SUMMARY

The present disclosure provides a description of systems and methods for validating receipt of hashed data.

According to an aspect of the present disclosure, there is provided a method for validating receipt of hashed data, comprising: storing, in a memory of a processing server, an acceptance frame and at least one hashing algorithm; receiving, by a receiving device of the processing server, a data value; hashing, by a hashing module of the processing server, the received data value using the at least one hashing algorithm to obtain a first hashed package; hashing, by the hashing module of the processing server, the received data value and the acceptance frame using the at least one hashing algorithm to obtain a second hashed package; electronically transmitting, by a transmitting device of the processing server, the first hashed package to a computing device; receiving, by the receiving device of the processing server, a received hashed package from the computing device; and validating, by a validation module of the processing server, the received hashed package as being created using the received data value and acceptance frame via comparison of the received hashed package to the second hashed package.

According to an aspect of the present disclosure, there is provided a system for validating receipt of hashed data, comprising: a validation module of a processing server; a memory of the processing server configured to store an acceptance frame and at least one hashing algorithm; a receiving device of the processing server configured to receive a data value; a hashing module of the processing server configured to hash the received data value using the at least one hashing algorithm to obtain a first hashed package, and hash the received data value and the acceptance frame using the at least one hashing algorithm to obtain a second hashed package; and a transmitting device of the processing server configured to electronically receive the first hashed package to a computing device, wherein the receiving device of the processing server is further configured to receive a received hashed package from the computing device, and the validation module of the processing server is configured to validate the received hashed package as being created using the received data value and acceptance frame via comparison of the received hashed package to the second hashed package.

WHAT IS CLAIMED IS:

1. A method for validating receipt of hashed data, comprising:

storing, in a memory of a processing server, an acceptance frame and at least one hashing algorithm;

receiving, by a receiving device of the processing server, a data value;

hashing, by a hashing module of the processing server, the received data value using the at least one hashing algorithm to obtain a first hashed package;

hashing, by the hashing module of the processing server, the received data value and the acceptance frame using the at least one hashing algorithm to obtain a second hashed package;

electronically transmitting, by a transmitting device of the processing server, the first hashed package to a computing device;

receiving, by the receiving device of the processing server, a received hashed package from the computing device; and

validating, by a validation module of the processing server, the received hashed package as being created using the received data value and acceptance frame via comparison of the received hashed package to the second hashed package.

2. The method of claim 1, further comprising:

storing, in the memory of the processing server, a subsequent frame;

receiving, by the receiving device of the processing server, a second received hashed package from the computing device;

hashing, by the hashing module of the processing server, the subsequent frame and additional data using the at least one hashing algorithm to obtain a third hashed package; and

validating, by the validation module of the processing server, the second received hashed package as being created using the subsequent frame and additional data via comparison of the second received hashed package to the third hashed package.

3. The method of claim 2, wherein the additional data is one of: (i) the second hashed package, and (ii) the returned data value and the returned acceptance frame.

4. The method of claim 1, wherein

the at least one hashing algorithm includes a first hashing algorithm and a second hashing algorithm,

the first hashed package is obtained using the first hashing algorithm, and

the second hashed package is obtained using the second hashing algorithm.

5. The method of claim 1, further comprising:

electronically transmitting, by the transmitting device of the processing server, the second hashed package to a blockchain network for inclusion in an associated blockchain.

6. The method of claim 1, wherein the data value is received from an input device interfaced with the processing server.

7. The method of claim 1, further comprising:

generating, by a generation module of the processing server, a transaction message formatted based on one or more standards, wherein the transaction message includes a tertiary bitmap and includes a plurality of data elements including at least a data element configured to store the first hashed package, wherein

electronically transmitting the first hashed package includes electronically transmitting the generated transaction message.

8. The method of claim 7, wherein the generated transaction message is electronically transmitted to the computing device via a payment network.

9. The method of claim 1, wherein receiving the second hashed package includes receiving a transaction message formatted based on one or more standards, wherein the transaction message includes a tertiary bitmap and includes a plurality of data elements including at least a data element configured to store the second hashed package.

10. The method of claim 9, wherein the transaction message is received from a payment network configured to route the transaction message from the computing device.

11. A system for validating receipt of hashed data, comprising:

a validation module of a processing server;

a memory of the processing server configured to store an acceptance frame and at least one hashing algorithm;

a receiving device of the processing server configured to receive a data value;

a hashing module of the processing server configured to

hash the received data value using the at least one hashing algorithm to obtain a first hashed package, and

hash the received data value and the acceptance frame using the at least one hashing algorithm to obtain a second hashed package; and

a transmitting device of the processing server configured to electronically receive the first hashed package to a computing device, wherein

the receiving device of the processing server is further configured to receive a received hashed package from the computing device, and

the validation module of the processing server is configured to validate the received hashed package as being created using the received data value and acceptance frame via comparison of the received hashed package to the second hashed package.

12. The system of claim 11, wherein

the memory of the processing server is further configured to store a subsequent frame,

the receiving device of the processing server is further configured to receive a second received hashed package from the computing device,

the hashing module of the processing server is further configured to hash the subsequent frame and additional data using the at least one hashing algorithm to obtain a third hashed package, and

the validation module of the processing server is further configured to validate the second received hashed package as being created using the subsequent frame and additional data via comparison of the second received hashed package to the third hashed package.

13. The system of claim 12, wherein the additional data is one of: (i) the second hashed package, and (ii) the returned data value and the returned acceptance frame.

14. The system of claim 11, wherein

the at least one hashing algorithm includes a first hashing algorithm and a second hashing algorithm,

the first hashed package is obtained using the first hashing algorithm, and

the second hashed package is obtained using the second hashing algorithm.

15. The system of claim 11, wherein the transmitting device of the processing server is further configured to electronically transmit the second hashed package to a blockchain network for inclusion in an associated blockchain.

16. The system of claim 11, wherein the data value is received from an input device interfaced with the processing server.

17. The system of claim 11, further comprising:

a generation module of the processing server configured to generate a transaction message formatted based on one or more standards, wherein the transaction message includes a tertiary bitmap and includes a plurality of data elements including at least a data element configured to store the first hashed package, wherein

electronically transmitting the first hashed package includes electronically transmitting the generated transaction message.

18. The system of claim 17, wherein the generated transaction message is electronically transmitted to the computing device via a payment network.

19. The system of claim 11, wherein receiving the second hashed package includes receiving a transaction message formatted based on one or more standards, wherein the transaction message includes a tertiary bitmap and includes a plurality of data elements including at least a data element configured to store the second hashed package.

20. The system of claim 19, wherein the transaction message is received from a payment network configured to route the transaction message from the computing device.