

**CLAIMS:**

1. A computer-implemented method for claim verification, comprising:  
receiving, from a first entity, a request for verifying a verifiable claim (VC) that comprises a digital signature;  
obtaining, based on the VC, a public key associated with a second entity;  
determining that the digital signature is created based on a private key associated with the public key; and  
verifying the VC based on the determination.
2. The method of claim 1, wherein the obtaining a public key associated with a second entity comprises:  
identifying the second entity based on an identifier in the VC.
3. The method of claim 2, wherein the identifier is a decentralized identifier (DID), and wherein the obtaining a public key associated with a second entity comprises:  
sending, to a blockchain node of a blockchain, a blockchain transaction comprising information associated with the DID, wherein the blockchain transaction is for retrieving a DID document corresponding to the DID;  
obtaining the DID document from the blockchain; and  
retrieving a public key from the DID document.
4. The method of claim 3, wherein the blockchain transaction invokes a blockchain contract for managing relationships between DIDs and DID documents.
5. The method of any of the preceding claims, further comprising:  
obtaining a status of the VC; and  
determining that the status of the VC is valid.
6. The method of claim 5, wherein the obtaining a status of the VC comprises:  
obtaining the status from a blockchain storing information associated with a plurality of VCs.

7. The method of claim 6, wherein the determining that the status of the VC is valid comprises:

- obtaining a first hash value associated with the VC along with the status of the VC;
- determining a second hash value by applying a hash function on the VC; and
- authenticating the status of the VC by comparing the first hash value with the second hash value.

8. The method of claim 7, wherein the obtaining a first hash value associated with the VC along with the status of the VC comprises:

- sending, to a blockchain node of the blockchain, a blockchain transaction for retrieving the first hash value and the status, the blockchain transaction comprising the DID associated with the subject of the VC.

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

- receiving, from the first entity, an account identifier associated with a subject of the VC;
- obtaining a DID associated with the subject of the VC based on a pre-stored mapping relationship between the account identifier and the DID;
- obtaining a DID document associated with the DID;
- obtaining information associated with a service endpoint for managing VCs from the DID document; and
- obtaining the VC from the service endpoint.

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

- sending a message to the first entity confirming that the VC is verified.

11. The method of any of the preceding claims, wherein the verifying the VC comprises:

- obtaining, from the VC, an issuance date of the VC; and
- validating the obtained issuance date based on a comparison between the obtained issuance date and a current date.

12. The method of any of the preceding claims, wherein the verifying the VC comprises:

obtaining, from the VC, an expiration date of the VC; and  
validating that the VC has not expired based on the expiration date and a current date.

13. A system for verifiable-claim verification, 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.

15. An apparatus for verifiable-claim verification comprising a plurality of modules  
for performing the method of any of claims 1 to 12.