CLAIMS:

1. A method of scheduling and validating a multiple-participant process, the method comprising:

submitting, by a submitting node associated with a participant in the multiple-participant process, a proposed transaction by sending a cryptographically-protected message to one or more recipient nodes, wherein the proposed transaction includes a plurality of sub-transactions that each involves at least one of the one or more recipient nodes and the cryptographically-protected message comprises at least an unencrypted submessage readable by an external node and a cryptographically-protected submessage to preserve privacy from at least the external node;

determining, by the external node, an order of the proposed transaction relative to other transactions;

by way of at least some of the recipient nodes, validating the cryptographically-protected message;

receiving a confirmation of validity of the cryptographically-protected message from at least some of the recipient nodes;

finalizing the proposed transaction, as a confirmed transaction, based on receiving one or more confirmations from at least some of the recipient nodes that satisfy a confirmation condition; and

writing the confirmed transaction to a distributed ledger according to the order determined by the external node.

2. The method of claim 1, wherein the one or more recipient nodes includes at least a first recipient node and a second recipient node, and wherein the cryptographically-protected submessage is readable by the first recipient node, but not readable by the second recipient node.

3. The method of claim 2, wherein the first recipient node has access to a decryption key to decrypt the cryptographically-protected submessage, but the second recipient node does not.

4. The method of claim 1, wherein the cryptographically-protected message is sent to the external node, and the external node sends the cryptographically-protected message to the one or more recipient nodes.

5. The method of claim 1, wherein the one or more recipient nodes use pseudonymous addresses to hide their identity from other recipient nodes.

6. The method of claim 5, further comprising an identity manager that maintains associations between the submitting node and a pseudonymous address, and the one or more recipient nodes and a pseudonymous address.

7. The method of claim 1, wherein determining validity of the cryptographically-protected message is based on the unencrypted submessage, and further including:

determining if a transaction time of the proposed transaction is within a window of a timestamp provided by the external node.

8. The method of claim 1, wherein determining validity of the cryptographically-protected message is based on the cryptographically-protected submessage, wherein determining the validity of the cryptographically-protected message includes one or more of the following:

identifying whether the proposed transaction conflicts with a previous transaction;

determining whether the proposed transaction is well-formed; or

determining if the proposed transaction conforms with a set of conformance rules.

9. The method of claim 1, wherein the confirmation condition is one or more of the following:

receiving a confirmation from each recipient node corresponding to a participant in the multi-participant process;

receiving a specified amount of confirmations within an allocated period of time;

receiving confirmations from a specified subset of the one or more recipient nodes; or

receiving confirmation from a verifiable attestation mechanism such as a cryptographic prover or trusted hardware.

10. The method of claim 1, further comprising a referee node that determines if the one or more recipient nodes do not act in accordance with an expected action for the respective recipient node, wherein the referee node determines one or more of the following:

whether the proposed transaction is well-formed;

whether the confirmation provided by the one or more recipient nodes conflicts with one or more other confirmations; or

whether the proposed transaction falsely indicates a capacity promise exhaustion.

11. The method of claim 10, wherein determining whether the proposed transaction is well-formed includes checking one or more of the following:

that the proposed transaction conforms with the conformance rules;

that the proposed transaction is authorised by a required subset of the one or more recipient nodes; and

that the proposed transaction has a correct declaration of resource requirements.

12. The method of claim 1, wherein determining the order of the proposed transaction is based on the unencrypted submessage.

13. The method of claim 12, wherein the order of the proposed transaction is based on a physical timestamp corresponding to the time the cryptographically-protected message is received by the external node, or a logical time stamp assigned to the proposed transaction.

14. The method of claim 1, further comprising:

determining, by the external node, one or more recipient nodes associated with the participants in the multiple-participant process based on the unencrypted submessage;

sending, by the external node, at least the cryptographically-protected submessage to the one or more recipient nodes;

wherein receiving the confirmation of validity of the cryptographically-protected submessage from the one or more recipient nodes is performed by the external node;

determining, by the external node, one or more nodes that should receive the confirmation; and

sending, by the external node, the confirmation to the one or more nodes;

wherein finalizing the proposed transaction and

writing the confirmed transaction to the distributed ledger is performed by the submitting node.

15. The method of claim 1, further comprising:

receiving and aggregating, by a mediator node, the confirmations provided by the one or more recipient nodes and

performing one or more of the following:

storing the aggregation of the confirmations;

sending the aggregation of the confirmations to another node; or

confirming the proposed transaction based on the aggregation of the confirmations.

16. The method of claim 1, wherein the distributed ledger records messages between at least two of the submitting node, external node, or recipient nodes, wherein the confirmed transaction written to the distributed ledger comprises the recorded messages, whereby the order determined by the external node is evidenced, or can be derived, from the recorded messages.

17. The method of claim 1, wherein the distributed ledger comprises a plurality of distinct ledgers, each maintaining a respective partial copy of the ledger, wherein the distributed ledger is constructed from partial records of the plurality of distinct ledgers.

18. The method of claim 1, further including a change of the multiple-participant process from a first domain associated with the external node to a target domain associated with a target external node, the method further comprising:

receiving, by the external node of the first domain, a transfer request from an initiator node, wherein the transfer request specifies the target domain and the target external node;

determining, by the external node of the first domain, validity of the target domain and the target external node to host the proposed transaction,

wherein based on determining the target domain can validly host the proposed transaction, sending an authorization to the initiator node to schedule and validate the proposed transaction at the target node, wherein ordering the proposed transaction is performed by the target external node.

19. The method of claim 18, further comprising:

receiving, at the submitting node and/or the recipient node, the transfer request; and

determining, at least one of the submitting node or recipient node, validity of the target domain and target external node to host the proposed transaction,

wherein based on determining the target domain can validly host the proposed transaction, sending authorization to the initiator node to schedule and validate the proposed transaction at the target node.

20. The method of claim 1, wherein each subtransaction is associated with a corresponding cryptographically-protected submessage with private information readable by an involved recipient node to the subtransaction, but not readable by one or more recipient nodes that are not involved in the subtransaction, and

wherein the cryptographically-protected submessage includes private information validation data to validate confirmations that, at least in part, are representative of private information of at least one other subtransaction in the proposed transaction, and the method further comprises:

validating that the confirmation of at least one other subtransaction corresponds with the private information validation data.

21. A method of scheduling and validating a transaction or series of transactions in a multiple-participant process comprising:

submitting a proposed transaction by at least sending a partially encrypted message to one or more recipient nodes associated with a participant in the multi-participant process, wherein the proposed transaction includes a plurality of sub-transactions that each involves at least one of the one or more recipient nodes and the partially encrypted message comprises at least an unencrypted submessage readable by an external node and an encrypted submessage to preserve privacy from at least the external node;

receiving a confirmation of validity of the partially encrypted message from the recipient node;

finalizing the proposed transaction, as a confirmed transaction, based on receiving one or more confirmations from at least some of the recipient nodes that satisfy a confirmation condition;

receiving, from the external node, an order of the confirmed transaction relative to other transactions; and

writing the confirmed transaction to a ledger according to the order determined by the external node.

22. The method of claim 21, wherein the proposed transaction is part of a proposed multi-participant transaction across multiple domains, the method further comprising:

determining from a proposed multi-participant transaction: the first proposed transaction for a first domain including the one or more recipient nodes and the external node; and at least another proposed transaction for another domain including one or more other recipient node and another external node;

submitting the other proposed transaction by at least sending another partially encrypted message to the one or more other recipient nodes associated with a participant in the multi-participant process in the other domain, wherein the other partially encrypted message comprises at least an unencrypted submessage readable by the other external node and an encrypted submessage to preserve privacy from at least the other external node;

receiving another confirmation of validity of the other partially encrypted submessage from the one or more other recipient node;

wherein finalizing the proposed transaction further includes finalizing the other proposed transaction, as another confirmed transaction, based on receiving one or more confirmations from at least some of the other recipient nodes that satisfy the confirmation condition;

receiving, from the other external node, an order of the other confirmed transaction relative to other transactions in the other domain; and

writing the other confirmed transaction to a ledger, or other ledger, according to the order determined by the other external node.

23. The method of claim 22, further comprising:

sending the confirmation of validity of the cryptographically-protected message from the recipient node in the first domain to the other recipient node in the other domain; and

sending the other confirmation of validity of the cryptographically-protected message from the other recipient node in the other domain to the recipient node in the first domain.

24. A method of scheduling and validating a plurality of transactions in a multiple-participant process comprising:

by way of a node or series of related nodes:

determining an order of a plurality of messages corresponding to the plurality of transactions that make up the multi-participant process;

receiving, from a submitting node associated with a participant in the multi-participant process, a proposed transaction submitted to one or more recipient nodes associated with a participant in the multi-participant process, wherein the proposed transaction includes a plurality of sub-transactions that each involves at least one of the one or more recipient nodes and the proposed transaction includes a partially encrypted message, the partially encrypted message comprising at least an unencrypted submessage readable by the node or series of related nodes;

determining a recipient node associated with a participant in the multi-participant process based on the unencrypted submessage;

sending the partially encrypted message to the recipient node;

receiving a confirmation of validity of the partially encrypted message from the recipient node; and

sending the confirmation to the submitting node.