CLAIMS

1. A computer-implemented method, the method comprising:

receiving a first identifier of a first phone event involving a first user;

comparing the first identifier with a list of phone fraud identifiers stored in a blockchain managed by one or more devices on a decentralized network; and

in response to the first identifier matches a phone fraud identifier in the list of phone fraud identifiers, notifying the first user that the first phone event involves a risk of phone fraud.

2. The method of claim 1, further comprising:

receiving a second identifier of a second phone event involving a second user; and

adding the second identifier to the list of phone fraud identifiers stored in the blockchain.

3. The method of claim 2, wherein the second identifier includes a caller identification of the second phone event or a fingerprint of the second phone event.

4. The method of claim 3, wherein the fingerprint of the second phone event includes an audio characteristic of the second phone event.

5. The method of claim 2, wherein the second identifier is received from the second user based on a smart contract stored in the blockchain.

6. The method of claim 2, further comprising adding a second user behavior with respect to the second phone event into the blockchain.

7. The method of claim 2, wherein the adding the second identifier into the list of phone fraud identifiers includes:

adding the second identifier into the blockchain; and

classifying the second identifier into the list of phone fraud identifiers.

8. The method of claim 7, wherein the classifying includes:

based on a smart contract stored in the blockchain,

accumulating a number of times the second identifier has been added to the blockchain; and

comparing the number with a threshold number to determine whether the second identifier is classified into the list of phone fraud identifiers.

9. The method of claim 2, wherein the second identifier is received directly from the second user.

10. A system, comprising:

one or more processors; and

one or more computer-readable memories coupled to the one or more processors and having instructions stored thereon that are executable by the one or more processors to perform acts including:

receiving a first identifier of a first phone event involving a first user;

comparing the first identifier with a list of phone fraud identifiers stored in a blockchain managed by one or more nodes on a blockchain network; and

in response to the first identifier matches a phone fraud identifier in the list of phone fraud identifiers, notifying the first user that the first phone event involves a risk of phone fraud.

11. The system of claim 10, wherein the acts include:

receiving a second identifier of a second phone event involving a second user; and

adding the second identifier to the list of phone fraud identifiers stored in the blockchain.

12. The system of claim 11, wherein the second identifier includes a caller identification of the second phone event or a fingerprint of the second phone event.

13. The system of claim 12, wherein the fingerprint of the second phone event includes an audio characteristic of the second phone event.

14. The system of claim 11, wherein the second identifier is received from the second user based on a smart contract stored in the blockchain.

15. The system of claim 11, wherein the acts include adding a second user behavior with respect to the second phone event into the blockchain.

16. The system of claim 11, wherein the adding the second identifier into the list of phone fraud identifiers includes:

adding the second identifier into the blockchain; and

classifying the second identifier into the list of phone fraud identifiers.

17. The system of claim 16, wherein the classifying includes:

based on a smart contract stored in the blockchain,

accumulating a number of times the second identifier has been added to the blockchain; and

comparing the number with a threshold number to determine whether the second identifier is classified into the list of phone fraud identifiers.

18. The system of claim 11, wherein the second identifier is received directly from the second user.

19. A method, comprising:

receiving information of a first fingerprint of a first phone event and a first behavior of a first user with respect to the phone event;

batching the first fingerprint of the first phone event and the first behavior of the first user into a transaction data;

broadcasting the transaction data to nodes of a blockchain network for each of the nodes to add the transaction data into a respective copy of a blockchain maintained at the node.

20. The method of claim 19, further comprising:

receiving information of a second fingerprint of a second phone event;

comparing the second fingerprint of the second phone event with the first fingerprint of the first phone event obtained from a copy of the blockchain to determine whether the second fingerprint matches the first fingerprint; and

in response to the second fingerprint matches the first fingerprint, determining that the second phone event has a same source as the first phone event.