

ABSTRACT

Disclosed is a system, method, and computer program product for determining solvency of a digital asset exchange system. The method includes identifying a plurality of blockchain addresses corresponding to a plurality of users of the digital asset exchange system, generating a first commitment to an amount of digital assets corresponding to the plurality of blockchain addresses, generating a second commitment to a balance of each user of the plurality of users, generating a first component of a zero-knowledge algorithm configured to receive, as input, the first commitment, and to output a value generated based on each public key corresponding to each blockchain address, generating a second component of the zero-knowledge algorithm configured to receive, as input, the second commitment, and to output a value generated based on each user balance, and determining, with at least one processor, that the digital asset exchange system is solvent based on the zero-knowledge algorithm.

<FIG. 2>