

What is claimed is:

1. In a transaction system where transactions are organized in blocks, wherein the transaction system comprises a plurality of workstations connected via a network, and each of the plurality of workstations executes a method of constructing new blocks B^r and B^{r+1} relative to a sequence of prior blocks $B^0, B^1, \dots, B^{r-1}$, the method comprising:

causing the block B^r to be constructed by one or more workstations of the plurality of workstations after confirming that the block B^r indicates initial states of transactions that are consistent with a state of the transactions in the block B^{r-1} ;

causing the block B^{r+1} to be constructed by one or more workstations of the plurality of workstations after confirming that the block B^{r+1} indicates initial states of transactions that are consistent with a state of the transactions in the block B^r ; and

causing a plurality of verifiers to verify previously- unverified transactions of the block B^r after the block B^{r+1} is constructed, wherein the plurality of verifiers comprises one or more workstations of the plurality of workstations.

2. A method, according to claim 1, wherein the transactions are smart contracts.

3. A method, according to claim 2, wherein the block B^r is constructed in connection with posting a transaction to at least one of the smart contracts in the block B^r .

4. A method, according to claim 3, wherein transaction results are posted for the smart contracts in the block B^r .

5. A method, according to claim 4, wherein a number of steps for execution of the smart contracts results are posted for the smart contracts in the block B^r .

6. A method, according to claim 5, wherein a fee is posted, wherein the fee is received by one or more of the plurality of verifiers for verifying transactions of the block B^r .

7. A method, according to claim 1, wherein the plurality of verifiers is a subset of all users of the block B^r .

8. A method, according to claim 7, wherein the plurality of verifiers is chosen randomly.
9. A method, according to claim 8, wherein choosing the plurality of verifiers randomly includes applying a cryptographic hash function to data that includes at least one of: time information, information about one or more of the blocks, data included in one or more of the blocks, or data deduced from one or more of the blocks.
10. Computer software, provided in a non-transitory computer-readable medium, comprising:
executable code that causes a workstation in the transaction system to execute the method of one of the preceding claims 1-9.