

METHODS AND DEVICES FOR VERIFYING VALIDITY OF SIGNATURE
ATTRIBUTE OF ASSET REPRESENTED BY 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 signature attribute of an asset represented by a privacy-preserving token, wherein a privacy-preserving representation of a set of attributes associated with the asset 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, the value associated with each attribute of the set of attributes has a corresponding hash stored on a leaf node of the Merkle tree, and the set of attributes comprises a signature attribute associated with a value signed by an author of the asset. One of the methods includes: generating a proof for proving that the value associated with the signature attribute is a valid signature signed by the author of the asset; and providing the proof to a verifier to facilitate a verification of whether the value associated with the signature attribute is the valid signature signed by the author of the asset without revealing the value associated with the signature attribute.

Fig. 9