CLAIMS

1. A hash updating method of a dedicated blockchain node device, comprising:

sending, by a cryptographic acceleration card assembled on the 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;

receiving, 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;

replacing, 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.

2. The method according to claim 1, wherein the disk image deployed in the dedicated blockchain node device comprises:

a binary disk image corresponding to a blockchain node and deployed in the dedicated blockchain node device; or,

a platform disk image deployed in the dedicated blockchain node device, wherein the platform disk image comprises the binary disk image.

3. The method according to claim 1, wherein replacing, by the cryptographic acceleration card, the stored old hash value corresponding to the old version of disk image with the new hash value comprising:

after receiving the new hash value encrypted by the deployment key, obtaining, by the cryptographic acceleration card, the new hash value by decrypting using the deployment key;

replacing, by the cryptographic acceleration card, the stored old hash value with the new hash value.

4. The method according to claim 1, wherein the old hash value and the new hash value are calculated and generated in a trusted execution environment using the old version of disk image and the new version of disk image provided by the provider, respectively.

5. The method according to claim 1, wherein the negotiation information is signed by a root-of-trust key pre-stored in the cryptographic acceleration card, wherein a public key corresponding to the root-of-trust key is disclosed or the public key corresponding to the root-of-trust key is maintained only by the provider.

6. A hash updating method of a dedicated blockchain node device, comprising:

in response to negotiation information sent by a cryptographic acceleration card assembled on the 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;

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.

7. The method according to claim 6, wherein the disk image deployed in the dedicated blockchain node device comprises:

a binary disk image corresponding to a blockchain node and deployed in the dedicated blockchain node device; or,

a platform disk image deployed in the dedicated blockchain node device, wherein the platform disk image comprises the binary disk image.

8. The method according to claim 6, wherein the old hash value and the new hash value are calculated and generated in a trusted execution environment using the old version of disk image and the new version of disk image provided by the provider, respectively.

9. The method according to claim 6, wherein the negotiation information is signed by a root-of-trust key pre-stored in the cryptographic acceleration card, wherein a public key corresponding to the root-of-trust key is disclosed or the public key corresponding to the root-of-trust key is maintained only by the provider.

10. A cryptographic acceleration card, comprising:

a processor; and

a memory for storing processor executable instructions ;

wherein the processor implements a method according to any of claims 1-5 by running the executable instructions.

11. A dedicated blockchain node device, comprising:

a processor; and

a memory for storing processor executable instructions;

wherein the processor implements a method according to any of claims 6-9 by running the executable instructions.

12. A computer readable storage medium having computer instructions stored thereon, wherein the instructions are executed by a processor to implement steps in a method according to any of claims 1-9.