WHAT IS CLAIMED IS:

1. A method comprising:

receiving distribution instructions for output data relating to a user of a client device, the distribution instructions comprising an indication of a plurality of data consumers;

encrypting the output data using a first cryptographic key;

providing access to the encrypted output data to each of the plurality of data consumers;

receiving, from each of the plurality of data consumers, an indication that the access to the encrypted output data was received by that data consumer; and

posting a record comprising a plurality of indications that access to the encrypted output data was received by the plurality of data consumers to a blockchain ledger,

wherein, upon confirming with the blockchain ledger that each of the plurality of data consumers has been provided access to the encrypted output data, a second cryptographic key is released to a plurality of private enclaves associated with computing devices operated by the plurality of data consumers, the second cryptographic key being configured to be used to decrypt the encrypted output data by the plurality of data consumers.

2. The method of claim 1, wherein the plurality of private enclaves includes a compute enclave and a delivery enclave, the compute enclave delivering the encrypted output data to the delivery enclave.

3. The method of claim 1, wherein the indication that the access to the encrypted output data was received by a data consumer comprises a signed delivery receipt from that data consumer.

4. The method of claim 3, wherein the signed delivery receipt is signed using a private key of the data consumer.

5. The method of claim 1, wherein the output data, after being encrypted using the first cryptographic key, is further encrypted using a plurality of third cryptographic keys.

6. The method of claim 5, wherein the plurality of third cryptographic keys comprises public keys associated with each of the plurality of data consumers, wherein each of the plurality of data consumers is provided access to the encrypted output data that is further encrypted using its respective public key.

7. The method of claim 1, wherein the first cryptographic key and the second cryptographic key are the same cryptographic key, wherein the plurality of private enclaves are embedded in the computing devices.

8. The method of claim 1, wherein the first cryptographic key is an encryption key and the second cryptographic key is a decryption key corresponding to, and different from, the encryption key.

9. The method of claim 1, wherein the second cryptographic key is not released to any of the plurality of data consumers if an indication that the access to the encrypted output data was received is not received from all of the plurality of data consumers within a timeout window.

10. The method of claim 1, further comprising:

confirming that each of the plurality of data consumers has not already been provided access to the encrypted output data; and

writing an entry to the blockchain ledger indicating that the plurality of data consumers has been provided access to the encrypted output data.

11. A computing system comprising:

a processor; and

a memory including instructions that, when executed by the processor, cause the computing system to, at least:

receive distribution instructions for output data relating to a user of a client device, the distribution instructions comprising an indication of a plurality of data consumers;

encrypt the output data using a first cryptographic key;

provide access to the encrypted output data to each of the plurality of data consumers;

receive, from each of the plurality of data consumers, an indication that the access to the encrypted output data was received by that data consumer; and

post a record comprising a plurality of indications that access to the encrypted output data was received by the plurality of data consumers to a blockchain ledger

wherein, upon confirming with the blockchain ledger that each of the plurality of data consumers has been provided access to the encrypted output data, a second cryptographic key is released to a plurality of private enclaves associated with computing devices operated by the plurality of data consumers, the second cryptographic key being configured to be used to decrypt the output data by the plurality of data consumers.

12. The computing system of claim 11, wherein the memory comprises an isolated region of memory protected by a trusted execution environment platform which is separate from other memory of the computing device.

13. The computing system of claim 12, wherein the output data is not available to other applications running on the computing device outside the memory.

14. The computing system of claim 11, wherein the computing system is operated by a data consumer of the plurality of data consumers.

15. The computing system of claim 11, wherein the plurality of data consumers are determined based on a specification for a computation used to generate the output data, the specification being retrieved from a public ledger.

16. The computing system of claim 11, wherein the encrypted output data is transmitted to each of the plurality of data consumers.

17. The computing system of claim 11, wherein the encrypted output data is written to a memory location at which each of the plurality of data consumers is able to access the encrypted output data.

18. The computing system of claim 11, wherein the instructions further cause the computing system to generate an aggregate encoding of each of the plurality of indications that the access to the encrypted output data was received.

19. The computing system of claim 11, wherein the plurality of data consumers are untrusted entities.

20. The computing system of claim 11, wherein the first cryptographic key is encrypted using a third cryptographic key associated with the processor and stored outside of the memory.