CLAIMS

1. A computer-implemented method for testing signature verification for a blockchain system, comprising:

obtaining a testing configuration from a configuration file, wherein the testing configuration specifies a cryptography algorithm used in the blockchain system, a group of one or more private keys corresponding to the cryptography algorithm, and a predetermined execution result based on the cryptography algorithm and the group of one or more private keys, wherein the group of one or more private keys specified by the test configuration includes duplicative private keys, a first one of the duplicative private keys being valid, and a second one of the duplicative private keys being invalid;

signing a transaction, by encrypting data representing the transaction based on the cryptography algorithm and the group of one or more private keys, to generate one or more signed transactions;

sending the one or more signed transactions to the blockchain system and receiving an execution result from the blockchain system, the execution result indicating whether the one or more signed transactions correspond to a valid transaction or an invalid transaction; and

determining whether the predetermined execution result is satisfied based on the execution result received from the blockchain system.

2. The method of any preceding claim, wherein the cryptography algorithm used in the blockchain system comprises at least one of an RSA algorithm, an ECDSA algorithm, or an SM2 algorithm.

3. The method of any preceding claim, wherein the testing configuration includes a representation of each of the group of one or more private keys, the method further comprising:

mapping the representation of each of the group of one or more private keys to a corresponding private key; and

obtaining the corresponding private key.

4. The method of any preceding claim, further comprising:

generating a transaction; and

determining a hash value for the generated transaction as the data representing the transaction.

5. The method of any preceding claim, wherein determining whether the predetermined execution result is satisfied comprises:

comparing the execution result received from the blockchain system with the predetermined execution result to make the determination.

6. The method of any preceding claim, further comprising:

receiving the execution result based on a weight corresponding to each private key in the group of one or more private keys.

7. The method of any preceding claim, further comprising:

in response to a determination that the predetermined execution result is satisfied, displaying a testing result indicating that signature verification in the blockchain system operates properly.

8. The method of any preceding claim, further comprising:

obtaining a plurality of testing configurations from the configuration file, wherein the plurality of testing configurations specify a plurality of cryptography algorithms used in the blockchain system, a plurality of groups of one or more private keys, and a plurality of predetermined execution results; and

performing the testing in parallel based on the plurality of testing configurations.

9. A device for testing signature verification for a blockchain system, comprising:

one or more processors; and

one or more computer-readable memories coupled to the one or more processors and having instructions stored thereon that are executable by the one or more processors to perform the method of any of claims 1 to 8.

10. An apparatus for testing signature verification for a blockchain system, the apparatus comprising a plurality of modules for performing the method of any of claims 1 to 8.

11. A non-transitory computer-readable medium having stored therein instructions that, when executed by a processor of a device, cause the device to perform the method of any of claims 1 to 8.