XCP - Counterparty

Le protocole Counterparty, lancé en janvier 2014, est une extension open-source du protocole Bitcoin qui permet d'ajouter des fonctionnalités avancées telles que l'émission de tokens, un échange d'actifs décentralisé, des contrats intelligents et des oracles natifs. Il fonctionne en intégrant des données supplémentaires dans les transactions Bitcoin existantes, ce qui signifie qu'il ne nécessite pas de modification du protocole Bitcoin lui-même et s'appuie sur la sécurité et la décentralisation du réseau Bitcoin pour ses propres opérations. Les transactions Counterparty sont essentiellement des transactions Bitcoin auxquelles sont ajoutées des données interprétables par le logiciel Counterparty.

Le token natif, XCP, a été créé par un processus appelé 'proof-of-burn' entre janvier et février 2014. Durant cette période, les utilisateurs pouvaient détruire des Bitcoins en les envoyant à une adresse spécifique, déclenchant ainsi la création automatique d'une quantité correspondante de XCP. Ce mécanisme visait à offrir une égalité des chances d'acquisition et à éviter la centralisation ou la confiance envers des tiers, contrairement à une pré-vente ou un ICO traditionnel. La quantité totale de XCP créée est d'environ 2,6 millions.

L'utilité principale du XCP réside dans le paiement des frais de réseau pour certaines transactions au sein du protocole Counterparty, ainsi qu'en tant qu'unité de compte. Par exemple, l'émission d'un nouvel actif nommé (un token personnalisé) coûte 0,5 XCP, qui sont ensuite brûlés (retirés de la circulation). D'autres transactions, comme les simples transferts d'actifs ou l'émission d'actifs numériques (sans identifiant lisible par l'homme), ne requièrent pas l'utilisation de XCP car leur charge computationnelle est faible.

Counterparty permet la création de deux types d'actifs : les actifs nommés (4 à 12 caractères alphanumériques) et les actifs numériques (une séquence d'entiers). Les actifs nommés ont des frais d'émission uniques de 0,5 XCP pour décourager le spam. La plateforme propose également un marché décentralisé pour l'échange de ces actifs. Elle a été pionnière dans la création de tokens fongibles et non fongibles (NFTs) avant même que ces termes ne soient largement adoptés, permettant des cas d'usage tels que les objets de collection numériques (comme les 'Rare Pepes') et les jeux sur blockchain.

La sécurité du protocole est intrinsèquement liée à celle de Bitcoin, car les mineurs Bitcoin

valident toutes les transactions Counterparty. Il est donc aussi difficile d'attaquer Counterparty que d'attaquer Bitcoin lui-même.

Bien que le développement ait connu des périodes d'accalmie, des efforts ont été entrepris pour stabiliser et améliorer le protocole. Des portefeuilles spécifiques comme Casa Tookan et Horizon Wallet, ainsi que des places de marché comme Memepool et XCP.io, soutiennent l'écosystème Counterparty. Le protocole a également influencé le développement d'autres technologies, notamment dans le domaine des contrats intelligents.