

accordance with a program of each of the functional units. For example, the CPU 10 functions as the public template generating unit 1030 by processing in accordance with a public template generating program. The above similarly applies to other programs as well. Furthermore, the CPU 10 also operates as a functional unit that provides each function of a plurality of pieces of processing executed by each program. A computer or a computer system is a device or a system that includes these functional units.

[0178]

The programs and information such as tables for implementing each function can be stored in a storage device such as a nonvolatile semiconductor memory, a hard disk drive, an SSD (Solid State Drive) or the like comprising the auxiliary storage device 30, or a storage device such as an IC card, an SD card, a DVD can be stored in a computer-readable non-transitory data storage medium.

[0179]

As described above, according to the first embodiment, a public template certificate is generated from biometric information of a user, a pair of a secret key and a public key is generated, a public key certificate is generated by attaching a biometric signature to the public key by using the biometric information of the user as a key, attaching a signature to a message by using the secret key when the

user generates the signature, when the signature is

FIG. 19 is a sequence diagram illustrating an example of registration processing performed in the blockchain system. This processing is a registration processing that a user using the blockchain system initially performs like in FIGS. 2 and 3 of the first embodiment. Hereinafter, exemplary registration processing of the user A will be described.

[0207]

First, in the registration terminal 1400, a biometric information acquiring unit 1420 acquires biometric information of the user A (S301).

[0208]

A public template generating unit 1430 generates a public template by applying unidirectional conversion to the biometric information acquired in step S301 (S302). The public template generating unit 1430 transmits the generated public template to the public template repository 1200 (S303).

[0209]

A key pair generating unit 1440 of the registration terminal 1400 generates a key pair of a secret key and a public key (S304).

[0210]

A public key certificate generating unit 1450 of the registration terminal 1400 generates a public key

certificate by attaching, to the generated public key, a biometric signature using the biometric information acquired in step S301 as a key (S305).

[0211]

The registration terminal 1400 stores the secret key, the public key, and the public key certificate in a key storing unit 1491 (S306).

[0212]

Next, in the public template repository 1200, a public template certificate generating unit 1220 attaches a signature to the received public template to generate a public template certificate (S309). In the third embodiment, signature is added using the secret key of the certificate authority like in the first embodiment.

[0213]

The public template repository 1200 registers the generated public template certificate in a public template certificate storing unit 1290 (S310) and further transmits the public template certificate to the registration terminal 1400 (S311). When receiving the public template certificate, the registration terminal 1400 registers the public template certificate in the public template certificate storing unit 1492 (S307).

[0214]

Next, the registration terminal 1400 transmits the

key pair, the public key certificate, and the public template certificate to the user terminal 1300-A that the user A is using (S308). The user terminal 1300-A registers the received key pair and the public key certificate in a key storing unit 1491 and registers the public template certificate in a public template certificate storing unit 1492 (S312).

[0215]

Next, the user terminal 1300-A transmits the public key and the public template to the user terminal 1300-B or other terminals to which the transaction is to be transmitted (S313). The user terminal 1300-A registers the received public key and the public template in a storing unit (S314).

[0216]

In this manner, the key pair and the public key certificate are generated, the registration processing is completed, and preparation for transmitting and receiving the transaction is completed.

[0217]

FIG. 20 is a sequence diagram illustrating an example of transaction verification processing performed in the blockchain system. This processing is similar to that of FIGS. 4 to 6 of the first embodiment. In FIG. 20, an example in which the user A receives an existing

the first embodiment, and the verification terminal 1100 generates a hash value to verify the validity of the signature by using the generated hash value and the public key certificate.

[0224]

The verification terminal 1100 notifies the user terminals 1300-A and 1300-C of the verification results of the public template certificate, the public key certificate, and the signature.

[0225]

As described above, the verification terminal 1100 can verify the contents of the transactions.

[0226]

FIG. 21 is a sequence diagram illustrating an example of key reissuance processing performed in the blockchain system. This processing is similar to that FIGS. 7 and 8 of the first embodiment, and FIG. 21 illustrates an example in which the user A loses a secret key.

[0227]

The user A of the user terminal 1300-A has lost the secret key (S501), and thus the registration terminal 1400 starts key reissuance processing. The registration terminal 1400 acquires the public key certificate and the public template certificate of the user A from the key storing unit 1491 and the public template certificate

storing unit 1492 to generate a public key revocation application form (S502) and transmits the public key revocation application form to the public template repository 1200 (S503).

[0228]

The public template repository 1200 verifies the validity of the public key revocation application form (S503). In this verification, the public template repository 1200 verifies that the signature value assigned to the public key revocation application form is genuine by using the public template certificate. If the verification is successful, the public template repository 1200 issues a public key revocation list (S504). The public template repository 1200 registers the public key revocation list in a certificate revocation list storing unit 1291 and transmits the public key revocation list to the registration terminal 1400.

[0229]

After receiving the public key revocation list, the registration terminal 1400 acquires biometric information of the user A (S505). Using the biometric signature of the public template certificate, the registration terminal 1400 verifies whether the biometric information with which the public template certificate has been generated and the acquired biometric information have been acquired from the

same person, and if from the same person, the verification is regarded as being successful.

[0230]

If the verification is successful, the registration terminal 1400 generates a key pair like in the first embodiment (S507) and generates a public key certificate by attaching a signature to the public key (S508). The registration terminal 1400 registers the key pair and the public key certificate in the key storing unit 1491 (S509) and then transmits the key pair and the public key certificate to the user terminal 1300-A of the user A (S510).

[0231]

The user terminal 1300-A deletes the old key pair and public key certificate and registers the received new key pair and the public key certificate in the key storing unit 1091 (S511). Next, the user terminal 1300-A transmits the public key to the user terminal 1300-B which a transaction is transmitted to or received from (S512).

[0232]

The user terminal 1300-B deletes the old public key of the user A and registers the newly received public key in a key storing unit 1091 (S513).

[0233]

As described above, in the third embodiment, a public

key certificate can be reissued by attaching a signature to the public key using user's biometric information acquired using the registration terminal 1400 as a key. In the third embodiment, for example, the registration terminal 1400 may be installed in an organization that manages the blockchain system, thereby enabling acquisition of biometric information after the administrator or the like of the blockchain system confirms identity of the user. With this configuration, registration by impersonation can be suppressed.

[0234]

Note that the registration terminal 1400 and the public template repository 1200 may be configured by a single computer. In this case, the registration units (the public key certificate generating unit 1450, the public template certificate generating unit 1220, and the public key revocation application form generating unit 1480) may be provided by a single computer. Alternatively, the registration terminal 1400, the public template repository 1200, and the verification terminal 1100 may be configured by a single computer. In this case, the registration units and the verifying units (public key certificate verifying unit 1120) can be provided by a single computer.

[Fourth Embodiment]

[0235]