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;

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;

receiving a second identifier of a second phone event involving a second user and a behavior of the second user in the second phone event;

adding the second identifier to the blockchain based on the behavior of the second user in the second phone event;

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.

2. The method of claim 1, wherein the second identifier includes a caller identification of the second phone event or a fingerprint of the second phone event.

3. The method of claim 2, wherein the fingerprint of the second phone event includes an audio characteristic of the second phone event.

4 . The method of claim 1, wherein the second identifier is received directly from the second user.

5 . 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;

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;

receivinga second identifier of a second phone event involving a second user and a behavior of the second user in the second phone event;

adding the second identifier to the blockchain based on the behavior of the second user in the second phone event;

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.

6 . The system of claim 5, wherein the second identifier includes a caller identification of the second phone event or a fingerprint of the second phone event.

7 . The system of claim 6, wherein the fingerprint of the second phone event includes an audio characteristic of the second phone event.

8 . The system of claim 5, wherein the second identifier is received directly from the second user.