

CLAIMS

What is claimed is:

1. A method for blockchain-based smart contract invocation, the method comprising:
 - receiving a target transaction used to initiate invocation of a 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;
 - performing a verification of a content on the target data by determining whether an execution condition is satisfied;
 - in response to determining that the verification on the 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 a mapping relationship between the target data and the data digest of the target data.
3. The method according to claim 2, 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 performing the verification of the content on the target data comprises:
 - computing a data digest of the target data based on a predetermined digest algorithm;
 - determining whether the computed data digest is consistent with the data digest of the target data in the target transaction; and
 - in response to determining that the computed data digest is consistent with the data digest of the target data in the target transaction, determining that the verification on the target data succeeds.

5. 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.
6. The method according to claim 1, wherein the blockchain is any member blockchain in a consortium blockchain that comprises a plurality of member blockchains.
7. The method according to claim 6, 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.
8. The method according to claim 1, wherein the third-party storage system comprises a centralized content addressable storage system, or a decentralized distributed system.
9. The method according to claim 8, wherein the third-party storage system comprises a distributed system that is deployed in the blockchain and is interconnected with each member of the blockchain according to an object storage service architecture.
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 blockchain-based smart contract invocation, the apparatus comprising a plurality of modules configured to perform the method of any one of claims 1 to 12.