ERG - Ergo

Ergo est une plateforme blockchain conçue pour développer et exécuter des contrats financiers décentralisés de manière sécurisée et efficace. Elle a été lancée en 2019 avec l'objectif de combler le fossé entre Bitcoin et des blockchains plus avancées comme Ethereum en combinant le modèle UTXO de Bitcoin avec des fonctionnalités de contrats intelligents plus complexes grâce à son modèle eUTXO (extended UTXO). Ce modèle permet aux UTXO (Unspent Transaction Outputs) de contenir des données arbitraires et des scripts sophistiqués, offrant ainsi une grande flexibilité pour la création de contrats intelligents.

La technologie clé d'Ergo repose sur plusieurs innovations. ErgoScript est son langage de script propriétaire, conçu pour définir les règles des contrats financiers de manière sûre et efficace. Les protocoles Sigma, basés sur des preuves à divulgation nulle de connaissance (zero-knowledge proofs), permettent des applications de confidentialité avancées et la création de contrats complexes. Pour la sécurité et la décentralisation, Ergo utilise un algorithme de preuve de travail (Proof-of-Work) appelé Autolykos, conçu pour être résistant aux ASICs (circuits intégrés spécifiques à une application), favorisant ainsi le minage par des GPU (cartes graphiques) et une meilleure répartition du pouvoir de minage. De plus, les NIPoPoWs (Non-Interactive Proofs of Proof-of-Work) améliorent l'accessibilité de la blockchain en permettant le fonctionnement de « light clients » (clients légers), qui peuvent interagir avec le réseau sans avoir à télécharger l'intégralité de la blockchain, rendant Ergo plus accessible sur des appareils moins puissants comme les téléphones mobiles.

Le token natif d'Ergo est l'ERG. Son utilité principale est de servir de moyen de paiement pour les frais de transaction et la « location de stockage » (storage rent) sur le réseau, garantissant ainsi la sécurité et la stabilité à long terme de la plateforme. L'ERG est également utilisé comme garantie dans diverses applications DeFi au sein de l'écosystème Ergo, telles que le stablecoin SigmaUSD.

En termes de tokenomics, Ergo présente une offre maximale plafonnée à 97 739 924 ERG. Le projet a été lancé sans ICO (Initial Coin Offering) ni pré-allocation de tokens pour les fondateurs ou les investisseurs, adhérant à un principe de décentralisation dès le départ. L'émission des tokens ERG s'est étalée sur une période initiale de huit ans, avec une partie

des récompenses de bloc allouée au Trésor de la Fondation Ergo pour financer le développement et la promotion du projet au cours des 2,5 premières années. Le modèle d'émission a été ajusté par la suite pour assurer la durabilité du réseau à long terme, prolongeant la période d'émission et modifiant la diminution des récompenses par bloc. Le protocole de « storage rent » d'Ergo vise à rendre les UTXO dormants coûteux à maintenir, encourageant ainsi leur utilisation et contribuant à un modèle potentiellement déflationniste à mesure que des UTXO non dépensés après une certaine période (quatre ans) entraînent des frais.

Les cas d'usage d'Ergo sont variés. Il vise à être une « couche intelligente » pour Bitcoin, permettant d'étendre ses fonctionnalités DeFi sans avoir à modifier le réseau Bitcoin lui-même. Cela inclut des applications comme les stablecoins garantis par Bitcoin, la finance décentralisée (DeFi) avec des opportunités de yield farming, et l'amélioration de la confidentialité pour les transactions Bitcoin via des outils comme ErgoMixer. D'autres cas d'usage incluent les contrats financiers sécurisés, les systèmes financiers alternatifs, et même des applications pour des économies expérimentales ou dans des régions à connectivité limitée. Le projet Ergo met l'accent sur la gouvernance communautaire, permettant aux détenteurs de tokens de participer aux décisions concernant l'évolution du réseau, bien qu'il utilise un mécanisme de preuve de travail plutôt qu'un staking traditionnel. L'écosystème Ergo est en croissance constante avec le développement de decentralized exchanges (DEX), de ponts inter-chaînes comme Rosen Bridge, et d'autres dApps.