WHAT IS CLAIMED IS:

1. A method comprising:

receiving, by a secure platform computer operating a secure memory space, a first portion and a second portion of project data corresponding to a federated project involving a first entity and a second entity, the first portion of the project data corresponding to the first entity and the second portion of the project data corresponding to the second entity;

receiving, by the secure platform computer, a first data set of the first entity and a second data set of the second entity;

generating, by the secure platform computer, a machine-learning model based at least in part on the first data set, the second data set, and the project data; and

providing, by the secure platform computer, access to the machine-learning model to the first entity and the second entity, the machine-learning model being stored within the secure memory space.

2. The method of claim 1, wherein the first data set and the second data set are encrypted and wherein the method further comprises decrypting, by the secure platform computer, the first data set and the second data set prior to generating the machine-learning model.

3. The method of claim 1, further comprising:

receiving, by the secure platform computer, a first public key for the first entity; and

verifying, by the secure platform computer, integrity of the first data set based at least in part on verifying one or more digital signatures corresponding to one or more received messages comprising the first data set, the one or more digital signatures being verified utilizing the first public key.

4. The method of claim 1, further comprising:

receiving, by the secure platform computer via an application programming interface (API), input data from a computing device associated with the first entity;

providing, by the secure platform computer, the input data to the machine-learning model as input;

receiving, by the secure platform computer, output data from the machine-learning model; and

providing, by the secure platform computer via the API, the output data to the computing device associated with the first entity.

5. The method of claim 4, further comprising:

modifying, by the secure platform computer, the first data set to include the input data; and

updating, by the secure platform computer, the machine-learning model based at least in part on the first data set as modified.

6. The method of claim 1, wherein the project data comprises a first schema associated with the first data set, the first schema defining a data structure for data of the first data set, and wherein the method further comprises validating, by the secure platform computer, the first data set based at least in part on the first schema.

7. The method of claim 1, wherein the project data comprises permissive use information, and wherein the method further comprises:

generating, by the secure platform computer, a usage policy associated with the machine-learning model based at least in part on the permissive use information; and

verifying, by the secure platform computer, that subsequent use of the machine-learning model is in conformance with the usage policy.

8. The method of claim 1, further comprising:

providing, by the secure platform computer, an interface for verifying security of the secure memory space and integrity of the first data set and the second data set.

91. A computing device, comprising:

one or more processors;

a secure platform computer operating a secure memory space, the secure memory space comprising computer-executable instructions that, when

executed by the one or more processors, causes the secure platform computer to:

receive a first portion and a second portion of project data corresponding to a federated project involving a first entity and a second entity, the first portion of the project data corresponding to the first entity and the second portion of the project data corresponding to the second entity;

receive a first data set of the first entity and a second data set of the second entity;

maintain an immutable ledger comprising information corresponding to receipt of the first data set and the second data set by the secure platform computer;

generate a machine-learning model based at least in part on the first data set, the second data set, and the project data;

provide access to the machine-learning model to the first entity and the second entity, the machine-learning model being stored within the secure memory space.

~~10~~2. The computing device of claim ~~9~~1, wherein the secure memory space is an enclave managed by a chip set of the one or more processors, wherein the enclave is encrypted by the chip set and accessible only by the chip set.

~~11. The computing device of claim 9, wherein the instructions further cause the secure platform computer to maintain an immutable ledger comprising information corresponding to receipt of the first data set and the second data set by the secure platform computer.~~

~~12~~3. The computing device of claim ~~11~~1, wherein the instructions further cause the secure platform computer to:

receive, from a requesting entity, a task request requesting the immutable ledger be verified;

compare a first identifier of the requesting entity to a second identifier of the project data;

when the first identifier matches the second identifier, verifying the immutable ledger; and

providing, to the requesting entity, an indication that the immutable ledger was verified.

~~134~~. The computing device of claim ~~123~~, wherein the immutable ledger further comprises an identifier for a provider of the data, and where the instructions further cause the secure platform computer to verify, that the provider of the data corresponds to the first entity or the second entity.

~~145~~. The computing device of claim ~~123~~, wherein the instructions further cause the secure platform computer to generate one or more first keys for retrieving the first data set from the secure memory space and one or more second keys for retrieving the second data set from the secure memory space.

~~156~~. The computing device of claim ~~145~~, wherein information maintained in the immutable ledger comprises first hash values corresponding to the one or more first keys and second hash values corresponding to the one or more second keys.

~~167~~. The computing device of claim ~~91~~, wherein the instructions further cause the secure platform computer to:

generate an additional machine-learning model based at least in part on the first data set, the second data set, and the project data; and

provide access to the additional machine-learning model for the first entity, the additional machine-learning model being stored within the secure memory space.

~~178~~. The computing device of claim ~~91~~, wherein the instructions further cause the secure platform computer to:

transmit a notification to the second entity in response to receiving the first portion of the project data, the notification being transmitted prior to receiving the second portion of the project data, wherein the notification indicates receipt of the first portion of the project data.

~~189~~. The computing device of claim ~~91~~, wherein the first data set is inaccessible by the second entity and wherein the second data set is inaccessible by the first entity.

~~19~~10. The computing device of claim ~~9~~1, wherein the instructions further cause the secure platform computer to transmit a notification to the first entity and the second entity, wherein the notification indicates generation of the machine-learning model is complete.

~~20~~11. The computing device of claim ~~9~~1, wherein the instructions further cause the secure platform computer to:

receive, from a computing device of the first entity, a task request indicative of a request to update the machine-learning model;

update the machine-learning model utilizing a data set comprising the first data set, the second data set, and subsequent data received after receipt of the first data set and the second data set; and

transmit, to the computing device of the first entity, a notification indicating the task request was successful or unsuccessful.

12. A computing device, comprising:

one or more processors; and

a secure platform computer operating a secure memory space, the secure memory space comprising computer-executable instructions that, when executed by the one or more processors, causes the secure platform computer to:

receive a first portion and a second portion of project data corresponding to a federated project involving a first entity and a second entity, the first portion of the project data corresponding to the first entity and the second portion of the project data corresponding to the second entity;

receive a first data set of the first entity and a second data set of the second entity, wherein the first data set is inaccessible by the second entity and wherein the second data set is inaccessible by the first entity;

generate a machine-learning model based at least in part on the first data set, the second data set, and the project data;

provide access to the machine-learning model to the first entity and the second entity, the machine-learning model being stored within the secure memory space.