

WHAT IS CLAIMED IS:

1 1. A method comprising:
2 receiving, by a user device, a first biometric template of a user;
3 generating, by the user device, a derivative of the first biometric template;
4 generating, by the user device, an identity request message for an
5 electronic identity for the user, the identity request message comprising the derivative of
6 the first biometric template and an account identifier of the user;
7 sending, by the user device, the identity request message to a verification
8 server, wherein the verification server verifies the account identifier and generates the
9 electronic identity, and wherein the electronic identity is linked to the derivative of the
10 first biometric template in a database by a processing server computer, wherein the
11 processing server computer initiates publishing of a record to a blockchain, the record
12 comprising a record of the electronic identity and the derivative of the first biometric
13 template of the user being linked, wherein the record of the electronic identity and the
14 derivative of the first biometric template being linked is signed by the verification server
15 and the processing server computer using a digital signature encryption scheme;
16 receiving, by the user device, an identity response message comprising
17 the electronic identity;
18 storing, by the user device, the electronic identity in a memory of the user
19 device;
20 receiving, by ~~a-the~~ user device, a second biometric template of ~~a-the~~ user;
21 providing, by the user device, an authentication request message
22 comprising ~~an-the~~ electronic identity and a derivative of the second biometric template
23 of the user to a resource provider computer to conduct an interaction, the authentication
24 request message being forwarded to ~~a-the~~ processing server computer by the resource
25 provider computer; and
26 receiving, by the user device, an authentication response message
27 comprising an authentication result from the processing server computer,
28 wherein the authentication result is determined by the processing server
29 computer based on a comparison of the derivative of the second biometric template to ~~a~~
30 the derivative of ~~a-the~~ first biometric template accessible to the processing server

31 computer, and wherein the authentication result is also based on a validity of the
32 electronic identity.

1 2. ~~_____ The method of claim 1, further comprising: _____~~
2 ~~receiving, by the user device, the first biometric template of the user;~~
3 ~~generating, by the user device, the derivative of the first biometric~~
4 ~~template;~~
5 ~~generating, by the user device, an identity request message for an~~
6 ~~electronic identity for the user, the identity request message comprising the derivative of~~
7 ~~the first biometric template and an account identifier of the user;~~
8 ~~sending, by the user device, the identity request message to a verification~~
9 ~~server, wherein the verification server verifies the account identifier and generates the~~
10 ~~electronic identity, and wherein the electronic identity is linked to the derivative of the~~
11 ~~first biometric template in a database by the processing server computer;~~
12 ~~receiving, by the user device, an identity response message comprising~~
13 ~~the electronic identity; and~~
14 ~~storing, by the user device, the electronic identity in a memory of the user~~
15 ~~device for later use in an interaction.~~

1 ~~3. The method of claim 2, wherein the processing server computer~~
2 ~~initiates the publishing of a record to a blockchain, the record comprising a record of the~~
3 ~~electronic identity and the derivative of the first biometric template of the user being~~
4 ~~linked.~~

1 24. The method of claim 13, wherein the validity of the electronic
2 identity is based at least upon the record published on the blockchain of the electronic
3 identity and the derivative of the first biometric template of the user being linked.

1 ~~5. The method of claim 3, wherein the record of the electronic identity~~
2 ~~and the derivative of the first biometric template being linked is signed by the verification~~
3 ~~server and the processing server computer using a digital signature encryption scheme.~~

1 36. The method of claim 15, wherein the validity of the electronic
2 identity is based at least upon ~~the~~ validation of one or more digital signatures appended
3 to the record of the electronic identity and the derivative of the first biometric template
4 being linked.

1 47. The method of claim 12, wherein the derivative of the first biometric
2 template and the derivative of the second biometric template are derived from the first
3 biometric template and the second biometric template of the user, respectively, by
4 passing the first and second biometric templates through an algorithm.

1 58. The method of claim 12, wherein the derivative of the first biometric
2 template is stored and retrieved by the processing server computer by communicating
3 with an authentication server.

1 69. A server computer comprising:
2 a network interface;
3 a processor; and
4 a non-transitory computer-readable medium comprising code for
5 instructing the processor to implement a method, the method comprising:

6 receiving, by the server computer, an identity request message
7 comprising a derivative of a first biometric template and an electronic identity,
8 wherein the electronic identity is received from a verification server after the
9 verification server verifies an account identifier of a user;

10 linking, by the server computer, the derivative of the first biometric
11 template and the electronic identity in a mapping table;

12 storing, by the server computer, the derivative of the first biometric
13 template in a database;

14 generating, by the server computer, an identity response message
15 comprising the electronic identity, wherein the identity response message is
16 received by a user device, and wherein the user device stores the electronic
17 identity in a memory of the user device for later use in an interaction,

18 initiating, by the server computer, publishing of a record to a
19 blockchain, the record comprising a record of the electronic identity and the
20 derivative of the first biometric template being linked, wherein the record on the
21 blockchain of the electronic identity and the derivative of the first biometric
22 template being linked is signed by the verification server and the server computer
23 using a digital signature encryption scheme;

24 receiving, by the server computer, an authentication request
25 message comprising ~~an~~ the electronic identity and a derivative of a second
26 biometric template of ~~a~~ the user of ~~a~~ the user device;

27 determining, by the server computer, ~~a~~ that the derivative of ~~a~~ the
28 first biometric template is linked to the electronic identity;

29 retrieving, by the server computer, the derivative of the first
30 biometric template;

31 comparing, by the server computer, the derivative of the first
32 biometric template to the derivative of the second biometric template; and

33 determining, by the server computer, an authentication result based
34 at least upon the ~~comparison~~ comparing of the derivative of the first biometric
35 template to the derivative of the second biometric template and at least upon ~~the~~
36 a validity of the electronic identity.

1 10. ~~The server computer of claim 9, wherein the method further~~
2 ~~comprises:~~
3 ~~receiving, by the server computer, an identity request message comprising~~
4 ~~the derivative of the first biometric template and the electronic identity, wherein the~~
5 ~~electronic identity is received from a verification server after the verification server~~
6 ~~verifies an account identifier of the user;~~
7 ~~linking, by the server computer, the derivative of the first biometric~~
8 ~~template and the electronic identity in a mapping table;~~
9 ~~storing, by the server computer, the derivative of the first biometric~~
10 ~~template in a database; and~~
11 ~~generating, by the server computer, an identity response message~~
12 ~~comprising the electronic identity, wherein the identity response message is received by~~
13 ~~the user device, and wherein the user device stores the electronic identity in a memory~~
14 ~~of the user device for later use in an interaction.~~

1 11. ~~The server computer of claim 10, wherein the method further~~
2 ~~comprises:~~

3 ~~initiating, by the server computer, the publishing of a record to a~~
4 ~~blockchain, the record comprising a record of the electronic identity and the derivative of~~
5 ~~the first biometric template being linked.~~

6 712. The server computer of claim 611, wherein determining the
7 authentication result based at least upon the validity of the electronic identity comprises:
8 comparing, by the server computer, the electronic identity to a record on
9 the blockchain of the electronic identity and the derivative of the first biometric template
10 being linked; and
11 validating, by the server computer, the electronic identity if the electronic
12 identity matches the record published on the blockchain.

1 ~~13. The server computer of claim 11, wherein the record on the~~
2 ~~blockchain of the electronic identity and the derivative of the first biometric template~~
3 ~~being linked is signed by the verification server and the server computer using a digital~~
4 ~~signature encryption scheme.~~

1 814. The server computer of claim 613, wherein determining the
2 authentication result based at least upon the validity of the electronic identity comprises:
3 validating, by the server computer, ~~the~~ digital signatures appended to the
4 record published on the blockchain using ~~the~~ public keys of at least the verification
5 server.

1 915. The server computer of claim 610, wherein the derivative of the first
2 biometric template and derivative of the second biometric template are derived from the
3 first biometric template and the second biometric template of the user respectively by
4 passing the first and second biometric template through an algorithm.

1 1016. The server computer of claim 610, wherein storing the derivative of
2 the first biometric template in ~~a~~ the database comprises:
3 sending, by the server computer, the derivative of the first biometric
4 template to an authentication server, wherein the authentication server stores the
5 derivative of the first biometric template in the database, and wherein retrieving the

derivative of the first biometric template comprises sending a request to the authentication server.

1117. A resource provider computer comprising:
a network interface;
a processor; and
a non-transitory computer-readable medium comprising code for instructing the processor to implement a method, the method comprising:
receiving, by the resource provider computer, an authentication request message from a user device of a user, the authentication request message comprising an electronic identity and a derivative of a second biometric template of the user, wherein the electronic identity is generated by a verification server upon verification of an account identifier of the user;
sending, by the resource provider computer, the authentication request message to a processing server computer, the processing server computer determining an authentication result based at least upon ~~the a~~ comparison of the derivative of the second biometric template to a derivative of a first biometric template and based at least upon ~~the a~~ validity of the electronic identity, wherein the validity of the electronic identity is based at least upon a record published on a blockchain of the electronic identity and the derivative of the first biometric template being linked, wherein the record published on the blockchain is signed by the verification server and the processing server computer using a digital signature encryption scheme;
receiving, by the resource provider computer, from the processing server computer, an authentication response message comprising the authentication result;
sending, by the resource provider computer, the authentication response message to the user device; and
authenticating, by the resource provider computer, the user if the authentication result indicates that the derivative of the second biometric template and the derivative of the first biometric template match, and if the authentication result indicates that the electronic identity is valid, ~~wherein the~~

30 ~~electronic identity is generated by a verification server upon verification of an~~
31 ~~account identifier of the user.~~

1 ~~18. The resource provider computer of claim 17, wherein the validity of~~
2 ~~the electronic identity is based at least upon a record published on a blockchain of the~~
3 ~~electronic identity and the derivative of the first biometric template being linked.~~

1 ~~19. The resource provider computer of claim 18, wherein the record~~
2 ~~published on the blockchain is signed by the verification server and the processing~~
3 ~~server computer.~~

1 1220. The resource provider computer of claim 1119, wherein the validity
2 of the electronic identity is based at least upon the validation of one or more digital
3 signatures appended to the record published on the blockchain.