

CLAIMS

What is claimed is:

1. An ecosystem security platform that is executed by a processing system of a VDAX, the ecosystem security platform comprising:
 - a root DNA module configured to:
 - manage a digitally generated genomic data set assigned to the VDAX, the genomic data set being unique to the VDAX and including a genomic eligibility object, a genomic correlation object, and a genomic differentiation object; and
 - 10 modify the genomic data set using one or more computationally complex functions;
 - a link module configured to:
 - receive a link from a second VDAX, the link containing encoded genomic regulation instructions; and
 - decode the link based on the genomic eligibility object and a modified genomic correlation object to obtain decoded genomic regulation instructions, wherein the modified genomic correlation object is modified from the genomic correlation object by the root DNA module;
 - 15 a sequence mapping module configured to:
 - obtain a sequence from a digital object that is to be provided to the second VDAX,
 - 20 wherein the sequence is extracted from a first portion of the digital object; and
 - map the sequence into a modified genomic differentiation object to obtain a genomic engagement factor, wherein the modified genomic differentiation object is modified from the genomic differentiation object by the root DNA module based on the decoded genomic regulation instructions; and
 - 25 a binary transformation module configured to:
 - encode a second portion of the digital object based on the genomic engagement factor to obtain an encoded digital object; and
 - generate a virtual binary language script (VBLS) object that includes the encoded digital object and the first portion of the digital object;
 - 30 wherein the VBLS object is provided to the second VDAX as part of a series of VBLS objects.
 2. The ecosystem security platform of claim 1, wherein the digital object is part of a series of digital objects that are each encoded into a respective VBLS object of the series of respective VBLS objects.

35

3. The ecosystem security platform of claim 2, wherein each digital object is encoded using a different respective genomic engagement factor.
4. The ecosystem security platform of claim 3, wherein the sequence mapping module
5 obtains a respective sequence from each respective digital object and maps the respective sequence into the modified genomic differentiation object to obtain the respective genomic engagement factor that is used to encode the respective digital object.
5. The ecosystem security platform of claim 1, wherein the series of VBLS objects are a non-
10 recurring language that is unique to the VDAX and the second VDAX.
6. The ecosystem security platform of claim 1, wherein the sequence is a public sequence that is defined in the first portion of the digital object in accordance with a publicly known protocol and format.
- 15 7. The ecosystem security platform of claim 1, wherein the sequence is a private sequence that is defined in the first portion of the digital object in accordance with a proprietary protocol and format that is not publicly available.
- 20 8. The ecosystem security platform of claim 1, wherein the binary transformation module includes a disambiguation module that encodes the second portion of the digital object based on the genomic engagement factor by determining a disjunctive union of the second portion and the genomic engagement factor using an XOR operation.
- 25 9. The ecosystem security platform of claim 1, wherein the binary transformation module includes an encryption module that encodes the second portion of the digital object based on the genomic engagement factor by encrypting the second portion of the digital object using an encryption function and the genomic engagement factor.
- 30 10. The ecosystem security platform of claim 1, wherein the link module decodes the link from the second VDAX as part of a link exchange process with the second VDAX.
11. The ecosystem security platform of claim 10, wherein the link exchange process in a one-time process.

12. The ecosystem security platform of claim 11, wherein the link exchange process includes authenticating an ecosystem member associated with the second VDAX based on the genomic eligibility object of the VDAX.

5 13. The ecosystem security platform of claim 10, wherein the link module is further configured to spawn a second link that contains second encoded genomic regulation instructions, wherein the second link is provided to the second VDAX as part of the link exchange process.

10 14. The ecosystem security platform of claim 13, wherein the link exchange process is a dissymmetric process, such that the second link is spawned independent of the link received from the second VDAX.

15 15. The ecosystem security platform of claim 13, wherein in spawning the second link, the link module is further configured to:

15 determine second genomic regulation instructions;
 encode the second genomic regulation instructions using a link genomic engagement factor to obtain the second encoded genomic regulation instructions, wherein the link genomic engagement factor is determined by the sequence mapping module based on a link mapping sequence and a second modified genomic correlation object that is modified from the genomic correlation object by the root DNA module;
20 generate genomic engagement cargo that contains the link mapping sequence, the second encoded genomic regulation instructions, and encoded link decoding information, wherein the link mapping sequence is not obfuscated in the genomic engagement cargo and the second link contains the genomic engagement cargo; and
25 provide the second link to the second VDAX, whereby the second VDAX decodes the second encoded genomic regulation instructions based on the link mapping sequence, the encoded link decoding information, and a second genomic data set that is assigned to the second VDAX.

30 16. The ecosystem security platform of claim 15, wherein the link mapping sequence is left unencoded in the genomic engagement cargo.

17. The ecosystem security platform of claim 15, wherein the binary transformation module is further configured to:

35 receive a second VBLS object from the second VDAX, the second VBLS object containing a second encoded digital object and unencoded metadata; and

decode the second digital object based on a second genomic engagement factor to obtain an unencoded second digital object, wherein the second genomic engagement factor is determined by the sequence mapping module based on a second sequence and a second modified genomic differentiation object that is derived from the genomic differentiation object of the genomic data set by the root DNA module based on the second genomic regulation instructions.

18. The ecosystem security platform of claim 1, wherein the link module is configured to perform a link exchange process across a set of interoperable digital communications media.

19. The ecosystem security platform of claim 1, wherein the link module is configured to perform a link exchange process across a set of interoperable digital networks.

20. The ecosystem security platform of claim 1, wherein the link module is configured to perform a link exchange process across a set of interoperable digital devices.

21. The ecosystem security platform of claim 1, wherein the link module is configured to perform a link exchange that is executed asynchronously with respect to the second VDAX.

22. The ecosystem security platform of claim 1, wherein the link module is configured to perform a link exchange process in a symmetric manner, such that the VDAX does not provide a second link to the second VDAX.

23. The ecosystem security platform of claim 1, wherein the link module is further configured to confirm eligibility correlation with respect to the second VDAX based on the genomic eligibility correlation object of the VDAX.

24. The ecosystem security platform of claim 1, wherein the link module is further configured to confirm link-exchange correlation with respect to the second VDAX based on the link received from the second VDAX and the genomic correlation object of the VDAX.

25. The ecosystem security platform of claim 1, wherein the link module is configured to prosecute a secure exchange of link information using a set of computationally complex functions.

26. The ecosystem security platform of claim 25, wherein the set of computationally complex functions are one of cipher-based functions, cipherless functions, or hybrid functions that include at least one cipher-based function and at least one cipherless function.
- 5 27. The ecosystem security platform of claim 1, wherein the link module is configured to execute a set of processes to securely exchange link information with the second VDAX to enable a di-symmetric engagement, whereby the exchange of link information exhibits a same level entropy as the di-symmetric engagement.
- 10 28. The ecosystem security platform of claim 1, wherein the link module includes a static link module that is configured to spawn and decode static links.
29. The ecosystem security platform of claim 28, wherein the static link module generates static links in accordance with rules and processes prescribed by a highest-class ecosystem VDAX
15 in the digital ecosystem.
30. The ecosystem security platform of claim 1, wherein the link module includes a dynamic link module that is configured to spawn and decode dynamic links, wherein the link received from the second VDAX is a dynamic link that further includes an instruction set that, when executed
20 by the VDAX, overrides a respective configuration of at least one of the root DNA module, the sequence mapping module, or the binary transformation module, such that the modified configurations are executed only when generating VBLS that is provided to the second VDAX.
31. The ecosystem security platform of the claim 1, wherein the sequence mapping module is
25 configured to select public sequences from respective first portions of respective digital objects that are formatted in accordance with a publicly available protocol.
32. The ecosystem security platform of claim 1, wherein in mapping the sequence into the modified genomic differentiation object, the sequence mapping module is configured to:
30 processes the sequence to derive an intermediate value; and
generate the genomic engagement factor based on the intermediate value and the modified genomic differentiation object using a set of information theory-facilitated computationally complex functions.

33. The ecosystem security platform of claim 32, wherein the set of information theory-facilitated computationally complex functions are one of cipher-based functions, cipherless functions, or hybrid functions that include at least one cipher-based function and at least one cipherless function.

5

34. The ecosystem security platform of the claim 1, wherein the genomic engagement factor is a binary vector exhibiting specific entropy.

35. The ecosystem security platform of claim 34, wherein the specific entropy of the genomic engagement factor is greater than or equal to an inherent entropy of the sequence.

10

36. The ecosystem security platform of the claim 1, wherein the sequence mapping module is configured to select sequences from respective first portions of respective digital objects that are formatted in accordance with a proprietary protocol.

15

37. The ecosystem security platform of claim 1, wherein the root DNA module includes a CNA module that formulates and constructs the genomic eligibility object.

38. The ecosystem security platform of claim 37, wherein the CNA module is configured to employ information theory-facilitated genomic processes to establish a specific relationship with other VDAXs in a respective digital ecosystem.

20

39. The ecosystem security platform of claim 37, wherein the link module uses the genomic eligibility object to confirm genomic engagement integrity with the second VDAX.

25

40. The ecosystem security platform of claim 37, wherein the genomic eligibility object is a CNA object that exhibits specific entropy, wherein the CNA object enables difference and correlation-based genomic processes.

41. The ecosystem security platform of claim 40, wherein the CNA object is an N-dimensional binary vector that exhibits the specific entropy.

30

42. The ecosystem security platform of claim 40, wherein the specific entropy of the CNA object is configurable by a community owner.

35

43. The ecosystem security platform of claim 40, wherein the CNA module is configured to generate a set of respective CNA objects based on the PNA object of the VDAX, wherein the set of respective CNA objects are respectively allocated to a set of respective progeny VDAXs and each CNA object exhibits specific entropy that is equal to the entropy of the CNA object of the
5 VDAX.

44. The ecosystem security platform of claim 40, wherein the CNA module is configured to prosecute eligibility correlation with respect to another VDAX based on the CNA object and engagement information provided by the other VDAX using a set of information theory-facilitated computationally complex functions.
10

45. The ecosystem security platform of claim 44, wherein the set of information theory-facilitated computationally complex functions are one of cipher-based functions, cipherless functions, or hybrid functions that include at least one cipher-based function and at least one
15 cipherless function.

46. The ecosystem security platform of claim 40, wherein the CNA module is configured to establish specific relationships between other VDAXs in a digital ecosystem to which the VDAX belongs based in part on the CNA object of the VDAX.
20

47. The ecosystem security platform of claim 1, wherein the root DNA module includes a PNA module that formulates and constructs the genomic eligibility object.

48. The ecosystem security platform of claim 47, wherein the PNA module is configured to
25 employ information theory-facilitated genomic processes to establish a specific relationship with other VDAXs in a respective digital ecosystem.

49. The ecosystem security platform of claim 47, wherein the link module uses the genomic eligibility object to confirm genomic engagement eligibility with the second VDAX.

30 50. The ecosystem security platform of claim 47, wherein the genomic eligibility object is a PNA object that exhibits specific entropy, wherein the PNA object enables difference and correlation-based genomic processes.

51. The ecosystem security platform of claim 50, wherein the PNA object includes a first N-
35 dimensional binary vector and a second N-dimensional binary vector that exhibit the specific

entropy, wherein the first N-dimensional vector consists of M randomly chosen binary primitive polynomials of degree T such that $M \times T$ is equal to N, and the second N-dimensional vector is determined based on the first N-dimensional binary vector.

5 52. The ecosystem security platform of claim 50, wherein the specific entropy of the PNA object is configurable by a community owner.

53. The ecosystem security platform of claim 50, wherein the PNA module is configured to generate a set of respective PNA objects based on the PNA object of the VDAX, wherein the set
10 of respective PNA objects are respectively allocated to a set of respective progeny VDAXs and each PNA object exhibits specific entropy that is equal to the entropy of the PNA object of the VDAX.

54. The ecosystem security platform of claim 50, wherein the PNA module is configured to
15 prosecute eligibility correlation with respect to another VDAX based on the PNA object and engagement information provided by the other VDAX using a set of information theory based computationally complex functions.

55. The ecosystem security platform of claim 54, wherein the set of information theory-
20 facilitated computationally complex functions are one of cipher-based functions, cipherless functions, and hybrid functions that include at least one cipher-based function and at least one cipherless function.

56. The ecosystem security platform of claim 50, wherein the PNA module is configured to
25 establish specific relationships between other VDAXs in a digital ecosystem to which the VDAX belongs based in part on the PNA object of the VDAX.

57. The ecosystem security platform of claim 1, wherein the root DNA module includes an
LNA module that formulates and constructs the genomic correlation object.

30

58. The ecosystem security platform of claim 57, wherein the LNA module is configured to employ information theory-facilitated genomic processes to establish a specific relationship with other VDAXs in a respective digital ecosystem.

59. The ecosystem security platform of claim 57, wherein the link module uses the genomic eligibility object to confirm link exchange correlation with the second VDAX based on the link.

60. The ecosystem security platform of claim 57, wherein the genomic eligibility object is an LNA object that exhibits specific entropy, wherein the LNA object enables difference and correlation-based genomic processes that are performed during link exchange.

61. The ecosystem security platform of claim 60, wherein the LNA object is sufficiently correlated with a second LNA object of the second VDAX.

10

62. The ecosystem security platform of claim 60, wherein the specific entropy of the LNA object is configurable by a community owner.

63. The ecosystem security platform of claim 60, wherein the LNA object is an N-dimensional binary vector that exhibits the specific entropy.

15

64. The ecosystem security platform of claim 60, wherein the LNA module is configured to prosecute link eligibility correlation with respect to another VDAX based on the LNA object and genomic engagement cargo provided in a respective link provided by the other VDAX using a set of information theory based computationally complex functions.

20

65. The ecosystem security platform of claim 64, wherein the set of information theory-facilitated computationally complex functions are one of cipher-based functions, cipherless functions, and hybrid functions that include at least one cipher-based function and at least one cipherless function.

25

66. The ecosystem security platform of claim 60, wherein the LNA module is configured to establish specific relationships between other VDAXs in a digital ecosystem to which the VDAX belongs based in part on the LNA object of the VDAX.

30

67. The ecosystem security platform of claim 57, wherein the LNA module is configured to generate a set of respective LNA objects based on the LNA object of the VDAX, wherein the set of respective LNA objects are respectively allocated to a set of respective progeny VDAXs, wherein each LNA object exhibits specific entropy that is equal to the entropy of the LNA object of the VDAX.

35

68. The ecosystem security platform of claim 57, wherein the LNA module is configured to modify the genomic correlation object based on a set of specific set of instructions using a set of information theory-facilitated computationally complex functions, wherein the set of information theory-facilitated computationally complex functions are one of cipher-based functions, cipherless functions and hybrid functions that include at least one cipher-based function and at least one cipherless function.

69. The ecosystem security platform of claim 68, wherein the LNA module modifies the genomic correlation object based on the set of instructions received from a progenitor VDAX, such that the modification to the genomic correlation object is used to establish future engagements with respect to a digital ecosystem to which the VDAX belongs while previously established engagements are not affected.

70. The ecosystem security platform of claim 68, wherein the LNA module modifies the genomic correlation object based on the set of instructions received from the second VDAX in the link to obtain the modified genomic correlation object, such that the modified genomic correlation object is used to determine a link genomic engagement factor that is used to decode the encoded GRI.

71. The ecosystem security platform of claim 1, wherein the root DNA module includes an XNA module that performs genomic processes involving the genomic correlation object, including at least one of generation of new genomic correlation objects and modification of the genomic correlation object of the VDAX.

72. The ecosystem security platform of claim 71, wherein the XNA module is configured to employ information theory-facilitated genomic processes to modify the genomic differentiation object of the VDAX in an identical manner as the second VDAX in accordance with the genomic regulation instructions decoded from the link obtained from the second VDAX.

73. The ecosystem security platform of claim 71, wherein the genomic eligibility object is an XNA object that exhibits specific entropy.

74. The ecosystem security platform of claim 73, wherein the XNA object is sufficiently correlated with a second XNA object of the second VDAX.

75. The ecosystem security platform of claim 73, wherein the specific entropy of the XNA object is configurable by a community owner.

5 76. The ecosystem security platform of claim 73, wherein the XNA object is an N-dimensional binary vector that exhibits the specific entropy.

77. The ecosystem security platform of claim 73, wherein the XNA object is used to establish future differentiation with other VDAX in possession of sufficiently correlated XNA objects.

10

78. The ecosystem security platform of claim 73, wherein the XNA module is configured to generate a set of respective XNA objects based on the XNA object of the VDAX, wherein the set of respective XNA objects are respectively allocated to a set of respective progeny VDAXs, wherein each XNA object exhibits specific entropy that is equal to the entropy of the XNA object of the VDAX.

15

79. The ecosystem security platform of claim 73, wherein the XNA module is configured to modify the XNA based on a set of specific set of instructions using a set of information theory-facilitated computationally complex functions.

20

80. The ecosystem security platform of claim 79, wherein the XNA module updates the XNA based on the set of instructions received from a progenitor VDAX, such that the updated XNA is used to establish future differentiation with respect to other VDAXs in a digital ecosystem to which the VDAX belongs.

25

81. The ecosystem security platform of claim 80, wherein the second VDAX is unable to establish future differentiation with the VDAX unless the second VDAX is in possession of sufficiently correlated persistently updated XNA.

30 82. The ecosystem security platform of claim 79, wherein the set of information theory-facilitated computationally complex functions are one of cipher-based functions, cipherless functions and hybrid functions that include at least one cipher-based function and at least one cipherless function.

83. The ecosystem security platform of claim 1, wherein the ecosystem security platform further comprises an authentication module that prosecutes secure genomic-based engagement correlation with respect to the second VDAX in accordance with information theory-facilitated computationally complex functions, wherein the information theory-facilitated computationally complex functions are one of cipher-based functions, cipherless functions and hybrid functions that include at least one cipher-based function and at least one cipherless function.

84. The ecosystem security platform of claim 1, wherein the ecosystem security platform further comprises a master integrity controller that includes a genomic process controller, an authorization module, and an engagement instances module, wherein the genomic process controller has a master controller genomic data set assigned thereto.

85. The ecosystem security platform of claim 84, wherein the genomic process controller is configured to engage with one or more platform modules to authenticate and confirm integrity of the one or more platform modules.

86. The ecosystem security platform of claim 85, wherein the genomic process controller confirms the integrity and authenticates the one or more platform modules based on the master controller genomic data set and a set of computationally complex functions.

87. The ecosystem security platform of claim 86, wherein the genomic process controller confirms the integrity and authenticates the one or more platform modules without determining any processes or functions performed by the one or more platform modules.

88. The ecosystem security platform of claim 86, wherein the genomic process controller is further configured to confirm integrity and authenticate any underlying operational processes and functions that connect the one or more platform modules using the set of computationally complex functions.

89. The ecosystem security platform of claim 88, wherein the genomic process controller is further configured to confirm, disqualify, or initiate modification of the one or more platform modules and the underlying operational processes and functions.

90. The ecosystem security platform of claim 84, wherein the authorization module is configured to confirm or deny an operational configuration of another VDAX in a digital

ecosystem based on the genomic controller genomic data and a set of information theory-facilitated computationally complex functions.

91. The ecosystem security platform of claim 90, wherein in response to determining to deny
5 the operational configuration of the other VDAX, the authorization module disqualifies or initiate modification of the operational configuration of the other VDAX.

92. The ecosystem security platform of claim 84, wherein the engagement instances module
is configured to track security instances in a digital ecosystem of the VDAX in accordance with a
10 set of one or more engagement tracking policies that define one or more definitions of a security instance.

93. The ecosystem security platform of claim 92, wherein the engagement instances module
is further configured to determine a number of security instances in the digital ecosystem of the
15 VDAX in accordance with a set of one or more engagement accounting policies that respectively define a manner by which security instances are counted.

94. The ecosystem security platform of claim 93, wherein the engagement instances modules
is further configured to report the number of security instances in the digital ecosystem to another
20 VDAX in accordance with a set of one or more engagement reporting policies that respectively define a manner by which the security instances are reported, to which VDAXs to report the security instances and how often to report the security instances.

95. The ecosystem security platform of claim 1, wherein the VDAX is a member of a digital
25 ecosystem.

96. The ecosystem security platform of claim 95, wherein the digital ecosystem is an enterprise
information technology system.

30 97. The ecosystem security platform of claim 95, wherein the digital ecosystem is a computing device and the progeny VDAXs respectively correspond to hardware components and digital components of the computing device.

98. The ecosystem security platform of claim 95, wherein the digital ecosystem is a traffic
35 grid.

99. The ecosystem security platform of claim 95, wherein the digital ecosystem is a home network.

5 100. The ecosystem security platform of claim 95, wherein the digital ecosystem is a classified computing infrastructure.

101. A system for performing genomic security-related control of a digital ecosystem, comprising:

10 an ecosystem VDAX, that is executed by a processing system associated with an owner of the digital ecosystem, that is configured with an ecosystem instance of an ecosystem security platform, wherein the ecosystem VDAX is configured to:

maintain a progenitor genomic data set corresponding to the digital ecosystem that includes one or more different digitally generated progenitor genomic data objects,
15 wherein each progenitor genomic data object exhibits a respective specific entropy.

generate a plurality of respective progeny genomic data sets based on the progenitor genomic data set, wherein each respective progeny genomic data set includes one or more different progeny genomic data objects that were respectively derived from the one or more digitally generated progenitor genomic data objects and exhibit the
20 respective specific entropy of the progenitor genomic data object from which it was derived;

for each respective progeny genomic data set:

allocate the progeny genomic data set to a respective progeny VDAX of a plurality of progeny VDAXs, wherein the progeny VDAX establishes unique non-recurring
25 engagements with other progeny VDAXs in the digital community based on the respective progeny genomic data set allocated to the progeny VDAX without any further interaction from the ecosystem VDAX; and

control a genomic topology of the digital ecosystem by selectively updating one or more of the progeny genomic data sets to affect an ability of specific progeny VDAXs to engage
30 with other VDAXs in the digital ecosystem.

102. The system of claim 101, wherein the progenitor genomic data set includes a progenitor genomic differentiation object and each progeny genomic data set includes a respective progeny genomic differentiation object.

35

103. The system of claim 102, wherein a pair of progeny VDAXs from the plurality of progeny VDAXs can exchange virtual binary language script (VBLS) only if the respective progeny genomic differentiation objects of the pair of progeny VDAXs are sufficiently correlated.

5 104. The system of claim 103, wherein the pair of progeny VDAXs are prevented from future exchange of VBLS when a first progeny genomic differentiation object of a first progeny VDAX of the pair of progeny VDAXs is updated and a second progeny genomic differentiation object of a second progeny VDAX of the pair of progeny VDAXs is not updated.

10 105. The system of claim 103, wherein the progenitor genomic differentiation and the respective progeny genomic differentiation objects are XNA objects.

106. The system of claim 105, wherein the digital ecosystem is at least one of:

15 a static ecosystem, wherein the ecosystem platform is configured in accordance with a directed architecture;

an interactive ecosystem, wherein the ecosystem platform is configured in accordance with a free form architecture; or

a dynamic ecosystem, wherein the ecosystem platform is configured in accordance with a dynamic-state spontaneous architecture.

20

107. The system of claim 106 further comprising a set of one or more enclave VDAXs, wherein each enclave VDAX corresponds to a respective digital enclave of the digital ecosystem and is allocated a respective enclave-specific XNA object with which the enclave VDAX controls an enclave genomic topology of the respective enclave.

25

108. The system of claim 107, wherein each respective digital enclave includes one or more progeny VDAXs that respectively represent one or more respective cohorts that are admitted to the digital enclave, wherein each respective progeny VDAX that is included in the respective digital enclave is allocated a progeny enclave-specific XNA object that is derived from the
30 enclave-specific XNA object of the enclave VDAX and is sufficiently correlated with respective progeny enclave XNA objects of other progeny VDAXs that are included in the digital enclave.

109. The system of claim 108, wherein a respective enclave VDAX controls membership to the corresponding respective digital enclave by allocating enclave-specific XNA objects to the
35 cohorts of the digital enclave.

110. The system of claim 108, wherein each enclave VDAX is further allocated a respective enclave genomic correlation object that is derived from a progenitor correlation object of the progenitor genomic data set.

5

111. The system of claim 110, wherein for each digital enclave, each progeny VDAX in the digital enclave is allocated a respective progeny enclave-specific genomic correlation object that is derived from the enclave from the respective enclave genomic correlation object of the enclave VDAX of the digital enclave.

10

112. The system of claim 111, wherein each progeny VDAX is allocated the respective enclave-specific genomic correlation object directly from the enclave VDAX of the digital enclave.

113. The system of claim 111, wherein each progeny VDAX is allocated the respective enclave-specific genomic correlation object directly from the ecosystem VDAX.

15

114. The system of claim 111, wherein each progeny VDAXs uses its respective progeny enclave-specific genomic correlation object to spawn links that respectively establish unique non-recurring engagements with other progeny VDAXs that are formed with respect to the respective digital enclave.

20

115. The system of claim 114, wherein each spawned link by the progeny VDAX provides unique genomic regulation instructions that define a manner by which a link hosting progeny VDAX modifies its enclave-specific XNA object to generate non-recurring VBLS that only the progeny VDAX can decode.

25

116. The system of claim 111, wherein each progeny VDAXs uses its respective progeny enclave-specific genomic correlation object to host links provided by other progeny VDAXs in the digital ecosystem, wherein the other progeny VDAXs provide the links to the progeny VDAX to establish unique non-recurring engagements with the progeny VDAX with respect to the respective digital enclave.

30

117. The system of claim 116, wherein each hosted link by the progeny VDAX provides unique genomic regulation instructions that define a manner by which the progeny VDAX modifies its

enclave-specific genomic differentiation object to generate non-recurring VBLS that only the other progeny VDAX that provided the link can decode.

118. The system of claim 107, wherein the enclave VDAX controls the genomic network topology by selectively updating progeny enclave-specific genomic data objects of a subset of progeny VDAXs that participate in the digital enclave.

119. The system of claim 107, wherein the enclave VDAX controls the genomic network topology of the digital enclave without requiring modification to a physical network topology of the digital enclave.

120. The system of claim 106, wherein the digital ecosystem includes multiple genomic topologies that overlay one or more physical network topologies, wherein the multiple genomic topologies exist simultaneously and interoperably.

121. The system of claim 106, wherein the ecosystem VDAX constructs and controls a genomic network topology that supports applications having dynamic state attributes.

122. The system of claim 121 further comprising a set of one or more enclave VDAXs, wherein each enclave VDAX corresponds to a respective digital enclave of the digital ecosystem and is allocated a respective enclave-specific genomic data set with which the enclave VDAX controls portions of the genomic network topology that are responsible for ecosystem-designated functions and processes of the digital ecosystem.

123. The system of claim 122, further comprising a set of cohort VDAXs that participate in the digital ecosystem, wherein the set of cohort VDAXs include one or more cohorts that respectively control respective subportions of the genomic network topology that are responsible for specific ecosystem-designated and/or enclave-designated functions and processes.

124. The system of claim 123, wherein interaction by the set of cohort VDAXs are controlled by respective cohort genomic data sets allocated to respective cohort VDAXs of the set of cohort VDAXs.

125. The system of claim 124, wherein the set of progeny VDAXs include the set of cohort VDAXs.

126. The system of claim 124, wherein the cohort genomic data set of each cohort of the set of cohort VDAXs includes:

5 one or more cohort genomic eligibility objects that include one or both of one unique CNA object and one unique PNA object;

one or more cohort genomic correlation objects that include one or more LNA objects, wherein each LNA object corresponds to a respective enclave to which the cohort VDAX is admitted; and

10 one or more cohort genomic differentiation objects that include one or more XNA objects, wherein each XNA object corresponds to a respective enclave to which the cohort VDAX is admitted.

127. The system of claim 121, wherein the digital ecosystem is a dynamic ecosystem and the ecosystem security platform is configured in accordance with a spontaneous architecture that
15 retains its operational integrity regardless a frequency in which one or more metric states of the dynamic ecosystem is updated.

128. The system of claim 127, wherein the ecosystem VDAX and the progeny VDAXs collectively control the genomic network topology in response to specific dynamic metric states.
20

129. The system of claim 127, supports multiple genomic network topologies overlaid on a physical network topology that exist simultaneously.

130. The system of claim 127, wherein the genomic digital network topology is constructed to
25 realize controlled levels of interoperability.

131. The system of claim 102, wherein the progenitor genomic differentiation and the respective progeny genomic differentiation objects are ZNA objects.

30 132. The system of claim 131, wherein the digital ecosystem is a virtual trusted execution domain implemented with respect to a device having the progeny VDAXs correspond to respective components of the device, wherein the components of the device may include one or more hardware components and one or more digital components.

133. The system of claim 131, wherein the progeny VDAXs from the plurality of progeny VDAXs are configured to perform component binary isolation (CBI) with respect to the virtual trusted execution domain.

5 134. The system of claim 101, further comprising the set of progeny VDAXs.

135. The system of claim 134, wherein each progeny VDAX is configured with a respective progeny instance of the ecosystem security platform, such that each progeny instance of the ecosystem security platform is configured with a respective set of functionally congruent modules
10 that are respectively configured to execute one or more information theory-facilitated computationally complex functions.

136. The system of 135, wherein the set of modules of each progeny instance of the ecosystem security platform includes a DNA module that is configured to manage the genomic data set of
15 the progeny VDAX and perform a set of genomic processes based on the genomic data set.

137. The system of claim 135, wherein the set of modules includes a link module that is configured to facilitate secure exchange of links with another VDAX to facilitate unique di-
20 symmetric engagement.

138. The system of claim 135, wherein the set of modules include a sequence mapping module that is configured to genomically process sequences to derive genomic engagement factors having specific entropy, wherein the genomic engagement factors are used to encode digital objects in a non-recurring manner, and wherein the sequences are at least one of public sequences or private
25 sequences.

139. The system of claim 138, wherein the set of modules include a binary transformation module that is configured to encode digital objects into VBLS objects based on genomic engagement factors determined by the sequence mapping module, wherein each VBLS object
30 contains an encoded digital object and metadata that is indicative of a public or private sequence that was used to generate a respective genomic engagement factor that was used to encode the encoded digital object.

140. The system of claim 138, wherein the binary transformation module is further configured to decode received encoded digital objects that are included in received VBLS objects based on respective recreated genomic engagement factors.
- 5 141. The system of claim 101, wherein the ecosystem instance of the ecosystem security platform is configured with a respective set of modules that are each configured to execute a respective set of computationally complex information theory-facilitated computationally complex functions.
- 10 142. The system of claim 141, wherein each set of information theory-facilitated based computationally complex functions is selected from cipher-based functions, cipherless functions, and hybrid functions that include at least one stage of at least one stage that is performed using a cipher-based function and at least one stage is performed using a cipherless function.
- 15 143. The system of claim 142, wherein the set of modules of the ecosystem instance includes a root DNA module that manages the progenitor genomic data set and generates the progeny genomic data set.
144. The system of claim 101, wherein the digital ecosystem is a cloud services system.
- 20 145. The system of claim 101, wherein the digital ecosystem is an enterprise information technology system.
146. The system of claim 101, wherein the digital ecosystem is a computing device and the progeny VDAXs respectively correspond to hardware components and digital components of the computing device.
- 25 147. The system of claim 101, wherein the digital ecosystem is a traffic grid.
148. The system of claim 147, wherein the traffic grid is an air traffic control grid.
- 30 149. The system of claim 147, wherein the traffic grid is an autonomous vehicle traffic grid.
150. The system of claim 101, wherein the digital ecosystem is a classified computing infrastructure.
- 35

151. A method for managing a set of digital entities in a digital ecosystem, the method comprising:

generating, by a processing system of an ecosystem VDAX, a progenitor genomic data set
5 having specific entropy, wherein the progenitor genomic data set is assigned to the ecosystem VDAX;

generating, by the processing system, a plurality of different progeny genomic data sets that each exhibit the specific entropy; and

for each progeny of the plurality of different progeny genomic data sets, allocating, by the
10 processing system, the progeny genomic data set to a respective digital entity of the set of digital entities, wherein the set of digital entities are enabled to achieve precision control of differences and correlation based on the respective progeny genomic data set of each respective digital entity.

152. The method of claim 151, wherein any pair of digital entities in the set of digital entities
15 are configured to confirm correlation of the respective genomic data sets of the pair of digital entities and differentiate the respective progeny genomic data sets from any other progeny genomic data set based on the confirmed correlation of the progeny genomic data sets of the pair of digital entities to form a unique non-recurring relationship within the digital community.

20 153. The method of claim 152, wherein the pair of digital entities are each configured to independently confirm correlation using a specific set of information theory-facilitated computationally complex functions.

154. The method of claim 153, wherein the set of information theory-facilitated
25 computationally complex functions are one of cipher-based functions, cipherless functions, and hybrid functions that include at least one cipher-based function and at least one cipherless functions.

155. The method of claim 153, wherein each digital entity of the pair of digital entities is
30 configured to independently differentiate its respective progeny genomic data set using a second set of information theory-facilitated computationally complex functions.

156. The method of claim 155, wherein the second set of computationally complex functions
35 are one of cipher-based functions, cipherless functions, and hybrid functions that include at least one cipher-based function and at least one cipherless functions.

157. The method of claim 152, wherein in response to forming a unique non-recurring relationship, the pair of entities engage by generating and exchanging unique non-recurring virtual binary language script (VBLS) that is only decodable by the pair of entities based on the
5 differentiated progeny genomic data.

158. The method of claim 157, wherein the VBLS is comprised of encoded digital objects that retain information theory-facilitated genomic attributes of the respective genomic data sets of the pair of digital entities.

10

159. The method of claim 151, wherein the specific entropy is a configurable level of entropy that is defined by a community owner associated with the ecosystem VDAX.

160. The method of claim 151, wherein the digital entities collectively enable virtual
15 authentication, virtual affiliation, and virtual agility.

161. The method of claim 151, wherein each progeny genomic data set includes a genomic correlation object that exhibits the specific entropy and a genomic differentiation object that exhibits the specific entropy.

20

162. The method of claim 162, wherein each progeny genomic data set includes a respective genomic eligibility object that exhibits the specific entropy.

163. The method of claim 151, wherein the digital ecosystem includes one or more digital
25 enclaves that are formed on a respective mutual identity of interest expressed by controlled differences and correlation in the progeny genomic data sets.

164. The method of claim 163, wherein each digital enclave includes one or more cohorts that share the respective mutual interest expressed by the controlled differences and correlation in the
30 progeny genomic data sets.