

[0085] It can be understood that the number of the transaction-related parties may be multiple or may be one.

[0086] The preset encoding method may be any encoding method in which original data cannot be easily obtained by encoding the data, for example, a
5 hash encoding method.

[0087] The first confirmation result is used for indicating whether the transaction-related party approves the target transaction.

[0088] The signed data can be used for proving the identity, each member of the blockchain has a member ID and a pair of public and private keys, where
10 the public key is public, and the public and private key can be used for proving the identity. For example, A may sign data D using a private key to obtain a signature string S; A sends data D and signature string S to B; B performs signature verification on data D and signature string S through a public key of A, and if they match, it indicates that the data received by B really comes from A.

15 [0089] Afterwards, at step 33, the transaction data is encoded using the preset encoding method to generate second encoded data; and a second confirmation result is generated.

[0090] It can be understood that the transaction initiator and the transaction-related party have the same manner of generating encoded data;
20 theoretically, the first encoded data and the second encoded data should also be the same, and whether they are the same may be subsequently checked by the blockchain network.

[0091] The second confirmation result is used for indicating whether the transaction initiator approves the target transaction.

25 [0092] Then, at step 34, by using a private key of the transaction initiator, a second data block including the second encoded data, the second confirmation result, and an identifier of the transaction initiator is signed, so as to obtain second signed data.

[0093] The manner of the signature computation has been described
30 previously, and will not be described herein again.