

## CLAIMS

1. A computer-implemented method, comprising acts of:  
using a pointer to access from a distributed ledger system, at least one attestation for at  
5 least one attribute of an identity owner, wherein:  
the at least one attestation is movable between at least two states in the  
distributed ledger system, the at least two states including a VERIFIED state, and  
the at least one attestation comprises a cryptographic proof;  
receiving a value corresponding to the at least one attribute; and  
10 determining whether the at least one attestation for the at least one attribute is in the  
VERIFIED state;  
determining whether to trust an entity indicated as being responsible for verifying the at  
least one attestation;  
determining whether the cryptographic proof in the at least one attestation is a valid  
15 proof of the received value corresponding to the at least one attribute;  
determining whether the at least one attestation is electronically signed by the entity  
indicated as being responsible for verifying the at least one attestation; and  
in response to determining that the at least one attestation is in the VERIFIED state, that  
the entity indicated as being responsible for verifying the at least one attestation is to be trusted,  
20 that the cryptographic proof is a valid proof of the received value, and that the at least one  
attestation is electronically signed by the entity responsible for verifying the at least one  
attestation:  
proceeding with a transaction with the identity owner.
- 25 2. The computer-implemented method of claim 1, wherein:  
the distributed ledger system is implemented using at least one blockchain.
3. The computer-implemented method of claim 1, wherein the at least one attestation is  
stored in a badge associated with the identity owner, and wherein the pointer includes a  
30 reference to the badge.

4. The computer-implemented method of claim 3, wherein:

the badge is generated according to a schema selected from a plurality of schemas for badges, the schema comprising a plurality of attributes, the plurality of attributes comprising the at least one attribute.

5

5. The computer-implemented method of claim 1, wherein the at least two states of the at least one attestation include a PENDING state, and wherein the method further comprises an act of:

causing the at least one attestation to transition from the PENDING state to the  
10 VERIFIED state when the value corresponding to the at least one attribute has been verified by the entity indicated as being responsible for verifying the at least one attestation.

6. The computer-implemented method of claim 1, wherein the at least two states of the at least one attestation include an EXPIRED state, and wherein the method further comprises an  
15 act of:

causing the at least one attestation to transition from the VERIFIED state to the EXPIRED state after expiration of a timer that was set when the value corresponding to the at least one attribute was last verified.

20 7. The computer-implemented method of claim 1, wherein:

access to the cryptographic proof in the at least one attestation is allowed only if the at least one attestation is in the VERIFIED state.

8. The computer-implemented method of claim 1, wherein the identity owner is a user.

25

9. The computer-implemented method of claim 1, wherein the at least one attestation is accessed from a digital identity representation stored in the distributed ledger, and wherein the digital identity representation is associated with the identity owner and includes program code that implements rules for attestation.

30

10. The computer-implemented method of claim 1, wherein the value corresponding to the at least one attribute is received via a channel outside the distributed ledger.

11. A computer system, comprising:

at least one processor; and

at least one non-transitory computer-readable medium having stored thereon, a plurality of instructions that, when executed by the at least one processor, cause the at least one processor to:

use a pointer to access from a distributed ledger system, at least one attestation for at least one attribute of an identity owner, wherein:

the at least one attestation is movable between at least two states in the distributed ledger system, the at least two states including a VERIFIED state, and

the at least one attestation comprises a cryptographic proof;

receive a value corresponding to the at least one attribute; and

determine whether the at least one attestation for the at least one attribute is in the VERIFIED state;

determine whether to trust an entity indicated as being responsible for verifying the at least one attestation;

determine whether the cryptographic proof in the at least one attestation is a valid proof of the received value corresponding to the at least one attribute;

determine whether the at least one attestation is electronically signed by the entity indicated as being responsible for verifying the at least one attestation; and

in response to determining that the at least one attestation is in the VERIFIED state, that the entity indicated as being responsible for verifying the at least one attestation is to be trusted, that the cryptographic proof is a valid proof of the received value, and that the at least one attestation is electronically signed by the entity responsible for verifying the at least one attestation:

proceed with a transaction with the identity owner.

12. The computer system of claim 11, wherein:

the distributed ledger system is implemented using at least one blockchain.

13. The computer system of claim 11, wherein the at least one attestation is stored in a badge associated with the identity owner, and wherein the pointer includes a reference to the badge.

14. The computer system of claim 13, wherein:

the badge is generated according to a schema selected from a plurality of schemas for badges, the schema comprising a plurality of attributes, the plurality of attributes comprising the at least one attribute.

15. The computer system of claim 11, wherein the at least two states of the at least one attestation include a PENDING state, and wherein the plurality of instructions, when executed by the at least one processor, further cause the at least one processor to:

cause the at least one attestation to transition from the PENDING state to the VERIFIED state when the value corresponding to the at least one attribute has been verified by the entity indicated as being responsible for verifying the at least one attestation.

16. The computer system of claim 11, wherein the at least two states of the at least one attestation include an EXPIRED state, and wherein the plurality of instructions, when executed by the at least one processor, further cause the at least one processor to:

cause the at least one attestation to transition from the VERIFIED state to the EXPIRED state after expiration of a timer that was set when the value corresponding to the at least one attribute was last verified.

17. The computer system of claim 11, wherein:

access to the cryptographic proof in the at least one attestation is allowed only if the at least one attestation is in the VERIFIED state.

18. The computer system of claim 11, wherein the identity owner is a user.

19. The computer system of claim 11, wherein the at least one attestation is accessed from a digital identity representation stored in the distributed ledger, and wherein the digital identity representation is associated with the identity owner and includes program code that implements rules for attestation.

5

20. The computer system of claim 11, wherein the value corresponding to the at least one attribute is received via a channel outside the distributed ledger.

21. A non-transitory computer-readable medium encoded with a plurality of instructions  
10 that, when executed by at least one processor, perform a method comprising:  
    using a pointer to access from a distributed ledger system, at least one attestation for at  
least one attribute of an identity owner, wherein:  
        the at least one attestation is movable between at least two states in the  
distributed ledger system, the at least two states including a VERIFIED state, and  
15       the at least one attestation comprises a cryptographic proof;  
        receiving a value corresponding to the at least one attribute; and  
        determining whether the at least one attestation for the at least one attribute is in the  
VERIFIED state;  
        determining whether to trust an entity indicated as being responsible for verifying the at  
20 least one attestation;  
        determining whether the cryptographic proof in the at least one attestation is a valid  
proof of the received value corresponding to the at least one attribute;  
        determining whether the at least one attestation is electronically signed by the entity  
indicated as being responsible for verifying the at least one attestation; and  
25       in response to determining that the at least one attestation is in the VERIFIED state, that  
the entity indicated as being responsible for verifying the at least one attestation is to be trusted,  
that the cryptographic proof is a valid proof of the received value, and that the at least one  
attestation is electronically signed by the entity responsible for verifying the at least one  
attestation:  
30       proceeding with a transaction with the identity owner.

22. The non-transitory computer-readable medium of claim 21, wherein:  
the distributed ledger system is implemented using at least one blockchain.

23. The non-transitory computer-readable medium of claim 21, wherein the at least one  
attestation is stored in a badge associated with the identity owner, and wherein the pointer  
includes a reference to the badge.

24. The non-transitory computer-readable medium of claim 23, wherein:  
the badge is generated according to a schema selected from a plurality of schemas for  
badges, the schema comprising a plurality of attributes, the plurality of attributes comprising  
the at least one attribute.

25. The non-transitory computer-readable medium of claim 21, wherein the at least two  
states of the at least one attestation include a PENDING state, and wherein the method further  
comprises an act of:

causing the at least one attestation to transition from the PENDING state to the  
VERIFIED state when the value corresponding to the at least one attribute has been verified by  
the entity indicated as being responsible for verifying the at least one attestation.

26. The non-transitory computer-readable medium of claim 21, wherein the at least two  
states of the at least one attestation include an EXPIRED state, and wherein the method further  
comprises an act of:

causing the at least one attestation to transition from the VERIFIED state to the  
EXPIRED state after expiration of a timer that was set when the value corresponding to the at  
least one attribute was last verified.

27. The non-transitory computer-readable medium of claim 21, wherein:  
access to the cryptographic proof in the at least one attestation is allowed only if the at  
least one attestation is in the VERIFIED state.

28. The non-transitory computer-readable medium of claim 21, wherein the identity owner is a user.

29. The non-transitory computer-readable medium of claim 21, wherein the at least one  
5 attestation is accessed from a digital identity representation stored in the distributed ledger, and wherein the digital identity representation is associated with the identity owner and includes program code that implements rules for attestation.

30. The non-transitory computer-readable medium of claim 1, wherein the value  
10 corresponding to the at least one attribute is received via a channel outside the distributed ledger.