

Claims

1. A method of implementing a private but traceable primary transaction implementing a transfer of an asset from an originator to a recipient using a third party, using a distributed network of computers implementing a distributed ledger, comprising:
 - (a) recording at the third party information relative to the originator that allows determination of the identity of the originator;
 - (b) recording on the distributed ledger a transfer of the asset from the originator to the third party and verifying that said transfer has been recorded on the distributed ledger;
 - (c) communicating from the originator to the third party an identifier of the recipient, where said communication is not recorded on the distributed ledger;
 - (d) defining a plurality of secondary transactions, each comprising the recipient and a secondary originating party and an asset portion, wherein the combination of asset portions corresponds to the asset and at least some of which secondary originating parties indicate a party other than the originator; and
 - (e) recording on the distributed ledger the plurality of secondary transactions.
2. The method of claim 1, wherein the number of the plurality of secondary transactions is determined by a predetermined method and is at least equal to a predetermined lower bound.
3. The method of claim 2, wherein the number of the plurality of secondary transactions is a random number no more than a predetermined upper bound.
4. The method of claim 1, wherein the third party controls a plurality of wallets on the distributed ledger, and where at least one of the plurality of secondary originating parties is associated with a different wallet than at least one other of the plurality of secondary originating parties.
5. The method of claim 1, wherein recording the plurality of secondary transactions comprises recording the plurality of secondary transactions at a plurality of times.
6. The method of claim 5, wherein at least two of the plurality of times are separated by a time interval determined by a predetermined method and no less than a predetermined lower bound.
7. The method of claim 5, wherein at least two of the plurality of times are separated by a time interval determined by a predetermined method and no more than a predetermined upper bound.

8. The method of claim 1, wherein the third party receives communications specifying a plurality of primary transactions, at least one of which is from the originator and at least one of which is from a party other than the originator, and all of which are to the recipient, and wherein the third party combines the plurality of primary transactions to the recipient and the combined transaction is treated as the primary transaction for the remainder of the method.
9. The method of claim 8, wherein the number of the plurality of secondary transactions is determined by a predetermined method and at least equal to a predetermined lower bound.
10. The method of claim 9, wherein the number of the plurality of secondary transactions is determined by a predetermined method and no more than a predetermined upper bound.
11. The method of claim 1, wherein the third party controls a plurality of wallets on the distributed ledger, and where at least one of the plurality of secondary originating parties is associated with a different wallet than at least one other of the plurality of secondary originating parties.
12. The method of claim 1, wherein recording the plurality of secondary transactions comprises recording the plurality of secondary transactions at a plurality of times.
13. The method of claim 12, wherein at least two of the plurality of times are separated by a time interval determined by a predetermined method and no less than a predetermined lower bound.
14. The method of claim 12, wherein at least two of the plurality of times are separated by a time interval determined by a predetermined method and no more than a predetermined upper bound.
15. The method of claim 1, wherein the originator and the recipient are the same entity.