

CLAIMS

What is claimed is:

1. A system, comprising:
 - a memory; and
 - a processor configured to execute computer instructions stored in the memory that when executed cause the system to perform operations, the computer instructions further comprising:
 - a blockchain storage component to create a subsequent data block N+1 of a blockchain having N data blocks in response to a storage command, N being a positive integer;
 - an activity token that represents at least one previous network action of an entity operating the blockchain storage component; and
 - a blockchain processing component to generate the storage command based on cryptographic processing of at least one of the N data blocks of the blockchain, the N+1 data block, and the activity token, wherein the activity token is employed by the blockchain processing component to reduce the cryptographic processing of the N+1 data block.
2. The system of claim 1, wherein the activity token enables the blockchain processing component to select a reduced set of hash data from the Nth data block in the cryptographic processing of the N+1 data block.
3. The system of claim 2, wherein the activity token enables the blockchain processing component to solve a cryptographic hash function represented as $H(H(N+1), \text{Nonce})$ that removes at least one binary digit from a previous hash function applied to the Nth data block, where H is a hash operation, $H(N+1)$ is a hash function applied to the N+1 data block of the blockchain, and the Nonce is an arbitrary number that is used singularly in a cryptographic process.

4. The system of claim 1, wherein the activity token is expressed as a numerical value, a mathematical function, or a probability value that indicates reliability of the blockchain storage component to create the subsequent data block in the blockchain based on previous network activities.
5. The system of claim 4, further comprising an activity monitor component to record activity data relating to the network activities of the blockchain storage component, and to assign a weighting parameter to the activity data associated with each of the respective network activities.
6. The system of claim 5, wherein the activity data can include at least one of prior blockchain storage activity data for the blockchain storage component, a rate of transaction data for the blockchain storage component, and associations activity data relating to prior interactions of the blockchain storage component and other network components.
7. The system of claim 6, wherein the rate of transaction data is related to at least one of quantity of interactions the blockchain storage component has with other network components, types of interactions the blockchain storage component has with other network components, time of interactions the blockchain storage component has with other network components, and influence of the blockchain storage component has with respect to other network components.
8. The system of claim 5, further comprising a token generator component to process the weighting parameters received from the activity monitor component and to generate a weighting score that assigns a relative value to the weighting parameters, wherein the weighting score is compared to a threshold value to determine whether to issue the activity token to the blockchain storage component.

9. The system of claim 1, further comprising at least one of a validator component to facilitate a transaction with a transactor for transaction data, and a blockchain responder component entrusted to update the blockchain, wherein at least one of the validator component and the blockchain responder component executes the blockchain storage component to store the transaction data in the blockchain.

10. The system of claim 9, wherein the validator component operates with a transaction component to form a transaction system to facilitate collecting the transaction data from the transactor.

11. The system of claim 10, wherein the at least one transaction component includes a transaction interface to interact with the transactor to facilitate performing at least one of a financial exchange between parties, a file exchange between parties, and a property exchange between parties, wherein the N+1 data block in the blockchain is employed to record the exchanges.

12. A computer-implemented method, comprising:

receiving, by a system having a processor and a memory, an activity token that is derived from at least one previous network action of an entity operating in accordance with a blockchain, the blockchain having N data blocks, N being a positive integer;

selecting, by the system, a reduced set of hash data from the Nth data block in the cryptographic processing of a subsequent data block N+1 based on the activity token;

generating, by the system, a storage command to update transaction data in the N+1 data block based on cryptographic processing of at least one of the N data blocks of the blockchain, the N+1 data block, and the reduced set of hash data from the Nth data block; and

creating, by the system, the subsequent data block of the blockchain in response to the storage command.

13. The computer-implemented method of claim 12, further comprising solving, by the system, a cryptographic hash function represented as $H(H(N+1), \text{Nonce})$, that removes at least one binary digit from a previous hash function applied to the Nth data block, where H is a hash operation, $H(N+1)$ is a hash function applied to the N+1 data block of the blockchain, and the Nonce is an arbitrary number that is used singularly in a cryptographic process.

14. The computer-implemented method of claim 12, wherein the activity token is expressed as a numerical value, a mathematical function, or a probability value that indicates a reliability to create the subsequent data block in the blockchain based on previous network activities.

15. The computer-implemented method of claim 14, further comprising:
recording, by the system, activity data relating to the network activities of storing data to the blockchain; and
assigning a weighting parameter to the activity data associated with each of the respective network activities.

16. The computer-implemented method of claim 15, wherein the activity data can include at least one of prior blockchain storage activity data, a rate of transaction data, and associations activity data relating to other network components.

17. The computer-implemented method of claim 15, further comprising:
processing the weighting parameters received from the activity monitor; and
generating a weighting score that assigns a relative value to the weighting parameters.

18. The computer-implemented method of claim 17, further comprising comparing the weighting score to a threshold value to determine whether to issue the activity token.

19. A non-transitory machine-readable medium having machine-readable instructions that when executed by a processor cause the processor to:

- generate an activity token that is derived from at least one previous network action of an entity operating in accordance with a blockchain, the blockchain having N data blocks, N being a positive integer;
- select a reduced set of hash data from the Nth data block in the cryptographic processing of a subsequent data block N+1 based on the activity token;
- generate a storage command to update transaction data in the N+1 data block based on cryptographic processing of at least one of the N data blocks of the blockchain, the N+1 data block, and the reduced set of hash data from the Nth data block; and
- store the transaction data in the subsequent data block of the blockchain in response to the storage command.

20. The non-transitory machine-readable medium of claim 19, the instructions further causing the processor to solve a cryptographic hash function represented as $H(H(N+1), \text{Nonce})$, that removes at least one binary digit from a previous hash function applied to the Nth data block, where H is a hash operation, $H(N+1)$ is a hash function applied to the Nth data block of the blockchain, and the Nonce is an arbitrary number that is used singularly in a cryptographic process.