

CLAIMS

1. A computer-implemented method for data storage on a blockchain performed by a computing device, the method comprising:

determining that data stored in a cache storage satisfies a predetermined condition;

adding a blockchain address of a second smart contract to a configuration file, wherein the configuration file includes a plurality of addresses corresponding to a plurality of smart contracts stored on a blockchain; and

invoking a virtual machine to execute the configuration file, wherein execution of the configuration file initiates a consensus algorithm to generate the second smart contract at the blockchain address and a corresponding smart contract pool for storing at least a portion of the data on the blockchain, and wherein the smart contract pool is a data structure to be stored on the blockchain.

2. The computer-implemented method of claim 1, wherein the data is mutable data included in a document for custom clearance, and the data includes one or more of a document type of the document, a document status of the document, association information of the document with one or more other documents for custom clearance.

3. The computer-implemented method of claim 2, wherein the document is one of an order document, a logistics document, or a payment document, and wherein the document includes the mutable data, immutable data including an encrypted version of at least a portion of content of the document encrypted by an encryption key associated with an owner of the document, and index data including one or more of an identifier of the document and hash values of a plurality of blockchain transactions associated with the document.

4. The computer-implemented method of any previous claim, wherein the predetermined condition is satisfied if a volume of the data stored in the cache storage exceeds a predetermined threshold.

5. The computer-implemented method of claim 4, wherein the blockchain includes a plurality of smart contract pools, and the method further comprising invoking an application programming interface (API) to enable a blockchain node to initiate a consensus algorithm to record at least a portion of the data exceeding the predetermined threshold to the plurality of smart contract pools in a round-robin manner.

6. The computer-implemented method of claim 4, wherein the blockchain includes a plurality of smart contract pools, and the method further comprising invoking an application programming interface (API) to enable a blockchain node to initiate a consensus algorithm to record at least a portion of the data exceeding the predetermined threshold to the plurality of smart contract pools based on an ID of the data and IDs of the plurality of the smart contract pools.

7. The computer-implemented method of any previous claim, wherein the at least a portion of data is associated with a plurality of documents for custom clearance, and the method further comprising associating a document ID of each of the plurality of documents with corresponding data in the at least a portion of data.

8. The computer-implemented method of any of claims 1 to 7, wherein the at least a portion of data is associated with a plurality of transactions associated with a document, and the method further comprising associating a hash value of each of the plurality of transactions with corresponding data in the at least a portion of data.

9. The computer-implemented method of any of claims 1 to 3, wherein the predetermined condition is satisfied if the at least a portion of the data is received at a predetermined time period different from a remainder of the data other than the at least a portion of the data.

10. The computer-implemented method of claim 9, wherein the blockchain includes a plurality of smart contract pools created during the predetermined time period, and the method further comprising invoking an API to enable a blockchain node to initiate a

consensus algorithm to record the at least a portion of the data to the plurality of smart contract pools.

11. The computer-implemented method of any previous claim, the configuration file is executed in response to restarting the computing device.

12. The computer-implemented method of any previous claim, wherein the data structure of the smart contract pool is a state Merkle tree including a plurality of key-value pairs.

13. The computer-implemented method of any previous claim, wherein the second smart contract and the corresponding smart contract pool are associated with a smart contract ID of the second smart contract, wherein the smart contract ID is stored in the second smart contract and the smart contract pool to link the second smart contract with the smart contract pool.

14. A system for blockchain data storage, 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 13.

15. An apparatus for blockchain data storage, the apparatus comprising a plurality of modules for performing the method of any of claims 1 to 13.