir directement les blocs Bitcoin et de traiter les transactions qu'ils contiennent. Cette capacité permet à l'ICP de maintenir l'ensemble de l'ensemble des Unspent Transaction Outputs (UTXO) du Bitcoin sur la chaîne. Deux canisters principaux fournissent la fonctionnalité ckBTC : le "ckBTC minter" et le "ckBTC ledger". Le "ckBTC minter" est responsable de la création (minting) de nouveaux ckBTC lorsqu'il reçoit du Bitcoin et de la destruction (burning) de ckBTC lorsqu'un utilisateur demande le retrait de BTC. Le "ckBTC ledger" gère les soldes des comptes et les transferts de ckBTC entre les utilisateurs. Des canisters d'archivage et d'indexation sont également utilisés pour gérer l'historique des transactions.

Les avantages du ckBTC sont multiples. Premièrement, sa sécurité est renforcée car il évite les risques associés aux ponts centralisés, qui ont été la cible de nombreux hacks. Deuxièmement, les transactions en ckBTC sont extrêmement rapides, avec une finalisation en 1 à 2 secondes, contre plusieurs minutes voire heures pour les transactions Bitcoin classiques. Troisièmement, les frais de transaction sont négligeables, fixés à 0,0000001 ckBTC (environ 10 satoshis), ce qui rend les micropaiements économiquement viables. Ces caractéristiques ouvrent de nouvelles possibilités pour le commerce basé sur Bitcoin, les applications de finance décentralisée (DeFi) et l'intégration de Bitcoin dans les dApps de l'ICP.

Le ckBTC se distingue également des solutions de couche 2 comme le Lightning Network.

Bien que les deux visent à accélérer et à réduire les coûts des transactions Bitcoin, le ckBTC n'exige pas l'établissement de canaux de paiement peer-to-peer. Cela signifie que l'intégralité du solde ckBTC d'un utilisateur est toujours disponible pour le transfert, sans limitations de liquidité du réseau. De plus, les canisters intelligents de l'ICP peuvent détenir et transférer programmablement le ckBTC, permettant le développement d'applications de couche 2 entièrement on-chain pour Bitcoin, ce qui n'est pas possible avec le Lightning Network.

La vérifiabilité est un autre pilier du ckBTC. Toutes les activités ckBTC sont vérifiables sur la chaîne, et les transactions passent par des vérifications "Know Your Transaction" (KYT) pour s'assurer qu'aucun Bitcoin potentiellement compromis n'est utilisé sur l'ICP ou transféré vers des adresses Bitcoin réputées comme "taintées". Un petit frais de 100 satoshis est appliqué par UTXO pour cette vérification, et des frais similaires sont appliqués pour les transferts sortants de BTC.

En résumé, le ckBTC représente une avancée significative pour l'utilité et l'accessibilité du Bitcoin, en le rendant plus rapide, moins cher et plus sûr à utiliser dans un écosystème de contrats intelligents avancé comme celui de l'Internet Computer.