CLAIMS

What is claimed is:

1.A method, comprising:

obtaining, at a blockchain manager of a private blockchain that is associated with a master entity, a request to initiate a token transaction that includes a transfer of assignment of a crypto-token of a crypto-medium from a first entity to a second entity, wherein the private blockchain includes a blockchain record of a plurality of transactions of the crypto-medium;

maintaining, by a token database, key information associated with a plurality of entities, wherein the key information includes a first private key associated with the first entity, and wherein the token database maintains the key information such that the first private key is not accessible to a plurality of blockchain nodes used to validate the plurality of transactions of the crypto-medium;

generating, by the token database, a transaction signature for the token transaction, wherein the transaction signature includes transaction details, for the token transaction, that have been encrypted by the token database using the first private key associated with the first entity;

validating, by one or more of the plurality of blockchain nodes, the token transaction based on the transaction signature, including by:

decrypting at least a portion of the transaction signature using a first public key associated with the first entity; and

in response to the decrypting to validate the token transaction, generating, by the one or more blockchain nodes, a new block for the private blockchain, wherein the new block includes an update, to the blockchain record for the private blockchain, that indicates at least a portion of the transaction details.

2. The method of claim 1, further comprising:

mining a plurality of crypto-tokens at an initialization of the private blockchain; and

storing assignment of the plurality of crypto-tokens in a master wallet at the initialization of the private blockchain, wherein the token transaction is a first token transaction of the crypto-medium that occurs after initialization of the private blockchain.

3. The method of claim 1, further comprising:

detecting that the token database has been corrupted; and

in response to the detecting, reconstructing data stored in the token database using the private blockchain by sequentially moving a series of blocks of the private blockchain.

4. The method of claim 3, wherein the reconstructed data includes one or more data portions selected from a list of data portions consisting of: a first token balance of a first wallet of the first entity stored on the token database and a second token balance of a second wallet of the second entity stored on the token database.

5. The method of claim 1, wherein the new block for the private blockchain includes the token transaction and no other token transactions.

6. The method of claim 1, further comprising:

applying a hash function to the new block to generate a hash based on the new block of the private blockchain;

communicating the hash to a public blockchain such that the hash is included in the public blockchain; and

validating the private blockchain based on the hash as included in the public blockchain.

7. The method of claim 6, wherein applying the hash function to the new block includes applying the hash function to the new block and one or more other blocks of the private blockchain.

8. The method of claim 6, wherein applying the hash function to the new block includes applying the hash function only to the new block.

9. The method of claim 6, further comprising:

generating a smart contract that is used by the public blockchain in which the smart contract includes the hash,

wherein communicating the hash to the public blockchain includes communicating the smart contract to the public blockchain.

10. The method of claim 1, further comprising:

in response to detecting that the private blockchain is corrupted, reconstructing the private blockchain, including by sequentially recreating each block of the private blockchain based on each transaction starting from an earliest transaction in which a new block is created for each transaction.

11. A system, comprising:

a token database configured to store:

a database record related to transactions conducted with respect to a crypto-medium associated with a private blockchain, wherein the private blockchain is associated with a master entity and includes a blockchain record of a plurality of transactions of the crypto-medium; and

a first wallet of a first entity, wherein the first wallet includes a first private key of the first entity, a first public key of the first entity, and a first token balance of crypto-tokens of the crypto-medium owned by the first entity, wherein the token database maintains the first wallet such that the first private key is not accessible to a plurality of blockchain nodes used to validate the plurality of transactions of the crypto-medium;

one or more processors; and

one or more non-transitory, computer-readable media containing instructions which, when executed by the one or more processors, cause the system to perform operations comprising:

obtaining a request to initiate a token transaction that includes a transfer of assignment of a crypto-token from the first entity to a second entity;

generating, by the token database, a transaction signature for the token transaction, including by encrypting, using the first private key of the first entity, transaction details that indicate the transfer of assignment of the crypto-token from the first entity to the second entity;

validating, by one or more of the plurality of blockchain nodes, the token transaction using the transaction signature, including by decrypting at least a portion of the transaction signature using the first public key of the first entity; and

subsequent to the decrypting to validate the token transaction, generating a new block for the private blockchain, wherein the new block includes an update, to the blockchain record, that indicates the transaction details.

12. The system of claim 11, wherein the operations further comprise:

obtaining, from at least one of the one or more blockchain nodes, confirmation of the validation of the token transaction; and

directing the token database to update the database record based on the updated blockchain record in response to obtaining confirmation of the validation of the token transaction.

13. The system of claim 11, wherein the operations further comprise:

mining a plurality of crypto-tokens at an initialization of the private blockchain; and

storing assignment of the plurality of crypto-tokens in a master wallet at initialization of the private blockchain, wherein the first wallet is the master wallet and the token transaction is a first token transaction of the crypto-medium that occurs after initialization of the private blockchain.

14. The system of claim 11, wherein the operations further comprise:

applying a hash function to the new block to generate a hash based on the new block of the private blockchain;

communicating the hash to a public blockchain such that the hash is included in the public blockchain; and

validating the private blockchain based on the hash as included in the public blockchain.

15. The system of claim 14, wherein applying the hash function to the new block includes applying the hash function to the new block and one or more other blocks of the private blockchain.

16. The system of claim 14, wherein the new block for the private blockchain includes the token transaction and no other token transactions.

17. One or more non-transitory, computer-readable media including instructions which, when executed by one or more processors, cause a system to perform operations comprising:

obtaining, for a private blockchain that is associated with a master entity, a request to initiate a token transaction that includes a transfer of assignment of a crypto-token of a crypto-medium from a first entity to a second entity, wherein the private blockchain includes a blockchain record of a plurality of transactions of the crypto-medium;

maintaining, by a token database of the system, key information associated with a plurality of entities, wherein, for the first entity, the key information includes:

a first public key that is accessible to a plurality of blockchain nodes used to validate the plurality of transactions of the crypto-medium; and

a first private key that is accessible only by the token database;

generating, by the token database, a transaction signature for the token transaction, including by encrypting, using the first private key of the first entity, transaction details associated with the transfer of assignment of the crypto-token from the first entity to the second entity;

validating, by one or more of the plurality of blockchain nodes, the token transaction based on the transaction signature, including by decrypting at least a portion of the transaction signature using the first public key of the first entity; and

in response to the decrypting to validate the token transaction, generating, by the one or more blockchain nodes, a new block for the private blockchain, wherein the new block includes an update, to the blockchain record, that indicates at least a portion of the transaction details.

18. The computer-readable media of claim 17, wherein the operations further comprise:

mining a plurality of crypto-tokens at an initialization of the private blockchain; and

storing assignment of the plurality of crypto-tokens in a master wallet at initialization of the private blockchain, wherein the token transaction is a first token transaction of the crypto-medium that occurs after the initialization of the private blockchain.

19. The method of claim 1, wherein the generating the new block does not require the one or more blockchain nodes to perform a proof-of-work consensus operation; and wherein the plurality of transactions of the crypto-medium are each represented in the private blockchain using separate blocks.

20. The computer-readable media of claim 17, wherein the new block for the private blockchain includes the token transaction and no other token transactions.