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 block of transaction data comprising an identifier of a smart contract and a second identifier of a second phone event involving a second user, and wherein the block of transaction data is generated based on requirements of the smart contract;

identifying the smart contract stored in the blockchain based on the identifier included in the block and adding the second identifier to the list of phone fraud identifiers stored in the blockchain based on the smart contract;

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, further comprising adding a second user behavior with respect to the second phone event into the blockchain.

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

6. 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;

receiving a block of transaction data comprising an identifier of a smart contract and a second identifier of a second phone event involving a second user, and wherein the block of transaction data is generated based on requirements of the smart contract;

identifying the smart contract stored in the blockchain based on the identifier included in the block and adding the second identifier to the list of phone fraud identifiers stored in the blockchain based on the smart contract;

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.

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

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

9. The system of claim 6, wherein the acts include adding a second user behavior with respect to the second phone event into the blockchain.

10. The system of claim 6, wherein the second identifier is received directly from the second user.