too large, a mobile node (for example, a smartphone) with a limited storage capacity (or a limited memory capacity) has difficulty in storing the integrated ledger as it is.

Each bank node 200 included in the blockchain system 100 according to the present invention, which is devised to solve such problems, registers (also referred to as "records" or "stores") ledgers 210, 220, 230, 240, 250, 261, 263, …, and 265 each separated by function instead of a single ledger like the conventional integrated ledger.

For example, an amount of data registered in each of the ledgers 210, 220, 230, 240, 250, 261, 263, …, and 265 in the form of a blockchain is significantly less than an amount of data stored in the conventional integrated ledger in the form of a blockchain. In addition, since unnecessary ledgers (for example, ledgers of digital currencies that are not used any longer) can be deleted, the amount of data can be further reduced by deleting the unnecessary ledgers.

Since each mobile nodes 300-1 and 300-2 (collectively referred to as "300") does not store a single ledger like the conventional integrated ledger itself by receiving it downloaded from the bank node 200, but stores only a summary ledger that records only an account balance of a digital currency required for financial transactions by receiving it downloaded from the bank node 200 or updates an existing summary ledger by receiving only an updated account balance, the amount of transaction data stored in the summary ledger of each mobile node 300 is significantly reduced as compared to the amount of transaction data stored in the conventional integrated ledger.

Computing power of each mobile node 300 that processes only the summary ledger or updates only the account balance is significantly reduced as compared to computing power required for processing the conventional integrated ledger, and an amount of communication data transmitted or received between each bank node 200 and each mobile node 300 to process the summary ledger or the account balance is significantly reduced as compared to the amount of

currency in the blockchain network 110 are executed using the digital IDs of each of the nodes 200-1 to 200-4, 300-1, and 300-2, even though each of the nodes 200-1 to 200-4, 300-1, and 300-2 loses its own private key, each of the nodes 200-1 to 200-4, 300-1, and 300-2 may execute financial transactions in a digital currency registered in the digital currency ledger by registering a new public key in the identity ledger 210 again.

The identity ledger 210 may function as a decentralized public key infrastructure (PKI).

Each of the digital identifications (IDs) DID1 to DID4, DIDm1, and DIDm2 refers to identity information that can uniquely identify the identity of each of the nodes 200-1 to 200-4, 300-1, and 300-2 or a user of each of the nodes 200-1 to 200-4, 300-1, and 300-2.

Identity information collectively refers to personal information and unique information linked to the personal information. Personal information refers to information that can directly or indirectly identify an individual among information regarding the individual. For example, personal information, as information regarding an individual, refers to information on codes, texts, voice, sound, images, and biometric characteristics that can identify the individual by a name (or one's real name), a resident registration number, and the like (even if a specific individual cannot be identified by the information alone, information that can be easily combined with other types of information to identify the specific individual is included).

Examples of identity information for identifying the identity of a user include at least one of a name (or a title), a resident registration number (a corporate registration number), a smartphone phone number, fingerprint information, iris information, facial recognition information, and voice information; however, the present invention is not limited thereto.

Here, each of the digital IDs DID1 to DID4, DIDm1, and DIDm2 is information different from an address defined by a public key arbitrarily generated by the user of each of the nodes 200-1 to 200-4, 300-1, and 300-2 or an arbitrary hash value derived from the public key.

CLAIMS

1. A blockchain system comprising:

a plurality of bank nodes, each of the bank nodes comprising an on-line server capable of issuing a digital currency; and

a plurality of mobile nodes, each of the mobile nodes comprising a portable computing device,

wherein each of the bank nodes includes an identity ledger that includes:

a public key of each of the bank nodes,

a digital ID for identifying an identity of each of the bank nodes,

a public key of a user of each of the mobile nodes, and

a digital ID for identifying an identity of the user of each of the mobile nodes,

wherein the identity ledger functions as a decentralized public key infrastructure,

wherein financial transactions in the digital currency in a blockchain network are executed using the digital ID for identifying the identity of the user of each of the mobile nodes, and when the user of each of the mobile nodes loses its own private key that is used for signing a transaction, each of the bank nodes registers a new public key of the user of each of the mobile nodes in the identity ledger again, and

wherein each of the bank nodes receives the public key of each of the bank nodes, the digital ID for identifying the identity of each of the bank nodes corresponding to the public key of each of the bank nodes, the public key of the user of each of the mobile nodes, and the digital ID for identifying the identity of the user of each of the mobile nodes corresponding to the public key of the user of each of the mobile nodes, and registers the received public key of each of the bank nodes, the received digital ID for identifying the identity of each of the bank nodes corresponding to the public key of each of the bank nodes, the received public key of the user of

each of the mobile nodes, and the received digital ID for identifying the identity of the user of each of the mobile nodes corresponding to the public key of the user of each of the mobile nodes in the identity ledger included in each of the bank nodes in a blockchain method using a blockchain consensus.

2. The blockchain system of claim 1,

wherein each of the bank nodes further includes a chaincode registration ledger in which chaincodes generated by the bank nodes are registered according to a consensus between the bank nodes and the mobile nodes,

wherein the chaincodes include:

a digital currency issuance chaincode for issuing the digital currency; and

a digital currency transaction chaincode downloaded to at least one mobile node with which transactions are desired using the digital currency among the mobile nodes.

3. The blockchain system of claim 2,

wherein each of the bank nodes further includes a chaincode execution ledger,

when any one of the bank nodes executes the digital currency issuance chaincode registered in the chaincode registration ledger,

each of the bank nodes registers chaincode execution information, which includes issuance conditions of a first digital currency and a result of execution indicating whether the first digital currency is issued, in the chaincode execution ledger included in each of the bank nodes in the blockchain method using the blockchain consensus.

4. The blockchain system of claim 3,

wherein the chaincode execution information includes a total issuance amount of the digital currency, a transaction unit of the digital currency, and an ID of the digital currency transaction chaincode.

5. The blockchain system of any one of claims 2 to 4,

wherein each of the bank nodes further includes a collateral asset registration ledger,

when any one of the bank nodes issues the digital currency by executing the digital currency issuance chaincode registered in the chaincode registration ledger,

each of the bank nodes registers collateral asset registration information in the collateral asset registration ledger included in each of the bank nodes using the blockchain consensus when the any one of the bank nodes generates the collateral asset registration information on a collateral asset for securing an issuance of the digital currency.

6. The blockchain system of claim 5,

wherein the collateral asset registration information includes a type of the collateral asset, an amount of the collateral asset, and information on a collateral asset storage bank in which the collateral asset is stored.

7. The blockchain system of claim 2 or claim 3,

wherein each of the bank nodes further includes a digital currency registration ledger,

any one of the bank nodes issues the digital currency by executing the digital currency issuance chaincode registered in the chaincode registration ledger, generates digital currency issuance information including an issuance amount and transaction conditions of the issued digital currency,

each of the bank nodes registers the digital currency issuance information in the digital currency registration ledger included in each of the bank nodes in the blockchain method using the blockchain consensus.

8. The blockchain system of claim 7,

wherein the digital currency issuance information includes an ID of the digital currency, a total issuance amount of the digital currency, a transaction unit of the digital currency, and an ID of the digital currency transaction chaincode.

9. The blockchain system of claim 7 or 8,

wherein the digital currency issuance information is downloaded to the at least one mobile node.

10. The blockchain system of claim 2,

wherein each of the bank nodes further includes digital currency ledgers,

a first digital currency ledger among the digital currency ledgers stores transactional information made between transaction parties using a first digital currency among different digital currencies,

each of the bank nodes registers the transactional information in a digital currency registration ledger included in each of the bank nodes in the blockchain method using the blockchain consensus, and

wherein the transaction parties include at least one of the bank nodes and at least one of the mobile nodes.

11. The blockchain system of claim 10,

wherein the first digital currency ledger includes:

an event source ledger that stores all of the transactional information made between the transaction parties in a form of a blockchain; and

a summary ledger that stores some transactional information among all of the transactional information made between the transaction parties.

12. The blockchain system of claim 11,

wherein the some transactional information or the summary ledger is downloaded to the at least one mobile node.

13. An operation method of a blockchain system that includes a blockchain network including a plurality of bank nodes, each of the bank nodes comprising an on-line server capable of issuing a digital currency, and a plurality of mobile nodes, each of the mobile nodes comprising a portable computing device, the operation method comprising:

publishing, by each of the bank nodes, a public key of each of the bank nodes and a digital ID for identifying an identity of each of the bank nodes in the blockchain network;

publishing, by each of the mobile nodes, a public key of a user of each of the mobile nodes and a digital ID for identifying an identity of the user of each of the mobile nodes in the blockchain network;

receiving, by each of the bank nodes, the public key of each of the bank nodes, the digital ID for identifying the identity of each of the bank nodes, the public key of the user of each of the mobile nodes, and the digital ID for identifying the identity of the user of each of the mobile nodes; and

registering, by each of the bank nodes, the received public key of each of the bank nodes, the received digital ID for identifying the identity of each of the bank nodes corresponding to the public key of each of the bank nodes, the received public key of the user of each of the mobile nodes, and the received digital ID for identifying the identity of the user of each of the mobile nodes corresponding to the public key of the user of each of the mobile nodes in an identity ledger included in each of the bank nodes in a blockchain method using a blockchain consensus,

wherein the identity ledger functions as a decentralized public key infrastructure, and

wherein financial transactions in the digital currency in the blockchain network are executed using the digital ID for identifying the identity of the user of each of the mobile nodes, and when the user of each of the mobile nodes loses its own private key that is used for signing a transaction, each of the bank nodes registers a new public key of the user of each of the mobile nodes in the identity ledger again.

14. The operation method of claim 13, further comprising:

generating, by each of the bank nodes, chaincodes to publish the chaincodes in the blockchain network; and

registering, by each of the bank nodes, chaincodes published by each of the bank nodes in a chaincode registration ledger included in the each of the bank nodes according to a consensus among the bank nodes and the mobile nodes,

wherein the chaincodes include:

a digital currency issuance chaincode for issuing the digital currency; and

a digital currency transaction chaincode downloaded to at least one mobile node with which transactions are desired using the digital currency among the mobile nodes.

15. The operation method of claim 13 or 14,

wherein each of the bank nodes further includes digital currency ledgers,

the operation method further comprises storing, by each of the bank nodes, transactional information made between transaction parties using a first digital currency among digital currencies in a first digital currency ledger among the digital currency ledgers, and

wherein the transaction parties include at least one of the bank nodes and at least one of the mobile nodes.

16. The operation method of claim 15,

wherein the first digital currency ledger includes an event source ledger and a summary ledger, and

the storing transactional information in the first digital currency ledger includes:

storing, by each of the bank nodes, all of the transactional information made between the transaction parties in the event source ledger in a form of a blockchain; and

extracting some transactional information from all of the transactional information made between the transaction parties to store the extracted transactional information in the summary ledger.