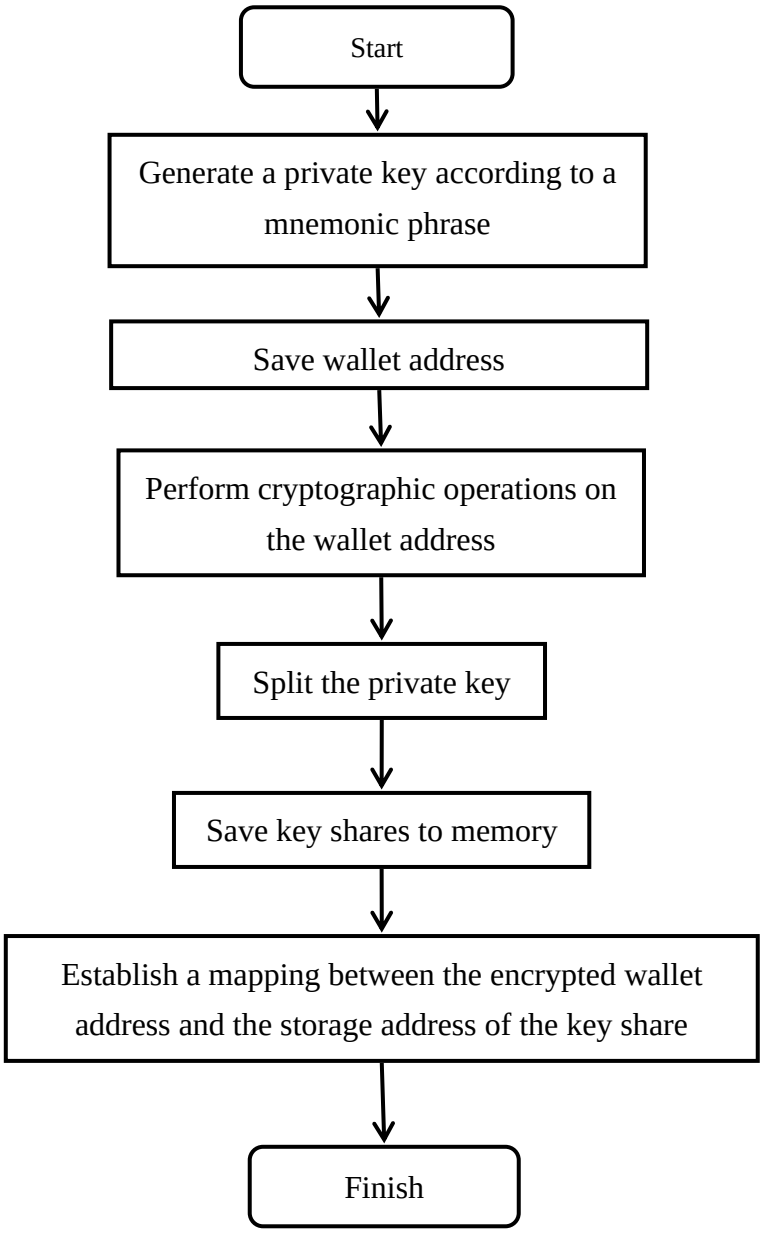
Start
Generate a private key according to a mnemonic phrase
Save wallet address
Perform cryptographic operations on the wallet address
Split the private key
Save key shares to memory
Establish a mapping between the encrypted wallet address and the storage address of the key share
Finish

Fig. 1

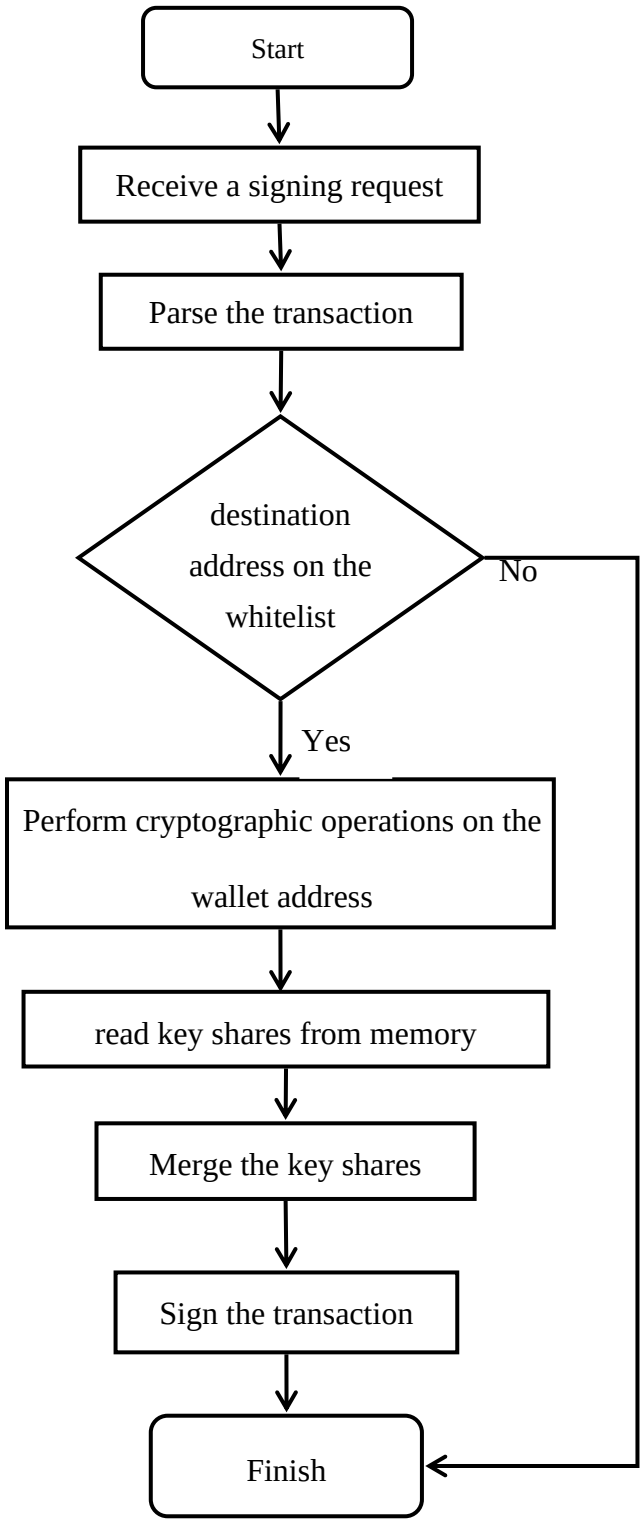
Start
Receive a signing request
Parse the transaction
destination address on the whitelist
No
Yes
Perform cryptographic operations on the wallet address
read key shares from memory
Merge the key shares
Sign the transaction
Finish

Fig. 2

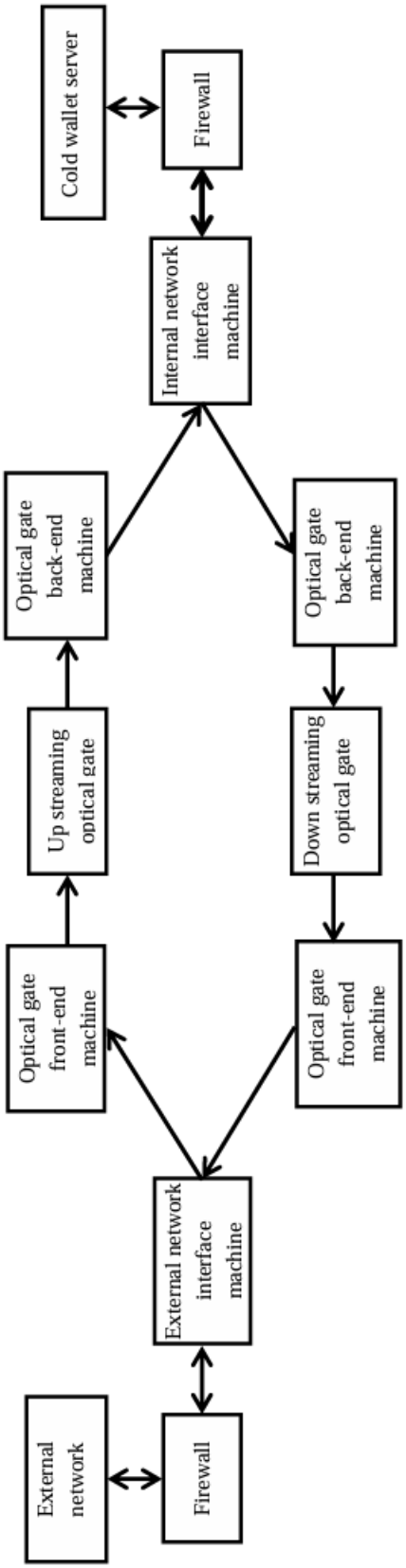
Cold wallet server
Firewall
Internal network interface machine
Optical gate back-end machine
Optical gate back-end machine
Up streaming optical gate
Down streaming optical gate
Optical gate front-end machine
Optical gate front-end machine
External network interface machine
External network
Firewall

Fig. 3