the dedicated blockchain node device or the above-mentioned smart contract processing chip, thereby improving the processing efficiency.

[0043] Software optimization can be realized for the dedicated blockchain node device. For example, a certificate authority service can be built in the dedicated blockchain node device to realize automatic certificate issuing, node identity authentication, automatic blockchain construction, and automatic adding of blockchain node, thereby realizing the plug and play of the dedicated blockchain node device. In this case, a user can realize fast deployment of the dedicated blockchain node device. In addition to quickly establishing a private blockchain network among a plurality of dedicated blockchain node devices, the dedicated blockchain node device can integrate a standardized on-cloud service interface to enable the dedicated blockchain node device to automatically connect to on-cloud service, thereby realizing hybrid deployment between the dedicated blockchain node device and the cloud-deployed blockchain node to construct a hybrid blockchain network. The dedicated blockchain node device can also integrate a standardized cross-chain service interface to enable the dedicated blockchain node device to realize cross-chain services based on a standardized cross-chain protocol or standardized cross-chain service, thereby greatly expanding the application scenarios of the dedicated blockchain node device, and satisfying the cross-chain needs of users. For example, cross-chain data interaction between different blockchain networks is achieved, and for another example, cross-chain data interaction between the blockchain network and an off-chain computing node and the like is achieved (for example, the off-chain computing node shares computation task for the blockchain node and the like).

[0044] Based on a unified software logic, the cryptographic acceleration card assembled on the dedicated blockchain node device can realize the process of updating a self-stored old hash value corresponding to an old version of disk image. In this updating process, the cryptographic acceleration card firstly determines a deployment key together with a provider of a new version of disk image (hereinafter called provider for short) through negotiation information, and then a new hash value corresponding to the new version of disk image is encrypted and transmitted to the cryptographic acceleration card from the provider and finally, the cryptographic acceleration card replaces the locally-stored old hash value with the new hash value obtained through decryption, thereby the old hash value is updated. The process will be described below in combination with accompanying drawings.

[0045] FIG. 1 is a flowchart of a hash updating method of a dedicated blockchain node device according to example embodiments of the present disclosure. The method is applied to a cryptographic acceleration card assembled on the dedicated blockchain node device. In order to distinguish from the cryptographic acceleration card, the dedicated blockchain node

device in the subsequent descriptions of the present disclosure can be understood as a CPU of the dedicated blockchain node device, or another component other than the cryptographic acceleration card assembled in the dedicated blockchain node device. As shown in FIG. 1, the method can include the following steps.

[0046] At step 102, the cryptographic acceleration card assembled on the dedicated blockchain node device sends negotiation information to a provider of a new version of disk image, where the negotiation information is respectively used 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.

[0047] In this embodiment, a disk image (that has not been executed yet) is locally pre-deployed in the dedicated blockchain node device. The specific form of the disk image is not limited herein in the present disclosure. For example, the disk image can be an executable disk image, for example, an executable file of .exe format. At this time, the executable file can be pre-installed in an execution component of the dedicated blockchain node device, such as a hard disk drive. The disk image can also be a binary disk image, for example, a binary image of .bin format. At this time, the binary image can be pre-stored at a proper position of an execution component of the dedicated blockchain node device, such as a hard disk drive to be invoked and executed. Further, the disk image can be a binary disk image corresponding to a blockchain node and deployed in the dedicated blockchain node device. Correspondingly, when the binary disk image is executed, the dedicated blockchain node device is implemented as a blockchain node, for example, realize one or more functions of blockchain visualization, contract creation and deployment, contract execution, key management and privacy computing and the like. The disk image can also be a platform disk image including the above-mentioned binary disk image corresponding to the blockchain node and deployed in the dedicated blockchain node device. When the platform disk image is executed, the dedicated blockchain node device is implemented not only as a blockchain node, but also can realize one or more other functions such as image processing, node monitoring and service monitoring, which will not be redundantly described herein.

[0048] Correspondingly, the cryptographic acceleration card currently already stored an old hash value corresponding to the old version of disk image. The solution of the present disclosure aims to replace the old hash value with a new hash value corresponding to the above-mentioned new version of disk image so as to update the old hash value, thus ensuring the hash value stored in the cryptographic acceleration card always corresponds to the new

herein.

[0057] In an embodiment, the provider can encrypt the new hash value obtained in the above-mentioned calculation process by using the deployment key determined in the above-mentioned key negotiation process and then transmit the encrypted new hash value to the cryptographic acceleration card, thus ensuring the privacy of the new hash value in transmission process. For example, the provider can transmit the encrypted new hash value directly to the cryptographic acceleration card to reduce the possibility of information leakage of the new hash value in the transmission process; or, in a case of inability to perform direct communication with the cryptographic acceleration card due to unavailability of a network address of the cryptographic acceleration card and the like, the provider can also firstly send the encrypted new hash value to the dedicated blockchain node device which then forwards the encrypted new hash value to the cryptographic acceleration card.

[0058] At step 106, the cryptographic acceleration card replaces the stored old hash value corresponding to the old version of disk image with the new hash value, where 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.

[0059] In an embodiment, after receiving the new hash value encrypted using the deployment key, the cryptographic acceleration card can obtain the new hash value in plaintext status by performing decryption using the deployment key determined in the above-mentioned key negotiation process in the TEE corresponding to the cryptographic acceleration card, and then replace the currently-stored old hash value with the new hash value. Thus, with the pre-deployed root-of-trust key, the temporarily-determined deployment key can be used in the transmission process of the new hash value, which not only ensures the privacy of the new hash value in the transmission process but also reduces the possibility that the root-of-trust key of the cryptographic acceleration card is leaked, thereby improving the security of the cryptographic acceleration card. In a case that a plurality of old versions of disk image respectively correspond to different new versions of disk image in the dedicated blockchain node device at the same time, the cryptographic acceleration card can establish an association relationship between a new hash value corresponding to any new version of disk image and a file identifier of the new version of disk image, and encrypt and store various new hash values according to respective association relationships, so as to specifically update any old hash value.

[0060] In this embodiment, the above-mentioned old hash value stored in the cryptographic

between the cryptographic acceleration card and the provider can be directly transmitted between the cryptographic acceleration card and the provider or can be forwarded by the dedicated blockchain node device, which will be described below in combination with FIGS. 3 and 4.

[0067] FIG. 3 is an interaction flowchart of a hash updating method of a dedicated blockchain node device. In combination with FIG. 3, the process in which the old hash value stored in the cryptographic acceleration card is updated by directly sending data between the cryptographic acceleration card and the provider will be described below. As shown in FIG. 3, the process can include the following steps.

[0068] At step 302, a root-of-trust key is locally pre-stored in the cryptographic acceleration card.

[0069] In this embodiment, the cryptographic acceleration card can pre-store a root-of-trust key in a TEE. For example, the root-of-trust key can be pre-stored in the cryptographic acceleration card when the dedicated blockchain node device leaves factory or the root-of-trust key can be deployed into the cryptographic acceleration card by the dedicated blockchain node device or another object in an offline secure environment. For example, when the cryptographic acceleration card is a cryptographic acceleration card based on FPGA chip, the root-of-trust key can be programmed to be deployed into the FPGA structure of the cryptographic acceleration card, for example, programmed into a secure key zone of the e cryptographic acceleration card. However, due to volatility of the FPGA chip, the stored root-of-trust key will be lost upon power down, so that the cryptographic acceleration card needs to re-deploy the root-of-trust key after power up. To reduce the number of deployments of a client device, the FPGA structure can further include a memory connected with the FPGA chip, so that the root-of-trust key is deployed in the memory and the FPGA chip can read the root-of-trust key from the memory to realize relevant functions. Due to non-volatility of the memory, the memory can still store the root-of-trust key even upon power down, and the cryptographic acceleration card only needs to re-read the root-of-trust key from the memory to the FPGA chip after power up, without re-deploying. The above-mentioned memory can be in several forms, for example, can be a re-writable non-volatile memory such as flash memory, or can be a non-rewritable memory such as fuse memory, which will not be limited herein.

[0070] The above-mentioned the root-of-trust key is an asymmetric key and a public key corresponding to the root-of-trust key is disclosed or maintained only by the provider. In this case, even if the root-of-trust key is not deployed (pre-built by the provider, or deployed by another object) by the provider, the provider can still verify, by using the disclosed public key,

node device, when the cryptographic acceleration card sends the negotiation information to the provider and the provider sends the new hash value encrypted by the negotiated deployment key to the cryptographic acceleration card, the dedicated blockchain node device can forward the above-mentioned negotiation information and the new hash value in ciphertext status. FIG. 4 is an interaction flowchart of another hash updating method of a dedicated blockchain node device according to example embodiments of the present disclosure. In combination with FIG. 4, the process in which the old hash value stored in the cryptographic acceleration card is updated by forwarding data through the dedicated blockchain node device between the cryptographic acceleration card and the provider will be described below. As shown in FIG. 4, the process can include the following steps.

[0092] At step 402, the cryptographic acceleration card locally pre-stores a root-of-trust key.

[0093] At step 404, the provider of the new version of disk image calculates the new hash value in its own TEE according to the new version of disk image.

[0094] At step 406a, the cryptographic acceleration card sends negotiation information and a signature performed using the root-of-trust key to the dedicated blockchain node device.

[0095] At step 406b, the dedicated blockchain node device forwards the negotiation information and the signature performed using the root-of-trust key to the provider.

[0096] In the steps 406a-406b, the negotiation information and the signature performed using the root-of-trust key are forwarded through the dedicated blockchain node device to the provider, so that the cryptographic acceleration card and the provider are connected through the dedicated blockchain node device.

[0097] At step 408, the provider verifies the signature of the negotiation information.

[0098] At step 410 (i.e. 410a and 401b), the provider determines a deployment key according to the negotiation information.

[0099] At step 412a, the provider sends a new hash value encrypted by the deployment key to the dedicated blockchain node device.

[00100] At step 412b, the dedicated blockchain node device forwards the new hash value encrypted by the deployment key to the cryptographic acceleration card.

[00101] In the steps 412a-412b, the new hash value encrypted by the deployment key is forwarded through the dedicated blockchain node device to the cryptographic acceleration card, so that the cryptographic acceleration card and the provider are connected through the dedicated blockchain node device.

[00102] At step 414, the cryptographic acceleration card obtains the new hash value by performing decryption using its own deployment key and replaces a currently-stored old hash value with the new hash value.

[00103] The above-mentioned specific process of various steps in this embodiment is basically identical to step 314 of the embodiment shown in FIG. 3 and thus can referred to the previous descriptions and will not be repeated herein.

[00104] FIG. 5 is a structural schematic diagram of a cryptographic acceleration card according to example embodiments of the present disclosure. As shown in FIG. 5, from the hardware level, the device includes a processor 502, an internal bus 504, a network interface 506, a memory 508, a non-volatile memory 510, a crypto-operation unit 512 and a secure key zone 514. Of course, the device may further include hardware needed for other services. The crypto-operation unit 512 stores received or generated relevant keys in the secure key zone 514 so that the processor 502 invokes the keys to realize relevant functions such as encryption, decryption, signature obtaining and/or signature verification. The processor 502 reads corresponding computer programs from the non-volatile memory 510 to the memory 508 for running, so as to logically form a hash updating apparatus of a dedicated blockchain node device. Of course, in addition to the software implementation, one or more embodiments of the present disclosure do not preclude other implementations, for example, logic device or a combination of software and hardware or the like. That is, the executing subject of the following processing flow is not limited to each logic unit and can also be hardware or logic device.

[00105] As shown in FIG. 6, in a software implementation, a hash updating apparatus of a dedicated blockchain node device can include:

[00106] a negotiating module 601, configured to enable a cryptographic acceleration card assembled on the dedicated blockchain node device to send negotiation information to a provider of a new version of disk image, where 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;

[00107] a receiving module 602, configured to enable the cryptographic acceleration card to receive a new hash value encrypted by the provider using the deployment key, where the new hash value corresponds to the new version of disk image; and

[00108] a replacing module 603, configured to enable the cryptographic acceleration card to replace a stored old hash value corresponding to the old version of disk image with the new hash value, where 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.

[00109] Optionally, the disk image deployed in the dedicated blockchain node device