Abstract

System and Method for Hierarchical Token Distribution on Blockchain Network

A method to participate in a blockchain-implemented token distribution process is disclosed. The token distribution process divides an initial quantity of tokens at an input address associated with an input node into a plurality of sub-quantities and distributes the sub-quantities to multiple output addresses associated with respective output nodes using a blockchain. The token distribution process is implemented collectively by the input node, the output nodes, and a plurality of mixer nodes. The method, which may be implemented at a mixer node *(Uij)*, includes: identifying an upstream node *(Ui)* and a plurality of downstream nodes *(Uijk)* associated with the mixer node; collaborating with the upstream node to generate a first commitment channel *(Ui→ Uij)* for a first transaction between the upstream node and the mixer node; and for each of the plurality of downstream nodes: collaborating with the downstream node to generate a second commitment channel *(Uij→ Uijk)* for a second transaction between the mixer node and the downstream node, wherein an unlocking script for the first transaction is derived from an unlocking script for any one of the second transactions.

Fig.1