METHODS AND DEVICES FOR VERIFYING ATTRIBUTE VALUE 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 an attribute value 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, 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: generating a proof for proving that the value associated with a particular attribute of the set of attributes satisfies a condition; and providing the proof to a verifier to facilitate a verification of whether the value associated with the particular attribute of the set of attributes satisfies the condition without revealing the value associated with the particular attribute.

Fig. 9