

protocols disclosed herein can be used to implement wide-area consensus in computer networks for certain settings.

In ~~one embodiment~~ a first aspect, the present disclosure provides an apparatus ~~comprises comprising~~: a first processing node comprising a processor coupled to a memory; the first processing node being configured to participate in a consensus protocol with ~~a plurality of~~ additional processing nodes, the first processing node and the additional processing nodes comprising respective processing devices configured to communicate with one another over at least one network; ~~the first processing node is being~~ further configured in conjunction with its participation in the consensus protocol to implement repeated polling of respective distinct selected subsets of the additional processing nodes, each of the distinct selected subsets comprising fewer than all of the additional processing nodes, with at least portions of results of the repeated polling being stored at least in part utilizing one or more counters implemented by the processor and memory of the first processing node; to ~~resolve-determine~~ a resolved state for a given transaction ~~to as~~ a particular one of a plurality of possible states for the given transaction responsive to results of the repeated polling of the respective distinct selected subsets that each comprise fewer than all of the additional processing nodes; to store in the memory of the first processing node an indication of the resolved state in association with at least one value that reinforces the particular state as the resolved state within the first processing node, the value controlling a likelihood that the first processing node will subsequently modify the resolved state to a state other than the particular state; to transmit the indication of the resolved state from the first processing node over the network to one or more other processing nodes under one or more specified conditions including at least one of (i) in response to a query received from a given one of the additional processing nodes in conjunction with polling performed by the given additional processing node as part of its participation in the consensus protocol, and (ii) in response to a query received from another processing node not currently participating in the consensus protocol; and to initiate at least one automated action based at least in part on the resolved state for the given transaction.

In a second aspect, the present disclosure provides configuring a method comprising: configuring a first processing node comprising a processor coupled to a memory to participate in

a distributed consensus protocol with additional processing nodes, the first processing node and the additional processing nodes comprising respective processing devices configured to communicate with one another over at least one network; in conjunction with its participation in the consensus protocol, the first processing node: implementing repeated polling of respective distinct selected subsets of the additional processing nodes, each of the distinct selected subsets comprising fewer than all of the additional processing nodes, with at least portions of results of the repeated polling being stored at least in part utilizing one or more counters implemented by the processor and memory of the first processing node; determining a resolved state for a given transaction as a particular one of a plurality of possible states for the given transaction based at least in part on the counters and responsive to the results of the repeated polling of the respective distinct selected subsets that each comprise fewer than all of the additional processing nodes; storing in the memory of the first processing node an indication of the resolved state in association with at least one value that reinforces the particular state as the resolved state within the first processing node, the value controlling a likelihood that the first processing node will subsequently modify the resolved state to a state other than the particular state; transmitting the indication of the resolved state from the first processing node over the network to one or more other processing nodes under one or more specified conditions including at least one of (i) in response to a query received from a given one of the additional processing nodes in conjunction with polling performed by the given additional processing node as part of its participation in the consensus protocol, and (ii) in response to a query received from another processing node not currently participating in the consensus protocol; and initiating at least one automated action based at least in part on the resolved state for the given transaction.

In a third aspect, the present disclosure provides a computer program product comprising a non-transitory processor-readable storage medium having stored therein program code of one or more software programs, wherein the program code when executed by a first processing node, the first processing node comprising a processor coupled to a memory and being configured to participate in a consensus protocol with additional processing nodes, the first processing node and the additional processing nodes comprising respective processing devices configured to

communicate with one another over at least one network, causes the first processing node in conjunction with its participation in the consensus protocol: to implement repeated polling of respective distinct selected subsets of the additional processing nodes, each of the distinct selected subsets comprising fewer than all of the additional processing nodes, with at least portions of results of the repeated polling being stored at least in part utilizing one or more counters implemented by the processor and memory of the first processing node; to determine a resolved state for a given transaction as a particular one of a plurality of possible states for the given transaction based at least in part on the counters and responsive to the results of the repeated polling of the respective distinct selected subsets that each comprise fewer than all of the additional processing nodes; to store in the memory of the first processing node an indication of the resolved state in association with at least one value that reinforces the particular state as the resolved state within the first processing node, the value controlling a likelihood that the first processing node will subsequently modify the resolved state to a state other than the particular state; to transmit the indication of the resolved state from the first processing node over the network to one or more other processing nodes under one or more specified conditions including at least one of (i) in response to a query received from a given one of the additional processing nodes in conjunction with polling performed by the given additional processing node as part of its participation in the consensus protocol, and (ii) in response to a query received from another processing node not currently participating in the consensus protocol; and to initiate at least one automated action based at least in part on the resolved state for the given transaction.

Resolving the state for the given transaction in some embodiments comprises utilizing the results of the repeated polling to make a determination as to whether or not the given transaction should be accepted as a valid transaction. Such accepting of a given transaction as a valid transaction is considered an example of what is more generally referred to herein as “resolving the state” for the given transaction. A wide variety of other types of transactions each having multiple possible states subject to consensus-based resolution to a particular state can be processed in other embodiments.

In some embodiments, the repeated polling is repeated for a plurality of iterations, where a given one of the iterations comprises selecting a sample of the additional processing nodes, and sending queries to respective ones of the selected additional processing nodes. The sample in some embodiments comprises a probabilistic sample, illustratively selected at random. As another
5 example, the sample can be selected deterministically, possibly using a seed.

Responsive to receipt of at least a threshold number of responses to the queries, the first processing node determines if at least a designated portion of the received responses indicate a particular state for the given transaction that differs from a current state for the given transaction in the first processing node. Alternatively, such a determination can be made responsive to a
10 particular timeout being reached, if sufficient responses are not received prior to the particular timeout being reached.

Claims

What is claimed is:

1. An apparatus comprising:

a first processing node comprising a processor coupled to a memory;

5 the first processing node being configured to participate in a consensus protocol with additional processing nodes, the first processing node and the additional processing nodes comprising respective processing devices configured to communicate with one another over at least one network;

10 the first processing node being further configured in conjunction with its participation in the consensus protocol:

to implement repeated polling of respective distinct selected subsets of the additional processing nodes, each of the distinct selected subsets comprising fewer than all of the additional processing nodes, with at least portions of results of the repeated polling being stored at least in part utilizing one or more counters implemented by the processor and memory of the first

15 processing node;

to ~~resolve-determine~~ a resolved state for a given transaction ~~to-as~~ a particular one of a plurality of possible states for the given transaction responsive to results of the repeated polling of the respective distinct selected subsets that each comprise fewer than all of the additional processing nodes;

20 to store in the memory of the first processing node an indication of the resolved state in association with at least one value that reinforces the particular state as the resolved state within the first processing node, the value controlling a likelihood that the first processing node will subsequently modify the resolved state to a state other than the particular state;

25 to transmit the indication of the resolved state from the first processing node over the network to one or more other processing nodes under one or more specified conditions including at least one of (i) in response to a query received from a given one of the additional processing nodes in conjunction with polling performed by the given additional processing node

as part of its participation in the consensus protocol, and (ii) in response to a query received from another processing node not currently participating in the consensus protocol; and

to initiate at least one automated action based at least in part on the resolved state for the given transaction.

5

2. The apparatus of claim 1 wherein the consensus protocol is configured to provide Byzantine fault tolerance.

10 3. The apparatus of claim 1 wherein the at least one automated action comprises adding an entry characterizing the given transaction to a distributed ledger collectively maintained by the first and additional processing nodes.

15 4. The apparatus of claim 3 wherein the entry comprises a block and the distributed ledger comprises a blockchain.

15

5. The apparatus of claim 1 wherein participation of the first and additional processing nodes in the consensus protocol is controlled in accordance with at least one specified control mechanism requiring submission of one or more designated proofs by each of the first and additional processing nodes.

20

6. The apparatus of claim 5 wherein the designated proof comprises a proof other than a proof-of-work.

25 7. The apparatus of claim 1 wherein a given instance of the repeated polling comprises polling a random sample of the additional processing nodes.

8. The apparatus of claim 1 wherein a given instance of the repeated polling comprises polling a deterministic sample of the additional processing nodes.

9. The apparatus of claim 1 wherein the repeated polling is repeated for a plurality of iterations with each such iteration polling a different selected subset of the additional processing nodes.

5

10. The apparatus of claim 1 wherein the first processing node is further configured to utilize the results of the repeated polling to maintain a data structure that characterizes relationships between the given transaction and a plurality of other transactions, the data structure comprising at least one of a directed acyclic graph, a linked list and a hash-linked chain.

10

11. The apparatus of claim 1 wherein resolving the state for a given transaction responsive to results of the repeated polling comprises utilizing the results of the repeated polling to make a determination as to whether or not the given transaction should be accepted as a valid transaction.

15

12. The apparatus of claim 1 wherein the repeated polling is repeated for a plurality of iterations, a given one of the iterations comprising:

selecting a sample of the additional processing nodes;

sending queries to respective ones of the selected additional processing nodes;

responsive to receipt of at least a threshold number of responses to the queries,

20

determining if at least a designated portion of the received responses indicate a particular state for the given transaction that differs from a current state for the given transaction in the first processing node; and

responsive to the designated portion of the received responses indicating a particular state for the given transaction that differs from a current state for the given transaction

25

in the first processing node, updating the current state for the given transaction in the first processing node to the particular state.

13. The apparatus of claim 12 wherein resolving the state for the given transaction responsive to results of the repeated polling comprises resolving the state for the given transaction to the current state at the completion of the plurality of iterations.

5 14. The apparatus of claim 12 wherein the first processing node is further configured to maintain a conviction strength counter that indicates a number of consecutive iterations of the repeated polling for which at least a designated portion of the received responses indicate the particular state for the given transaction.

10 15. The apparatus of claim 14 wherein resolving the state for the given transaction responsive to results of the repeated polling comprises resolving the state for the given transaction to the particular state responsive to the conviction strength counter exceeding a threshold.

15 16. The apparatus of claim 12 wherein the first processing node is further configured to maintain confidence counters for respective ones of the possible states for the given transaction, with each of the confidence counters indicating a total number of queries over multiple ones of the iterations that have yielded responses indicating the corresponding state.

20 17. The apparatus of claim 16 wherein resolving the state for the given transaction responsive to results of the repeated polling comprises resolving the state for the given transaction to one of the possible states responsive to the confidence counter for that possible state exceeding the confidence counter for at least one other one of the possible states.

25 18. The apparatus of claim 1 wherein the first processing node is further configured to maintain a directed acyclic graph of transactions that characterizes relationships between the given transaction and a plurality of other transactions with the transactions being partitioned into mutually exclusive conflict sets.

19. The apparatus of claim 18 wherein maintaining the directed acyclic graph comprises:
selecting a sample of the additional processing nodes;
sending queries to respective ones of the selected additional processing nodes; and
updating the directed acyclic graph based at least in part on responses to the queries;
5 wherein updating the directed acyclic graph comprises one or more of:
inserting one or more additional transactions into the directed acyclic graph;
updating confidence values for respective ones of the transactions of the directed
acyclic graph; and
repartitioning the transactions of the directed acyclic graph into mutually exclusive
10 conflict sets.

20. The apparatus of claim 19 wherein resolving the state for the given transaction
responsive to results of the repeated polling comprises resolving the state responsive to the given
transaction being the only transaction in its conflict set and the given transaction having a
15 confidence value that exceeds a threshold.

21. The apparatus of claim 19 wherein resolving the state for the given transaction
responsive to results of the repeated polling comprises resolving the state to one of the possible
states responsive to a confidence counter for that possible state exceeding a confidence counter for
20 at least one other one of the possible states.

22. A method comprising:
configuring a first processing node comprising a processor coupled to a memory to
participate in a distributed consensus protocol with additional processing nodes, the first
25 processing node and the additional processing nodes comprising respective processing devices
configured to communicate with one another over at least one network;
in conjunction with its participation in the consensus protocol, the first processing
node:

implementing repeated polling of respective distinct selected subsets of the additional processing nodes, each of the distinct selected subsets comprising fewer than all of the additional processing nodes, with at least portions of results of the repeated polling being stored at least in part utilizing one or more counters implemented by the processor and memory of the first processing node;

resolving-determining a resolved state for a given transaction ~~to as~~ a particular one of a plurality of possible states for the given transaction based at least in part on the counters and responsive to the results of the repeated polling of the respective distinct selected subsets that each comprise fewer than all of the additional processing nodes;

storing in the memory of the first processing node an indication of the resolved state in association with at least one value that reinforces the particular state as the resolved state within the first processing node, the value controlling a likelihood that the first processing node will subsequently modify the resolved state to a state other than the particular state;

transmitting the indication of the resolved state from the first processing node over the network to one or more other processing nodes under one or more specified conditions including at least one of (i) in response to a query received from a given one of the additional processing nodes in conjunction with polling performed by the given additional processing node as part of its participation in the consensus protocol, and (ii) in response to a query received from another processing node not currently participating in the consensus protocol; and

initiating at least one automated action based at least in part on the resolved state for the given transaction.

23. The method of claim 22 wherein the repeated polling is repeated for a plurality of iterations, a given one of the iterations comprising:

selecting a sample of the additional processing nodes;
sending queries to respective ones of the selected additional processing nodes;
responsive to receipt of at least a threshold number of responses to the queries,
determining if at least a designated portion of the received responses indicate a particular state for

the given transaction that differs from a current state for the given transaction in the first processing node; and

responsive to the designated portion of the received responses indicating a particular state for the given transaction that differs from a current state for the given transaction in the first processing node, updating the current state for the given transaction in the first processing node to the particular state.

24. The method of claim 22 further comprising the first processing node maintaining a directed acyclic graph of transactions that characterizes relationships between the given transaction and a plurality of other transactions with the transactions being partitioned into mutually exclusive conflict sets, wherein maintaining the directed acyclic graph comprises:

selecting a sample of the additional processing nodes;

sending queries to respective ones of the selected additional processing nodes; and

updating the directed acyclic graph based at least in part on responses to the queries;

wherein updating the directed acyclic graph comprises one or more of:

inserting one or more additional transactions into the directed acyclic graph;

updating confidence values for respective ones of the transactions of the directed acyclic graph; and

repartitioning the transactions of the directed acyclic graph into mutually exclusive conflict sets.

25. A computer program product comprising a non-transitory processor-readable storage medium having stored therein program code of one or more software programs, wherein the program code when executed by a first processing node, the first processing node comprising a processor coupled to a memory and being configured to participate in a consensus protocol with additional processing nodes, the first processing node and the additional processing nodes comprising respective processing devices configured to communicate with one another over at

least one network, causes the first processing node in conjunction with its participation in the consensus protocol:

to implement repeated polling of respective distinct selected subsets of the additional processing nodes, each of the distinct selected subsets comprising fewer than all of the additional processing nodes, with at least portions of results of the repeated polling being stored at least in part utilizing one or more counters implemented by the processor and memory of the first processing node;

to ~~resolve~~ determine a resolved state for a given transaction ~~to as~~ a particular one of a plurality of possible states for the given transaction based at least in part on the counters and responsive to the results of the repeated polling of the respective distinct selected subsets that each comprise fewer than all of the additional processing nodes;

to store in the memory of the first processing node an indication of the resolved state in association with at least one value that reinforces the particular state as the resolved state within the first processing node, the value controlling a likelihood that the first processing node will subsequently modify the resolved state to a state other than the particular state;

to transmit the indication of the resolved state from the first processing node over the network to one or more other processing nodes under one or more specified conditions including at least one of (i) in response to a query received from a given one of the additional processing nodes in conjunction with polling performed by the given additional processing node as part of its participation in the consensus protocol, and (ii) in response to a query received from another processing node not currently participating in the consensus protocol; and

to initiate at least one automated action based at least in part on the resolved state for the given transaction.

26. The computer program product of claim 25 wherein the repeated polling is repeated for a plurality of iterations, a given one of the iterations comprising:

selecting a sample of the additional processing nodes;

sending queries to respective ones of the selected additional processing nodes;

responsive to receipt of at least a threshold number of responses to the queries, determining if at least a designated portion of the received responses indicate a particular state for the given transaction that differs from a current state for the given transaction in the first processing node; and

5 responsive to the designated portion of the received responses indicating a particular state for the given transaction that differs from a current state for the given transaction in the first processing node, updating the current state for the given transaction in the first processing node to the particular state.

10 27. The computer program product of claim 25 further comprising the first processing node maintaining a directed acyclic graph of transactions that characterizes relationships between the given transaction and a plurality of other transactions with the transactions being partitioned into mutually exclusive conflict sets, wherein maintaining the directed acyclic graph comprises:

 selecting a sample of the additional processing nodes;

15 sending queries to respective ones of the selected additional processing nodes; and
 updating the directed acyclic graph based at least in part on responses to the queries;

 wherein updating the directed acyclic graph comprises one or more of:

 inserting one or more additional transactions into the directed acyclic graph;

20 updating confidence values for respective ones of the transactions of the directed
acyclic graph; and

 repartitioning the transactions of the directed acyclic graph into mutually exclusive conflict sets.