What Is Claimed Is:

1. A computer-implemented method for providing a privacy-preserving blockchain-based auction, the method comprising:

receiving, from an offeror, data representing one or more assets offered to be auctioned;

receiving a plurality of shared pieces of a private key from a plurality of key holders, the private key being generated by the offeror and being split into the share pieces for safekeeping;

reconstructing the private key based on the plurality of shared pieces received from the plurality of key holders, the reconstructed private key being configured to decrypt one or more encrypted bids; and

settling the auction based on the encrypted bids and submission times at which the encrypted bids are received.

2. The method of claim 1, further comprising:

receiving, from the offeror, a set of parameters for the auction, the set of parameters comprising a total quantity of the assets offered, an auction period, a start price, and an end price.

3. The method of claim 2, further comprising:

receiving a command to start the auction; and

starting the auction in response to receiving the command.

4. The method of claim 3, further comprising:

receiving the one or more encrypted bids after the start of the auction and before an end of the auction period.

5. The method of claim 4, further comprising:

receiving the plurality of shared pieces of the private key after the end of the auction period.

6. The method of any of claims 2 to 5, wherein the settling the auction further comprises:

arranging the encrypted bids based on their corresponding submission times;

decrypting the encrypted bids using the reconstructed private key;

identifying an i-th bid at which an accumulated bid quantity equals to or exceeds a total quantity of the assets offered;

determining a price P_i corresponding to a time T_i at which the i-th bid was submitted; and

settling the auction based on the determined price P_i.

7. The method of claim 6, wherein the settling the auction based on the determined price P_i further comprises:

for each encrypted bid received at or prior to the time T_i:

determining a quantity specified in the decrypted bid corresponding to the encrypted bid;

automatically transferring the specified quantity of the assets from the offeror to a bidder who submitted the bid; and

automatically transferring an amount equal to the determined price P_i multiplied by the specified quantity from the bidder to the offeror.

8. The method of claim 6 or 7, wherein the determined price P_i is determined as a function of the auction period, the start price, and the end price.

9. The method of claim 8, wherein the determined price P_i decreases linearly from the start price to the end price over the auction period after the auction starts.

10. A device for providing a privacy-preserving blockchain-based auction, comprising:

one or more processors; and

one or more computer-readable memories coupled to the one or more processors and having instructions stored thereon that are executable by the one or more processors to perform the method of any of claims 1 to 9.

11. An apparatus for providing a privacy-preserving blockchain-based auction, the apparatus comprising a plurality of modules for performing the method of any of claims 1 to 9.

12. A non-transitory computer-readable medium having stored therein instructions that, when executed by a processor of a device, cause the device to perform the method of any of claims 1 to 9.