

CLAIMS:

- ~~1. A computer implemented method for verifiable claim issuance, comprising:
receiving, from a first entity, a request for creating a verifiable claim (VC) for a decentralized identifier (DID) associated with a second entity;
obtaining, in response to receiving the request, a digital signature associated with the first entity; and
generating the VC based on the received request and the obtained digital signature.~~
- ~~2. The method of claim 1, wherein the receiving a request for creating a VC for a DID associated with a second entity comprises:
obtaining an account identifier associated with a second entity from the request; and
identifying the DID based on a pre-stored mapping relationship between the account identifier and the DID.~~
- ~~3. The method of any of the preceding claims, further comprising:
uploading the VC to a service endpoint associated with the DID.~~
- ~~4. The method of claim 3, wherein the uploading the VC to a service endpoint associated with the DID comprises:
sending a blockchain transaction to a blockchain node for adding to a blockchain, wherein the blockchain transaction comprises information associated with the DID and is for retrieving a DID document corresponding to the DID;
obtaining the DID document from the blockchain; and
determining the service endpoint associated with the DID based on the DID document.~~
- ~~5. The method of any of the claims 3-4, wherein the service endpoint is associated with a blockchain.~~
- ~~6. The method of claim 5, wherein the uploading the VC to the service endpoint comprises:
sending, to a blockchain node of the blockchain associated with the service endpoint, a blockchain transaction for adding information associated with the VC to the blockchain associated with the service endpoint.~~

~~7. The method of claim 6, wherein the blockchain transaction invokes a blockchain contract for managing VCs.~~

~~8. The method of any of the preceding claims, wherein the obtaining a digital signature associated with the first entity comprises:~~
~~determining, based on the received request, a key alias associated with the first entity;~~
~~sending a request to a key management system (KMS) for the digital signature associated with the first entity, the request comprising the key alias; and~~
~~receiving the digital signature from the KMS.~~

~~9. The method of any of the claims 1-7, wherein the obtaining a digital signature associated with the first entity comprises:~~
~~obtaining a message from the received request;~~
~~creating an un-signed VC based at least in part on the message;~~
~~determining a hash value of the un-signed VC;~~
~~sending a request to a key management system (KMS) for the digital signature, the request comprising the hash value; and~~
~~receiving the digital signature from the KMS.~~

~~10. The method of any of the claims 1-8, wherein the received request comprises an encrypted message, and wherein the generating the VC comprises generating the VC based on the encrypted message.~~

~~11. The method of any of the preceding claims, wherein:~~
~~the generated VC comprises a claim corresponding to real-name authentication of the second entity.~~

~~12. The method of any of the preceding claims, further comprising:~~
~~storing the generated VC and a status associated with the generated VC.~~

~~13. The method of any of the preceding claims, further comprising:~~

sending the generated VC and a status associated with the generated VC to an online agent accessible to the second entity via an application programming interface (API) for storing.

14. The method of any of the preceding claims, further comprising:
sending a success message to the first entity, the success message comprising the generated VC.

15. A system for verifiable claim issuance, comprising:
one or more processors; and
one or more computer readable memories coupled to the one or more processors and having instructions stored thereon that are executable by the one or more processors to perform the method of any of claims 1 to 14.

16. A non-transitory computer readable storage medium configured with instructions executable by one or more processors to cause the one or more processors to perform the method of any of claims 1 to 14.

17. An apparatus for verifiable claim issuance comprising a plurality of modules for performing the method of any of claims 1 to 14.

CLAIMS:

1. A computer-implemented method for verifiable-claim issuance, comprising:
receiving, from a first entity, a request for creating a verifiable claim, VC, for a
decentralized identifier, DID, associated with a second entity;
obtaining, in response to receiving the request, a digital signature associated with the
first entity; and
generating the VC based on the received request and the obtained digital signature,
characterized by:
sending a blockchain transaction to a blockchain node for adding to a blockchain,
wherein the blockchain transaction comprises information associated with the DID and is for
retrieving a DID document corresponding to the DID;
obtaining the DID document from the blockchain; and
determining a service endpoint associated with the DID based on the DID document;
and
uploading the VC to the service endpoint associated with the DID.
2. The method of claim 1, wherein the receiving a request for creating a VC for a DID
associated with a second entity comprises:
obtaining an account identifier associated with a second entity from the request; and
identifying the DID based on a pre-stored mapping relationship between the account
identifier and the DID.
3. The method of claim 1, wherein the service endpoint is associated with a blockchain.
4. The method of claim 3, wherein the uploading the VC to the service endpoint
comprises:
sending, to a blockchain node of the blockchain associated with the service endpoint,
a blockchain transaction for adding information associated with the VC to the blockchain
associated with the service endpoint.
5. The method of claim 4, wherein the blockchain transaction invokes a blockchain
contract for managing VCs.

6. The method of any of the preceding claims, wherein the obtaining a digital signature associated with the first entity comprises:
determining, based on the received request, a key alias associated with the first entity;
sending a request to a key management system, KMS, for the digital signature associated with the first entity, the request comprising the key alias; and
receiving the digital signature from the KMS.
7. The method of any of the claims 1 to 5, wherein the obtaining a digital signature associated with the first entity comprises:
obtaining a message from the received request;
creating an un-signed VC based at least in part on the message;
determining a hash value of the un-signed VC;
sending a request to a key management system, KMS, for the digital signature, the request comprising the hash value; and
receiving the digital signature from the KMS.
8. The method of any of the claims 1 to 6, wherein the received request comprises an encrypted message, and wherein the generating the VC comprises generating the VC based on the encrypted message.
9. The method of any of the preceding claims, wherein:
the generated VC comprises a claim corresponding to real-name authentication of the second entity.
10. The method of any of the preceding claims, further comprising:
storing the generated VC and a status associated with the generated VC.
11. The method of any of the preceding claims, further comprising:
sending the generated VC and a status associated with the generated VC to an online agent accessible to the second entity via an application programming interface, API, for storing.
12. The method of any of the preceding claims, further comprising:

_____ sending a success message to the first entity, the success message comprising the generated VC.

13. A system for verifiable-claim issuance, comprising:

_____ one or more processors; and

_____ one or more computer-readable memories coupled to the one or more processors and having instructions stored thereon that are executable by the one or more processors to perform the method of any of claims 1 to 12.

14. A non-transitory computer-readable storage medium configured with instructions executable by one or more processors to cause the one or more processors to perform the method of any of claims 1 to 12.