CLAIMS

What is claimed is:

1. A method for an invocation of a smart contract, the method comprising:

receiving a target transaction used to initiate the invocation of the smart contract, wherein the target transaction comprises invocation data, and wherein at least a part of the invocation data comprises a data digest of target data stored in a third-party storage system interconnected with a blockchain;

querying the target data corresponding to the data digest from the third-party storage system;

receiving a query result from the third-party storage system, wherein the query result comprises encrypted target data and key metadata corresponding to a key used to decrypt the encrypted target data;

obtaining the key and decrypting the encrypted target data to obtain decrypted target data based on the key, wherein obtaining the key comprises querying a mapping relationship between the key and the key metadata;

performing content verification on the decrypted target data;

in response to determining that the content verification on the decrypted target data succeeds, invoking the smart contract to perform smart contract computation on the invocation data in the target transaction; and

storing a computation result in a distributed database of the blockchain after the smart contract computation is completed.

2. The method according to claim 1, wherein the third-party storage system stores an additional mapping relationship between the target data and the data digest of the target data.

3. The method according to claim 1, wherein querying the target data corresponding to the data digest from the third-party storage system comprises:

initiating a query to the third-party storage system by using the data digest as a query index, to query the target data corresponding to the data digest.

4. The method according to claim 1, wherein obtaining the key and decrypting the encrypted target data comprises:

sending the encrypted target data and the key metadata to a third-party decryption

system interconnected with the blockchain, wherein the third-party decryption system obtains the key corresponding to the key metadata based on the mapping relationship between the key and the key metadata, and decrypts the encrypted target data based on the key to provide the decrypted target data; and

receiving the decrypted target data returned by the third-party decryption system.

5. The method according to claim 1, wherein performing the content verification on the decrypted target data comprises:

computing a data digest of the target data based on a predetermined digest algorithm;

determining whether the data digest is consistent with the data digest of the target data in the target transaction; and

in response to determining that the data digest is consistent with the data digest of the target data in the target transaction, determining that the content verification on the target data succeeds.

6. The method according to claim 1, wherein the third-party storage system comprises a centralized content addressable storage (CAS) system or a distributed CAS system.

7. The method according to claim 1, wherein the blockchain is any member blockchain in a consortium blockchain that comprises several member blockchains.

8. The method according to claim 7, wherein the third-party storage system is another member blockchain that has a cross-chain data reference relationship with the blockchain in the consortium blockchain.

9. The method according to claim 7, wherein the key comprises a pair of public key and private key returned by the consortium blockchain.

10. The method according to claim 1, further comprising:

performing consensus processing on the target transaction in a transaction queue.

11. The method according to claim 10, wherein performing consensus processing is based on a consensus algorithm.

12. The method according to claim 11, wherein the consensus algorithm comprises a Practical Byzantine Fault Tolerance algorithm.

13. An apparatus for an invocation of a smart contract, the apparatus comprising a plurality of modules configured to perform the method of any one of claims 1 to 12.