

CLAIMS:

1. A computer-implemented method comprising, at a first computing entity:
 - determining, 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;
 - 5 making a subset of the set of elliptic curve points available to the second computing
 - entity;
 - receiving 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;
 - 10 determining, based at least in part on the power of the secret, a common reference
 - string comprising a verification key and an evaluation key, wherein the
 - common reference string is also determinable by the second computing entity
 - as a result of the first computing entity providing the subset to the second
 - computing entity; and
 - 15 generating a smart contract comprising a first transaction input provided by the first
 - computing entity and a second transaction input provided by the second
 - computing entity, wherein correct execution of the smart contract by a third
 - computing entity results in the third computing entity being able to generate a
 - blockchain transaction using an output of the smart contract.
- 20 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
- 25 curve points.
5. A method according to any preceding claim, wherein the secret is shared between the
- first computing entity and the second computing entity without using a
- cryptographically protected communications channel.

6. A method according to any preceding claim, wherein the first computing entity and the second computing entity collectively determine the first digital asset and the second digital asset.
7. A method according to any preceding claim, further comprising:
 - 5 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;
making a second subset of the third set of elliptic curve points available to the second computing entity;
receiving a fourth set of elliptic curve points;
 - 10 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 as a result of the first computing entity providing the second subset to the second computing entity; and
wherein the determining of the common reference string is based further at least in
15 part on the parameter.
8. A method according to any preceding claim, further comprising sharing an elliptic curve parameter between the first computing entity and the second computing entity using Shamir's Secret Sharing Scheme.
9. A method according to any preceding claim, further comprising exchanging a scalar
20 parameter between the first computing entity and the second computing entity using a Diffie-Hellman scheme.
10. A method according to any preceding claim, wherein the smart contract comprises a P2SH type unlocking script that allows the third computing entity to unlock the first digital asset and the second digital asset in response to providing a proof of correct
25 execution.
11. A method according to any preceding claim, wherein the first computing entity makes the subset available to the second computing entity 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.
13. A method according to any preceding claim, wherein the at least two elliptic curve points are two different elliptic curve points.
- 5 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.
- 10 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.

15

20