CLAIMS

WHAT IS CLAIMED IS:

1. A method of internet protocol traceback, comprising:

receiving an init transaction associated with a set of packets to be switched from a first autonomous system to a second autonomous system;

verifying the init transaction;

generating a verify transaction associated with the set of packets when the verifying of the init transaction is successful; and

storing the verify transaction in a global ledger,

wherein the init transaction is generated by the first autonomous system and stored in a neighbor ledger of the second autonomous system.

~~2. The method of claim 1, wherein the init transaction is generated by the first autonomous system and stored in a neighbor ledger of the second autonomous system.~~

~~3~~2. The method of claim 1, wherein the set of packets is identified by an identifier created based on a source internet protocol address of the set of packets, a destination internet protocol address of the set of packets, source ports of the set of packets, destination ports of the set of packets, a protocol associated with the set of packets, a timestamp associated with the set of packets, and a hash of payloads of the set of packets, wherein the init transaction comprises the identifier of the set of packets.

~~4~~3. The method of claim ~~3~~2, wherein the init transaction comprises a digital signature generated by the first autonomous system using a private key of the first autonomous system.

~~5~~4. The method of claim ~~4~~3, wherein the verifying of the init transaction comprises:

determining whether the set of packets associated with the init transaction is received at the second autonomous system;

verifying the digital signature included in the init transaction using a public key of the first autonomous system;

identifying a previous transaction of the init transaction by searching the global ledger; and

verifying that a hash value included in the init transaction matches a hash output of the previous transaction.

~~6~~5. The method of claim ~~5~~4, wherein the set of packets is received at the second autonomous system when a difference between a timestamp associated with packets received at the second autonomous system and the timestamp associated with the set of packets satisfies a threshold value, and other components of an identifier of the received packets and the identifier of the set of packets are the same.

~~7~~6. The method of claim ~~5~~4, wherein the verifying of the init transaction is successful when the set of packets is received at the second autonomous system, and the verifying of the digital signature is successful, and the verifying of the hash value included in the init transaction is successful.

~~8~~7. The method of claim 1, wherein a hash value included in the verify transaction is a hash output of the init transaction.

~~9~~8. A method of internet protocol traceback, comprising:

receiving, by a first autonomous system, a verify transaction recorded in a global ledger, the verify transaction generated by a second autonomous system;

verifying, by the first autonomous system, the verify transaction; and

generating an auditor digital signature using a private key of the first autonomous system when the verifying of the verify transaction is successful, wherein the auditor digital signature is appended to the verify transaction.

~~10~~9. The method of claim ~~9~~8, wherein the verifying of the verify transaction comprises:

verifying a digital signature included in the verify transaction using a public key of the second autonomous system;

identifying an init transaction corresponding to the verify transaction by searching a neighbor ledger of the second autonomous system; and

verifying that a hash value included in the verify transaction matches a hash output of the init transaction.

~~11~~10. The method of claim ~~10~~9, wherein the verifying of the verify transaction is successful when the verifying of the digital signature included in the verify transaction is successful and the verifying of the hash value included in the verify transaction is successful.

~~12~~11. The method of claim ~~10~~9, further comprising:

verifying, by the first autonomous system, the init transaction.

~~13~~12. The method of claim ~~12~~11, wherein the verifying of the init transaction comprises:

identifying a previous transaction of the init transaction by searching the global ledger;

verifying a digital signature included in the init transaction using a public key of a third autonomous system that generates the init transaction; and

verifying that a hash value included in the init transaction matches a hash output of the previous transaction.

~~14~~13. The method of claim ~~13~~12, further comprising:

generating a second auditor digital signature using a private key of the first autonomous system when the verifying of the digital signature included in the init transaction is successful and the verifying of the hash value included in the init transaction is successful, wherein the second auditor digital signature is appended to the init transaction.

~~15~~14. A method of internet protocol traceback, comprising:

retrieving a verify transaction recorded in a global ledger, the verify transaction associated with a set of packets and generated by a destination device for the set of packets, wherein the verify transaction has been successfully audited by at least a threshold number of autonomous systems;

retrieving recursively a previous verify transaction of the verify transaction by searching the global ledger, wherein the previous verify transaction is associated with the set of packets and has been successfully audited by at least the threshold number of autonomous systems; and

identifying a source device for the set of packets when the recursive retrieving terminates.

~~16~~15. The method of claim ~~15~~14, wherein the recursive retrieving terminates when the previous verify transaction fails to be retrieved via searching the global ledger.

~~17~~16. The method of claim ~~15~~14, further comprising deploying preventive or mitigate action on the source device.

~~18~~17. The method of claim ~~15~~14, wherein the previous verify transaction is retrieved based on an initiator value included in the verify transaction.

~~19~~18. The method of claim ~~15~~14, wherein the previous verify transaction is retrieved based on a value in a reserved field of the verify transaction.

~~20~~19. The method of claim ~~15~~14, wherein the verify transaction and the previous verify transaction are successfully audited by at least the threshold number of autonomous systems when each of the verify transaction and the previous verify transaction is appended with at least the threshold number of auditor digital signatures.