Claims

1. A computer-implemented method comprising, at a first computing entity (102, 302, 402):

   determining (502), based at least in part on a first polynomial and at least two elliptic curve points, a set of elliptic curve points for a second computing entity (104, 304, 404);

   making (504) a subset of the set of elliptic curve points available to the second computing entity (104, 304, 404);

   receiving (506) a second set of elliptic curve points generated using a second polynomial;

   determining a power of a secret based at least in part on the first set and the second set;

   determining (508), based at least in part on the power of the secret, a common reference string (108) comprising a verification key (114, 306) and an evaluation key (112), wherein the common reference string (108) is also determinable by the second computing entity (104, 304, 404) as a result of the first computing entity (102, 302, 402) providing the subset to the second computing entity (104, 304, 404); and

   generating a smart contract (110) comprising a first transaction input provided by the first computing entity (102, 302, 402) and a second transaction input provided by the second computing entity (104, 304, 404), wherein correct execution of the smart contract (110) by a third computing entity (106, 406) results in the third computing entity (106, 406) being able to generate a blockchain transaction using an output of the smart contract (110).

2. A method according to any preceding claim, wherein the set of elliptic curve points comprises corresponding elliptic curve points for powers of the first polynomial.

3. A method according to any preceding claim, wherein the first polynomial is of at least order 2.

4. A method according to any preceding claim, wherein the subset is the set of elliptic curve points.

5. A method according to any preceding claim, wherein the secret is shared between the first computing entity (102, 302, 402) and the second computing entity (104, 304, 404) without using a cryptographically protected communications channel.

6. A method according to any preceding claim, wherein the first computing entity (102, 302, 402) and the second computing entity (104, 304, 404) collectively determine the first digital asset and the second digital asset.

7. A method according to any preceding claim, further comprising:
   determining, based on a third polynomial and the at least two elliptic curve points, a third set of elliptic curve points for the second computing entity (104, 304, 404);
   making a second subset of the third set of elliptic curve points available to the second computing entity (104, 304, 404);
   receiving a fourth set of elliptic curve points;
   determining a parameter based at least in part on the third set and the fourth set, the parameter also determinable by the second computing entity (104, 304, 404) as a result of the first computing entity (102, 302, 402) providing the second subset to the second computing entity (104, 304, 404); and
   wherein the determining of the common reference string is based further at least in part on the parameter.

8. A method according to any preceding claim, further comprising sharing an elliptic curve parameter between the first computing entity (102, 302, 402) and the second computing entity (104, 304, 404) using Shamir's Secret Sharing Scheme.

9. A method according to any preceding claim, further comprising exchanging a scalar parameter between the first computing entity (102, 302, 402) and the second computing entity (104, 304, 404) using a Diffie-Hellman scheme.

10. A method according to any preceding claim, wherein the smart contract (110) comprises a P2SH type unlocking script that allows the third computing entity (106, 406) to unlock the first digital asset and the second digital asset in response to providing a proof of correct execution (116).

11. A method according to any preceding claim, wherein the first computing entity (102, 302, 402) makes the subset available to the second computing entity (104, 304, 404) via an off-chain communications channel.

12. A method according to any preceding claim, wherein the second polynomial is inaccessible to the first computing entity (102, 302, 402).

13. A method according to any preceding claim, wherein the at least two elliptic curve points are two different elliptic curve points.

14. A system, comprising:
    a processor; and
    memory including executable instructions that, as a result of execution by the processor, causes the system to perform the computer-implemented method according to any preceding claim.

15. A non-transitory computer-readable storage medium having stored thereon executable instructions that, as a result of being executed by a processor of a computer system, cause the computer system to at least perform the computer-implemented method according to any of claims 1 to 13.