

METHODS AND DEVICES FOR VERIFYING VALIDITY OF TOKEN
RECORDED ON BLOCKCHAIN

ABSTRACT

Disclosed herein are methods, devices, and apparatuses, including computer programs stored on computer-readable media, for verifying validity of a privacy-preserving token, wherein a privacy-preserving representation of a set of attributes is calculated by calculating a Merkle tree root hash based on a value associated with each attribute of the set of attributes and is recorded on a blockchain system as metadata of the token, and the value associated with each attribute of the set of attributes has a corresponding hash stored on a leaf node of the Merkle tree. One of the methods includes: identifying hashes stored on a plurality of nodes of the Merkle tree that can be utilized to calculate the Merkle tree root hash; and providing the identified hashes stored on the plurality of nodes of the Merkle tree to a verifier, to facilitate a verification of the validity of the token without revealing the value associated with each attribute of the set of attributes.

Fig. 8