Claims

1. A computer-implemented method comprising:

encrypting a plaintext message to a cryptographic public key in accordance with an identity-based encryption scheme using at least a congress public key to generate an encrypted message, wherein the congress public key is associated with members of a congress, respective members of the congress having access to private key shares usable in a threshold decryption scheme in which at least a threshold of private key shares are sufficient to derive a decryption key through the combination of partial contributions to the decryption key on behalf of the congress;

generating, using at least a cryptographic private key corresponding to the cryptographic public key, a digital signature over a first set of instructions to perform cryptographic operations upon an occurrence of an event; and

broadcasting one or more transactions to a proof-of-work blockchain network, the one or more transactions comprising the encrypted message, the cryptographic public key, at least the first set of instructions, and a second set of instructions to the members of the congress to cooperate to:

in response to reaching a consensus on the event occurring and contingent upon the digital signature being authentic, deploy a ghost chain to perform the first set of instructions, wherein performing the first set of instructions includes at least deriving the decryption key from the cryptographic public key and a plurality of private key shares that satisfies the threshold, the decryption key being sufficient cryptographic material to obtain the plaintext message from the encrypted message, wherein the ghost chain is a block-based distributed proof-of-stake distributed ledger comprising at least a genesis block and a terminal block, wherein each block includes a share of the decryption key and wherein the terminal block is generated upon deriving the decryption key from the cryptographic public key.

2. The computer-implemented method of claim 1, wherein the decryption key is derivable based at least in part on a scheme based on pairings on elliptic curves.

3. The computer-implemented method of any one of claims 1 or 2, wherein the identity-based encryption scheme is in accordance with a Boneh-Franklin identity-based encryption scheme.

4. The computer-implemented method of any one of claims 1 to 3, wherein the one or more transactions comprise a transaction that includes a fee to the public group address associated with the congress, the fee being distributed to at least some of the miners of the ghost chain that cooperate to derive the decryption key.

5. The computer-implemented method of any one of claims 1 to 4, wherein the miners of the ghost chain reach the consensus on the event based on information obtainable from the proof-of-work blockchain.

6. The computer-implemented method of claim 5, wherein the information

obtainable from the proof-of-work blockchain is a timestamp of a transaction submission to the proof-of-work blockchain.

7. The computer-implemented method of claim 5, wherein the information

obtainable from the proof-of-work blockchain is a detection of a valid block of at least a particular height.

8. The computer-implemented method of any one of claims 1 to 4, wherein the consensus is reached based at least in part on detecting that the members of the congress emit at least a threshold of attestations that the event has occurred, wherein occurrence of the event is determined based at least in part on information outside of the proof-of-work blockchain, and further wherein authenticity of the attestations are cryptographically verifiable using cryptographic public keys associated with respective members of the congress.

9. The computer-implemented method of claim 8, wherein the attestations are emitted for a predetermined duration.

10. The computer-implemented method of any one of claims 1 to 9, wherein the cryptographic operations include one or more decryption operations.

11. The computer-implemented method of any one of claims 1 to 10, wherein the cryptographic operations include one or more authentication operations.

12. The computer-implemented method of any one of claims 1 to 11, wherein a respective private key share of a member of the congress is generated and used to perform cryptographic operations within a trusted execution environment within a node associated with the member.

13. A computer readable storage medium comprising computer-executable

instructions which, when executed, configure a processor to perform the method of any one of claims 1 to 12.

14. An electronic device comprising:

an interface device;

a processor coupled to the interface device;

a memory coupled to the processor, the memory having stored thereon computer executable instructions which, when executed, configure the processor to perform the method of any one of claims 1 to 12.

15. The electronic device of claim 14, wherein the processor includes a trusted execution environment and wherein the computer executable instructions are executed within the trusted execution environment.