

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 one or more recipient nodes each being associated with a respective stakeholder affected by the proposed transaction, wherein the proposed transaction includes a set of sub-transactions that each involves at least one of the one or more recipient nodes and specifies each respective stakeholder, wherein the set of sub-transactions are created prior to receiving the proposed transaction 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 ~~any one of the preceding claims~~ 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 any of the preceding claims, wherein determining validity of the cryptographically-protected message is based on the unencrypted submessage.~~

~~8.7.~~ The method of claim 7~~1~~, wherein determining validity of the cryptographically-protected message is based on the unencrypted submessage, and further includes including:
_____determining if a transaction time of the proposed transaction is within a window of a timestamp provided by the external node.

~~9. The method of claim 8, wherein the transaction time of the proposed transaction is a range of timestamps.~~

~~10. The method of any of the preceding claims, wherein determining validity of the cryptographically-protected message is based on the cryptographically-protected submessage.~~

~~11.8.~~ The method of claim 10~~1~~, wherein determining validity of the cryptographically-protected message is based on the cryptographically-protected submessage, includes 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.

~~12. The method of claim 10 or 11, wherein determining validity of the cryptographically-protected message based on the encrypted submessage includes determining whether the proposed transaction is well-formed.~~

~~13. The method of any of claims 10-12, wherein determining validity of the cryptographically-protected message based on the cryptographically-protected submessage includes determining if the proposed transaction conforms with a set of conformance rules.~~

~~14. The method of claim 11, wherein identifying whether the proposed transaction conflicts with the previous transaction includes checking if the previous transaction has been recorded on the distributed ledger.~~

~~15. The method of any of the preceding claims, wherein determining validity of the cryptographically-protected message is based on the unencrypted submessage and the cryptographically-protected submessage.~~

~~16. The method of claim 15, wherein determining validity comprises determining if the unencrypted submessage is consistent with the cryptographically-protected submessage.~~

~~17.9.~~ The method of ~~any of the preceding claims~~ 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.

~~18.10.~~ The method of ~~the any of the preceding claims~~ 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.

19. ~~The method of claim 18, 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; and~~

~~— whether the proposed transaction falsely indicates a capacity promise exhaustion.~~

20. ~~The method of claim 18, further comprising the referee node performing a dispute resolution process.~~

21.11. The method of claim 19~~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.

22. ~~The method of any of claims 18-21, wherein a first of the one or more recipient nodes forwards the proposed transaction to the referee node to initiate the dispute resolution process.~~

23. ~~The method of claim 22, wherein the dispute resolution process is resolved by the referee node imposing a punishment on a misbehaving node determined from the submitting node or the one or more recipient nodes.~~

24. ~~The method of claim 23, wherein the punishment is one or more of the following:~~

~~— removing the ability for the misbehaving node to submit transactions;~~

~~— flagging the proposed transaction associated with the misbehaving node as frozen;~~

~~— a custom punishment for the misbehaving node as determined by the referee node; and~~

~~—— a punishment for the misbehaving node as defined in the domain rules.~~

~~25. The method of any of claims 22-24, wherein the referee node communicates the result of the dispute resolution process to the submitting node and/or the first recipient node.~~

~~26. The method of any of claims 22-25, wherein the dispute resolution process is defined in domain rules.~~

~~27. The method of any of claims 22-26, wherein other recipient nodes besides the first recipient node provide one or more messages as evidence for the dispute resolution process to the referee node.~~

~~28.~~12. The method of ~~any of the preceding claims~~claim 1, wherein determining the order of the proposed transaction is based on the unencrypted submessage.

~~29.~~13. The method of claim ~~28~~12, wherein the order of the proposed transaction is given 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.

~~30. The method of claim 29, wherein the order of the proposed transaction relative to the other transactions is based on the physical timestamp.~~

~~31. The method of any of the preceding claims, wherein the order of the proposed transaction is based on a logical timestamp assigned to the proposed transaction.~~

~~32. The method of claim 31 when dependent on any of claims 29-30, wherein the logical timestamp corresponds to a time within a defined time window of the physical timestamp.~~

~~33. The method of any of the preceding claims, wherein the cryptographically-protected submessage is an encrypted submessage.~~

~~34.14. A~~The method of scheduling and validating a multiple-participant process claim 1, the ~~method~~further 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 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;~~

~~determining, by the external node, one or more recipient nodes associated with a~~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;~~

~~determining, by the one or more recipient nodes, validity of the cryptographically-protected submessage;~~

~~wherein receiving, by the external node, a~~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, by the submitting node, the proposed transaction, as a confirmed transaction, based on whether the confirmations provided by the one or more recipient nodes satisfy a confirmation condition; and~~

~~writing, by the submitting node, the confirmed transaction to a~~the distributed ledger according to the order determined by the external node is performed by the submitting node.

~~35.15. The~~ method of any of the preceding claims 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.

~~36. The method of claim 35, further comprising one or more of the following:~~
~~— storing the aggregation of the confirmations;~~
~~— sending the aggregation of the confirmations to another node; and~~
~~— confirming the proposed transaction based on the aggregation of the confirmations.~~

~~37. A non-transitory, tangible, computer-readable medium comprising program instructions that, when executed, cause a node or series of related nodes to perform the method of any of the preceding claims.~~

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 the encrypted submessage includes expected confirmation data to cryptographically validate all expected confirmations in the proposed transaction,
wherein the method further comprises:
executing a cryptographic function to cryptographically validate each of the received one or more confirmations corresponds with the expected confirmation data.
21. The method of claim 20, wherein the expected confirmation data is in the form of one or more public keys, and wherein the expected confirmation includes an electronic signature with a private key corresponding to the one or more the public keys.
22. 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.

~~38-23.~~ 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 one or more recipient nodes each being associated with a respective stakeholder affected by the proposed transaction, wherein the proposed transaction includes a set of sub-transactions that each involves at least one of the one or more recipient nodes and specifies each respective stakeholder, wherein the set of sub-transactions are created prior to receiving the proposed transaction 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.

24. The method of claim 23, 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.

25. The method of claim 24, 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.

~~39. The method of claim 38 wherein the one or more recipient nodes includes at least a first recipient node and a second recipient node, and the method further comprising sending the encrypted submessage to the first recipient node, the encrypted submessage being decryptable by a decryption key controlled by the first recipient node, but not the second recipient node.~~

~~40. The method of claim 39 wherein the encrypted submessage is not sent to the second recipient node.~~

~~41. The method of any of claims 38-40, further comprising determining a pseudonymous address of each recipient node, wherein each pseudonymous address is used to hide an identity of the respective recipient node from the other recipient nodes.~~

~~42. A non-transitory, tangible, computer-readable medium comprising program instructions that, when executed, cause a submitting node to perform the method of any of claims 38-41.~~

~~43.~~26. 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:

- A. determining an order of a plurality of messages corresponding to the plurality of transactions that make up the multi-participant process;
- B. receiving, from a submitting node associated with a participant in the multi-participant process, a proposed transaction ~~that includes a partially encrypted message, wherein the partially encrypted message comprises~~submitted to one or more recipient nodes associated with a participant in the multi-participant process, the one or more recipient nodes each being associated with a respective stakeholder affected by the proposed transaction, wherein the proposed transaction includes a set of sub-transactions that each involves at least one of the one or more recipient nodes and specifies each respective stakeholder, wherein the set of sub-transactions are created prior to receiving the proposed transaction 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;
- C. determining a recipient node associated with a participant in the multi-participant process based on the unencrypted submessage;
- D. sending the partially encrypted message to the recipient node;
- E. receiving a confirmation of validity of the partially encrypted message from the recipient node; and
- F. sending the confirmation to the submitting node.

~~44. The method of claim 42, further comprising determining a pseudonymous address of the recipient node, wherein the pseudonymous address is used to hide an identity of the recipient node from other nodes.~~

~~45. A non-transitory, tangible, computer-readable medium comprising program instructions that, when executed, cause a node or series of related nodes to perform the method of any of claims 42-44.~~

~~46. A method according to any one of claims 1 to 36, wherein the distributed ledger records messages between the submitting node, external node, and/or recipient nodes, wherein the confirmed transaction(s) 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.

47. — A method according to any one of claims 1 to 36 and 46, 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.

48. — A method according to any one of claims 1 to 36, 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 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 the step of ordering the proposed transaction is performed by the target external node.

49. — A method according to claim 48 further comprising:

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

— determining, at the submitting node and/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.

50. — A method according to either claim 48 or 49 wherein the authorization to the initiator node is associated with a specified timeout condition, wherein the authorization is effective and/or exclusive based on the specified time-out condition.

51. — A method of scheduling and validating a multiple-participant process involving:

~~— a first domain that is associated with a first external node, a first recipient node, and a submitting node that is associated with participants in the multiple-participant process;~~
~~— a second domain that is associated with a second external node, a second recipient node, and the submitting node or a separate relay node, and wherein the submitting node or the relay node is in communication with both the first external node and the second node;~~

~~wherein the method comprises:~~

- ~~— determining, by the submitting node, a first proposed transaction for the first domain and a second proposed transaction for the second domain, wherein the first and second proposed transaction in combination form a proposed multi-participant transaction involving the first and second recipient nodes, wherein each of the first and second proposed transactions include a cryptographically-protected message to the respective recipient nodes, and the cryptographically-protected message comprises at least an unencrypted submessage readable by the external node of the respective domain and a cryptographically-protected submessage to preserve privacy from at least the external node;~~
- ~~— submitting, by the submitting node and/or the relay node, the first proposed transaction to the first recipient node and the second proposed transaction to the second recipient node;~~
- ~~— determining, by the first external node, a first order for the first proposed transaction;~~
- ~~— determining, by the second external node, a second order for the second proposed transaction;~~
- ~~— by way of the first and second recipient nodes, validating the respective cryptographically-protected message;~~
- ~~— receiving a confirmation of validity of the cryptographically-protected messages from the first and second recipient nodes;~~
- ~~— finalizing the proposed multi-participant transaction, as a combination of a confirmed first transaction and a confirmed second transaction, based on receiving the confirmations from the first and second recipient nodes that satisfy a confirmation condition; and~~
- ~~- writing the first confirmed transaction, according to the first order, to a distributed ledger associated with the first domain and writing the second confirmed transaction, according to the second order, to a distributed ledger associated with the second domain.~~

52. ~~A method according to claim 51, wherein the submitter node is a relay to receive and send messages between the first domain and the second domain, wherein the method further comprises:~~

~~— sending, by the submitting node and/or the relay node, the confirmation of validity of the cryptographically protected message from the first recipient node to the second external node and/or second recipient node of the second domain; and~~

~~— sending, by the submitting node and/or the relay node, the confirmation of validity of the cryptographically protected message from the second recipient node to the first external node and/or first recipient node of the first domain.~~

53. ~~A method according to either claim 51 or 52 wherein an authorization to finalize the proposed multi-participant transaction is associated with a specified timing condition, wherein the authorization is effective and/or exclusive based on the specified timing condition.~~

54. ~~A method according to any one of claims 38 to 41, 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 the step of 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.~~

~~55. A method according to claim 54 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.~~

~~56. A method according to claim 54 or 55, wherein an authorization to finalize the proposed transaction and other proposed transaction is associated with a specified timing condition, wherein the authorization is effective and/or exclusive based on the specified timing condition.~~

~~57. A method according to any one of claims 1 to 36, 38 to 41, and 43 to 56, wherein the encrypted submessage includes expected confirmation data to cryptographically validate all expected confirmations in the proposed transaction, wherein the method further comprises:~~

~~—executing a cryptographic function to cryptographically validate each of the received one or more confirmations corresponds with the expected confirmation data.~~

~~58. A method according to claim 57 wherein the expected confirmation data is in the form of public key(s), and wherein the expected confirmation includes an electronic signature with a private key corresponding to the public key(s).~~

~~59. A method according to any one of claims 1 to 36, 38 to 41 and 43 to 56 wherein the proposed transaction includes a plurality of subtransactions that each involve at least one recipient node, and 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 recipient node(s) 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.~~
60. A method according to claim 59 wherein the confirmation of a subtransaction includes, at least in part, a cryptographic hash of the private information of that subtransaction.
61. A method according to claim 60 wherein the proposed transaction has a tree structure with a plurality of subtrees, wherein a subtree includes one or more of the plurality of subtransactions.
62. A method according to any one of claims 59 to 61 wherein the cryptographically protected submessage includes private information validation data to cryptographically validate any one of the confirmations of the plurality of subtransactions in the proposed transaction.