WHAT IS CLAIMED IS:

1. A node in a blockchain network, the node comprising:

a processor that when executing one or more instructions stored in an associated memory is configured to:

receive data from another node in the blockchain network, the data identifying a context of an object managed by a blockchain of the blockchain network;

validate the data based on an endorsement policy;

receive an identifier for the object;

generate an event comprising a first field for data associated with the event, a second field dedicated to the validation of the event, and a third field containing information associated with a transaction associated with the event;

execute a pseudo-write operation to store the identifier only in the second field, wherein the identifier links the event to the object;

automatically validate the event based on a pre-authorisation assigned to the identifier for the object from an authority of the blockchain network without querying other peer nodes in the blockchain network; and

submit the event to the blockchain for consensus processing.

2. The node of claim 1, wherein the identifier includes key information previously validated for the object.

3. The node of claim 2, wherein the key information links the event to a validation authority that validates the event based on the key information.

4. The node of claim 1, wherein the context comprises a tuple that includes at least two of:

a channel name, a namespace, a collection, or a key name corresponding to the blockchain.

5. The node of claim 1, wherein the presence of the key information in the identifier causes a second node in the blockchain network to automatically validate the event based on the presence of the key information without checking ledgers of other nodes in the blockchain network.

6. The node of claim 1, wherein the data has a format including a plurality of data fields, and wherein, when the processor is configured to generate the event, the processor is further configured to add a new data field storing the key information to the format.

7. The node of claim 1, wherein the data indicates a change in a state of the object.

8. A method, comprising:

receiving, by a node in a blockchain network, data from another node in the blockchain network, the data identifying a context of an object managed by a blockchain of the blockchain network;

validating, by the node, the data based on an endorsement policy;

receiving, by the node, an identifier for the object;

generating, by the node, an event comprising a first field for data associated with the event, a second field dedicated to the validation of the event, and a third field containing information associated with a transaction associated with the event;

executing, by the node, a pseudo-write operation to store the identifier only in the second field, wherein the identifier links the event to the object;

automatically validating, by the node, the event based on a pre-authorisation assigned to the identifier for the object from an authority of the blockchain network without querying other peer nodes in the blockchain network; and

submitting, by the node, the event to the blockchain for consensus processing.

9. The method of claim 8, wherein the identifier includes key information previously validated for the object.

10. The method of claim 9, wherein the key information links the event to a validation authority that validates the event based on the key information.

11. The method of claim 8, wherein the context comprises a tuple including at least two of:

a channel name, a namespace, a collection, or a key name corresponding to the blockchain.

12. The method of claim 8, wherein the presence of the key information in the identifier causes a second node in the blockchain network to automatically validate the event based on the presence of the key information without checking ledgers of other nodes in the blockchain network.

13. The method of claim 8, wherein the data has a format including a plurality of data fields, and wherein generating the event further comprises adding a new data field storing the key information to the format.

14. The method of claim 8, wherein the data indicates a change in a state of the object.

15. A non-transitory computer-readable medium storing one or more instructions which, when executed by a processor of a node in a blockchain network, configure the processor to:

receive data from another node in the blockchain network, the data identifying a context of an object managed by a blockchain of the blockchain network;

validate the data based on an endorsement policy;

receive an identifier for the object;

generate an event which includes a first field for data associated with the event, a second field dedicated to the validation of the event, and a third field containing information associated with a transaction associated with the event;

execute a pseudo-write operation to store the identifier only in the second field, wherein the identifier links the event to the object;

automatically validate the event based on a pre-authorisation assigned to the identifier for the object from an authority of the blockchain network without querying other peer nodes in the blockchain network; and

submit the event the blockchain for consensus processing.

16. The medium of claim 15, wherein the identifier includes key information previously validated for the object.

17. The medium of claim 16, wherein the key information links the event to a validation authority that validates the event based on the key information.

18. The medium of claim 15, wherein the context comprises a tuple including at least two of:

a channel name, a namespace, a collection, a or key name corresponding to the blockchain.

19. The medium of claim 15, wherein the data has a format including a plurality of data fields, and wherein, when the processor is configured to generate the event, the one or more instructions further configure the processor to add a new data field storing the key information to the format.

20. The medium of claim 15, wherein the presence of the key information in the identifier causes a second node in the blockchain network to automatically validate the event based on the presence of the key information without checking ledgers of other nodes in the blockchain network.