

# 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 according to a function defined 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. One of the methods includes: generating a proof for proving that the metadata recorded on the blockchain system is calculated according to the function defined based on the value associated with each attribute of the set of attributes; and providing the proof 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