WHAT IS CLAIMED IS:

1. A fraud detection method performed in a fraud detection server that collects transaction data of cryptocurrency, comprising:

generating a first data set by deriving a plurality of statistical features based on the transaction data for a specific wallet address;

performing a smart contract related to the wallet address and generating a second data set by using at least one input code included in the transaction data;

generating a third data set by using a bytecode of a contract address used in response to distributing the smart contract;

extracting first to third feature vectors with respect to the first to third data sets, respectively, by using a pre-learned deep learning module; and

inferring whether there is any fraudulent transaction for the wallet address by using the extracted first to third feature vectors, and

the extracting first to third feature vectors with respect to the first to third data sets includes:

extracting the first feature vector from the first data set, extracting the second feature vector from the second data set and extracting the third feature vector from the third data set using the pre-learned deep learning module; and

the inferring whether there is any fraudulent transaction for the wallet address by using the extracted first to third feature vectors includes:

outputting a prediction value regarding the fraudulent transaction based on the first feature vector related to the statistical feature, the second feature vector related to the input code, and the third feature vector related to the bytecode.

2. The fraud detection method of claim 1, further comprising:

performing oversampling to increase a number of data for at least one data set among the first to third data sets,

wherein the performing oversampling includes:

selecting a plurality of data included in the first to third data sets and adjacent to each other, and

generating additional data by using synthetic minority oversampling technique (SMOTE) for the plurality of selected data.

3. The fraud detection method of claim 2, wherein

the performing oversampling includes performing the oversampling on the second data set and the third data set.

4. The fraud detection method of claim 1, wherein the generating a first data set includes:

receiving a plurality of transaction data for the wallet address;

deriving different statistical features based on the plurality of transaction data; and

performing normalization so that values of the derived statistical features are distributed between 0 and 1.

5. The fraud detection method of claim 4, wherein the statistical features include:

a first statistical feature generated based on the transaction data received in the wallet address, and

a second statistical feature generated based on the transaction data transmitted from the wallet address.

6. The fraud detection method of claim 5, wherein the generating a first data set further includes replacing a missing value with a predetermined value in response to the received transaction data or the transmitted transaction data does not exist, and thereby the missing value is generated in the first statistical feature or the second statistical feature.

7. The fraud detection method of claim 1, wherein the generating a second data set includes:

receiving a plurality of transaction data for the wallet address,

extracting a plurality of input codes included in the plurality of transaction data,

concatenating the plurality of extracted input codes,

dividing the concatenated input codes into a predetermined unit, and

performing integer encoding on the divided input code.

8. The fraud detection method of claim 7, wherein the generating a second data set includes:

adding a predetermined character to a character string in response to a length of the character string for each of the integer-encoded data is shorter than a predetermined maximum character string length, and

deleting at least one part of the character string exceeding the maximum character string length from the character string in response to the length of the character string for each of the integer-encoded data is longer than the maximum character string length.

9. The fraud detection method of claim 1, wherein the generating a third data set includes:

extracting a bytecode related to the contract address,

dividing the extracted bytecode into predetermined units, and

performing integer encoding on the divided bytecode.

10. The fraud detection method of claim 9, wherein the generating a third data set includes:

adding a predetermined character to a character string in response to a length of the character string for each of the integer-encoded data is shorter than a predetermined maximum character string length, and

deleting at least one part of the character string exceeding the maximum character string length from the character string in response to the length of the character string for each of the integer-encoded data is longer than the maximum character string length.

11. The fraud detection method of claim 1, wherein the extracting first to third feature vectors includes:

applying the first data set to a pre-learned convolutional neural network,

applying maxpooling to a value that has passed through the convolutional neural network, and

applying softmax function to a value that has passed through the maxpooling.

12. The fraud detection method of claim 1, wherein the extracting first to third feature vectors includes:

applying the second data set or the third data set to a first pre-learned convolutional neural network,

applying first maxpooling to a value that has passed through the first convolutional neural network,

applying the second data set to a second pre-learned convolutional neural network,

applying second maxpooling to a value that has passed through the second convolutional neural network,

applying softmax function to a value to which the second maxpooling is applied, and

calculating an element-wise product of a first intermediate value to which the first maxpooling is applied and a second intermediate value to which the softmax function is applied.

13. The fraud detection method of claim 12, further comprising:

sequentially applying linear artificial neural network (ANN), rectified linear unit function (ReLU), and batch normalization to a result value of the element-wise product.

14. The fraud detection method of claim 12, further comprising:

sequentially applying linear artificial neural network (ANN) and leaky rectified linear unit function (Leaky ReLU) to a result value of the element-wise product.

15. The fraud detection method of claim 1, wherein the inferring whether there is any fraudulent transaction includes:

concatenating the first to third feature vectors,

performing layer normalization on the concatenated first to third feature vectors,

applying a layer normalized value to feed-forward network,

deriving an intermediate value obtained by adding a value that has passed through the feed-forward network to the concatenated first to third feature vectors, and

applying sigmoid function to the intermediate value and outputting a determination result for the fraudulent transaction.