

Claims

1. A computer-implemented method of generating a transaction for a blockchain, the transaction being for transferring an amount of a digital asset from a first party to a second party; the method being performed by the first party and comprising:

generating a first transaction comprising an output locking the amount of the digital asset, the output comprising an output script comprising a plurality of criterion components each requiring a respective input data item, and a plurality of counter script components, each criterion component being associated with one of the counter script components, and

wherein the output script is configured so as to, when executed alongside an input script of a second transaction, i) increment a counter each time a respective criterion component is satisfied by a respective input data item of the input script, and ii) to require the counter to increment to at least a predetermined number in order to be unlocked by the input script.

2. The method of claim 1, comprising transmitting the first transaction to one or more nodes associated with the blockchain for inclusion in the blockchain.

3. The method of claim 1 or claim 2, wherein a total number of the plurality of criterion components is greater than or equal to the predetermined number.

4. The method of any preceding claim, wherein one, some or all of the plurality of criterion components define a different respective criterion.

5. The method of any preceding claim, wherein one, some or all of the plurality of criterion components comprises a plurality of sub-criterion components each requiring respective sub-input data item.

6. The method of any preceding claim, wherein one, some or all of the plurality of criterion components and/or one, some or all of the plurality of sub-criterion components require, as input or sub-input data items respectively, a respective blockchain signature corresponding to a predetermined blockchain public key.

7. The method of any preceding claim, wherein one, some or all of the plurality of criterion components are associated with a counter script component that is configured to increment the counter by a different number.
8. The method of any preceding claim, wherein each input data item in the input script comprises either a first or a second element, and wherein one, some or all of the plurality of criterion components are associated with a respective check component, wherein each respective check component is configured so as to, when executed alongside the input script, i) determine whether each input data item comprises the first element, and ii) only execute the associated criterion component if the input data item comprises the first element.
9. The method of claim 8, wherein each output script is configured to invalidate the first transaction if an executed criterion component is not satisfied by input data of the input script.
10. The method of any preceding claim, comprising transmitting the respective criterion and/or sub-criterion to the second party.
11. Computer equipment of the first party, comprising:
 - memory comprising one or more memory units; and
 - processing apparatus comprising one or more processing units, wherein the memory stores code arranged to run on the processing apparatus, the code being configured so as when on the processing apparatus to perform the method of any of claims 1 to 10.
12. A computer program embodied on computer-readable storage and configured so as, when run on computer equipment of the first party, to perform the method of any of claims 1 to 10.

13. A first transaction for inclusion in a blockchain, the first transaction for transferring an amount of a digital asset from a first party to a second party, the first transaction being embodied on a computer-readable data medium or media and comprising executable code, the code comprising a plurality of criterion components each requiring a respective input data item, and a plurality of counter components, each criterion component being associated with one of the counter components, and wherein the code is configured so as to, when executed alongside an input script of a second transaction at a node of a blockchain network:

increment a counter, stored in memory of the node, each time a respective criterion component is satisfied by a respective input data item of the input script; and

transfer the amount of the digital asset to the second party based on the counter being incremented to at least a predetermined number.

14. A computer-implemented method of generating a transaction for a blockchain, the transaction being for transferring an amount of a digital asset from a first party to a second party, the first and second parties each being associated with the blockchain; the method being performed by the first party and comprising:

generating a first transaction comprising a plurality of outputs, each output locking a respective amount of the digital asset and comprising a respective first script condition, wherein each first script condition comprises a plurality of criterion components each requiring a respective input data item, and a plurality of counter components, each criterion component being associated with one of the counter components, and

wherein each first output script condition is configured so as to, when executed alongside an input script of a second transaction, i) increment a counter each time a respective criterion component is satisfied by a respective input data item of the input script, and ii) require the counter to increment to at least a respective predetermined number in order to be unlocked by that input script, and wherein one, some or all of the first script conditions require the counter to increment to a different predetermined number.

15. The method of claim 14, comprising transmitting the first transaction to one or more nodes associated with the blockchain for inclusion in the blockchain.

16. The method of claim 14 or claim 15, wherein one, some or all of the outputs lock a different respective amount of the digital asset.
17. The method of any of claims 14 to 16, wherein the respective amount of the digital asset locked by a respective output is based on the respective predetermined number to which the respective first script condition requires the counter to increment.
18. The method of any of claims 14 to 17, wherein to be unlocked by the input script, each first script condition is configured to require the input script to comprise a digital signature of the first party and/or a digital signature of the second party.
19. The method of claim 18, comprising:
for each output, generating a respective second transaction, wherein the input script of each second transaction comprises the predetermined signature of the first party; and
transmitting each second transaction to the second party.
20. The method of claim 19, wherein each second transaction comprises a different lock time, wherein each respective lock time is configured to prevent the respective second transaction from being included in the blockchain until after a respective predetermined time.
21. The method of any of claims 14 to 20, wherein each first script condition comprises a hash of a secret value, and wherein to be unlocked by the input script, each first script condition is configured to require the input script to comprise the secret value.
22. The method of any of claims 14 to 21, wherein each output comprises a respective second script condition configured so as to, when executed alongside an input script of a third transaction, require the input script of the third transaction to comprise a predetermined digital signature of the first party and a predetermined digital signature of the second party in order to be unlocked by that input script.

23. The method of claim 22, comprising:
for each output, receiving a respective third transaction from the second party,
wherein the input script of each third transaction comprises the predetermined signature of the first party and the predetermined digital signature of the second party.
24. The method of claim 23, wherein each third transaction comprises a different lock time, wherein each respective lock time is configured to prevent the respective second transaction from being included in the blockchain until after a respective predetermined time.
25. The method of claim 24 when dependent on at least claim 20, wherein each output is associated with a different one of the second transactions and a different one of the third transactions, and wherein for each output, the respective lock time of the third transaction prevents the third transaction from being included in the blockchain until a time later than a time at which the second transaction can be included in the blockchain.
26. The method of any of claims 14 to 25, wherein one, some or all of the outputs comprise a respective third script condition, wherein each third script condition is configured so as to, when executed alongside an input script of a fourth transaction, require the input script of the fourth transaction to comprise a predetermined digital signature of the first party in order to be unlocked by that input script.
27. The method of claim 26 when dependent on claim 21, wherein each third script condition comprises the hash of the secret value, and wherein to be unlocked by the input script of the fourth transaction, each third script condition is configured to require that input script to comprise the secret value.
28. The method of claim 27, comprising:
obtaining the secret value;
for one, some or all of the outputs, generating a respective fourth transaction,
wherein the input script of each fourth transaction comprises the predetermined signature of the first party and the secret value; and

transmitting each fourth transaction to one or more nodes associated with the blockchain for inclusion in the blockchain.

29. The method of any of claims 14 to 28, wherein a total number of the plurality of criterion components is greater than each of the respective predetermined numbers.

30. The method of any of claims 14 to 29, wherein one, some or all of the plurality of criterion components define a different respective criterion.

31. The method of any of claims 14 to 30, wherein one, some or all of the plurality of criterion components comprises a plurality of sub-criterion components each requiring respective sub-input data item.

32. The method of any of claims 14 to 31, wherein for one, some or all of the first script conditions, one, some or all of the plurality of criterion components and/or one, some or all of the plurality of sub-criterion components require, as input or sub-input data items respectively, a respective blockchain signature corresponding to a predetermined blockchain public key.

33. The method of any of claims 14 to 32, wherein for one, some or all of the first script conditions, one, some or all of the plurality of criterion components are associated with a counter script component that is configured to increment the counter by a different number.

34. The method of any of claims 14 to 33, wherein each input data item in the input script comprises either a first or a second element, and wherein one, some or all of the plurality of criterion components are associated with a respective check component, wherein each respective check component is configured so as to, when executed alongside the input script, i) determine whether each input data item comprises the first element, and ii) only execute the criterion script components corresponding to input data items comprising the first element.

35. The method of claim 34, wherein each first script condition is configured to invalidate the first transaction if an executed criterion script is not satisfied by input data of the input script.
36. The method of any of claims 14 to 35, comprising transmitting the respective criteria and/or sub-criteria to the second party.
37. Computer equipment of the first party, comprising:
memory comprising one or more memory units; and
processing apparatus comprising one or more processing units, wherein the memory stores code arranged to run on the processing apparatus, the code being configured so as when on the processing apparatus to perform the method of any of claims 14 to 36.
38. A computer program embodied on computer-readable storage and configured so as, when run on computer equipment of the first party, to perform the method of any of claims 14 to 36.
39. A computer-implemented method of generating a transaction for a blockchain, the transaction being for transferring an amount of a digital asset from a first party to a second party, the first and second parties each being associated with the blockchain, wherein the blockchain comprises a first transaction comprising an output locking the amount of the digital asset and comprising a first script condition, wherein the first script condition comprises a plurality of criterion components each requiring a respective input data item; the method being performed by the second party and comprising:
generating a second transaction comprising a first input script component, the first input script component comprising: i) a plurality of input data items each corresponding to a respective criterion component of the first script condition, ii) a secret value, iii) a predetermined digital signature of the first party, and iv) a predetermined signature of the second party; and
transmitting the second transaction to one or more nodes associated with the blockchain for inclusion in the blockchain.

40. The method of claim 39, wherein the first transaction comprises second and third script conditions, and wherein the second transaction comprises:

a second input script component configured to evaluate as false when executed against the second script condition; and

a third input script component configured to evaluate as false when executed against the third script condition.

41. The method of claim 39 or claim 40, wherein the first script condition comprises a plurality of check components, each associated with a respective one of the plurality of criterion components, and wherein each respective check component is configured so as to, when executed alongside the input script, i) determine whether each input data item comprises the first element, and ii) only execute the criterion script components corresponding to input data items comprising the first element; and wherein each input data item comprises either the first data element or a second, different data element.

42. The method of any of claims 39 to 41, wherein one, some or all of the input data items comprises a respective digital signature.

43. Computer equipment of the second party, comprising:

memory comprising one or more memory units; and

processing apparatus comprising one or more processing units, wherein the memory stores code arranged to run on the processing apparatus, the code being configured so as when on the processing apparatus to perform the method of any of claims 39 to 42.

44. A computer program embodied on computer-readable storage and configured so as, when run on computer equipment of the second party, to perform the method of any of claims 39 to 42.

45. A first transaction for inclusion in a blockchain, the first transaction for transferring an amount of a digital asset from a first party to a second party, the first transaction being embodied on a computer-readable data medium or media and comprising executable code,

the code comprising a plurality of output scripts, each output script locking a respective amount of the digital asset and comprising respective first, second, and third script conditions, each first script condition comprising i) a plurality of criterion components each requiring a respective input data item, and ii) a plurality of counter components, each criterion component being associated with one of the counter components, and wherein the code is configured so as to, when a respective output script is executed alongside an input script of a second transaction at a node of a blockchain network:

if the respective first script condition is executed, increment a counter, stored in memory of the node, each time a respective criterion component is satisfied by a respective input data item of the input script, and transfer the amount of the digital asset to the second party based on the counter being incremented to at least a predetermined number;

if the respective second script condition is executed, determine if the input script comprises a predetermined digital signature of the first party and a predetermined digital signature of the second party, and transfer the amount of the digital asset to the first party; and

if the respective third script condition is executed, determine if the input script comprises the predetermined digital signature of the first party and a secret value, and transfer the amount of the digital asset to the first party.

46. A computer-readable storage medium having stored thereon the first transaction of claim 45.

47. A computer-readable storage medium having stored thereon the first transaction of claim 13.