

CLAIMS

1. A computer-implemented method for processing data with different levels of data privacy based on blockchain technologies, the method comprising:

———receiving (1802), at a blockchain node (410, 412) in a blockchain (409) connected to an internal system (400) of a service platform,~~receiving, and~~ from a computing device associated with a user, an encryption key and data for storage on ~~a~~the blockchain, wherein the data includes public data and private data, and the encryption key encrypts the private data;

———storing (1804), by the blockchain node, the encryption key and an identifier~~(ID)~~ of the data in a cache storage dedicated to storing smart contract data for executing a smart contract;~~and~~

———generating, by the service platform, one or more zero-knowledge proofs related to values associated with the private data, wherein at least one of the one or more zero-knowledge proofs comprises a proof under a homomorphic encryption scheme, a range proof, and a zero test, wherein

i) the homomorphic encryption scheme separately encrypts the values associated with the private data such that after the homomorphic encryption scheme is performed, the encrypted values cannot be revealed without decryption,

ii) the range proof proves whether an amount is within a range without revealing the amount, and

iii) the zero test proves whether that an amount is zero;

providing, by the service platform, the one or more zero-knowledge proofs and encrypted values to the blockchain nodes of the blockchain to enable the blockchain nodes to verify the legitimacy of the private data without knowing its content, wherein the blockchain nodes of the blockchain perform a consensus algorithm to record the values on the blockchain in response to verifying that the private data is legitimate; and

in response to verifying the private data, invoking ~~an~~(1806), by the blockchain node, first application programming interface (~~API~~)of the service platform to enable ~~a~~the blockchain node to initiate a consensus algorithm to record the data and the ~~ID~~identifier of the data on ~~a~~the blockchain.

2. The computer-implemented method of claim 1, wherein the encryption key is a symmetric key and the private data is in cyphertext encrypted using the symmetric key.

3. The computer-implemented method of claim 1, wherein the private data is in plaintext and the encryption key is a symmetric key, and the method further comprises encrypting, by the internal system, the private data using the symmetric key before ~~invoking~~ the first application programming interface—is invoked.

4. The computer-implemented method of claim 3~~any previous claim~~, wherein the method further comprises:

——receiving, by the internal system and from the computing device associated with the user, a list of one or more other users permitted to access the plaintext of the private data;

——encrypting, by the internal system, the encryption key by using each of public keys of the one or more other users to generate encrypted encryption keys; and

——storing, by the internal system, the encrypted encryption keys in the cache storage.

5. The computer-implemented method of any of claims 1 to 3, wherein the user is a first user, the encryption key is a symmetric key encrypted by a public key of a second user, and the private data is encrypted by the symmetric key.

6. The computer-implemented method of claim 5, wherein the method further ~~comprising~~:

——~~providing an API~~comprises:

providing, by the internal system, a second application programming interface to enable the first user or the second user to:

retrieve the encryption key from the cache storage and the private data from the blockchain;

retrieve the symmetric key by decrypting the encryption key by using a private key corresponding to the public key; and

decrypt the private data by using the symmetric key.

7. The computer-implemented method of claim 6, wherein the public data is recorded on the blockchain and wherein the method further ~~comprising~~ comprises:

storing the private data in the cache storage;

providing an APIapplication programming interface to enable the first user or the second user to retrieve the public data from the blockchain and the private data from the cache storage based on the IDidentifier of the data to recover the data~~-, optionally wherein the identifier of the data is a hash value of the data or an identifier of a document associated with the data.~~

~~8. The computer implemented method of claim 7, wherein the ID of the data is a hash value of the data or an ID of a document associated with the data.~~

~~89.~~ The computer-implemented method of claim 7 ~~or 8~~, wherein the APIsecond application programming interface further enables the first user to record an updated version of the data associated with the IDidentifier of the data on the blockchain, and disables the second user to record the updated version of the data associated with the IDidentifier of the data on the blockchain.

~~109.~~ The computer-implemented method of any previous claim, wherein the data is associated with a purchase order and includes one or more of order data, logistics data, and payment data.

~~110.~~ The computer-implemented method of any previous claim, wherein the encryption key is derived based on a linear secret sharing scheme through negotiations among at least two of (i) a custom clearance agent platform managed by at least one custom clearance agent or broker who represents importers in preparing and submitting information related to custom clearance to ~~the~~ customs authority, (ii) a service platform, or (iii) the customs authority.

~~1211.~~ The computer-implemented method of any previous claim, wherein the consensus algorithm is one of proof of work ~~(PoW)~~, proof of stake ~~(PoW)~~, or practical Byzantine fault tolerance ~~(PBFT)~~.

~~1312.~~ The computer-implemented method of any previous claim, wherein an address of the smart contract is stored on the blockchain in a database storage.

~~14. The computer implemented method of any previous claim, wherein the method further comprising generating one or more zero knowledge proofs (ZKPs) related to one or more values associated with the private data.~~

~~15. The computer implemented method of claim 13, wherein the data includes at least one of order data or payment data, and the ZKPs are related to one or more values associated with at least one of the order data or the payment data.~~

~~16. The computer implemented method of claim 13 or 14, wherein at least one of the one or more ZKPs is generated based on homomorphic encryption and is at least one of a range proof or a zero test, and wherein the consensus algorithm is performed after the one or more ZKPs are verified.~~

~~17~~13. A system for managing user authorizations, 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 ~~12~~16.

~~18. An apparatus for managing user authorizations, the apparatus comprising a plurality of modules for performing the method of any of claims 1 to 16.~~