

Claims:

1. 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 another entity that generated the block based on new valid transactions relative to a sequence of certified blocks $B^0, \dots, B^{r-1}$;

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 $B^0, \dots, B^{r-1}$ 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 r th block B^r or a predetermined number of the entities individually certified the new block B' .

2. A method, according to claim 1, wherein the blocks are certified by digital signatures.

3. A method, according to claim 1, 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.

4. A method, according to claim 1, 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 .

5. A method, according to claim 4, wherein the entity generates a new block B' based on new valid transactions relative to a sequence of certified blocks $B^0, \dots, B^{r-1}$ in response to a sufficient number of the other entities providing an indication that a new block should be generated.

6. A method, according to claim 1, 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 .

7. 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, $B^0, \dots, B^{r-1}$, 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 .

8. A method, according to claim 7, wherein the entity propagates the proposed hash value of the new block B^r prior to receiving the new block B^r .

9. Computer software, provided in a non-transitory computer-readable medium, comprising: executable code that implements the method of one of the preceding claims 1-8.