

Claims

1. 1. A computer-implemented method (600) comprising, by a given proxy node (230A-C):

~~Receiving (610),~~ receiving, via a computer network, a transaction (500) generated and partially signed by an originator node (100), the transaction (500) including a first input (510) and a first (520) and second (530) output, wherein the first input (510) takes $x + r$ units of computing resources and wherein the first output (520) provides x units to an output address and the second output (530) provides $d + r$ units to a 1-of- n multi-signature address unlockable using any one of a plurality of second private keys, each of the second private keys being associated with a respective one of a plurality of proxy nodes (230A-C), the plurality of proxy nodes (230A-C) including the given proxy node (230A-C), and each of the second private keys derivable by the respective one of the plurality of proxy nodes (230A-C) based on a private key of an asymmetric encryption key pair of that proxy node (230A-C) and a secret value that proxy node (230A-C) shares with the originator node (100);

~~Selecting (620),~~ selecting a quantity of computing resources, t units, to be allocated to the given proxy node (230A-C) for broadcasting the transaction and having the transaction included in the blockchain and selecting a quantity of computing resources, f units, to be allocated to a third-party for including the transaction (500) in the blockchain, wherein $f \leq r$ and $t \leq (r - f)$;

digitally signing (630) an updated transaction (700) generated by adding a second input (710) taking $d + f$ units to the transaction;

generating and digitally signing (640) a further transaction (800) including an input (810) taking $d + r$ units sourced from the 1-of- n multi-signature address using the second private key of the proxy node and an output (820) providing t units to the given proxy node; and

broadcasting (650) the updated transaction (700) and the further transaction (800),² timed to permit their inclusion in the same block of the blockchain.

~~2.~~ 2._____The method according to any preceding claim wherein receiving the transaction (500) includes receiving an identifier of the transaction.

3._____

3. The method according to any preceding claim wherein the broadcast (650) of the updated transaction (700) and the broadcast of the further transaction (800) are substantially concurrent.
4. 4. The method according to any preceding claim wherein the received identifier of the transaction (500) is encrypted using a public key of the given proxy node (230A-C).
5. 5. The method according to any preceding claim wherein the quantity f of computing resources to be allocated to the third-party for including the transaction (500) in the blockchain is selected based on an indication received via the computer network.
6. 6. The method of claim 5 wherein the indication is received from the originator node (100).
7. 7. The method according to any preceding claim wherein the quantity of computing resources, f , to be allocated to the third-party for including the transaction (500) in the blockchain is selected based on having the transaction (500) included in a next block in the blockchain.
8. 8. The method according to any preceding claim wherein at least one of the quantity of computing resources, f , to be allocated to the third-party for including the transaction (500) in the blockchain and the quantity of computing resources, t units, to be allocated to the given proxy node (100) for broadcasting the transaction (500) is further selected based on having the further transaction (800) included in a next block in the blockchain.

9. 9. The method according to any preceding claim wherein the originator node (100) has an associated asymmetric encryption key pair including a public key and a private key and wherein the secret value shared between the originator node (100) and the given proxy node (230A-C) is derivable by the originator node (100) based on its private key and the public key of the given proxy node (230A-C) and by the given proxy node (230A-C) based its private key and the public key of the originator node (100).

10.

10. The method according to any preceding claim wherein the asymmetric encryption key pairs are elliptical-curve key pairs and wherein establishing the secret value shared between the originator node and a particular proxy node corresponds to an Elliptical-Curve Diffie-Hellman (ECDH) key exchange.
11. 11. A computing device comprising
- a processor;
 - a memory;
 - a network interface; and
 - a non-transitory computer-readable storage medium storing computer-executable instructions that, when executed by the processor, cause the computing device to carry out the method according to any preceding claim.
- ~~executable instructions that, when executed by the processor, cause the computing device to carry out the method according to any preceding claim.~~
12. 12. A non-transitory computer-readable storage medium storing computer-executable instructions that, when executed by a processor of a computing device, cause the computing device to carry out the method in any one of claims 1 to 10.
13. 13. A computer-implemented method comprising, by an originator node:
- Determining (410)~~determining~~ a second public key for each of a plurality of proxy nodes (230A-C) based on a first public key associated with that proxy node (230A-C) and a secret value shared between the originator node (100) and that proxy node (230A-C); wherein a corresponding second private key for each of the proxy nodes (230A-C) is determinable by a given proxy node (230A-C) based on the secret value shared between the originator node (100) and the given proxy node (230A-C) and on a first private key associated with the given proxy node (230A-C) and corresponding to the first public key associated with the given proxy node (230A-C);

~~Generating (420), generating,~~ by the originator node (100), a blockchain transaction (500) including an input (510) and a first (520) and a second (530) output, wherein the input (510) takes $x + r$ units and wherein the first output (520) provides x units to an output address and the second output (530) provides $d + r$ units to a 1-of- n multi-signature address unlockable using any one of the second private keys;

digitally signing (430) the blockchain transaction (500); and

distributing (440) the signed transaction (500) to the proxy nodes (230A-C) via a network.

14. The method of claim 13 wherein distributing the signed transaction (500) includes sending an identifier of the transaction.
15. 15. The method of claim 13 or 14 wherein distributing the identifier of the signed transaction to the proxy nodes (230A-C) comprises sending a respective indication of the identifier of the signed transaction to each of the proxy nodes (230A-C).-
16. 16. The method of claim 15 wherein the respective indication sent to a given one of the proxy nodes (230A-C) is encrypted using a public key of that proxy node (230A-C).-
17. 17. The method of any one of claims 13 to 16, wherein the originator node (100) has an associated asymmetric encryption key pair comprising a public key and a private key and wherein the secret value shared between the originator node (100) and a given proxy node (230A-C) is derivable by the originator node (100) based on its private key and the public key of the given proxy node (230A-C) and by the given proxy node (230A-C) based its private key and the public key of the originator node (100).-
18. 18. The method of any one of claims 13 to 17 wherein the asymmetric encryption key pairs are elliptical-curve key pairs and wherein establishing the secret value shared between the originator node and a particular proxy node corresponds to an Elliptical-Curve Diffie-Hellman (ECDH) key exchange.
19. 19. A computing device comprising
 - a processor;
 - a memory;
 - a network interface; and

a non-transitory computer-readable storage medium storing computer-executable instructions that, when executed by the processor, cause the computing device to carry out the method of any one of claims 13 to 18.

~~executable instructions that, when executed by the processor, cause the computing device to carry out the method of any one of claims 13 to 18.~~

20. A non-transitory computer-readable storage medium storing computer-executable instructions that when executed by a processor of a computing device, cause the computing device to carry out the method in any one of claims 13 to 18.