WHAT IS CLAIMED IS:

1. A system comprising:

at least one processor programmed or configured to:

provision a client device for access to an online source of information;

transmit a private encryption key of a public/private encryption key pair to a software agent of the client device;

receive a first hash value from the software agent of the client device, wherein the first hash value is generated using the private encryption key;

receive a second hash value from the software agent of the client device;

determine whether to allow access to the online source of information by the software agent based on the first hash value and the second hash value received from the software agent of the client device;

process a request to access the online source of information involving the software agent of the client device, wherein, when processing the request to access the online source of information, the at least one processor is programmed or configured to:

allow the software agent to conduct a data transaction involving the online source of information based on determining to allow access to the online source of information by the software agent of the client device; and

store a data record associated with the data transaction involving the online source of information in a data structure.

2. The system of claim 1, wherein, when storing the data record associated with the data transaction involving the online source of information in the data structure, the at least one processor is programmed or configured to:

store the data record associated with the data transaction involving the online source of information in a distributed ledger.

3. The system of claim 1, wherein the at least one processor is further programmed or configured to:

store the first hash value with an identifier of the software agent of the client device in the data structure; and

wherein, when determining whether to allow access to the online source of information by the software agent of the client device, the at least one processor is programmed or configured to:

retrieve the first hash value from the data structure based on the identifier of the software agent of the client device;

compare the second hash value received from the software agent to the first hash value retrieved from the data structure; and

determine to allow access to the online source of information by the software agent of the client device based on determining that the second hash value received from the software agent corresponds to the first hash value retrieved from the data structure.

4. The system of claim 1, wherein, when receiving the second hash value from the software agent of the client device, the at least one processor is programmed or configured to:

receive the request to access the online source of information from the software agent, wherein the request to access the online source of information includes the second hash value and data associated with the software agent of the client device.

5. The system of claim 4, wherein, when determining whether to allow access to the online source of information by the software agent of the client device, the at least one processor is programmed or configured to:

determine whether to allow access to the online source of information by the software agent of the client device based on the first hash value, the second hash value and data associated with the software agent of the client device included in the request to access the online source of information; and

wherein, when processing the request to access the online source of information involving the software agent of the client device, the at least one processor is programmed or configured to:

allow the software agent to conduct the data transaction involving a specific type of data included in the online source of information based on the data associated with the software agent of the client device.

6. The system of claim 1, wherein, when receiving the second hash value from the software agent of the client device, the at least one processor is programmed or configured to:

receive the request to access sensitive data included in the online source of information from the software agent, wherein the request to access sensitive data included in the online source of information includes the second hash value.

7. The system of claim 6, wherein the at least one processor is further programmed or configured to:

transmit a challenge question to the software agent of the client device; and

receive a response to the challenge question from the software agent of the client device;

wherein, when determining whether to allow access to the online source of information by the software agent of the client device, the at least one processor is programmed or configured to:

determine whether to allow access to the sensitive data included in the online source of information by the software agent of the client device based on the first hash value, the second hash value, and the response to the challenge question from the software agent of the client device.

8. The system of claim 1, wherein the at least one processor is further programmed or configured to:

receive an initialization access request from the client device, wherein the initialization access request is a request for authorization to access the online source of information by the software agent of the client device; and

wherein, when transmitting the private encryption key of the public/private encryption key pair to the software agent of the client device, the at least one processor is programmed or configured to:

transmit the private encryption key of the public/private encryption key pair to the software agent of the client device based on receiving the initialization access request from the client device.

9. A computer-implemented method, comprising:

provisioning, with at least one processor, a client device for access to an online source of information;

transmitting, with at least one processor, a private encryption key of a public/private encryption key pair to a software agent of the client device;

receiving, with at least one processor, a first hash value from the software agent of the client device, wherein the first hash value is generated using the private encryption key;

receiving, with at least one processor, a second hash value from the software agent of the client device;

determining, with at least one processor, to allow access to the online source of information by the software agent based on the first hash value and the second hash value received from the software agent of the client device;

processing, with at least one processor, a request to access the online source of information involving the software agent of the client device, wherein processing the request to access the online source of information comprises:

allowing the software agent to conduct a data transaction involving the online source of information based on determining to allow access to the online source of information by the software agent of the client device; and

storing, with at least one processor, a data record associated with the data transaction involving the online source of information in a data structure.

10. The method of claim 9, wherein storing the data record associated with the data transaction involving the online source of information in the data structure comprises:

storing the data record associated with the data transaction involving the online source of information in a distributed ledger.

11. The method of claim 9, further comprising:

storing the first hash value with an identifier of the software agent of the client device in a data structure,

wherein determining to allow access to the online source of information by the software agent of the client device comprises:

retrieving the first hash value from the data structure based on the identifier of the software agent of the client device;

comparing the second hash value received from the software agent to the first hash value retrieved from the data structure; and

determining to allow access to the online source of information by the software agent of the client device based on determining that the second hash value received from the software agent corresponds to the first hash value retrieved from the data structure.

12. The method of claim 9, wherein receiving the second hash value from the software agent comprises:

receiving a request to access the online source of information from the software agent, wherein the request to access the online source of information includes the second hash value and data associated with the software agent of the client device.

13. The method of claim 12, further comprising:

wherein determining to allow access to the online source of information by the software agent of the client device comprises:

determining to allow access to the online source of information by the software agent of the client device based on the first hash value, the second hash value, and data associated with the software agent of the client device included in the request to access the online source of information; and

wherein processing the request to access the online source of information involving the software agent of the client device comprises:

allowing the software agent to conduct the data transaction involving a specific type of data included in the online source of information based on the data associated with the software agent of the client device.

14. The method of claim 9, further comprising:

transmitting a challenge question to the software agent of the client device; and

receiving a response to the challenge question from the software agent of the client device;

wherein determining to allow access to the online source of information by the software agent of the client device comprises:

determining to allow access to sensitive data included in the online source of information by the software agent of the client device based on the first hash value, the second hash value, and the response to the challenge question from the software agent of the client device.

15. The method of claim 9, further comprising:

receiving an initialization access request from the client device, wherein the initialization access request is a request for authorization to access to the online source of information by the software agent of the client device; and

wherein transmitting the private encryption key of the public/private encryption key pair to the software agent of the client device comprises:

transmitting the private encryption key of the public/private encryption key pair to the software agent of the client device based on receiving the initialization access request from the client device.

16. A computer program product, the computer program product comprising at least one non-transitory computer-readable medium including one or more instructions that, when executed by at least one processor, cause the at least one processor to:

provision a client device for access to an online source of information;

transmit a private encryption key of a public/private encryption key pair to a software agent of the client device;

receive a first hash value from the software agent of the client device, wherein the first hash value is generated using the private encryption key;

receive a second hash value from the software agent of the client device;

determine whether to allow access to the online source of information by the software agent based on the first hash value and the second hash value received from the software agent of the client device;

process a request to access the online source of information involving the software agent of the client device, wherein, when processing the request to access the online source of information, the at least one processor is programmed or configured to:

allow the software agent to conduct a data transaction involving the online source of information based on determining to allow access to the online source of information by the software agent of the client device; and

store a data record associated with the data transaction involving the online source of information in a distributed ledger.

17. The computer program product of claim 16, wherein the one or more instructions that cause the at least one processor to receive the second hash value from the software agent of the client device, cause the at least one processor to:

receive a request to access the online source of information from the software agent, wherein the request to access the online source of information includes the second hash value and data associated with the software agent of the client device.

18. The computer program product of claim 17, wherein, the one or more instructions that cause the at least one processor to determine whether to allow access to the online source of information by the software agent of the client device, cause the at least one processor to:

determine whether to allow access to the online source of information by the software agent of the client device based on the first hash value, the second hash value, and data associated with the software agent of the client device included in the request to access the online source of information; and

wherein, the one or more instructions that cause the at least one processor to process the request to access the online source of information involving the software agent of the client device, cause the at least one processor to:

allow the software agent to conduct the data transaction involving a specific type of data included in the online source of information based on the data associated with the software agent of the client device.

~~19. The computer program product of claim 16, wherein, the one or more instructions that cause the at least one processor to receive the second hash value from the software agent of the client device, cause the at least one processor to:~~

~~receive a request to access sensitive data included in the online source of information from the software agent, wherein the request to access sensitive data included in the online source of information includes the second hash value.~~

~~20. The computer program product of claim 19, wherein the at least one processor is further programmed or configured to:~~

~~transmit a challenge question to the software agent of the client device; and~~

~~receive a response to the challenge question from the software agent of the client device;~~

~~wherein, the one or more instructions that cause the at least one processor to determine whether to allow access to the online source of information by the software agent of the client device, cause the at least one processor to:~~

~~determine whether to allow access to the sensitive data included in the online source of information by the software agent of the client device based on the first hash value, the second hash value, and the response to the challenge question from the software agent of the client device.~~

1. A system comprising:

at least one processor programmed or configured to:

receive, from a client device, an initialization access request for access to an online source of information by an automated software agent of the client device;

generate software agent credential data associated with access credentials to the online source of information based on receiving the initialization access request, wherein the software agent credential data associated with access credentials to the online source of information comprises a private encryption key of a public/private encryption key pair,

wherein the private encryption key is assigned to the automated software agent of the client device;

transmit the private encryption key of the public/private encryption key pair to the automated software agent of the client device;

receive a first hash value from the automated software agent of the client device, wherein the first hash value is generated by the client device using the private encryption key;

store the first hash value in a database as a hash value assigned to the automated software agent of the client device;

process a request to access the online source of information involving the automated software agent of the client device, wherein, when processing the request to access the online source of information, the at least one processor is programmed or configured to:

receive a second hash value from the automated software agent of the client device and data associated with a role of the automated software agent included in the request to access the online source of information, wherein the second hash value is generated by the client device using the private encryption key;

determine whether to allow access to the online source of information by the automated software agent based on the hash value assigned to the automated software agent of the client device and the second hash value received from the automated software agent of the client device, wherein, when determining whether to allow access to the online source of information, the at least one processor is programmed or configured to:

determine whether the second hash value received from the automated software agent of the client device corresponds to the hash value assigned to the automated software agent of the client device;

determine a specific type of data included in the online source of information on which the automated software agent is to carry out an operation based on the data associated with a role of the automated software agent;

allow the automated software agent to conduct a data transaction involving the specific type of data included in the online source of information based on determining to allow access to the online source of information by the automated software agent of the client device; and

store a data record associated with the data transaction involving the online source of information in a data structure.

2. The system of claim 1, wherein, when storing the data record associated with the data transaction involving the online source of information in the data structure, the at least one processor is programmed or configured to:

store the data record associated with the data transaction involving the online source of information in a distributed ledger.

3. The system of claim 1, wherein, when determining whether to allow access to the online source of information by the automated software agent of the client device, the at least one processor is programmed or configured to:

retrieve the first hash value from the data structure based on an identifier of the automated software agent of the client device;

compare the second hash value received from the automated software agent to the first hash value retrieved from the data structure; and

determine to allow access to the online source of information by the automated software agent of the client device based on determining that the second hash value received from the automated software agent corresponds to the first hash value retrieved from the data structure.

4. The system of claim 1, wherein, when receiving the second hash value from the automated software agent of the client device, the at least one processor is programmed or configured to:

receive the request to access the online source of information from the automated software agent, wherein the request to access the online source of information includes the second hash value and the data associated with a role of the automated software agent of the client device.

5. The system of claim 1, wherein the at least one processor is further programmed or configured to:

transmit a challenge question to the automated software agent of the client device; and

receive a response to the challenge question from the automated software agent of the client device;

wherein, when determining whether to allow access to the online source of information by the automated software agent of the client device, the at least one processor is programmed or configured to:

determine whether to allow access to the data included in the online source of information by the automated software agent of the client device based on the first hash value, the second hash value, and the response to the challenge question from the automated software agent of the client device.

6. A computer-implemented method, comprising:

receiving, with at least one processor and from a client device, an initialization access request for access to an online source of information by an automated software agent of the client device;

generating, with at least one processor, software agent credential data associated with access credentials to the online source of information based on receiving the initialization access request, wherein the software agent credential data associated with access credentials to the online source of information comprises a private encryption key of a public/private encryption key pair, wherein the private encryption key is assigned to the automated software agent of the client device;

transmitting, with at least one processor, a private encryption key of a public/private encryption key pair to an automated software agent of the client device;

receiving, with at least one processor, a first hash value from the automated software agent of the client device, wherein the first hash value is generated by the client device using the private encryption key;

storing, with at least one processor, the first hash value in a database as a hash value assigned to the automated software agent of the client device;

processing, with at least one processor, a request to access the online source of information involving the automated software agent of the client device, wherein processing the request to access the online source of information comprises:

receiving a second hash value from the automated software agent of the client device and data associated with a role of the automated software agent included in the request to access the online source of information, wherein the second hash value is generated by the client device using the private encryption key;

determining whether to allow access to the online source of information by the automated software agent based on the hash value assigned to the automated software agent of the client device and the second hash value received from the automated software agent of the client device, wherein determining whether to allow access to the online source of information comprises:

determining whether the second hash value received from the automated software agent of the client device corresponds to the hash value assigned to the automated software agent of the client device;

determining a specific type of data included in the online source of information on which the automated software agent is to carry out an operation based on the data associated with a role of the automated software agent;

allowing the automated software agent to conduct a data transaction involving the specific type of data included in the online source of information based on determining to allow access to the online source of information by the automated software agent of the client device; and

storing, with at least one processor, a data record associated with the data transaction involving the online source of information in a data structure.

7. The method of claim 6, wherein storing the data record associated with the data transaction involving the online source of information in the data structure comprises:

storing the data record associated with the data transaction involving the online source of information in a distributed ledger.

8. The method of claim 6, wherein determining to allow access to the online source of information by the automated software agent of the client device comprises:

retrieving the first hash value from the data structure based on an identifier of the automated software agent of the client device;

comparing the second hash value received from the automated software agent to the first hash value retrieved from the data structure; and

determining to allow access to the online source of information by the automated software agent of the client device based on determining that the second hash value received from the automated software agent corresponds to the first hash value retrieved from the data structure.

9. The method of claim 6, wherein receiving the second hash value from the automated software agent comprises:

receiving the request to access the online source of information from the automated software agent, wherein the request to access the online source of information includes the second hash value and the data associated with a role of the automated software agent of the client device.

10. The method of claim 6, further comprising:

transmitting a challenge question to the automated software agent of the client device; and

receiving a response to the challenge question from the automated software agent of the client device;

wherein determining to allow access to the online source of information by the automated software agent of the client device comprises:

determining to allow access to sensitive data included in the online source of information by the automated software agent of the client device based on the first hash value, the second hash value, and the response to the challenge question from the automated software agent of the client device.

11. A computer program product, the computer program product comprising at least one non-transitory computer-readable medium including one or more instructions that, when executed by at least one processor, cause the at least one processor to:

receive, from a client device, an initialization access request for access to an online source of information by an automated software agent of the client device;

generate software agent credential data associated with access credentials to the online source of information based on receiving the initialization access request, wherein the software agent credential data associated with access credentials to the online source of information comprises a private encryption key of a public/private encryption key pair, wherein the private encryption key is assigned to the automated software agent of the client device;

transmit the private encryption key of the public/private encryption key pair to the automated software agent of the client device;

receive a first hash value from the automated software agent of the client device, wherein the first hash value is generated using the private encryption key;

receive a second hash value from the automated software agent of the client device;

determine whether to allow access to the online source of information by the automated software agent based on the first hash value and the second hash value received from the automated software agent of the client device;

process a request to access the online source of information involving the automated software agent of the client device, wherein, when processing the request to access the online source of information, the at least one processor is programmed or configured to:

receive a second hash value from the automated software agent of the client device and data associated with a role of the automated software agent included in the request to access the online source of information, wherein the second hash value is generated by the client device using the private encryption key;

determine whether to allow access to the online source of information by the automated software agent based on the hash value assigned to the automated software agent of the client device and the second hash value received from the automated software agent of the

client device, wherein, when determining whether to allow access to the online source of information, the at least one processor is programmed or configured to:

determine whether the second hash value received from the automated software agent of the client device corresponds to the hash value assigned to the automated software agent of the client device;

determine a specific type of data included in the online source of information on which the automated software agent is to carry out an operation based on the data associated with a role of the automated software agent;

allow the automated software agent to conduct a data transaction involving the specific type of data included in the online source of information based on determining to allow access to the online source of information by the automated software agent of the client device; and

store a data record associated with the data transaction involving the online source of information in a distributed ledger.

12. The computer program product of claim 11, wherein the one or more instructions that cause the at least one processor to receive the second hash value from the automated software agent of the client device, cause the at least one processor to:

receive the request to access the online source of information from the automated software agent, wherein the request to access the online source of information includes the second hash value and data associated with a role of the automated software agent of the client device.

13. The computer program product of claim 11, wherein the at least one processor is further programmed or configured to:

transmit a challenge question to the automated software agent of the client device; and

receive a response to the challenge question from the automated software agent of the client device;

wherein, the one or more instructions that cause the at least one processor to determine whether to allow access to the online source of information by the automated software agent of the client device, cause the at least one processor to:

determine whether to allow access to the data included in the online source of information by the automated software agent of the client device based on the first hash value, the second hash value, and the response to the challenge question from the automated software agent of the client device.