CLAIMS

What is claimed is:

1. A data read authority control system (100), comprising:

a block chain system (180);

a data owner device (110) arranged to operably receive data inputted by a target user to generate a target data, and to operably utilize a proof key to generate a proof;

a data source system (150) arranged to operably store a sensitive data corresponding to the target data, and to operably establish a zero-knowledge proof smart contract on the block chain system (180) according to a predetermined verification rule;

a data service system (160) arranged to operably receive the target data and the proof generated by the data owner device (110), and to operably request the block chain system (180) to verify the proof;

a data requester device (130) arranged to operably generate and transmit a sensitive data request corresponding to the target data to the data service system (160);

wherein the block chain system (180) is arranged to operably execute a token management smart contract to generate and transfer an authorization token to the data owner device (110);

wherein the data owner device (110) is further arranged to operably utilize the authorization token to transmit an encrypted data authorization policy to the block chain system (180), and the block chain system (180) is further arranged to operably record the encrypted data authorization policy in an authorization policy smart contract;

wherein the block chain system (180) is further arranged to operably execute the zero-knowledge proof smart contract to utilize a verification key to verify correctness of the proof, and to operably transmit a verification success notification to the data service system (160) when the proof is determined as correct;

wherein the data service system (160) is further arranged to operably transmit a read token request comprising an authorization token identification data corresponding to the authorization token to the block chain system (180) after receiving the sensitive data request transmitted from the data requester device (130);

wherein the block chain system (180) is further arranged to operably execute the authorization policy smart contract to decrypt the encrypted data authorization policy to inspect whether the read token request matches a predetermined authorization policy

configured by the target user, and to operably verify an activity of the authorization token corresponding to the authorization token identification data;

wherein the block chain system (180) is further arranged to operably generate and transfer a read token to the data service system (160) only if the block chain system (180) determines that the read token request matches the predetermined authorization policy and that the authorization token is active;

wherein the data service system (160) is further arranged to operably transmit the sensitive data request to the data source system (150) and transfer the read token to the data source system (150) after acquiring the read token;

wherein the data source system (150) is further arranged to operably transfer the read token to the block chain system (180) to request the block chain system (180) to verify an activity of the read token;

wherein if the block chain system (180) determines that the read token transferred from the data source system (150) is active, the data source system (150) operably transmits the sensitive data corresponding to the target data to the data service system (160), and the data service system (160) operably transmits the sensitive data to the data requester device (130).

2. The data read authority control system (100) of claim 1, wherein the proof key utilized by the data owner device (110) and the verification key utilized by the block chain system (180) are both provided by the data source system (150).

3. The data read authority control system (100) of claim 1, wherein the data owner device (110) is further arranged to operably request the target user to input one or more data to be verified, and to operably utilize the proof key to generate the proof based on the one or more data to be verified.

4. The data read authority control system (100) of claim 1, wherein the data service system (160) is further arranged to operably generate and transmit a data read request corresponding to a target requester to the data owner device (110) after receiving the sensitive data request transmitted from the data requester device (130), and the data service system (160) transmits the authorization token identification data to the block chain system (180) only if the data read request is accepted by the target user.

5. The data read authority control system (100) of claim 4, wherein the data owner device (110) is further arranged to operably inquire the target user whether to accept the data read request, and to operably transmit the authorization token identification data to the data service system (160) if the data read request is accepted by the target user.

6. The data read authority control system (100) of claim 1,

wherein the block chain system (180) is further arranged to operably verify the activity of the read token after acquiring the read token, and to operably generate and transmit a verification success notice to the data source system (150) when determining the read token as active;

wherein the data source system (150) is further arranged to operably transmit the sensitive data corresponding to the target data to the data service system (160) after receiving the verification success notice.

7. The data read authority control system (100) of claim 6, wherein the block chain system (180) is further arranged to operably set a corresponding expiration period for the read token when generating the read token;

wherein when the block chain system (180) verifies the activity of the read token, the block chain system (180) inspects whether the read token is transferred by the data service system (160) to the data source system (150) before the read token is transferred to the block chain system (180), and the block chain system (180) further inspects whether a time point at which the data source system (150) transfers the read token to the block chain system (180) has exceeded the expiration period or not.

8. The data read authority control system (100) of claim 6, wherein the block chain system (180) is further arranged to operably records an acquisition time of the read token or a verification time of the read token.

9. A data service system (160) of a data read authority control system (100), wherein the data read authority control system (100) comprises a data owner device (110), a data requester device (130), a data source system (150), and a block chain system (180), the data service system (160) comprising:

a communication circuit (161) arranged to operably receive a target data and a proof transmitted from the data owner device (110), and to operably receive a sensitive data request corresponding to the target data transmitted from the data requester device (130);

a block chain computing circuit (163) arranged to operably act as one node of the block chain system (180), and arranged to operably request the block chain system (180) to verify the proof, wherein the block chain system (180) executes a zero-knowledge proof smart contract established by the data source system (150) to utilize a verification key to verify correctness of the proof;

a database (165) arranged to operably store the target data and

a web server (167), coupled with the communication circuit (161), the block chain computing circuit (163), and the database (165), and arranged to operably transmit a read token request comprising an authorization token identification data to the block chain system (180) after the sensitive data request is received, and to operably acquire a read token transferred from the block chain system (180) through the communication circuit (161) or the block chain computing circuit (163) only if the block chain system (180) determines both that the read token request matches a predetermined authorization policy recorded in an authorization policy smart contract and that an authorization token corresponding to the authorization token identification data is active;

wherein the communication circuit (161) is further arranged to operably receive a verification success notification transmitted from the block chain system (180) when the proof is determined as correct by the block chain system (180);

wherein the web server (167) is further arranged to operably transmit the sensitive data request to the data source system (150) through the communication circuit (161) after acquiring the read token, and to operably transfer the read token to the data source system (150) through the communication circuit (161) or the block chain computing circuit (163);

wherein if the block chain system (180) determines that the read token transferred from the data service system (160) to the data source system (150) is active, the web server (167) operably receives a sensitive data corresponding to the target data transmitted from the data source system (150) through the communication circuit (161), and operably transmits the sensitive data to the data requester device (130) to the communication circuit (161).

10. The data service system (160) of claim 9, wherein the web server (167) is further arranged to operably generate a data read request corresponding to a target requester and transmit the data read request to the data owner device (110) through the communication circuit (161) after the sensitive data request transmitted from the data requester device (130) is received by the communication circuit (161), and the web server (167) transmits the authorization token identification data to the block chain system (180) through the communication circuit (161) or the block chain computing circuit (163) only if the data read request is accepted by the target user.

11. The data service system (160) of claim 10, wherein the data owner device (110) further inquires the target user whether to accept the data read request, and the communication circuit (161) receives the authorization token identification data transmitted from the data owner device (110) only if the data read request is accepted by the target user.

12. The data service system (160) of claim 9, wherein the data source system (150) is further arranged to operably transfer the read token to the block chain system (180) after acquiring the read token;

wherein the block chain system (180) is further arranged to operably verify an activity of the read token after acquiring the read token, and to operably generate and transmit a verification success notice to the data source system (150) when determining the read token as active;

wherein after the verification success notice is received by the data source system (150), the communication circuit (161) receives the sensitive data corresponding to the target data transmitted from the data source system (150).