CLAIMS

1. A method for verifying database query results, the method implemented by a query verification apparatus and comprising:

sending received data to at least one prover device for insertion into a table of a database after generating and storing, by a verifier device, a first commitment from the received data;

receiving a query result and an overall proof from the at least one prover device in response to a received query forwarded to the at least one prover device after the first commitment is generated and stored, wherein the received query is associated with the database table; and

returning the query result and an indication the query result was verified in response to the received query and after verifying the query result based on a second commitment to the query result generated using the first commitment and the overall proof.

2. The method of claim 1, wherein the overall proof is generated from one or more partial proofs generated from one or more commitments generated from one or more intermediate values using one or more graphics processing units (GPUs) of the at least one prover device and the method further comprises generating a query plan from the received query, wherein each of the one or more partial proofs is associated with at least one node of the query plan.

3. The method of claim 2, wherein the database is a structured query language (SQL) database and the method further comprises generating the query plan with a SQL engine, wherein the query plan comprises a directed acyclic graph (DAG) comprising the at least one node.

4. The method of claim 1, wherein the at least one prover device comprises a plurality of prover devices, the generating and storing the first commitment, receiving the query, and returning the query result are performed by the

verifier device, wherein the verifier device is separate from the plurality of prover devices, and the database comprises a decentralized database.

5. The method of claim 1, further comprising:

updating the stored first commitment following receipt of additional data to be appended to the database table; and

sending the additional data to the at least one prover device.

6. A query verification apparatus, comprising a prover device and a verifier device, the prover device comprising a first memory comprising first programmed instructions stored thereon, and a first processor, wherein the first processor is configured to execute the stored first programmed instructions to:

receive data from the verifier device, store the received data into a table of a database, and receive a query from the verifier device, wherein the query is associated with the database table;

generate a query plan and a query result for the query and an overall proof; and

return the overall proof along with the query result in response to the query to facilitate verification of the query result by the verifier device based on a first commitment generated and stored by the verifier device from the data before the data was received from the verifier device.

7. The query verification apparatus of claim 6, wherein the first processor is further configured to execute the stored first programmed instructions to generate one or more immediate values.

8. The query verification apparatus of claim 7, further comprising one or more graphics processing units (GPUs), wherein the one or more GPUs are configured to execute the stored first programmed instructions to generate one or more commitments from the one or more intermediate values.

9. The query verification apparatus of claim 8, wherein the first processor is further configured to execute the stored first programmed instructions to generate one or more partial proofs form the one or more commitments and to generate the overall proof from the one or more partial proofs.

10. The query verification apparatus of claim 6, wherein the verifier device comprises a second memory comprising second programmed instructions stored thereon and a second processor configured to execute the stored second programmed instructions to:

receive the data, generate and store the first commitment from the received data, and send the received data to the prover device;

receive the query, forward the query to the prover device, and receive the query result and the overall proof from the prover device in response to the query;

verify the query result based on a second commitment to the query result generated using the first commitment and the overall proof; and

return the query result and an indication the query result was verified in response to the query.

11. The query verification apparatus of claim 10, wherein the second processor is further configured to execute the stored second programmed instructions to:

update the stored first commitment following receipt of additional data to be appended to the database table; and

send the additional data to the prover device.

12. The query verification apparatus of claim 6, wherein the database is a structured query language (SQL) database and the first processor is further configured to execute the stored first programmed instructions to generate a query

plan with a SQL engine, wherein the query plan comprises a directed acyclic graph (DAG) comprising at least one node.

13. The query verification apparatus of claim 6, wherein the prover device comprises a plurality of prover devices hosting the database, the verifier device is separate from the plurality of prover devices, and the database comprises a decentralized database.

14. A non-transitory computer readable medium having stored thereon instructions for verifying query results comprising executable code which when executed by one or more processors, causes the one or more processors to:

send received data to at least one prover device for insertion into at least one table of a database after generating and storing, by a verifier device, a first commitment from the received data;

receive a query result and an overall proof from that at least one prover device in response to a received query forwarded to the at least one prover device after the first commitment is generated and stored, wherein the received query is associated with the database table; and

return the query result and an indication the query result was verified in response to the received query and after the query result is verified based on a second commitment to the query result generated using the first commitment and the overall proof.

15. The non-transitory computer readable medium of claim 14, wherein the executable code, when executed by the one or more processors, causes the one or more processors to generate one or more partial proofs from one or more commitments generated from one or more intermediate values using one or more graphics processing units (GPUs),

16. The non-transitory computer readable medium of claim 14, wherein the database is a structured query language (SQL) database and the

executable code, when executed by the one or more processors, causes the one or more processors to generate a query plan via a SQL engine

17. The non-transitory computer readable medium of claim 16, wherein the query plan comprises a directed acyclic graph (DAG) comprising at least one node.

18. The non-transitory computer readable medium of claim 14, wherein the at least one prover device comprises a plurality of prover devices and the database comprises a decentralized database.

19. The non-transitory computer readable medium of claim 14, wherein the first commitment is generated and stored, the query is received, and the query result is returned, by the verifier device, wherein the verifier device is separate from the at least one prover device.

20. The non-transitory computer readable medium of claim 14, wherein the executable code, when executed by the one or more processors, causes the one or more processors to:

update the stored first commitment following receipt of additional data to be appended to the database table; and

send the additional data to the at least one prover device.