What is claimed is:

1. A method for an entity to manage a transaction system in which transactions are organized in a sequence of blocks that are certified by digital signatures of a sufficient number of verifiers, the method comprising:

the entity proposing a hash of a block B' that includes new valid transactions relative to a sequence of certified blocks $B^0, \ldots, B^{r-1}$ if no rth block B^r has been certified; and

the entity proposing a hash of the block B^r if the rth block B^r has been verified by a sufficient number of other entities.

2. A method, according to claim 1, wherein a block is certified by the entity only in response to confirming transactions for the block and confirming that the block was constructed and propagated by an entity entitled to construct and propagate the block.

3. A method, according to claim 1, wherein the entity proposes a hash value by digitally signing the hash value to provide a digitally-signed version of the hash value and wherein the entity propagates the digitally-signed version of the hash value to a network that includes other entities.

4. A method, according to claim 3, wherein if no rth block B^r has been certified, the entity also digitally signs and propagates the block B'.

5. A method, according to claim 1, wherein the entity determines a quantity Q from the prior blocks and uses a secret key in order to compute a string S uniquely associated with Q and computes from S a quantity T that is at least one of: S itself, a function of S, and hash value of S and wherein the entity determines whether to propose a hash value by determining whether T possesses a given property.

6. A method, according to claim 5, wherein S is a signature of Q under a secret key of the entity, T is a hash of S and T possesses the given property if T is less than a given threshold.

7. A method, according to claim 1, wherein the entity is part of a network of entities and wherein a particular one of the entities constructs and propagates the block B^r.

8. A method, according to claim 7, wherein the rth block B^r is determined to be certified by the entity if the entity receives an indication that at least a predetermined number of the entities individually certify a hash value corresponding to the rth block B^r.

9. A method, according to claim 8, wherein, in response to the entity receiving the indication that a predetermined number of the entities individually certified the rth block B^r, the entity increments r to begin adding additional blocks to the sequence of blocks.

10. A method, according to claim 7, wherein the particular one of the entities is individually chosen by a predetermined number of the entities to be a leader.

11. A method, according to claim 10, wherein the rth block B^r is determined to be certifiable by the entity if the entity receives an indication that at least a predetermined number of the entities individually verify receiving an indication that the particular one of the entities has provided a hash value corresponding to the rth block B^r to each of the predetermined number of the entities.

12. A method for an entity to manage a transaction system in which transactions are organized in a sequence of certified blocks, the method comprising:

the entity receiving a hash value of a block B^r from an other entity that generated the block based on new valid transactions relative to a sequence of certified blocks $B^0, \ldots, B^{r-1}$;

the entity certifying the block B^r in response to a sufficient number of other entities having indicated receipt of the hash value of the block B^r from the other entity and the hash value being valid for the block B^r;

the entity generating a new block B' based on new valid transactions relative to a sequence of certified blocks $B^0, \ldots, B^{r-1}$ in response to an insufficient number of the other entities indicating receipt of the hash value of the block B^r from the other entity, wherein B' is different from B^r; and

the entity incrementing r to begin adding additional blocks to the sequence of blocks in response to the entity receiving the indication that a predetermined number of the entities individually certified the rth block B^r or a predetermined number of the entities individually certified the new block B'.

13. A method, according to claim 12, wherein the blocks are certified by digital signatures.

14. A method, according to claim 12, wherein new blocks are proposed by different ones of the entities until receiving the indication that a predetermined number of the entities individually certified a previously proposed block.

15. A method, according to claim 12, wherein the entity provides an indication that a new block should be generated in response to the hash value not being valid for the block B^r.

16. A method, according to claim 15, wherein the entity generates a new block B' based on new valid transactions relative to a sequence of certified blocks $B^0, \ldots, B^{r-1}$ in response to a sufficient number of the other entities providing an indication that a new block should be generated.

17. A method, according to claim 12, wherein the entity provides an indication that the hash value of the block B^r should be propagated in response to a sufficient number of the other entities having indicated receipt of the hash value of the block B^r from the other entity and the hash value being valid for the block B^r.

18. A method for an entity to verify a proposed hash value of a new block B^r of transactions relative to a given a sequence of blocks, $B^0, \ldots, B^{r-1}$, without access to the new block B^r in a transaction system in which transactions are organized in blocks and blocks are certified by a set of digital signatures, the method comprising:

having the entity determine a quantity Q from the prior blocks;

having the entity compute a digital signature S of Q;

having the entity compute from S a quantity T that is at least one of: S itself, a function of S, and hash value of S;

having the entity determine whether T possesses a given property; and

if T possesses the given property, having the entity verify the proposed hash value of the new block B^r independent of confirming whether the proposed hash value corresponds to the new block B^r.

19. A method, according to claim 18, wherein the entity propagates the proposed hash value of the new block B^r prior to receiving the new block B^r.

20. Computer software, provided in a non-transitory computer-readable medium, comprising: executable code that implements the method of one of the preceding claims 1-19.