SBTC - sBTC

sBTC est un actif synthétique qui vise à intégrer la fonctionnalité de Bitcoin (BTC) dans l'écosystème Stacks, une blockchain de couche 2 (L2) qui étend les capacités de Bitcoin avec des contrats intelligents et des applications décentralisées (dApps). Contrairement aux tokens encapsulés (wrapped tokens) sur d'autres blockchains, sBTC maintient une connexion directe avec la blockchain Bitcoin, garantissant ainsi une sécurité robuste et une véritable intégration.

Son fonctionnement repose sur un système de peg bidirectionnel entre les blockchains Bitcoin et Stacks. Le processus de "peg-in" permet aux utilisateurs d'envoyer du BTC à une adresse spéciale Bitcoin, contrôlée par un groupe décentralisé de signataires. Cette transaction est vérifiée sur la chaîne Bitcoin, puis confirmée sur Stacks, où une quantité équivalente de sBTC est frappée (minted) et envoyée au portefeuille Stacks de l'utilisateur. Inversement, le processus de "peg-out" permet aux utilisateurs de brûler leur sBTC sur Stacks pour récupérer leur BTC verrouillé.

L'un des principaux avantages de sBTC est sa capacité à améliorer l'utilité de Bitcoin. Il permet aux détenteurs de BTC de participer à des protocoles de finance décentralisée (DeFi), d'accéder à des plateformes de prêt, de générer des rendements et d'échanger sur des échanges décentralisés (DEX) directement avec leur Bitcoin "travaillant". Cela débloque un capital important qui, autrement, resterait inactif.

En termes de sécurité, sBTC est soutenu par le mécanisme de consensus Proof of Transfer (PoX) de Stacks, qui permet de régler les transactions sur Bitcoin sans modifier sa couche de base. La sécurité de sBTC est renforcée par un réseau décentralisé de signataires qui approuvent les opérations de dépôt et de retrait, nécessitant un consensus de 70% pour les transactions. Des audits complets et un programme de chasse aux bugs contribuent également à la sécurité du protocole. De plus, toutes les transactions Stacks, y compris celles impliquant sBTC, bénéficient de la finalité complète de Bitcoin.

Un autre avantage clé est la compatibilité native avec Bitcoin. La chaîne Stacks utilise des formats d'adresse identiques à ceux de la chaîne principale Bitcoin (y compris Taproot et Native SegWit), et permet aux transactions d'être signées directement avec des portefeuilles Bitcoin. Cela offre une expérience utilisateur familière et sécurisée. sBTC

simplifie également l'écosystème des frais de transaction, car les utilisateurs peuvent payer directement avec sBTC, éliminant le besoin de détenir le token natif de la chaîne, SIDE.

Le déploiement de sBTC vise à créer une économie Bitcoin plus active et programmable. Il réduit le risque de contrepartie par rapport aux solutions comme le Wrapped Bitcoin (WBTC) car il évite les intermédiaires et les dépositaires centralisés. Les signataires jouent un rôle crucial dans la sécurité et le fonctionnement du protocole sBTC en approuvant toutes les opérations de dépôt et de retrait de sBTC. Ils sont incités par des récompenses en BTC pour leurs efforts.

Bien que sBTC vise à minimiser les risques en évitant les dépositaires centraux, il conserve les risques inhérents à un réseau décentralisé, tels que les perturbations potentielles ou le comportement erratique des validateurs, bien que ces risques soient atténués par des incitations économiques et des mécanismes de consensus. L'arrivée de sBTC sur Stacks, en tant que première solution L2 Bitcoin, est susceptible d'attirer davantage d'intérêt et de participation dans le réseau, potentiellement remodeler l'utilisation de Bitcoin dans l'espace crypto.