TRANSACTION PROCESSING METHOD AND APPARATUS, TRANSACTION SYSTEM, STORAGE MEDIUM, AND COMPUTER SYSTEM

ABSTRACT

Embodiments of this specification disclose a transaction processing method. The method includes: receiving a transaction request, where the transaction request includes a first account, a second account, a first ciphertext balance, and a first ciphertext transaction amount obtained by homomorphically encrypting a transaction amount by using at least a public key of the first account; and performing a first update and a second update in response to determining that the transaction request is valid, where the first update includes: determining a ciphertext difference between a ciphertext balance at a queue tail of a first balance queue corresponding to the first account and the first ciphertext transaction amount, adding the ciphertext difference to the first balance queue as an updated queue tail, and deleting a ciphertext balance other than the updated queue tail from the first balance queue; and the second update includes: adding a ciphertext sum value between a ciphertext balance at a queue tail of a second balance queue corresponding to the second account and a second ciphertext transaction amount to the queue tail of the second balance queue, where the second ciphertext transaction amount is obtained by homomorphically encrypting the transaction amount, and is decryptable for the second account.

FIG. 2