TORN - Tornado Cash

Tornado Cash est une solution de confidentialité décentralisée qui opère sur la blockchain Ethereum, lancée en août 2019. Son objectif principal est de briser le lien on-chain entre les adresses d'expéditeurs et de destinataires de transactions, offrant ainsi un niveau de confidentialité accru pour les utilisateurs de cryptomonnaies. Le protocole fonctionne via des smart contracts qui créent des pools de fonds anonymisés.

Le processus d'anonymisation se déroule en deux étapes principales. Premièrement, un utilisateur dépose des fonds (comme de l'Ether ou certains stablecoins) dans un smart contract de Tornado Cash. Ce dépôt génère une clé chiffrée unique, servant de preuve de dépôt. Deuxièmement, l'utilisateur peut retirer ces fonds anonymisés en soumettant la clé chiffrée et en spécifiant une nouvelle adresse de retrait. Il est conseillé d'attendre un certain temps entre le dépôt et le retrait pour renforcer l'anonymisation, car cela permet que d'autres dépôts soient effectués, augmentant ainsi la taille du pool anonymisé.

La technologie sous-jacente de Tornado Cash repose sur des preuves à divulgation nulle de connaissance (zero-knowledge proofs), notamment les zk-SNARKs. Ces preuves cryptographiques permettent de valider une transaction sans révéler d'informations sensibles sur l'expéditeur ou le destinataire. Ce mécanisme assure que l'on ne peut pas retracer l'origine des fonds une fois qu'ils ont traversé le protocole.

Tornado Cash est conçu pour être non-custodial, ce qui signifie que les utilisateurs conservent toujours le contrôle de leurs fonds et de leurs clés privées. Le protocole est également décentralisé et fonctionne comme une Organisation Autonome Décentralisée (DAO). Cela implique qu'il n'y a pas d'autorité centrale contrôlant le système. Les décisions concernant l'évolution du protocole, telles que les tailles de pool ou les chaînes supportées, sont prises par la communauté des détenteurs du token TORN.

Le token TORN est le jeton de gouvernance de l'écosystème Tornado Cash. Il est de type ERC-20 et a une offre fixe. Les détenteurs de TORN peuvent soumettre des propositions et voter sur les changements du protocole, ce qui leur donne un droit de regard sur son développement. La distribution initiale de TORN comprenait un airdrop pour les premiers utilisateurs et une récompense pour l'utilisation du service ('anonymity mining'), afin d'inciter à l'adoption et à la participation à la gouvernance.

Les cas d'usage de Tornado Cash incluent la protection de la vie privée des transactions pour les utilisateurs soucieux de la confidentialité de leurs finances, qu'il s'agisse de particuliers, d'entreprises protégeant des secrets commerciaux, ou de toute autre entité nécessitant une confidentialité financière. Il est également déployé sur plusieurs blockchains, y compris Ethereum, Binance Smart Chain, Polygon et Avalanche, élargissant ainsi son accessibilité.

Cependant, Tornado Cash a été au centre de controverses. En août 2022, le Département du Trésor américain a imposé des sanctions contre le protocole, alléguant qu'il avait été utilisé pour blanchir des fonds illicites, notamment pour des montants considérables dans le cadre d'activités liées à la Corée du Nord. Ces sanctions ont suscité un débat sur l'équilibre entre la vie privée et la conformité réglementaire dans l'espace crypto. Par la suite, certaines décisions judiciaires ont remis en question ces sanctions.

En résumé, Tornado Cash est un outil puissant pour la confidentialité des transactions sur blockchain, propulsé par une technologie cryptographique avancée et une gouvernance communautaire via le token TORN. Bien qu'il offre des avantages significatifs en matière de protection de la vie privée, son utilisation reste un sujet de discussion complexe en raison des préoccupations réglementaires.