

INTELLIGENT ASSERTION TOKENS FOR AUTHENTICATING AND CONTROLLING NETWORK COMMUNICATIONS USING A DISTRIBUTED LEDGER

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority to and the benefit of U.S. Provisional Patent Application No. 63/010,598, filed April 15, 2020 and titled “Systems and Methods for Authenticating and Controlling Network Communications to Transfer Tokenized Trade-Related Assertions Via a Distributed Ledger,” the content of which is incorporated by reference herein in its entirety.

TECHNICAL FIELD

[0002] The present disclosure generally relates to authenticating and controlling network communications involving intelligent tokens on a distributed ledger such as a blockchain, within a digital processing system.

BACKGROUND

[0003] In a distributed ledger context, transaction speed can be defined as the rate at which data is transferred from one account to another. Distributed ledger transaction speeds can depend on a variety of factors, such as block size, block time, traffic on the network, and transaction fees. In some known distributed ledger systems, as the number of transactions increases, the transaction speed can be negatively impacted due to transaction delays and the placement of transactions into a pending, or “queued,” state. Moreover, fluctuations in transaction speed can result in poor consistency (and high variability / unpredictability) in the performance of the distributed ledger system. Such issues are slowing the widespread adoption of distributed ledger platforms. As such, methods for reducing network traffic, increasing transaction speeds, and improving the overall predictability of a distributed ledger system are desirable.

SUMMARY

[0003a] In an aspect, the present disclosure refers to a method, comprising:
generating, via a processor, a bill of materials (BOM) representation associated with a BOM indicating at least one good and including a representation of a plurality of dependencies to

qualify the at least one good for at least one of a regulatory claim, a duty benefit claim or an admissibility claim, each dependency from the plurality of dependencies being associated with an assertion token from a plurality of assertion tokens that indicate the at least one good is qualified for at least one of the regulatory claim, the duty benefit claim or the admissibility claim;

transmitting, via the processor and to a distributed ledger, smart contract code for a compliance declaration smart contract that references the BOM representation;

receiving, via the processor, from a plurality of remote compute devices, and in response to deploying the compliance declaration 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 compliance declaration smart contract, a compliance declaration token that indicates the plurality of dependencies are satisfied and the at least one good is qualified for at least one of the regulatory claim, the duty benefit claim or the admissibility claim; and

causing, via the processor, an ownership transfer of the compliance declaration token to a recipient, using the distributed ledger, by invoking a function of the compliance declaration smart contract.

[0003b] In another aspect, the present disclosure refers to a non-transitory processor-readable medium storing code representing processor-executable instructions to cause the one or more processors to:

generate, via a processor, a first smart contract including a representation of a plurality of rules to qualify for at least one of a regulatory claim, a duty benefit claim or an admissibility claim, each rule from the plurality of rules referencing an assertion token from a first plurality of assertion tokens that indicate qualifications for at least one of the regulatory claim, the duty benefit claim or admissibility claim are met;

transmit, via the processor and to a distributed ledger, smart contract code for a second smart contract that references the first smart contract;

receive, 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;

verify, via the processor, that the second plurality of assertion tokens satisfies the plurality of rules;

mint, via the processor, and based on the second smart contract, a compliance declaration token that indicates the plurality of rules are satisfied and the qualifications for at least one of the regulatory claim, the duty benefit claim or the admissibility claim are met; and cause, via the processor, a transfer of ownership of the compliance declaration token to a recipient by invoking a function of the second smart contract.

[0003c] In another aspect, the present disclosure refers to an apparatus, comprising:

- a processor; and

- a memory coupled to the processor, the memory storing code to cause the processor to:

- generate a first smart contract including a representation of a plurality of rules to qualify for a regulatory claim, each rule from the plurality of rules referencing an assertion token from a first plurality of assertion tokens that indicate qualifications for the regulatory claim is met;
- transmit, to a distributed ledger, smart contract code for a second smart contract that references the first smart contract;

- receive 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;

- verify that the second plurality of assertion tokens satisfies the plurality of rules;

- mint, based on the second smart contract, a compliance declaration token that indicates the plurality of rules are satisfied and the qualifications for at least one of the regulatory claim, the duty benefit claim or the admissibility claim are met; and

- cause a transfer of ownership of the compliance declaration token to a recipient by invoking a function of the second smart contract.

[0004] In an example, a method for generating assertion intelligent tokens (also referred to as “security tokens” or “assertion tokens”; hereinafter “tokens”) at multiple steps within a supply chain includes generating a first assertion token, in advance of and/or during a first step of a supply chain process. The generation of tokens can be based on a Country of Origin (COO) assertion,

a compliance declaration (also referred to herein as a non-COO assertion), a Bill of Materials (BOM), and/or duty/tariff rules. The first assertion token is transmitted or transferred to a receiving party, and the receiving party can inspect it to determine validity and/or applicability. If the first assertion token is not valid or applicable, the transfer transaction of the first assertion token is rejected. If the first assertion token is determined to be valid, the receiving party can approve the use of the first assertion token. The first assertion token can be passed to a second step of the supply chain process, and a second assertion token may be generated based on the first assertion token and transmitted or transferred to a second receiver. The second assertion token is inspected to determine validity and/or applicability. If the second assertion token is determined to be not valid or applicable, the transfer of the second assertion token is rejected. If the second assertion token is determined to be valid, a further transmission and/or transaction based on the second assertion token to a further step of the supply chain process or to an end consumer is authorized.

[0005] In some examples, a method for authenticating a network communication referencing a transaction of a good within a supply chain includes representing qualifications for one or more duty benefits as a set of dependencies on assertions made by one or more producers, exporters and/or suppliers. The assertions include assertions about attributes of goods, such as country of origin or admissibility (such as "no forced labor"). The assertions are tokenized on a distributed ledger such as a blockchain network, and the assertion tokens can reference one or more documents. One or more claims for the admissibility and/or duty benefit(s) are validated or invalidated based on the flow of the tokenized assertions. The assertions can include one or more claims (i.e., qualifies for reduced duties or tariffs on the goods, and/or produced without forced labor).

BRIEF DESCRIPTION OF THE DRAWINGS

[0006] FIG. 1 is a system diagram illustrating a system for transacting Certificate of Origin (CO) tokens, according to some embodiments.

[0007] FIG. 2A is a flow diagram showing a method for generating assertion tokens at multiple steps within a supply chain, according to some embodiments.

[0008] FIG. 2B is a flow diagram showing a method for generating CO tokens, according to some embodiments.

[0009] FIG. 3 is a flow diagram showing a multi-tiered supply chain use of COO contracts, BOM contracts, BOMs and CO tokens, according to some embodiments.

Claims

1. A method, comprising:
 - generating, via a processor, a bill of materials (BOM) representation associated with a BOM indicating at least one good and including a representation of a plurality of dependencies to qualify the at least one good for at least one of a regulatory claim, a duty benefit claim or an admissibility claim, each dependency from the plurality of dependencies being associated with an assertion token from a plurality of assertion tokens that indicate the at least one good is qualified for at least one of the regulatory claim, the duty benefit claim or the admissibility claim;
 - transmitting, via the processor and to a distributed ledger, smart contract code for a compliance declaration smart contract that references the BOM representation;
 - receiving, via the processor, from a plurality of remote compute devices, and in response to deploying the compliance declaration 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 compliance declaration smart contract, a compliance declaration token that indicates the plurality of dependencies are satisfied and the at least one good is qualified for at least one of the regulatory claim, the duty benefit claim or the admissibility claim; and
 - causing, via the processor, an ownership transfer of the compliance declaration token to a recipient, using the distributed ledger, by invoking a function of the compliance declaration smart contract.
2. The method of claim 1, wherein the compliance declaration token is a non-fungible token (NFT).
3. The method of claim 1, wherein the compliance declaration smart contract is associated with the at least one 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 at least one 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 representation and the compliance declaration 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 compliance declaration smart contract includes a template configured to provide information accessed during the minting of the compliance declaration 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 compliance declaration token, (2) an identity of a previous owner of the compliance declaration token, or (3) content of the compliance declaration token.
10. The method of claim 1, wherein the BOM representation is a smart contract.
11. The method of claim 1, wherein the BOM representation is a hash of an electronic version of the BOM.

12. The method of claim 1, wherein the BOM representation is a hash of a scanned image of the BOM.

13. The method of claim 1, wherein at least one assertion token from the plurality of assertion tokens is associated with a blanket period, the token is valid from a start date to an end date of the blanket period.

14. The method of claim 1, wherein at least one assertion token from the plurality of assertion token is associated with a specific shipment of goods referenced by that assertion token.

15. The method of claim 1, wherein at least one assertion token from the plurality of assertion tokens is associated with results of a certification or an audit by a third party.

16. A non-transitory processor-readable medium storing code representing processor-executable instructions to cause the one or more processors to:

generate, via a processor, a first smart contract including a representation of a plurality of rules to qualify for at least one of a regulatory claim, a duty benefit claim or an admissibility claim, each rule from the plurality of rules referencing an assertion token from a first plurality of assertion tokens that indicate qualifications for at least one of the regulatory claim, the duty benefit claim or admissibility claim are met;

transmit, via the processor and to a distributed ledger, smart contract code for a second smart contract that references the first smart contract;

receive, 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;

verify, via the processor, that the second plurality of assertion tokens satisfies the plurality of rules;

mint, via the processor, and based on the second smart contract, a compliance declaration token that indicates the plurality of rules are satisfied and the qualifications

for at least one of the regulatory claim, the duty benefit claim or the admissibility claim are met; and

cause, via the processor, a transfer of ownership of the compliance declaration token to a recipient by invoking a function of the second smart contract.

17. The processor-readable medium of claim 16, wherein the compliance declaration token is a non-fungible token (NFT).

18. The processor-readable medium of claim 16, 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.

19. The processor-readable medium of claim 16, wherein the second smart contract includes a template configured to provide information accessed during the minting of the compliance declaration token.

20. The processor-readable medium of claim 16, 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.

21. The processor-readable medium of claim 16, wherein the code further comprising code to:

generate a zero-knowledge proof (ZKP) to validate the transfer of ownership without revealing to third parties (1) an identify of a current owner of the compliance declaration token, (2) an identity of a previous owner of the compliance declaration token, or (3) content of the compliance declaration token.

22. An apparatus, comprising:
a processor; and

a memory coupled to the processor, the memory storing code to cause the processor to:

generate a first smart contract including a representation of a plurality of rules to qualify for a regulatory claim, each rule from the plurality of rules referencing an assertion token from a first plurality of assertion tokens that indicate qualifications for the regulatory claim is met;

transmit, to a distributed ledger, smart contract code for a second smart contract that references the first smart contract;

receive 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;

verify that the second plurality of assertion tokens satisfies the plurality of rules;

mint, based on the second smart contract, a compliance declaration token that indicates the plurality of rules are satisfied and the qualifications for at least one of the regulatory claim, the duty benefit claim or the admissibility claim are met; and

cause a transfer of ownership of the compliance declaration token to a recipient by invoking a function of the second smart contract.

23. The apparatus of claim 22, wherein the regulatory claim relates to at least one of (1) qualifying a good for a reduced duty or a reduced tariff, or (2) validating a tariff or a customs regulation.

24. The apparatus of claim 22, wherein the regulatory claim relates to an average labor cost for producing a good being at least a predefined value.

25. The apparatus of claim 22, wherein the regulatory claim relates to declaring no child labor or no forced labor was used in production of a good.

26. The apparatus of claim 22, wherein the regulatory claim relates to a declaration for regulated material.