FIRO - Firo

Firo, dont le lancement initial remonte à septembre 2016 sous le nom de Zcoin (XZC), est une cryptomonnaie axée sur la confidentialité. Fondée par Poramin Insom, elle visait à remédier aux lacunes de confidentialité de Bitcoin. Le projet a évolué en adoptant des protocoles de confidentialité de plus en plus sophistiqués et une approche communautaire pour sa gouvernance.

Technologie et Confidentialité

Le cœur de la technologie de Firo réside dans ses protocoles de confidentialité. Initialement basé sur le protocole Zerocoin, Firo a migré vers Lelantus en 2021, puis a développé Lelantus Spark. Ces protocoles utilisent des preuves à divulgation nulle de connaissance (zero-knowledge proofs), permettant de vérifier la validité d'une transaction sans révéler d'informations sensibles. Le mécanisme clé est le "burn-and-redeem" (brûler et échanger) : les utilisateurs peuvent détruire leurs Firo existants et en recevoir de nouveaux, sans aucun lien traçable entre les deux, créant ainsi une anonymat complet. Lelantus Spark, en particulier, améliore la scalabilité en regroupant divers actifs (Firo, stablecoins, NFTs) dans un même ensemble d'anonymat, rendant les transactions indiscernables.

Firo intègre également le protocole Dandelion++, qui obscurcit l'origine des transactions au niveau du réseau, empêchant ainsi le lien entre une adresse IP et une transaction sans nécessiter de services externes comme Tor. La fonctionnalité "Receiver Address Privacy" (RAP) a été introduite pour permettre la publication d'adresses publiques tout en maintenant la vie privée des transactions grâce à la génération d'adresses uniques.

Consensus et Sécurité

Firo utilise un mécanisme de consensus hybride Proof-of-Work (PoW) et Proof-of-Stake (PoS) via ses FiroNodes (masternodes). Le minage est basé sur l'algorithme FiroPoW, une variante de ProgPoW conçue pour être résistante aux ASICs et optimisée pour le minage par GPU, favorisant ainsi la décentralisation du minage. Les FiroNodes, qui nécessitent un dépôt de 1 000 FIRO, jouent un rôle crucial dans la sécurité, la finalité des transactions (via Chainlocks) et la gouvernance du réseau. Les Chainlocks, mis en œuvre avec le réseau LLMQ des masternodes, sécurisent les blocs et rendent les transactions finales très

rapidement, tout en protégeant contre les attaques à 51%.

Tokenomics et Gouvernance

L'offre maximale de tokens FIRO est fixée à 21,4 millions, une structure similaire à celle de Bitcoin, y compris un cycle de halving tous les quatre ans. La distribution des récompenses de bloc est répartie entre les mineurs, les masternodes, le fonds de développement et le fonds communautaire. Des changements récents dans la tokenomics incluent l'introduction d'une émission fixe de 6,25 FIRO par bloc jusqu'à ce que l'offre maximale soit atteinte, ainsi qu'une émission perpétuelle (tail emission) plus tard pour assurer la pérennité du réseau. La répartition des récompenses a également été ajustée, donnant une part plus importante aux masternodes pour refléter leur rôle essentiel dans la sécurité et le fonctionnement du réseau.

La gouvernance de Firo est communautaire, permettant aux détenteurs de tokens de proposer et de voter sur des changements et des allocations de fonds, renforçant ainsi la décentralisation et l'engagement de la communauté.

Cas d'Usage et Avantages

La principale utilité de Firo est de fournir des transactions privées pour les individus et les entreprises souhaitant une confidentialité financière. Elle peut être utilisée pour des transactions peer-to-peer anonymes, la création de tokens privés via la plateforme de tokenisation Elysium, et potentiellement pour des applications comme les systèmes de vote sécurisés et vérifiables (comme l'a démontré l'élection du parti démocrate thaïlandais en 2018). Firo vise également à répondre aux exigences réglementaires, comme le montre la compatibilité avec le règlement MiCA grâce aux adresses EX.

Limites et Perspectives

Bien que Firo offre des fonctionnalités de confidentialité avancées, la complexité de ces protocoles peut être un frein pour certains utilisateurs. L'adoption généralisée dépendra de la capacité de Firo à maintenir son avantage technologique tout en naviguant dans un environnement réglementaire de plus en plus strict. L'innovation continue dans les protocoles de confidentialité et l'expansion des cas d'usage, notamment dans la DeFi et la tokenisation, sont des axes de développement clés pour l'avenir de Firo.