

What is claimed is:

1. A system for providing blockchain-based multifactor personal identity verification, the system comprising:

one or more computer-readable storage media configured to store a blockchain;

a server-side computer system comprising one or more processors programmed to execute computer program instructions that, when executed, cause the server-side computer system to:

assign a verification address associated with the blockchain to an individual, the individual having a previously verified personal identity;

store, at the one or more computer-readable storage media, an identifier of the individual and a biometric hash of the individual in association with the verification address associated with the blockchain,

wherein the biometric hash is a hash of biometric data of the individual,

and

wherein each of the identifier, the biometric hash, and the verification address are different from one another and different from private and public keys from which the verification address was derived;

obtain, from a client-side device, the identifier and the biometric data in connection with a request to verify the individual's identity, the request indicating the verification address associated with the blockchain;

obtain the stored identifier and the stored biometric hash using the verification address indicated in the request; and

sign verification of the individual's identity responsive to a determination that the identifier of the request and the biometric data of the request match the stored identifier and the stored biometric hash.

2. The system of claim 1, wherein the server-side computer system is caused to: sign, using the private key from which the verification address was derived, the verification of the individual's identity responsive to the determination that the identifier of the request and the biometric data of the request match the stored identifier and the stored biometric hash.

3. The system of claim 2, wherein the server -side computer system is caused to: store, at the one or more computer-readable storage media, the private key in association with the verification address associated with the blockchain;
obtain, from the client-side device, the private key in connection with the request to verify the individual's identity;
obtain the stored private key using the verification address indicated in the request; and
sign, using the private key, the verification of the individual's identity responsive to a determination that the identifier of the request, the biometric data of the request, and the private key of the request match the stored identifier, the stored biometric hash, and the stored private key.

4. The system of claim 3, wherein the private key is also stored on the client-side device, and wherein the client-side device is a user device of the individual.

5. The system of claim 1, wherein the server-side computer system is caused to:

assign another verification address associated with the blockchain to the individual;

store, at the one or more computer-readable storage media, another biometric hash of the individual in association with the other verification address associated with the blockchain, the other biometric hash being a hash of other biometric data of the individual;

obtain, from the client-side device, the other biometric data in connection with the request to verify the individual's identity, the request further indicating the other verification address associated with the blockchain;

obtain the stored other biometric hash using the other verification address indicated in the request; and

sign the verification of the individual's identity responsive to a determination that the identifier of the request, the biometric data of the request, the other biometric data of the request match the stored identifier, the stored biometric hash, and the stored other biometric hash.

6. The system of claim 5, wherein the server-side computer system is caused to: obtain, via a user interface, a user-initiated command to add the other verification address as an address of the blockchain for the individual; and

assign the other verification address associated with the blockchain to the individual based on the user-initiated command.

7. The system of claim 5, wherein the server-side computer system is caused

to: obtain, via a user interface, a user-initiated command to remove the other verification address as an address of the blockchain for the individual; and
de-associate the other verification address associated with the blockchain from the individual based on the user-initiated command.

8. The system of claim 1, wherein the server-side computer system is caused to: provide a first user, different than the individual, access to data stored at the one or more computer-readable storage media in association with the verification address associated with the blockchain, the first user being provided access to the stored data based on verification that the first user has a first private key, the first private key being different the private key from which the verification address was derived; and
denying a second user, different than the individual, access to the stored data based on verification that the second user has a second private key.

9. The system of claim 1, wherein the biometric data comprises an image, a recording, or a template.

10. The system of claim 1, wherein the biometric data is related to a fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina, odor, gait, or voice.

11. A method of providing blockchain-based multifactor personal identity verification, the method being implemented by a server-side computer system comprising

one or more processors executing computer program instructions that, when executed, perform the method, the method comprising:

storing, by the server-side computer system, a blockchain at one or more computer-readable storage media of the server-side computer system;

assigning, by the server-side computer system, a verification address associated with the blockchain to an individual, the individual having a previously verified personal identity;

storing, by the server-side computer system, at the one or more computer-readable storage media, an identifier of the individual and a biometric hash of the individual in association with the verification address associated with the blockchain,

wherein the biometric hash is a hash of biometric data of the individual, and wherein each of the identifier, the biometric hash, and the verification address are different from one another and different from private and public keys from which the verification address was derived;

obtaining, by the server-side computer system, from a client-side device, the identifier and the biometric data in connection with a request to verify the individual's identity, the request indicating the verification address associated with the blockchain;

obtaining, by the server-side computer system, the stored identifier and the stored biometric hash using the verification address indicated in the request; and

signing, by the server-side computer system, verification of the individual's identity responsive to a determination that the identifier of the request and the biometric data of the request match the stored identifier and the stored biometric hash.

12. The method of claim 11, comprising:

signing, by the server-side computer system, using the private key from which the verification address was derived, the verification of the individual's identity responsive to the determination that the identifier of the request and the biometric data of the request match the stored identifier and the stored biometric hash.

13. The method of claim 12, comprising:

storing, by the server-side computer system, at the one or more computer-readable storage media, the private key in association with the verification address associated with the blockchain;

obtaining, by the server-side computer system, from the client-side device, the private key in connection with the request to verify the individual's identity;

obtain the stored private key using the verification address indicated in the request; and

signing, by the server-side computer system, using the private key, the verification of the individual's identity responsive to a determination that the identifier of the request, the biometric data of the request, and the private key of the request match the stored identifier, the stored biometric hash, and the stored private key.

14. The method of claim 11, comprising:

assigning, by the server-side computer system, another verification address associated with the blockchain to the individual;

storing, by the server-side computer system, at the one or more computer-readable storage media, another biometric hash of the individual in association with the other verification

address associated with the blockchain, the other biometric hash being a hash of other biometric data of the individual;

obtaining, by the server-side computer system, from the client-side device, the other biometric data in connection with the request to verify the individual's identity, the request further indicating the other verification address associated with the blockchain;

obtaining, by the server-side computer system, the stored other biometric hash using the other verification address indicated in the request; and

signing, by the server-side computer system, the verification of the individual's identity responsive to a determination that the identifier of the request, the biometric data of the request, the other biometric data of the request match the stored identifier, the stored biometric hash, and the stored other biometric hash.

15. The method of claim 14, comprising:

obtaining, by the server-side computer system, via a user interface, a user-initiated command to add the other verification address as an address of the blockchain for the individual; and

assigning, by the server-side computer system, the other verification address associated with the blockchain to the individual based on the user-initiated command.

16. The method of claim 14, comprising:

obtaining, by the server-side computer system, via a user interface, a user-initiated command to remove the other verification address as an address of the blockchain for the individual; and

de-associating, by the server-side computer system, the other verification address associated with the blockchain from the individual based on the user-initiated command.

17. The method of claim 11, comprising:

providing, by the server-side computer system, a first user, different than the individual, access to data stored at the one or more computer-readable storage media in association with the verification address associated with the blockchain, the first user being provided access to the stored data based on verification that the first user has a first private key, the first private key being different the private key from which the verification address was derived; and

denying, by the server-side computer system, a second user, different than the individual, access to the stored data based on verification that the second user has a second private key.

18. The method of claim 11, wherein the biometric data comprises an image, a recording, or a template.

19. The method of claim 11, wherein the biometric data is related to a fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina, odor, gait, or voice.

20. A system for providing blockchain-based multifactor personal identity verification, the system comprising:

one or more computer-readable storage media configured to store a blockchain;

a server-side computer system comprising one or more processors programmed to execute computer program instructions that, when executed, cause the server-side computer system to:

assign multiple verification addresses of the blockchain to the individual, the individual having a previously verified personal identity, the multiple verification addresses include a first verification address associated with the blockchain and a second verification address associated with the blockchain;

store, at the one or more computer-readable storage media, (i) an identifier of the individual and a first biometric hash of the individual in association with the first verification address associated with the blockchain and (ii) a second biometric hash of the individual in association with the second verification address associated with the blockchain,

wherein the first biometric hash is a hash of first biometric data of the individual, and the second biometric hash is a hash of second biometric data of the individual, and

wherein each of the identifier, the first biometric hash, the second biometric hash, the first verification address, and the second verification address are different from one another, different from first private and public keys from which the first verification address was derived, and different from second private and public keys from which the second verification address was derived;

obtain, from a client-side device, the identifier, the first biometric data, and the second biometric data in connection with a request to verify the individual's identity, the request indicating the first verification address associated with the blockchain and the second verification address associated with the blockchain;

obtain (i) the stored identifier and the stored first biometric hash using the first verification address indicated in the request and (ii) the stored second biometric hash using the second verification address indicated in the request; and

sign, using the private key from which the first verification address was derived, verification of the individual's identity responsive to a determination that the identifier of the request, the first biometric data of the request, and the second biometric data of the request match the stored identifier, the stored first biometric hash, and the stored second biometric hash;

provide a first user, different than the individual, access to data stored at the one or more computer-readable storage media in association with the first verification address associated with the blockchain, the first user being provided access to the stored data based on verification that the first user has a first private key, the first private key being different the private key from which the first verification address was derived and different from the private key from which the second verification address was derived; and

deny a second user, different than the individual, access to the stored data based on verification that the second user has a second private key.

21. A system for providing blockchain-based personal identity verification, the system comprising:

one or more computer-readable storage media configured to store a blockchain;

a computer system comprising one or more processors programmed to execute computer program instructions that, when executed, cause the computer system to:

assign a verification address associated with the blockchain to an individual, the individual having a previously verified personal identity;

store, at the one or more computer-readable storage media, an identifier of the individual and biometric information of the individual in association with the verification address associated with the blockchain, and

wherein the biometric information is related to biometric data of the individual, and the verification address is derived from private and public keys;

obtain, from a client-side device, the identifier and biometric data in connection with a request to verify the individual's identity, the request indicating the verification address associated with the blockchain;

obtain the stored identifier and the stored biometric information using the verification address indicated in the request; and

sign verification of the individual's identity responsive to a determination that the identifier of the request and the biometric data of the request match the stored identifier and the stored biometric information.

22. The system of claim 21, wherein the computer system is caused to: sign, using the private key from which the verification address was derived, the verification of the individual's identity responsive to the determination that the identifier of the request and the biometric data of the request match the stored identifier and the stored biometric information.

23. The system of claim 22, wherein the computer system is caused to: store, at the one or more computer-readable storage media, the private key in association with the verification address associated with the blockchain;

obtain, from the client-side device, the private key in connection with the request to verify the individual's identity;

obtain the stored private key using the verification address indicated in the request; and

sign, using the private key, the verification of the individual's identity responsive to a determination that the identifier of the request, the biometric data of the request, and the private key of the request match the stored identifier, the stored biometric information, and the stored private key.

24. The system of claim 23, wherein the private key is also stored on the client-side device, and wherein the client-side device is a user device of the individual.

25. The system of claim 21, wherein the computer system is caused to: assign another verification address associated with the blockchain to the individual;

store, at the one or more computer-readable storage media, additional biometric information of the individual in association with the other verification address associated with the blockchain, the additional biometric information being information related to additional biometric data of the individual;

obtain, from the client-side device, the additional biometric information in connection with the request to verify the individual's identity, the request further indicating the other verification address associated with the blockchain;

obtain the stored additional biometric information using the other verification address indicated in the request; and

sign the verification of the individual's identity responsive to a determination that the identifier of the request, the biometric data of the request, and the additional biometric data of the request match the stored identifier, the stored biometric information, and the stored additional biometric information,

wherein the additional biometric information is different from the biometric information.

26. The system of claim 25, wherein the server-side computer system is caused to: obtain, via a user interface, a user-initiated command to add the other verification address as an address of the blockchain for the individual; and assign the other verification address associated with the blockchain to the individual based on the user-initiated command.

27. The system of claim 25, wherein the computer system is caused to: obtain, via a user interface, a user-initiated command to remove the other verification address as an address of the blockchain for the individual; and de-associate the other verification address associated with the blockchain from the individual based on the user-initiated command.

28. The system of claim 21, wherein the computer system is caused to: provide a first user, different than the individual, access to data stored at the one or more computer-readable storage media in association with the verification address associated with the blockchain, the first user being provided access to the stored data based on verification that the first user has a first private key, the first private key being different the private key from

which the verification address was derived; and

denying a second user, different than the individual, access to the stored data based on verification that the second user has a second private key.

29. The system of claim 21, wherein the biometric information comprises an image, a recording, or a template and/or the biometric information is related to a fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina, odor, gait, or voice.

30. The system of claim 21, wherein the biometric information is stored on the blockchain.

31. The system of claim 21, wherein the stored biometric information is a biometric hash.

32. The system of claim 21, wherein the biometric information and the identifier are different from each other.

33. The system of claim 21, wherein the computer system includes a server-side computer.

34. A method of providing blockchain-based personal identity verification, the method being implemented by a computer system comprising one or more processors executing computer program instructions that, when executed, perform the method, the method comprising:

storing, by the computer system, a blockchain at one or more computer readable storage media of the computer system;

assigning, by the computer system, a verification address associated with the blockchain to an individual, the individual having a previously verified personal identity;

storing, by the computer system, at the one or more computer-readable storage media, an identifier of the individual and biometric information of the individual in association with the verification address associated with the blockchain,

wherein the biometric information is related to biometric data of the individual and wherein the verification address is derived from private and public keys,

obtaining, by the computer system, from a client-side device, the identifier and biometric data in connection with a request to verify the individual's identity, the request indicating the verification address associated with the blockchain;

obtaining, by the computer system, the stored identifier and the stored biometric information using the verification address indicated in the request; and

assigning, by the computer system, verification of the individual's identity responsive to a determination that the identifier of the request and the biometric data of the request match the stored identifier and the stored biometric information.

35. The method of claim 34, comprising:

signing, by the computer system, using the private key from which the verification address was derived, the verification of the individual's identity responsive to the determination that the identifier of the request and the biometric data of the request match the stored identifier and the stored biometric information.

36. The method of claim 35, comprising:

storing, by the computer system, at the one or more computer-readable storage media, the private key in association with the verification address associated with the blockchain;

obtaining, by the computer system, from the client-side device, the private key in connection with the request to verify the individual's identity;

obtain the stored private key using the verification address indicated in the request; and

signing, by the computer system, using the private key, the verification of the individual's identity responsive to a determination that the identifier of the request, the biometric data of the request, and the private key of the request match the stored identifier, the stored biometric information, and the stored private key.

37. The method of claim 34, comprising:

assigning, by the computer system, another verification address associated with the blockchain to the individual;

storing, by the computer system, at the one or more computer-readable storage media, additional biometric information of the individual in association with the other verification address associated with the blockchain, the additional biometric information being information related to additional biometric data of the individual;

obtaining, by the computer system, from the client-side device, the additional biometric data in connection with the request to verify the individual's identity, the request further indicating the other verification address associated with the blockchain;

obtaining, by the computer system, the stored additional biometric information using the other verification address indicated in the request; and
signing, by the computer system, the verification of the individual's identity responsive to a determination that the identifier of the request, the biometric data of the request, the other biometric data of the request match the stored identifier, the stored biometric information, and the stored additional biometric information.

38. The method of claim 37, comprising:

obtaining, by the computer system, via a user interface, a user-initiated command to add the other verification address as an address of the blockchain for the individual; and
assigning, by the computer system, the other verification address associated with the blockchain to the individual based on the user-initiated command.

39. The method of claim 37, comprising:

obtaining, by the computer system, via a user interface, a user-initiated command to remove the other verification address as an address of the blockchain for the individual; and
de-associating, by the computer system, the other verification address associated with the blockchain from the individual based on the user-initiated command.

40. The method of claim 34, comprising:

providing, by the computer system, a first user, different than the individual, access to data stored at the one or more computer-readable storage media in association with the verification address associated with the blockchain, the first user being provided access to

the stored data based on verification that the first user has a first private key, the first private key being different the private key from which the verification address was derived; and denying, by the computer system, a second user, different than the individual, access to the stored data based on verification that the second user has a second private key.

41. The method of claim 34, wherein the biometric data comprises an image, a recording, or a template and/or the biometric information is related to a fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina, odor, gait, or voice.

42. The method of claim 34, wherein the biometric information is stored on the blockchain.

43. The system of claim 34, wherein the stored biometric information is a biometric hash.

44. The system of claim 34, wherein the biometric information and the identifier are different from each other.

45. The system of claim 34, wherein the computer system includes a server-side computer.

46. A system for providing blockchain-based personal identity verification, the system comprising:

one or more computer-readable storage media configured to store a blockchain;

a computer system comprising one or more processors programmed to execute computer program instructions that, when executed, cause the computer system to:

assign multiple verification addresses of the blockchain to the individual, the individual having a previously verified personal identity, the multiple verification addresses include a first verification address associated with the blockchain and a second verification address associated with the blockchain;

store, at the one or more computer-readable storage media, (i) an identifier of the individual and first biometric information of the individual in association with the first verification address associated with the blockchain and (ii) second biometric information of the individual in association with the second verification address associated with the blockchain,

wherein the first biometric information is information related to first biometric data of the individual, and the second biometric information is information related to second biometric data of the individual, and

wherein the first verification address is different from first private and public keys from which the first verification address was derived, and the second verification address is different from second private and public keys from which the second verification address was derived;

obtain, from a client-side device, the identifier, the first biometric data, and the second biometric data in connection with a request to verify the individual's identity, the request indicating the first verification address associated with the blockchain and the second verification address associated with the blockchain;

obtain (i) the stored identifier and the stored first biometric information using the first verification address indicated in the request and (ii) the stored second biometric information using the second verification address indicated in the request; and

sign, using the private key from which the first verification address was derived, verification of the individual's identity responsive to a determination that the identifier of the request, the first biometric data of the request, and the second biometric data of the request match the stored identifier, the stored first biometric information, and the stored second biometric information;

provide a first user, different than the individual, access to data stored at the one or more computer-readable storage media in association with the first verification address associated with the blockchain, the first user being provided access to the stored data based on verification that the first user has a first private key, the first private key being different the private key from which the first verification address was derived and different from the private key from which the second verification address was derived; and

deny a second user, different than the individual, access to the stored data based on verification that the second user has a second private key.

47. The system of claim 46, wherein the stored first biometric information is a first biometric hash and the stored second biometric information is a second biometric hash.

48. The system of claim 46, wherein the identifier and the first biometric information and the second biometric information are each different from each other.

49. The system of claim 46, wherein the computer system includes a server-side computer.

50. A system for providing blockchain-based personal identity verification, the system

comprising:

one or more hardware processors configured by machine-readable instructions to:

establish verification addresses on a blockchain by: associating identifiers with individuals having previously verified personal identities, a first identifier being associated a first individual, the first individual having a previously verified personal identity;

assigning verification addresses on a blockchain to the individuals, a given verification address including a public key and a private key, a first verification address being assigned to the first individual, the first verification address including a first public key and a first private key; and

recording identifiers and biometric information associated with the individuals at corresponding verification addresses, the first identifier and first biometric data associated with the first individual being recorded at the first verification address; and

perform blockchain-based personal identity verification using the verification addresses by:

receiving one or more identifiers in connection with one or more requests to verify an identity of one or more individuals, the first identifier being received in connection with a request to verify an identity of the first individual;

extracting the biometric information associated with the one or more individuals from the corresponding verification addresses, the first biometric information associated with the first individual being extracted from the first verification address;

obtaining, from a client-side device, identifiers and biometric data in connection with a request to verify the identity of one or more individuals, the request indicating the verification address or addresses associated with the blockchain; and

verifying the identity of the one or more individuals upon receiving matching biometric data and private keys, the personal identity of the first individual being verified upon receipt of (1) biometric data matching the first biometric information and (2) a private key matching the first private key.

51. A system for providing blockchain-based personal identity verification, the system comprising:

one or more computer-readable storage media configured to store a blockchain;

a computer system comprising one or more processors programmed to execute computer program instructions that, when executed, cause the computer system to:

assign a verification address associated with the blockchain to an individual, the individual having a previously verified personal identity, wherein the verification address is a specific location on the blockchain where information is stored, and wherein the verification address is derived from a public key contained in a public and private key-pair;

store, at the one or more computer-readable storage media, an identifier of the individual and biometric information of the individual in association with the verification address associated with the blockchain, at least the biometric information being stored at the specific location on the blockchain, wherein the biometric information is derived from biometric data of the individual;

obtain, from a client-side device, a received identifier and one or more of received biometric data and received biometric information in connection with a request to verify the individual's identity, the request indicating the verification address associated with the blockchain;

obtain the stored identifier and the stored biometric information using the verification address indicated in the request, wherein at least the stored biometric information is obtained from the specific address on the blockchain; and

sign verification of the individual's identity responsive to a determination that the received identifier matches the stored identifier, and one or more of:

- (i) derived biometric information derived from the received biometric data matches the stored biometric information, and
- (ii) the received biometric information matches the stored biometric information.

52. The system of claim 51, wherein the computer system is caused to:

in the step of storing, store the identifier at the specific location on the blockchain corresponding to the verification address; and

in the step of obtaining the stored identifier and the stored biometric information using the verification address indicated in the request, obtain the identifier from the blockchain at the verification address.

53. The system of claim 51, wherein the computer system is caused to: in the step of storing, store at least the biometric information as a new transaction record on the blockchain at the specific location on the blockchain.

54. The system of claim 51, wherein the computer system is caused to: in the step of storing, store the identifier and the biometric information as a new transaction record on the blockchain at the specific location on the blockchain.

55. The system of claim 53, wherein the computer system is caused to: in the step of storing, store the new transaction record linked to a previous transaction record by a hash of the previous transaction record.

56. The system of claim 54, wherein the computer system is caused to: in the step of storing, store the new transaction record linked to a previous transaction record by a hash of the previous transaction record.

57. The system of claim 51, wherein the computer system is caused to: in the step of storing, store the biometric information as a hash of the biometric data.

58. The system of claim 51, wherein the signing step utilizes the private key of the public and private key-pair from which the verification address was derived.

59. The system of claim 58, wherein the computer system is caused to:
store, at the one or more computer-readable storage media, the private key in association with the verification address associated with the blockchain;
obtain, from the client-side device, a received private key in connection with the request to verify the individual's identity;
retrieve the stored private key using the verification address indicated in the request; and
sign, using the stored private key, the verification of the individual's identity responsive to a determination that the received identifier matches the stored identifier, the received private

key matches the stored private key, and one or more of (i) derived biometric information derived from the received biometric data matches the stored biometric information, and (ii) the received biometric information matches the stored biometric information.

60. The system of claim 59, wherein the private key is also stored on the client-side device, and wherein the client-side device is a user device of the individual.

61. The system of claim 51, wherein the computer system is caused to:
provide a first user, different than the individual, access to data stored at the one or more computer-readable storage media in association with the verification address associated with the blockchain, the first user being provided access to the stored data based on verification that the first user has a first private key, the first private key being different the private key from which the verification address was derived; and
denying a second user, different than the individual, access to the stored data based on verification that the second user has a second private key.

62. The system of claim 51, wherein the biometric data is related to a fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina, odor, gait, or voice.

63. The system of claim 51, wherein the biometric information and the identifier are different from each other.

64. The system of claim 51, wherein the computer system includes a server-side computer.

65. The system of claim 51, wherein the computer system is caused to:
prior to the step of storing, use the processor or processors to initially verify the individual's identity by use of government issued identification of the individual.

66. A method of providing blockchain-based personal identity verification, the method being implemented by a computer system comprising one or more processors executing computer program instructions that, when executed, perform the method, the method comprising:

storing, by the computer system, a blockchain at one or more computer readable storage media of the computer system;

assigning, by the computer system, a verification address associated with the blockchain to an individual, the individual having a previously verified personal identity, wherein the verification address is a specific location on the blockchain where information is stored and wherein the verification address is derived from a public key of a public and private key-pair;

storing, by the computer system, at the one or more computer-readable storage media, an identifier of the individual and biometric information of the individual in association with the verification address, at least the biometric information being stored at the specific location on the blockchain, wherein the biometric information is derived from biometric data of the individual;

obtaining, by the computer system, from a client-side device, a received identifier and one or more of received biometric data and received biometric information in connection with a request to verify the individual's identity, the request indicating the verification address;

obtaining, by the computer system, the stored identifier and the stored biometric information from the blockchain using the verification address indicated in the request; and

signing, by the computer system, verification of the individual's identity responsive to a determination that the received identifier matches the stored identifier and one or more of:

- (i) derived biometric information derived from the received biometric data matches the stored biometric information, and
- (ii) the received biometric information matches the stored biometric information.

67. The method of claim 66, wherein in the step of storing, the identifier is stored at the specific location on the blockchain corresponding to the verification address, and in the step of obtaining the stored identifier and the stored biometric information using the verification address indicated in the request, the identifier is obtained from the blockchain at the verification address.

68. The method of claim 66, wherein in the step of storing, at least the biometric information is stored as a new transaction record on the blockchain at the specific location on the blockchain.

69. The method of claim 66, wherein in the step of storing, the identifier and the biometric information are stored as a new transaction record on the blockchain at the specific location on the blockchain.

70. The method of claim 68, wherein in the step of storing, the new transaction record is linked to a previous transaction record by a hash of the previous transaction record.

71. The system of claim 69, wherein in the step of storing, the new transaction record is linked to a previous transaction record by a hash of the previous transaction record.

72. The method of claim 66, wherein in the step of storing, the biometric information is stored as a hash of the biometric data.

73. The method of claim 66, wherein in the step of signing, the private key of the public and private key-pair from which the verification address was derived is used, and the verification of the individual's identity is responsive to the determination that the identifier of the request and the biometric data of the request match the stored identifier and the stored biometric information from the blockchain.

74. The method of claim 73, wherein in the step of storing, at the one or more computer-readable storage media, the private key is stored in association with the verification address associated with the blockchain, and the method further comprises the steps of:

obtaining, from the client-side device, a received private key in connection with the request to verify the individual's identity;

retrieving the stored private key using the verification address indicated in the request; and

signing, using the stored private key, the verification of the individual's identity responsive to a determination that the received identifier matches the stored identifier, the received private key matches the stored private key, and one or more of:

- (i) derived biometric information derived from the received biometric data matches the stored biometric information, and
- (ii) the received biometric information matches the stored biometric information.

75. The method of claim 74, further comprising a step of storing the private key also on the client-side device, and wherein the client-side device is a user device of the individual.

76. The method of claim 66, further comprising the steps of:

providing a first user, different than the individual, access to data stored at the one or more computer-readable storage media in association with the verification address associated with the blockchain, the first user being provided access to the stored data based on verification that the first user has a first private key, the first private key being different the private key from which the verification address was derived; and

denying a second user, different than the individual, access to the stored data based on verification that the second user has a second private key.

77. The method of claim 66, wherein the biometric data is related to a fingerprint, palm

veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina, odor, gait, or voice.

78. The method of claim 66, wherein in the method, the biometric information and the identifier are different from each other.

79. The method of claim 66, wherein in the method, the computer system includes a server-side computer.

80. The method of claim 66, further comprising the steps of, prior to the step of storing, using the processor or processors to initially verify the individual's identity by use of government issued identification of the individual.

81. A system for providing blockchain-based personal identity verification, the system comprising:

one or more computer-readable storage media configured to store a blockchain;

a computer system comprising one or more processors programmed to execute computer program instructions that, when executed, cause the computer system to:

assign a verification address associated with the blockchain to an individual, the individual having a previously verified personal identity, wherein the verification address is a specific location on the blockchain where information is stored, and wherein the verification address is derived from a public key contained in a public and private key-pair;

store, at the one or more computer-readable storage media, an identifier of the individual and biometric information of the individual in association with the verification address associated with the blockchain, at least the biometric information being stored at the specific location on the blockchain, wherein the biometric information is derived from biometric data of the individual;

obtain, from a client-side device, a received identifier and one or more of received biometric data and received biometric information in connection with a request to verify the individual's identity, the request indicating the verification address associated with the blockchain;

obtain the stored identifier and the stored biometric information using the verification address indicated in the request, wherein at least the stored biometric information is obtained from the specific address on the blockchain; and

sign verification of the individual's identity responsive to a determination that the received identifier matches the stored identifier, and one or more of:

(iii) derived biometric information derived from the received biometric data matches the stored biometric information, and

(iv) the received biometric information matches the stored biometric information,

assign a second verification address associated with the blockchain to the individual, wherein the second verification address is a second specific location on the blockchain where information is stored;

store, at the one or more computer-readable storage media, second biometric information of the individual in association with the second verification address associated with the blockchain, the second biometric information derived from second biometric data of the

individual, the second biometric information being stored at the second specific location on the blockchain;

obtain, from the client-side device, one or more of second received biometric data and second received biometric information in connection with the request to verify the individual's identity, the request further indicating the second verification address associated with the blockchain;

obtain the second stored biometric information using the second verification address indicated in the request; and

sign the verification of the individual's identity responsive to a determination that the identifier of the request matches the stored identifier and one or more of:

(i) derived biometric information derived from the received biometric data matches the stored biometric information and second derived biometric information derived from the second received biometric data matches the second stored biometric information, and

(ii) the received biometric information matches the stored biometric information and the second received biometric information matches the second stored biometric information;

wherein the second biometric information is different from the biometric information and wherein the second specific location on the blockchain is different from the specific location on the blockchain.

82. The system of claim 81, wherein the server-side computer system is caused to:

obtain, via a user interface, a user-initiated command to add the second verification address as an address of the blockchain for the individual; and

assign the second verification address associated with the blockchain to the individual based on the user-initiated command.

83. The system of claim 81, wherein the computer system is caused to:
obtain, via a user interface, a user-initiated command to remove the second verification address as an address of the blockchain for the individual; and
de-associate the second verification address associated with the blockchain from the individual based on the user-initiated command.

84. The system of claim 81, wherein the computer system is caused to:
in the step of storing, store the identifier at the specific location on the blockchain corresponding to the verification address;
in the step of obtaining the stored identifier and the stored biometric information using the verification address indicated in the request, obtain the identifier from the blockchain at the verification address;
in the step of storing, store the second identifier at the second specific location on the blockchain corresponding to the second verification address;
in the step of obtaining the stored second identifier and the stored second biometric information using the second verification address indicated in the request, obtain the second identifier from the blockchain at the second verification address.

85. The system of claim 81, wherein the computer system is caused to:
in the step of storing, store at least the biometric information as a new transaction

record on the blockchain at the specific location on the blockchain; and

in the step of storing, store at least the second biometric information as another new transaction record on the blockchain at the second specific location on the blockchain.

86. The system of claim 85, wherein the computer system is caused to:

in the step of storing, store the new transaction record linked to a previous transaction record by a hash of the previous transaction record.

87. The system of claim 81, wherein the signing step utilizes the private key of the public and private key-pair from which the verification address was derived, and the second private key of the second public and second private key-pair from which the second verification address was derived.

88. The system of claim 81, wherein the biometric data is related to a fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina, odor, gait, or voice, wherein the biometric information and the identifier are different from each other.

89. The system of claim 81, wherein the computer system is caused to:

prior to the step of storing, use the processor or processors to initially verify the individual's identity by use of government issued identification of the individual.

90. A system for providing blockchain-based personal identity verification, the system comprising one or more computer-readable storage media configured to store a blockchain

and a first computing device comprising one or more processors programmed to execute computer program instructions that, when executed, cause the first computing device to:

assign a verification address to an individual, wherein the verification address corresponds to a location in the blockchain;

store identification information in the blockchain at the location corresponding to the verification address, wherein the identification information uniquely identifies an individual;

in response to a request received from a second computing device, retrieve information from a location in the blockchain corresponding to an address derived from the request; and

compare the information retrieved from the location in the blockchain corresponding to the address derived from the request with information obtained from the second computing device, and if a match is found, issue a verification that a person associated with the information obtained from the second computing device is the individual.

91. The system of claim 90, wherein the verification address is derivable from a public key associated with the individual.

92. The system of claim 90, wherein the identification information comprises biometric information of the individual.

93. The system of claim 90, wherein the identification information comprises information derived from the individual's passport.

94. The system of claim 90, wherein the identification information comprises information derived from the individual's driver's license.

95. The system of claim 90, wherein the computer system is caused to:
in the step of storing, store the identification information as a new transaction record on the blockchain at the location on the blockchain corresponding to the verification address.

96. The system of claim 95, wherein the computer system is caused to:
in the step of storing, store the new transaction record linked to a previous transaction record by a hash of the previous transaction record.

97. The system of claim 90, wherein the computer system is caused to:
in issuing the verification, utilize the private key of a public and private key-pair from which the verification address was derived to issue the verification.

98. The system of claim 90, wherein the computer system is caused to:
prior to the step of storing, use the processor or processors to initially verify the individual's identity by use of government issued identification of the individual.

99. A system for providing blockchain-based personal identity verification, the system comprising:

one or more computer-readable storage media configured to store a blockchain; and

a computer system comprising one or more processors programmed to execute computer program instructions that, when executed, cause the computer system to:

assign multiple verification addresses of the blockchain to the individual, the individual having a previously verified personal identity, the multiple verification addresses comprising a first verification address associated with the blockchain and a second verification address associated with the blockchain, wherein the first verification address provides a first specific location on the blockchain and the second verification address provides a second specific location on the blockchain;

store, at the one or more computer-readable storage media:

(i) a first identifier of the individual and first biometric information of the individual in association with the first verification address associated with the blockchain at the first specific location on the blockchain and

(ii) second identifier and second biometric information of the individual in association with the second verification address associated with the blockchain at the second specific location on the blockchain,

wherein the first biometric information is derived from first biometric data of the individual, and the second biometric information is derived from second biometric data of the individual, and

wherein the first verification address is different from the second verification address, the first verification address is derived from the first public key of the first public and private key-pair, and the second verification address is derived from the second public key of the second public and private key-pair;

obtain, from a client-side device, a first received identifier, one or more of first received biometric data and first received biometric information, a second identifier and one or more of second received biometric data and second received biometric information in connection with a request to verify the individual's identity, the request indicating the first verification address associated with the blockchain and the second verification address associated with the blockchain;

obtain:

- (i) the stored first identifier and the stored first biometric information from the blockchain using the first verification address indicated in the request, and
- (ii) the stored second identifier and the stored second biometric information from the blockchain using the second verification address indicated in the request; and

sign, using the private key from which the first verification address was derived and using the private key from which the second verification address was derived, verification of the individual's identity responsive to a determination that the first received identifier matches the first stored identifier, the second received identifier matches the second stored identifier, one or more of:

first derived biometric information derived from the first received biometric data matches the first stored biometric information and

second derived biometric information derived from the second received biometric data matches the second stored biometric information, and

the first received biometric information matches the first stored biometric information and the second received biometric information matches the second stored biometric information.

provide a first user, different than the individual, access to data stored at the one or more computer-readable storage media in association with the first verification address associated with the blockchain, the first user being provided access to the stored data based on verification that the first user has a first private key, the first private key being different the private key from which the first verification address was derived and different from the private key from which the second verification address was derived; and deny a second user, different than the individual, access to the stored data based on verification that the second user has a second private key.

100. The system of claim 99, wherein the computer system is caused to:

in the step of storing the first and second identifiers, store the identifier at the first and second specific locations on the blockchain corresponding to the first and second verification addresses, respectively; and

in the step of obtaining the stored first identifier and the stored first biometric information, obtain the first stored identifier and the stored first biometric information using the first verification address indicated in the request, and

in the step of obtaining the stored second identifier and the stored second biometric information, obtain the stored second identifier and the stored second biometric information using the second verification address indicated in the request.

101. The system of claim 99, wherein the computer system is caused to: in the step of storing, at the one or more computer-readable storage media, store at least the first biometric information as a first new transaction record on the blockchain at the first specific location

on the blockchain and store at least the second biometric information as a second new transaction record on the blockchain at the second specific location.

102. The system of claim 99, wherein the computer system is caused to:

in the step of storing,

store the first identifier and the first biometric information as a first new transaction record on the blockchain at the first specific location on the blockchain, and

store the second identifier and the second biometric information as a second new transaction record on the blockchain at the second specific location on the blockchain.

103. The system of claim 101, wherein the computer system is caused to:

in the step of storing,

store the first new transaction record linked to a first previous transaction record by a hash of the previous transaction record and

store the second new transaction record linked to a second previous transaction.

104. The system of claim 102, wherein the computer system is caused to:

in the step of storing,

store the first new transaction record linked to a first previous transaction record by a first hash of the first previous transaction record, and

store the second new transaction record linked to a second previous transaction record by a second hash of the second previous transaction record.

105. The system of claim 99, wherein the computer system is caused to:

in the step of storing,

store the first biometric information as a hash of the first biometric data, and

store the second biometric information as a hash of the second biometric data.

106. The system of claim 100, wherein the stored first biometric information is a hash of the first biometric data and the stored second biometric information is a hash of the second biometric data.

107. The system of claim 99, wherein the identifier and the first biometric information and the second biometric information are each different from each other.

108. The system of claim 99, wherein the computer system includes a server-side computer.

109. A system for providing blockchain-based personal identity verification, the system comprising one or more hardware processors configured by machine-readable instructions to:

establish verification addresses on a blockchain by:

associating identifiers with individuals having previously verified personal identities, a first identifier being associated with a first individual, the first individual having a previously verified personal identity;

assigning verification addresses on a blockchain to the individuals, a given verification address including a public key and a private key, a first verification address being assigned to the first individual, the first verification address including a first public key and a first private key, wherein the first verification address is a first specific location on the blockchain where information is stored; and

recording identifiers and biometric information associated with the individuals at corresponding verification addresses, the first identifier and first biometric information associated with the first individual being recorded at the first verification address, at least the first biometric information being stored at the first specific location on the blockchain; and

perform blockchain-based personal identity verification using the verification addresses by:

receiving one or more identifiers in connection with one or more requests to verify an identity of one or more individuals, the first identifier being received in connection with a request to verify an identity of the first individual;

extracting the biometric information associated with the one or more individuals from the corresponding verification addresses, the first biometric information associated with the first individual being extracted from the first verification address from the first specific location on the blockchain;

obtaining, from a client-side device, identifiers and one or more of biometric data and biometric information in connection with a request to verify the identity of one or more individuals, the request indicating the verification address or addresses associated with the blockchain; and

verifying the identity of the one or more individuals upon receiving matching biometric data or biometric information and private keys, the personal identity of the first individual being verified upon receipt of a received private key matching the first private key and one or more of:

- (i) derived biometric information derived from the received biometric data matching the first biometric information and
- (ii) received biometric information matching the first biometric information.

110. The system of claim 109, wherein the step of verifying the first individual's identity further requires the received identifier matching the recorded first identifier, and wherein the computer system is caused to:

in the step of storing the first and second identifiers, store the identifier at the first and second specific locations on the blockchain corresponding to the first and second verification addresses, respectively; and

in the step of obtaining the stored first identifier and the stored first biometric information, obtain the first stored identifier and the stored first biometric information using the first verification address indicated in the request, and

in the step of obtaining the stored second identifier and the stored second biometric information, obtain the stored second identifier and the stored second biometric information using the second verification address indicated in the request.

111. A system for providing blockchain-based multifactor personal identity verification, the system comprising:

one or more hardware processors configured by machine-readable instructions to:

- (a) establish verification addresses on a blockchain by:
 - (i) associating identifiers with individuals having previously verified personal identities, a first identifier being associated with a first individual, the first individual having a first previously verified personal identity;
 - (ii) assigning verification addresses on a blockchain to the individuals having previously verified personal identities, a given verification address including a public key and a private key, a first verification address being assigned to the first individual, the first verification address including a first public key and a first private key; and
 - (iii) recording identifiers including unique data associated with the individuals at corresponding verification addresses, the first identifier including the first unique data associated with the first individual being recorded at the first verification address;
- (b) perform blockchain-based multifactor personal identity verification using the verification addresses by:
 - (i) receiving one or more identifiers in connection with one or more requests to verify an identity of one or more individuals, the first identifier being received in connection with a request to verify an identity of the first individual;
 - (ii) obtaining the identifiers including the unique data associated with the one or more individuals from the corresponding verification addresses, the first identifier including the unique data associated with the first individual being obtained from the first verification address; and
 - (iii) verifying the identity of the one or more individuals upon receiving matching identifiers with the unique data and receiving matching private keys, the personal identity of the first individual, having the first previously verified identity, being verified upon receipt of an identifier with unique data matching the first identifier with the first unique data stored in association with the first verification address and a private key matching the first private key.

112. The system of claim 111, wherein the one or more hardware processors are also configured by machine-readable instructions such that verifying the personal identity of the first individual is performed by signing a verification transaction on the blockchain.

113. The system of claim 112, wherein the one or more hardware processors are also configured by machine-readable instructions such that the verification transaction is signed by a public node or a private node.

114. The system of claim 111, wherein the one or more hardware processors are also configured by machine-readable instructions to:

add or delete established verification addresses on the blockchain by providing an interface for presentation to individuals via associated computing platforms, the interface being configured to allow a given individual to add or delete verification addresses assigned to the given individual so long as at least one verification address is assigned to the given individual.

115. The system of claim 111, wherein the computer system is caused to: sign, using the private key from which the verification address was derived, the verification of the individual's identity responsive to the determination that the identifier of the request including the unique data of the request match the first identifier including the first unique data.

116. The system of claim 115, wherein the computer system is caused to: store, at the one or more computer-readable storage media, the private key in association with the verification address associated with the blockchain;

obtain, from the user device or devices, the private key in connection with the request to verify the individual's identity;

obtain the first private key using the verification address indicated in the request; and

sign, using the private key, the verification of the individual's identity responsive to a determination that the identifier of the request including the unique data of the request, and the private key of the request match the stored first identifier including the stored first unique data, and the stored first private key.

117. The system of claim 116, wherein the private key is also stored on a client-side device, and wherein the client-side device is a user device of the individual.

118. The system of claim 111, wherein the unique data relates to biometric information of the individual.

119. The system of claim 111, wherein the first unique data relates to first biometric information of the first individual and is stored on the blockchain at the first verification address.

120. The system of claim 111, wherein the unique data is one of an image, a recording, or a template and/or biometric information is related to a fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina, odor, gait, voice, a fingerprint hash or an eye retina hash.

121. The system of claim 111, wherein the unique data relates to one of a passport, extracted passport information, an identification card, extracted identification card information, a driver's license, and extracted driver's license information.

122. The system of claim 120, wherein the unique data is stored on the blockchain at the verification address.

123. The system of claim 121, wherein the unique data is stored on the blockchain at the verification address.

124. The system of claim 111, wherein the computer system is caused to: provide a first user, different than the individual, access to data stored at the one or more computer-readable storage media in association with the verification address associated with the blockchain, the first user being provided access to the stored data based on verification that the first user has a first private key, the first private key being different the private key from which the verification address was derived; and denying a second user, different than the individual, access to the stored data based on verification that the second user has a second private key.

125. The system of claim 111, wherein the unique data and the identifier are different from each other.

126. The system of claim 111, wherein the computer system includes a server-side computer.

127. The system of claim 111, wherein the computer system is caused to: assign another verification address associated with the blockchain to the individual;
store, at the one or more computer-readable storage media, additional unique data of the individual in association with the other verification address associated with the blockchain, the additional unique data being information related to biometric data of the individual;
obtain, from the client-side device, the additional unique data in connection with the request to verify the individual's identity, the request further indicating the other verification address associated with the blockchain;
obtain the stored additional unique information using the other verification address indicated in the request; and
sign the verification of the individual's identity responsive to a determination that the identifier of the request, the unique data of the request, and the additional unique data of the request match the stored identifier, the stored unique data, and the stored additional unique data, wherein the additional unique data is different from the unique data.

128. The system of claim 127, wherein the server-side computer system is caused to: obtain, via a user interface, a user-initiated command to add the other verification address as an address of the blockchain for the individual; and
assign the other verification address associated with the blockchain to the individual based on the user-initiated command.

129. The system of claim 127, wherein the computer system is caused to: obtain, via a user interface, a user-initiated command to remove the other verification address as an address of the blockchain for the individual; and
de-associate the other verification address associated with the blockchain from the individual based on the user-initiated command.

130. The system of claim 111, wherein the computer system is caused to store the unique data in an encrypted form as a hash of information.

131. The system of claim 111, wherein the computer system is caused to store the unique data on the blockchain in a block as a new transaction.

132. The system of claim 111, wherein the computer system is caused to store the unique data as a template or vector of information relating to the individual.

133. The system of claim 111, wherein the computer system is caused to enable a user to create a new record on the blockchain containing changes to the unique data.

134. The system of claim 111, wherein the computer system is caused to, in verifying identity, require M-of-N signatures for identity verification.

135. The system of claim 111, wherein the computer system is caused to provide access to personal data of the first individual whose identity is verified.

136. The system of claim 135, wherein the computer system is caused to enable multiple levels of access to the personal data of the first individual whose identity is verified.

137. The system of claim 135, wherein the computer system is caused to provide access to the personal data of the first individual whose identity is verified by a merchant.

138. A system for providing blockchain-based personal identity verification, the system comprising:

one or more computer-readable storage media configured to store a blockchain;

a computer system comprising one or more processors programmed to execute computer program instructions that, when executed, cause the computer system to:

assign a verification address associated with the blockchain to an individual, the individual having a previously verified personal identity;

store, at the one or more computer-readable storage media, an identifier of the individual and unique data relating to the individual in association with the verification address associated with the blockchain, and

wherein the unique data is related to biometric data of the individual, and the verification address is derived from private and public keys;

obtain, from a client-side device, the identifier and unique data in connection with a request to verify the individual's identity, the request indicating the verification address associated with the blockchain;

obtain the stored identifier and the stored unique data using the verification address indicated in the request; and

verify the individual's identity responsive to a determination that the identifier of the request and the unique data of the request match the stored identifier and the stored unique data.

139. The system of claim 138, wherein the one or more hardware processors are also configured by machine-readable instructions such that verifying the personal identity of the individual is performed by signing a verification transaction on the blockchain.

140. The system of claim 139, wherein the one or more hardware processors are also configured by machine-readable instructions such that the verification transaction is signed by a public node or a private node.

141. The system of claim 138, wherein the one or more hardware processors are also configured by machine-readable instructions to:

add or delete established verification addresses on the blockchain by providing an interface for presentation to individuals via associated computing platforms, the interface being configured to allow a given individual to add or delete verification addresses assigned to the given individual so long as at least one verification address is assigned to the given individual.

142. The system of claim 138, wherein the computer system is caused to: sign, using the private key from which the verification address was derived, the verification of the individual's identity responsive to the determination that the identifier of the request

including the unique data of the request match the stored identifier and the stored unique data.

143. The system of claim 142, wherein the computer system is caused to: store, at the one or more computer-readable storage media, the private key in association with the verification address associated with the blockchain;

obtain, from the user device or devices, the private key in connection with the request to verify the individual's identity;

obtain the stored private key using the verification address indicated in the request; and

sign, using the private key, the verification of the individual's identity responsive to a determination that the identifier of the request including the unique data of the request, and the private key of the request match the stored identifier including the stored unique data, and the stored private key.

144. The system of claim 143, wherein the private key is also stored on the client-side device, and wherein the client-side device is a user device of the individual.

145. The system of claim 138, wherein the unique data is biometric information of the individual.

146. The system of claim 138, wherein the unique data is biometric information of the individual and is stored on the blockchain at the verification address.

147. The system of claim 138, wherein the unique data is one of an image, a recording, or a template and/or biometric information is related to a fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina, odor, gait, voice, a fingerprint hash or an eye retina hash.

148. The system of claim 138, wherein the unique data relates to one of a passport, extracted passport information, an identification card, extracted identification card information, a driver's license, and extracted driver's license information.

149. The system of claim 147, wherein the unique data is stored on the blockchain at the verification address.

150. The system of claim 148, wherein the unique data is stored on the blockchain at the verification address.

151. The system of claim 138, wherein the computer system is caused to: provide a first user, different than the individual, access to data stored at the one or more computer-readable storage media in association with the verification address associated with the blockchain, the first user being provided access to the stored data based on verification that the first user has a first private key, the first private key being different the private key from which the verification address was derived; and denying a second user, different than the individual, access to the stored data based on verification that the second user has a second private key.

152. The system of claim 138, wherein the unique data and the identifier are different from each other.

153. The system of claim 138, wherein the computer system includes a server-side computer.

154. The system of claim 138, wherein the computer system is caused to: assign another verification address associated with the blockchain to the individual; store, at the one or more computer-readable storage media, additional unique data of the individual in association with the other verification address associated with the blockchain, the additional unique data related to the individual; obtain, from the client-side device, the additional unique data in connection with the request to verify the individual's identity, the request further indicating the other verification address associated with the blockchain; obtain the stored additional unique data using the other verification address indicated in the request; and

sign the verification of the individual's identity responsive to a determination that the identifier of the request, the unique data of the request, and the additional unique data of the request match the stored identifier, the stored unique data, and the stored additional unique data,

wherein the additional unique data is different from the unique data.

155. The system of claim 154, wherein the server-side computer system is caused to: obtain, via a user interface, a user-initiated command to add the other verification address as an address of the blockchain for the individual; and assign the other verification address associated with the blockchain to the individual based on the user-initiated command.

156. The system of claim 154, wherein the computer system is caused to: obtain, via a user interface, a user-initiated command to remove the other verification address as an address of the blockchain for the individual; and de-associate the other verification address associated with the blockchain from the individual based on the user-initiated command.

157. The system of claim 138, wherein the computer system is caused to store the unique data in an encrypted form as a hash of information.

158. The system of claim 138, wherein the computer system is caused to store the unique data on the blockchain in a block as a new transaction.

159. The system of claim 138, wherein the computer system is caused to store the unique data as a template or vector of information relating to the individual.

160. The system of claim 138, wherein the computer system is caused to enable a user to create a new record on the blockchain containing changes to the unique data.

161. The system of claim 138, wherein the computer system is caused to, in verifying identity, require M-of-N signatures for identity verification.

162. The system of claim 138, wherein the computer system is caused to provide access to personal data of the individual whose identity is verified.

163. The system of claim 162, wherein the computer system is caused to enable multiple levels of access to the personal data of the individual whose identity is verified.

164. The system of claim 162, wherein the computer system is caused to provide access to the personal data of the individual whose identity is verified by a merchant.

165. A system for providing blockchain-based multifactor personal identity verification, the system comprising:

one or more hardware processors configured by machine-readable instructions to:

(a) establish verification addresses on a blockchain by:

(i) associating identifiers with individuals having previously verified personal identities, a first identifier being associated with a first individual, the first individual having a first previously verified personal identity;

(ii) assigning verification addresses on a blockchain to the individuals having previously verified personal identities, a given verification address including a public key and a private key, a first verification address being assigned to the first individual, the first verification address including a first public key and a first private key; and

(iii) recording identifiers and unique data associated with the individuals at corresponding verification addresses, the first identifier and first unique data associated with the first individual being recorded at the first verification address;

(b) perform blockchain-based multifactor personal identity verification using the verification addresses by:

(i) receiving one or more identifiers in connection with one or more requests to verify an identity of one or more individuals, the first identifier being received in connection with a request to verify an identity of the first individual;

- (ii) obtaining the identifier including the unique data associated with the one or more individuals from the corresponding verification addresses, the first identifier and the first unique data associated with the first individual being obtained from the first verification address; and
- (iii) verifying the identity of the one or more individuals upon receiving matching identifiers and matching unique data and receiving matching private keys, the personal identity of the first individual, having the first previously verified identity, being verified upon receipt of an identifier and unique data matching the first identifier and the first unique data stored in association with the first verification address and a private key matching the first private key.

166. The system of claim 165, wherein the unique data is biometric data, and the first unique data is first biometric data.

167. The system of claim 166, wherein the one or more hardware processors are also configured by machine-readable instructions such that verifying the personal identity of the first individual is performed by signing a verification transaction on the blockchain.

168. The system of claim 167, wherein the one or more hardware processors are also configured by machine-readable instructions such that the verification transaction is signed by a public node or a private node.

169. The system of claim 166, wherein the one or more hardware processors are also configured by machine-readable instructions to:
add or delete established verification addresses on the blockchain by providing an interface for presentation to individuals via associated computing platforms, the interface being configured to allow a given individual to add or delete verification addresses assigned to the given individual so long as at least one verification address is assigned to the given individual.

170. The system of claim 166, wherein the computer system is caused to: sign, using the private key from which the verification address was derived, the verification of the

individual's identity responsive to the determination that the identifier of the request including the unique data of the request match the first identifier and the first unique data.

171. The system of claim 170, wherein the computer system is caused to: store, at the one or more computer-readable storage media, the private key in association with the verification address associated with the blockchain;

obtain, from the user device or devices, the private key in connection with the request to verify the individual's identity;

obtain the first private key using the verification address indicated in the request; and

sign, using the private key, the verification of the individual's identity responsive to a determination that the identifier of the request including the unique data of the request, and the private key of the request match the stored first identifier and the stored first unique data, and the stored first private key.

172. The system of claim 171, wherein the private key is also stored on a client-side device, and wherein the client-side device is a user device of the individual.

173. The system of claim 166, wherein the biometric data comprises a biometric hash.

174. The system of claim 166, wherein the first unique data relating to the biometric data of the first individual and is stored on the blockchain at the first verification address.

175. The system of claim 166, wherein the unique data is one of an image, a recording, or a template and/or biometric information is related to a fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina, odor, gait, voice, a fingerprint hash or an eye retina hash.

176. The system of claim 166, wherein the unique data relates to one of a passport, extracted passport information, an identification card, extracted identification card information, a driver's license, and extracted driver's license information.

177. The system of claim 175, wherein the unique data is stored on the blockchain at the verification address.

178. The system of claim 176, wherein the unique data is stored on the blockchain at the verification address.

179. The system of claim 166, wherein the computer system is caused to: provide a first user, different than the individual, access to data stored at the one or more computer-readable storage media in association with the verification address associated with the blockchain, the first user being provided access to the stored data based on verification that the first user has a first private key, the first private key being different the private key from which the verification address was derived; and denying a second user, different than the individual, access to the stored data based on verification that the second user has a second private key.

180. The system of claim 166, wherein the unique data and the identifier are different from each other.

181. The system of claim 166, wherein the computer system includes a server-side computer.

182. The system of claim 166, wherein the computer system is caused to: assign another verification address associated with the blockchain to the individual; store, at the one or more computer-readable storage media, additional unique data of the individual in association with the other verification address associated with the blockchain, the additional unique data being information related to biometric data of the individual; obtain, from the client-side device, the additional unique data in connection with the request to verify the individual's identity, the request further indicating the other verification address associated with the blockchain; obtain the stored additional unique information using the other verification address indicated in the request; and

sign the verification of the individual's identity responsive to a determination that the identifier of the request, the unique data of the request, and the additional unique data of the request match the stored identifier, the stored unique data, and the stored additional unique data,

wherein the additional unique data is different from the unique data.

183. The system of claim 182, wherein the server-side computer system is caused to: obtain, via a user interface, a user-initiated command to add the other verification address as an address of the blockchain for the individual; and assign the other verification address associated with the blockchain to the individual based on the user-initiated command.

184. The system of claim 182, wherein the computer system is caused to: obtain, via a user interface, a user-initiated command to remove the other verification address as an address of the blockchain for the individual; and de-associate the other verification address associated with the blockchain from the individual based on the user-initiated command.

185. The system of claim 166, wherein the computer system is caused to store the unique data in an encrypted form as a hash of information.

186. The system of claim 166, wherein the computer system is caused to store the unique data on the blockchain in a block as a new transaction.

187. The system of claim 166, wherein the computer system is caused to store the unique data as a template or vector of information relating to the individual.

188. The system of claim 166, wherein the computer system is caused to enable a user to create a new record on the blockchain containing changes to the unique data.

189. The system of claim 166, wherein the computer system is caused to, in verifying identity, require M-of-N signatures for identity verification.

190. The system of claim 166, wherein the computer system is caused to provide access to personal data of the first individual whose identity is verified.

191. The system of claim 190, wherein the computer system is caused to enable multiple levels of access to the personal data of the first individual whose identity is verified.

192. The system of claim 190, wherein the computer system is caused to provide access to the personal data of the first individual whose identity is verified by a merchant.