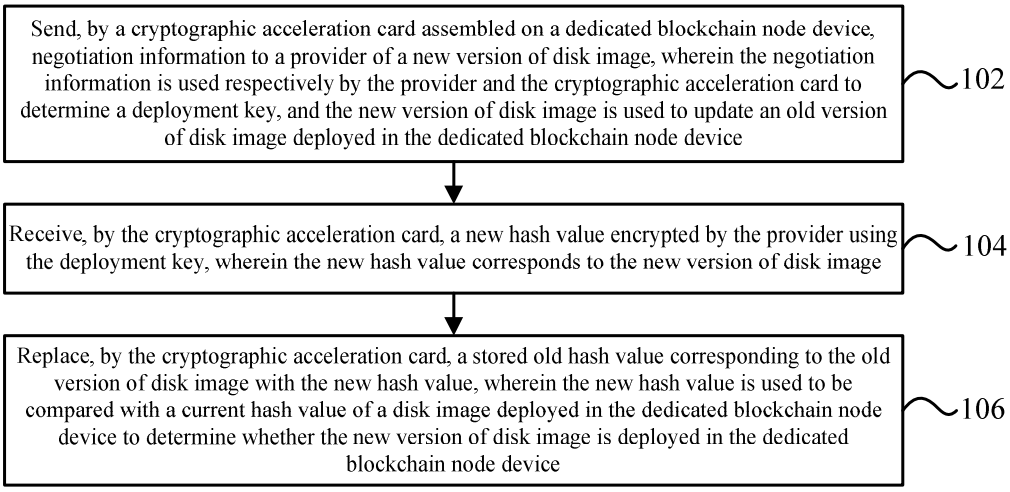
Send, by a cryptographic acceleration card assembled on a dedicated blockchain node device, negotiation information to a provider of a new version of disk image, wherein the negotiation information is used respectively by the provider and the cryptographic acceleration card to determine a deployment key, and the new version of disk image is used to update an old version of disk image deployed in the dedicated blockchain node device
102
Receive, by the cryptographic acceleration card, a new hash value encrypted by the provider using the deployment key, wherein the new hash value corresponds to the new version of disk image
104
Replace, by the cryptographic acceleration card, a stored old hash value corresponding to the old version of disk image with the new hash value, wherein the new hash value is used to be compared with a current hash value of a disk image deployed in the dedicated blockchain node device to determine whether the new version of disk image is deployed in the dedicated blockchain node device
106

FIG. 1

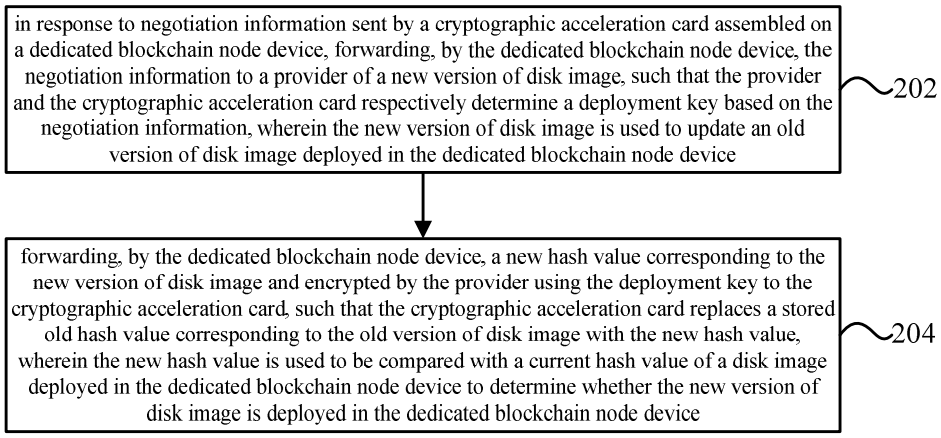
in response to negotiation information sent by a cryptographic acceleration card assembled on a dedicated blockchain node device, forwarding, by the dedicated blockchain node device, the negotiation information to a provider of a new version of disk image, such that the provider and the cryptographic acceleration card respectively determine a deployment key based on the negotiation information, wherein the new version of disk image is used to update an old version of disk image deployed in the dedicated blockchain node device
202
forwarding, by the dedicated blockchain node device, a new hash value corresponding to the new version of disk image and encrypted by the provider using the deployment key to the cryptographic acceleration card, such that the cryptographic acceleration card replaces a stored old hash value corresponding to the old version of disk image with the new hash value, wherein the new hash value is used to be compared with a current hash value of a disk image deployed in the dedicated blockchain node device to determine whether the new version of disk image is deployed in the dedicated blockchain node device
204

FIG. 2

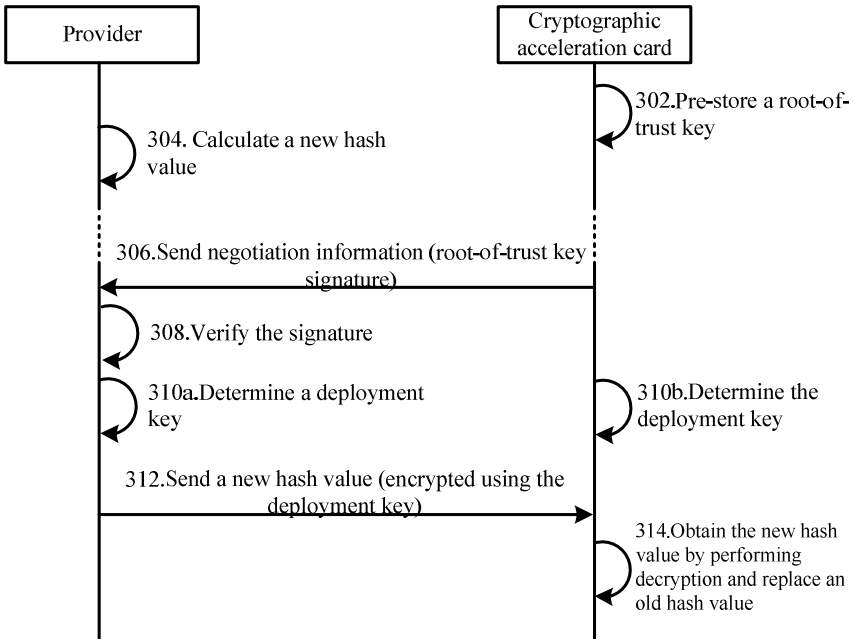
Provider
Cryptographic acceleration card
302.Pre-store a root-of-trust key
304. Calculate a new hash value
306.Send negotiation information (root-of-trust key signature)
308.Verify the signature
310a.Determine a deployment key
310b.Determine the deployment key
312.Send a new hash value (encrypted using the deployment key)
314.Obtain the new hash value by performing decryption and replace an old hash value

FIG. 3

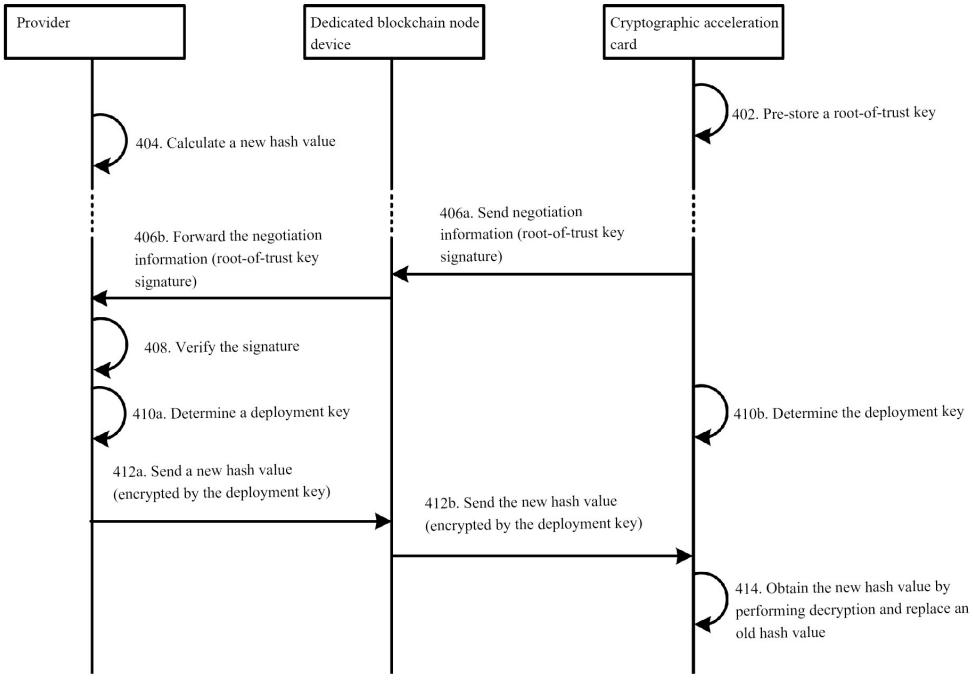
Provider
Dedicated blockchain node device
Cryptographic acceleration card
402. Pre-store a root-of-trust key
404. Calculate a new hash value
406a. Send negotiation information (root-of-trust key signature)
406b. Forward the negotiation information (root-of-trust key signature)
408. Verify the signature
410a. Determine a deployment key
410b. Determine the deployment key
412a. Send a new hash value (encrypted by the deployment key)
412b. Send the new hash value (encrypted by the deployment key)
414. Obtain the new hash value by performing decryption and replace an old hash value

FIG. 4

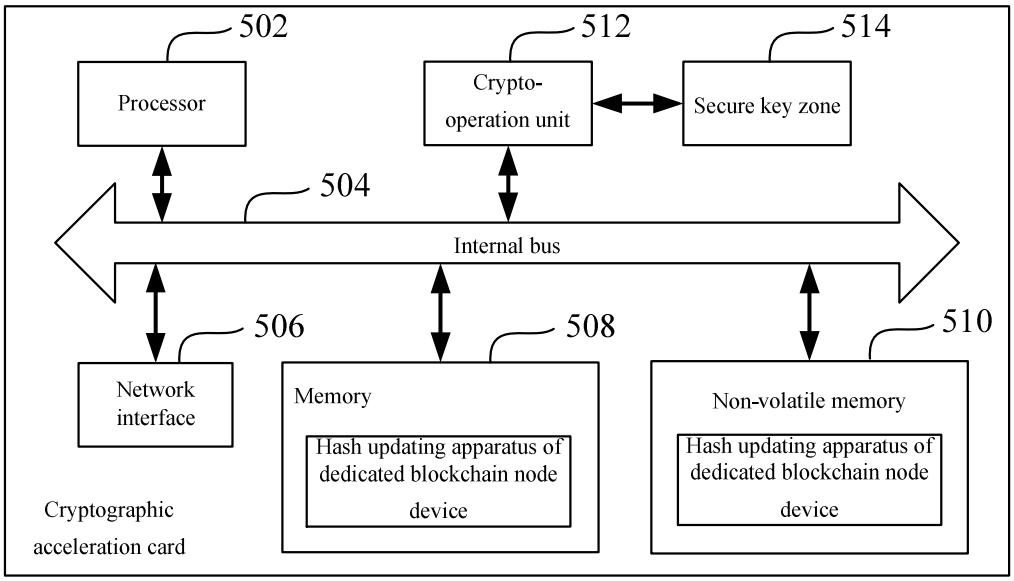

FIG. 5

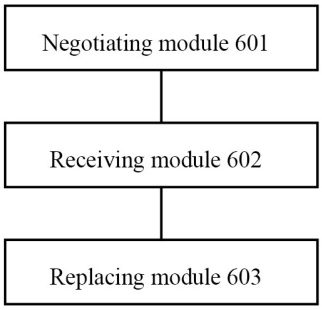

FIG. 6

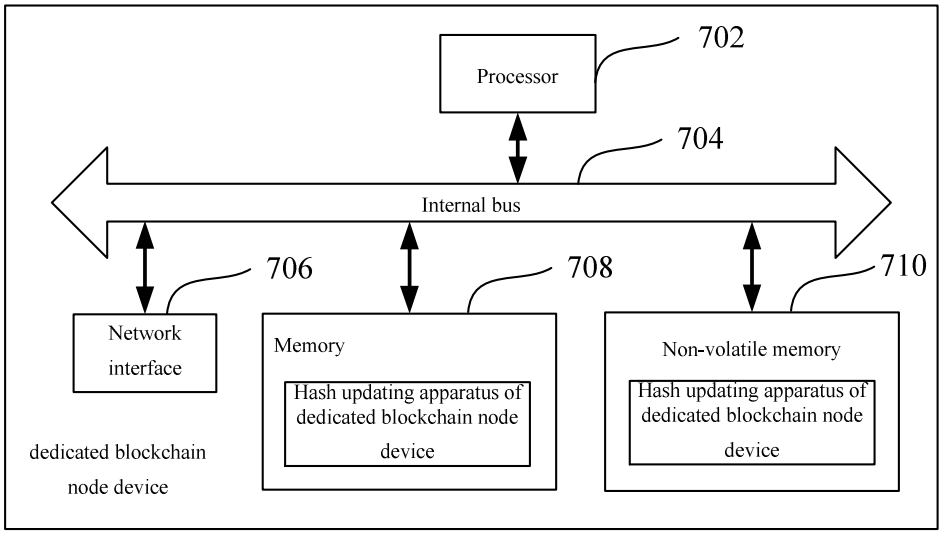

FIG. 7

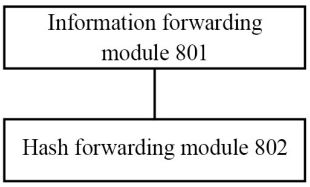
Information forwarding module 801
Hash forwarding module 802

FIG. 8