

CLAIMS:

1. A computer-implemented method of fault-resistant multi-node communication, the communication having a plurality of participating nodes, each node having its own public key and private key, each node having a respective output address to which the communication is to assign tokens, the method, comprising:
 - encrypting a first output address associated with said one of the participating nodes using a first public key associated with said one of the participating nodes;
 - adding the encrypted first output address to a set of encrypted output addresses;
 - shuffling the order of the encrypted output addresses in the set;
 - sending the set to a next node;
 - receiving a further shuffled set of addresses from another of the participating nodes, the further shuffled set of addresses including the encrypted first output address;
 - replacing the encrypted first output address in the further shuffled set of addresses with the first output address; and
 - forwarding the further shuffled set of addresses containing the first output address to a subsequent node.
2. The method claimed in claim 1, wherein replacing the encrypted first output address in the further shuffled set of addresses with the first output address comprises
 - encrypting the first output address with a originator's public key to obtain a final encrypted first output address, a second public key being associated with an originator node; and
 - replacing the encrypted first output address with the final encrypted first output address.

3. The method claimed in claim 1 or claim 2, wherein adding the encrypted first output address further comprises first receiving an encrypted set from a prior participating node and decrypting the encrypted set to obtain the set of encrypted output addresses.
4. The method claimed in claim 3, wherein sending the set to a next node comprises encrypting the set using a second public key associated with the next node.
5. The method claimed in claim 4, wherein encrypting the set using the second public key excludes encrypting the set with further public keys associated with other participating nodes.
6. The method claimed in any one of claims 1 to 5, wherein sending the set to a next node comprises determining that the one of the participating nodes is not a last node in a first sequence of the participating nodes, and sending the set to the next node in the first sequence.
7. The method claimed in any one of claims 1 to 5, wherein sending the set to a next node comprises determining that the one of the participating nodes is a last node in a first sequence of the participating nodes, and sending the set to a first node in the first sequence, and wherein the first node is an originator of the communication.
8. The method claimed in any one of claims 1 to 7, wherein forwarding the further shuffled set of addresses to the subsequent node comprises determining that the one of the participating nodes is not a final node in a second sequence of the participating nodes, and sending the set to the subsequent node in the second sequence.
9. The method claimed in any one of claims 1 to 7, wherein forwarding the further shuffled set of addresses to the subsequent node comprises determining that the one of the participating nodes is a final node in a second sequence of the participating nodes, and sending the set to a first node in the second sequence, and wherein the first node is an originator of the communication, and wherein the further shuffled set contains all output addresses for the communication.

10. The method claimed in any one of claims 1 to 9, wherein shuffling the order includes randomizing the order of the encrypted output addresses in the set.
11. The method claimed in any one of claims 1 to 10, further comprising first sending a request to participate in the communication, the request including the first public key.
12. The method claimed in any one of claims 1 to 11, wherein the communication includes a blockchain transaction, and wherein each of the respective output addresses comprises an unspent transaction output address owned by its associated participating node.
13. The method claimed in any one of claims 1 to 12, wherein the communication is structured to receive an equal quantity of tokens from a respective input address associated with each participating node and to allocate the same equal quantity of tokens to each of the respective output addresses.
14. The method claimed in any one of claims 1 to 13, further comprising a subsequent operation of approving the communication by signing an input address included in the communication and associated with said one of the participating nodes.
15. A computing device for fault-resistant multi-node communication among a plurality of participating nodes, the computing device being one of the participating nodes, the computer device comprising:
 - a processor;
 - memory;
 - a network interface to provide network connectivity;
 - an application containing computer-executable instructions that, when executed by the processor, cause the processor to carry out the method claimed in any one of claims 1 to 14.
16. A non-transitory processor-readable medium storing processor-executable instructions for fault-resistant multi-node communication among a plurality of

participating nodes, wherein the processor-executable instructions, when executed by a processor in one of the participating nodes, cause the processor to carry out the method claimed in any one of claims 1 to 14.