

METHODS AND DEVICES FOR PROVIDING PRIVACY-PRESERVING BLOCKCHAIN-BASED AUCTION

ABSTRACT

Disclosed herein are methods, devices, and apparatuses, including computer programs stored on computer-readable media, for providing a privacy-preserving blockchain-based auction. One of the methods includes: receiving, from a first user, data representing one or more assets offered to be auctioned off and a set of parameters for the auction; receiving one or more encrypted bids from one or more second users; receiving a plurality of shared pieces of a private key from a plurality of third users; reconstructing the private key based on the plurality of shared pieces received from the plurality of third users, the reconstructed private key being configured to decrypt the received encrypted bids; and automatically settling the auction based on the parameters for the auction, the received encrypted bids, and submission times at which the encrypted bids are received.

Fig. 3