

Claims

1. A method, comprising:
 - generating, via a processor, a bill of materials (BOM) smart contract including a representation of a plurality of dependencies, each dependency from the plurality of dependencies being associated with an assertion token from a plurality of assertion tokens;
 - transmitting, via the processor and to a distributed ledger, smart contract code for a country of origin (COO) smart contract that references the BOM smart contract;
 - receiving, via the processor, from a plurality of remote compute devices, and in response to deploying the COO smart contract, a representation of the plurality of assertion tokens;
 - minting, via the processor, in response to receiving the representation of the plurality of assertion tokens and based on the COO smart contract, a certificate of origin (CO) token; and
 - causing an ownership transfer of the CO token to a recipient, using the distributed ledger, by invoking a function of the COO smart contract.
2. The method of claim 1, wherein the CO token is a non-fungible token (NFT).
3. The method of claim 1, wherein the COO smart contract is associated with a good, the plurality of remote compute devices includes a plurality of supplier compute devices, and the recipient compute device is a compute device of a customer of the good.
4. The method of claim 1, further comprising storing, in a memory operably coupled to the processor, a representation of an association between the BOM smart contract and the COO smart contract.
5. The method of claim 1, further comprising validating the received representation of the plurality of assertion tokens, the minting being further in response to the validating.

6. The method of claim 1, wherein the COO smart contract includes a template configured to provide information accessed during the minting of the CO token.
7. The method of claim 1, wherein the minting is performed further in response to determining that the received representation of the plurality of assertion tokens satisfies the plurality of dependencies.
8. The method of claim 1, further comprising registering at least one dependency from the plurality of dependencies in a public registry that is subsequently audited, without revealing an identity of any party associated with the at least one dependency from the plurality of dependencies.
9. The method of claim 1, further comprising generating a zero-knowledge proof (ZKP) to validate the ownership transfer without revealing to third parties (1) an identity of a current owner of the CO token, (2) an identity of a previous owner of the CO token, or (3) content of the CO token.
10. The method of claim 1, wherein the plurality of assertion tokens includes at least one blanket token.
11. The method of claim 1, wherein the plurality of assertion tokens includes at least one shipment assertion token.
12. A method, comprising:
 - generating, via a processor, a first smart contract including a representation of a plurality of rules, each rule from the plurality of rules referencing an assertion token from a first plurality of assertion tokens;
 - transmitting, via the processor and to a distributed ledger, smart contract code for a second smart contract that references the first smart contract;
 - receiving, via the processor, from a plurality of remote compute devices, and in response to deploying the second smart contract, a representation of a second plurality of assertion tokens;
 - determining whether the second plurality of assertion tokens satisfies the plurality of rules;

in response to determining that the second plurality of assertion tokens satisfies the plurality of rules:

minting, via the processor, and based on the second smart contract, a certificate of origin (CO) token, and

causing a transfer of ownership of the CO token to a recipient by invoking a function of the second smart contract; and

in response to determining that the second plurality of assertion tokens does not satisfy at least one rule from the plurality of rules, sending a rejection message to at least one remote compute device from the plurality of remote compute devices.

13. The method of claim 12, wherein the CO token is a non-fungible token (NFT).

14. The method of claim 12, wherein the second smart contract is associated with a good, the plurality of remote compute devices includes a plurality of supplier compute devices, and the recipient compute device is a compute device of a customer of the good.

15. The method of claim 12, wherein the second smart contract includes a template configured to provide information accessed during the minting of the CO token.

16. The method of claim 12, further comprising registering at least one rule from the plurality of rules in a public registry that is subsequently audited, without revealing an identity of any party associated with the at least one rule from the plurality of rules.

17. The method of claim 12, further comprising generating a zero-knowledge proof (ZKP) to validate the transfer of ownership without revealing to third parties (1) an identity of a current owner of the CO token, (2) an identity of a previous owner of the CO token, or (3) content of the CO token.

18. The method of claim 12, wherein the second plurality of assertion tokens includes at least one blanket token.

19. The method of claim 18, wherein the at least one blanket token includes a representation of a plurality of purchase orders.

20. The method of claim 12, wherein the second plurality of assertion tokens includes at least one shipment assertion token.