CLAIMS

What is claimed is:

1. A method for providing anonymous validation of an anonymous query among a plurality of nodes in a network, the method comprising:

calculating a fingerprint of at least one data point of information of a requester node to be validated in the query by applying a first layer of encoding,

receiving at a first server a query from the requester node in the network, for validation of the query by at least one other node of the plurality of nodes;

wherein the query comprises a second layer encoded representation of the fingerprint; and

wherein the second layer encoded representation is divided into a first set of multiple shares;

receiving at the first server, from at least one validator node of the plurality of nodes, an encoded representation of at least one data point of information of the validator node;

wherein the encoded representation from the at least one validator node is divided into a second set of multiple shares;

comparing by a plurality of support servers the first set of multiple shares from the requestor node with the second set of multiple shares of the at least one validator node;

determining by a second server, based on the comparison, whether or not the at least one data point of information of the requester node matches the at least one data point of information of the at least one validator node; and

outputting a match result to the requestor node.

2. The method of claim 1 wherein the second layer encoded representation of the fingerprint and the encoded representation from the at least one validator node comprises a one-time encryption.

3. The method of claim 1, wherein the first and second sets of multiple shares are randomly generated for each node respectively.

4. The method of claim 1, wherein, the comparing step further comprises:

sending each share of the first set of multiple shares to a separate support server from the other shares of its set;

sending each share of the second set of multiple shares to a separate support server from the other shares of its set; and

at each support server, reconciling a value received from the requester node against an equivalent value received from the at least one validator node.

5. The method of claim 4, wherein, the determining step further comprises:

aggregating, by the second server, a set of resulting values from each of the plurality of support servers;

consolidating the sets of resulting values from the plurality of support servers; and

identifying, based on the consolidating, whether or not a sum equaling zero results.

6. The method of claim 1, wherein the at least one data point relates to an identity of a customer.

7. The method of claim 1, wherein the network is a closed network, and wherein each node in the closed network is a preapproved member of the closed network.

8. The method of claim 1, wherein each of the plurality of support servers comprises an ephemeral node and wherein the ephemeral node includes no persistent memory or storage capacity.

9. The method of claim 1, further comprising:

calculating, by the second server, a confidence score associated with the match result; and

outputting the confidence score with the match result.

10. A system for providing anonymous validation of an anonymous query among a plurality of nodes in a network, the system comprising:

a plurality of servers each having a processor and memory, and one or more code sets stored in the memory and configured to execute in the processor, and which, when executed, configure the system to:

calculate a fingerprint of at least one data point of information of a requestor node to be validated in the query by applying a first layer of encoding;

receive at a first server a query from the requester node in the network, for validation of the query by at least one other node of the plurality of nodes;

wherein the query comprises a second layer encoded representation of the fingerprint; and

wherein the second layer encoded representation is divided into a first set of multiple shares;

receive at the first server, from at least one validator node of the plurality of nodes, an encoded representation of at least one data point of information of the validator node;

wherein the encoded representation from the at least one validator node is divided into a second set of multiple shares;

compare by a plurality of support servers the first set of multiple shares from the requestor node with the second set of multiple shares of the at least one validator node;

determine by a second server, based on the comparison, whether or not the at least one data point of information of the requester node matches the at least one data point of information of the at least one validator node; and

output a match result to the requestor node.

11. The system of claim 10 wherein the second layer encoded representation of the fingerprint and the encoded representation from the at least one validator node comprises a one-time encryption.

12. The system of claim 10, wherein the first and second sets of multiple shares are randomly generated for each node respectively.

13. The system of claim 10, wherein, the comparing step further comprises:

sending each share of the first set of multiple shares to a separate support server from the other shares of its set;

sending each share of the second set of multiple shares to a separate support server from the other shares of its set; and

at each support server, reconciling a value received from the requester node against an equivalent value received from the at least one validator node.

14. The system of claim 13, wherein, the determining step further comprises:

aggregating, by the second server, a set of resulting values from each of the plurality of support servers;

consolidating the sets of resulting values from the plurality of support servers; and identifying, based on the consolidating, whether or not a sum equaling zero results.

15. The system of claim 10, wherein the at least one data point relates to an identity of a customer.

16. The system of claim 10, wherein the network is a closed network, and wherein each node in the closed network is a preapproved member of the closed network.

17. The system of claim 10, wherein each of the plurality of support servers comprises an ephemeral node and wherein the ephemeral node includes no persistent memory or storage capacity.

18. The system of claim 10, further configured to:

calculate, by the second server, a confidence score associated with the match result; and output the confidence score with the match result.