

CLAIMS

What is claimed is:

1. A computer-implemented method for retrieving data from a data source that is external to a blockchain network, the method comprising:

receiving, by a relay system smart contract executing within the blockchain network, a request for data from the data source, the request comprising a first portion and a second portion, the first portion comprising plaintext data and the second portion comprising encrypted data, the encrypted data comprising access data and a first hash value that are encrypted using a public key of a relay system component, the first hash value being generated as a hash of the plaintext data by a user computing device that submits the request;

transmitting, by the relay system smart contract, the request to the relay system component external to the blockchain network, wherein, in response to receiving the request, the relay system component:

decrypts the encrypted data using a private key of the relay system component to provide the first hash value,

calculates a second hash value based on the plaintext data included in the request,

compares the first hash value to the second hash value to determine that the first hash value is identical to the second hash value, and

transmits a result responsive to determining that the first hash value is identical to the second hash value;

receiving, by the relay system smart contract, the result from the relay system component, the result comprising result data and a third hash value, the result data being retrieved using the access data and the third hash value being generated based on the result data and digitally signed using the private key of the relay system component;

verifying, by the relay system smart contract, an integrity of the result based on the public key of the relay system component, a digital signature of the result and the third hash value; and

in response to verifying the integrity of the result, transmitting the result to the user computing device.

2. The method of any preceding claim 1, wherein the relay system component transmits a query request to the data source in response to verifying the request.
3. The method of any preceding claim, wherein the relay system component comprises a relay system node that receives the request from a relay system controller.
4. The method of any preceding claim, wherein the plaintext data comprises a uniform resource locator (URL) of the data source.
5. The method of any preceding claim, wherein the relay system component executes a trusted execution environment (TEE), and the private key and the public key of the relay system component are provisioned during an attestation process of the TEE.
6. The method of claim 5, wherein the relay system controller executes the attestation process with the relay system node and an attestation service.
7. The method of any preceding claim, wherein the data source comprises an Internet-based data source.
8. An apparatus for retrieving data from a data source that is external to a blockchain network, the apparatus comprising a plurality of modules for performing the method of any of claims 1 to 7.
9. A system for retrieving data from a data source that is external to a blockchain network, 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 7.