THE INVENTION CLAIMED IS:

1. A computer-implemented method comprising:

storing, with at least one processor, a local copy of a shared hash map, wherein the shared hash map includes a plurality of identifiers mapped to a plurality of buckets by at least one hash function, wherein one or more buckets of the plurality of buckets include at least one blockchain, wherein the at least one blockchain includes fraud data associated with one or more fraudulent transactions;

receiving, with at least one processor, transaction data associated with at least one transaction, wherein the transaction data includes at least one identifier;

accessing, with at least one processor, the fraud data in the at least one blockchain from the local copy of the shared hash map based on the at least one hash function and the at least one identifier; and

determining, with at least one processor, authorization data associated with the at least one transaction based on the fraud data, wherein the authorization data is associated with an authorization or a denial of the at least one transaction.

2. The computer-implemented method of claim 1, further comprising:

updating, with at least one processor, the at least one blockchain in the shared hash map based on the authorization data.

3. The computer-implemented method of claim 1, wherein the fraud data includes at least one of the following: an indication to automatically authorize a transaction associated with the at least one identifier, an indication to automatically deny a transaction associated with the at least one identifier, a probability that a transaction associated with the at least one identifier is a fraudulent transaction, or any combination thereof.

The computer-implemented method of claim 3, wherein the at least one blockchain includes a plurality of blocks corresponding to a plurality of prior transactions associated with the at least one identifier, wherein at least one block in the at least one blockchain includes the probability that a transaction associated with the at

least one identifier is a fraudulent transaction, and wherein the probability is based on the plurality of prior transactions in the plurality of blocks of the at least one blockchain.

5. The computer-implemented method of claim 1, wherein the one or more buckets of the plurality of buckets include a plurality of blockchains, wherein a first blockchain of the plurality of blockchains includes a first plurality of blocks corresponding to a first plurality of prior transactions associated with the at least one identifier, and wherein a second blockchain of the plurality of blockchains includes a second plurality of blocks corresponding to a second plurality of prior transactions associated with the at least one identifier.

6. The computer-implemented method of claim 1, wherein the at least one identifier includes personally identifiable information (PII), wherein the PII includes at least one of the following: a device fingerprint, a media access control (MAC) address, a personal account number (PAN), a bank account number, an email address, a telephone number, a social security number, an IP address, a shipping address, or any combination thereof.

7. A computer-implemented method comprising:

storing, with at least one processor, a shared hash map, wherein the shared hash map includes a plurality of identifiers mapped to a plurality of buckets by at least one hash function, wherein the plurality of buckets include a plurality of blockchains associated with the plurality of identifiers, wherein the plurality of blockchains include fraud data associated with a plurality of fraudulent transactions;

receiving, with at least one processor, a first update to the shared hash map from a first system, wherein the first update is associated with at least one identifier; and

providing, with at least one processor, a copy of the shared hash map to a second system different than the first system, wherein the copy of the shared hash map includes the first update in at least one blockchain mapped to the at least one first identifier in the shared hash map.

~~The computer-implemented method of claim 7, wherein the at least one blockchain includes a plurality of blocks corresponding to a plurality of prior transactions associated with the at least one identifier, wherein at least one block in the at least one blockchain includes a probability that a transaction associated with the at least one identifier is a fraudulent transaction, and wherein the probability is based on the plurality of prior transactions in the plurality of blocks of the at least one blockchain.~~

~~9. The computer-implemented method of claim 7, further comprising:~~

~~receiving, with at least one processor, a second update to the shared hash map from the second system different than the first system, wherein the second update is associated with the at least one identifier, wherein the copy of the shared hash map includes the second update in the at least one blockchain mapped to the at least one identifier in the shared hash map, and wherein the plurality of blocks in the at least one blockchain includes a first block including a first identifier of the first system stored in association with the first update and a second block including a second identifier of the second system stored in association with the second update.~~

~~10. The computer-implemented method of claim 9, wherein the first system includes a first payment gateway, and wherein the second system includes at least one of the following: a second payment gateway different than the first payment gateway, an issuer system, a transaction service provider system, or any combination thereof.~~

~~11. A system comprising at least one processor programmed and/or configured to:~~

~~store a local copy of a shared hash map, wherein the shared hash map includes a plurality of identifiers mapped to a plurality of buckets by at least one hash function, wherein one or more buckets of the plurality of buckets include at least one blockchain, wherein the at least one blockchain includes fraud data associated with one or more fraudulent transactions;~~

receive transaction data associated with at least one transaction, wherein the transaction data includes at least one identifier;

access the fraud data in the at least one blockchain from the local copy of the shared hash map based on the at least one hash function and the at least one identifier; and determine authorization data associated with the at least one transaction based on the fraud data, wherein the authorization data is associated with an authorization or a denial of the at least one transaction.

12. The system of claim 11, wherein the at least one processor is further programmed and/or configured to:

update the at least one blockchain in the shared hash map based on the authorization data.

13. The system of claim 11, wherein the fraud data includes at least one of the following: an indication to automatically authorize a transaction associated with the at least one identifier, an indication to automatically deny a transaction associated with the at least one identifier, a probability that a transaction associated with the at least one identifier is a fraudulent transaction, or any combination thereof.

14. The system of claim 13, wherein the at least one blockchain includes a plurality of blocks corresponding to a plurality of prior transactions associated with the at least one identifier, wherein at least one block in the at least one blockchain includes the probability that a transaction associated with the at least one identifier is a fraudulent transaction, and wherein the probability is based on the plurality of prior transactions in the plurality of blocks of the at least one blockchain.

15. The system of claim 11, wherein the one or more buckets of the plurality of buckets include a plurality of blockchains, wherein a first blockchain of the plurality of blockchains includes a first plurality of blocks corresponding to a first plurality of prior transactions associated with the at least one identifier, and wherein a second blockchain of the plurality of blockchains includes a second plurality of blocks

corresponding to a second plurality of prior transactions associated with the at least one identifier.

16. The system of claim 11, wherein the at least one identifier includes personally identifiable information (PII), wherein the PII includes at least one of the following: a device fingerprint, a media access control (MAC) address, a personal account number (PAN), a bank account number, an email address, a telephone number, a social security number, an IP address, a shipping address, or any combination thereof.

17. A system comprising at least one processor programmed and/or configured to:

store a shared hash map, wherein the shared hash map includes a plurality of identifiers mapped to a plurality of buckets by at least one hash function, wherein the plurality of buckets include a plurality of blockchains associated with the plurality of identifiers, wherein the plurality of blockchains include fraud data associated with a plurality of fraudulent transactions;

receive a first update to the shared hash map from a first system, wherein the first update is associated with at least one identifier; and

provide a copy of the shared hash map to a second system different than the first system, wherein the copy of the shared hash map includes the first update in at least one blockchain mapped to the at least one first identifier in the shared hash map.

18. The system of claim 17, wherein the at least one blockchain includes a plurality of blocks corresponding to a plurality of prior transactions associated with the at least one identifier, wherein at least one block in the at least one blockchain includes a probability that a transaction associated with the at least one identifier is a fraudulent transaction, and wherein the probability is based on the plurality of prior transactions in the plurality of blocks of the at least one blockchain.

~~19. The system of claim 17, wherein the at least one processor is further programmed and/or configured to:~~

~~receive a second update to the shared hash map from the second system different than the first system, wherein the second update is associated with the at least one identifier, wherein the copy of the shared hash map includes the second update in the at least one blockchain mapped to the at least one identifier in~~

~~the shared hash map, and wherein the plurality of blocks in the at least one blockchain includes a first block including a first identifier of the first system stored in association with the first update and a second block including a second identifier of the second system stored in association with the second update.~~

~~20. The system of claim 19, wherein the first system includes a first payment gateway, and wherein the second system includes at least one of the following: a second payment gateway different than the first payment gateway, an issuer system, a transaction service provider system, or any combination thereof.~~

1. A computer-implemented method comprising:

storing, with a first system, a local copy of a shared hash map stored at a hash map system, wherein the shared hash map includes a plurality of identifiers mapped to a plurality of buckets by at least one hash function, wherein one or more buckets of the plurality of buckets include at least one blockchain including a plurality of blocks corresponding to a plurality of prior transactions associated with at least one identifier of the plurality of identifiers, wherein the plurality of blocks in the at least one blockchain includes fraud data associated with the plurality of prior transactions, wherein the plurality of blocks includes a first block including an identification of the first system that added the first block to the at least one blockchain, wherein the identification of the first system is stored in association with a first update to the at least one blockchain in the first block, wherein the plurality of blocks includes a second block including an identification of a second system that added the second block to the at least one blockchain, wherein the second system is different than the first system, wherein the identification of the second system is stored in association with a second update to the at least one blockchain in the second block, and wherein the fraud data stored in a

latest block added to the at least one blockchain is determined based on the fraud data stored in the plurality of blocks including the first block and the second block;

receiving, with the first system, transaction data associated with at least one transaction, wherein the transaction data includes at least one identifier;

accessing, with the first system, the fraud data in the at least one blockchain from the local copy of the shared hash map based on the at least one hash function and the at least one identifier;

determining, with the first system, authorization data associated with the at least one transaction based on the fraud data stored in the latest block added to the at least one blockchain, wherein the authorization data is associated with an authorization or a denial of the at least one transaction;

authorizing or denying the at least one transaction based on the authorization data determined based on the fraud data accessed in the at least one blockchain from the local copy of the shared hash map;

determining, with the first system, based on the fraud data associated with the plurality of prior transactions in the at least one block chain and fraud data associated with the at least one transaction, updated fraud data fora further update to the at least one blockchain;

updating, with the first system, the at least one blockchain in the shared hash map stored at the hash map system to include a further block including the identification of the first system that added the further block to the at least one blockchain stored in association with the further update to the at least one blockchain in the further block including the updated fraud data; and

after updating the at least one blockchain in the shared hash map, refreshing, with the first system, based on the updated at least one blockchain in the shared hash map stored at the hash map system, the local copy of the shared hash map stored with the first system to include the at least one blockchain including the first block including the identification of the first system stored in association with the first update, the second block including the identification of the second system that added the second block and is different than the first system stored in association with the second update in the second block, and the further block including the identification of the first system that added the further block stored in association with the further update in the further block.

2. The computer-implemented method of claim 1, wherein the fraud data includes at least one of the following: an indication to automatically authorize a transaction associated with the at least one identifier, an indication to automatically deny a transaction associated with

the at least one identifier, a probability that a transaction associated with the at least one identifier is a fraudulent transaction, or any combination thereof.

3. The computer-implemented method of claim 2, wherein the latest block in the at least one blockchain includes the probability that a transaction associated with the at least one identifier is a fraudulent transaction.

4. The computer-implemented method of claim 1, wherein the one or more buckets of the plurality of buckets include a plurality of blockchains, wherein a first blockchain of the plurality of blockchains includes a first plurality of blocks corresponding to a first plurality of prior transactions associated with the at least one identifier, and wherein a second blockchain of the plurality of blockchains includes a second plurality of blocks corresponding to a second plurality of prior transactions associated with the at least one identifier.

5. The computer-implemented method of claim 1, wherein the at least one identifier includes personally identifiable information (PII), wherein the P1 includes at least one of the following: a device fingerprint, a media access control (MAC) address, a primary account number (PAN), a bank account number, an email address, a telephone number, a social security number, an IP address, a shipping address, or any combination thereof.

6. The computer-implemented method of claim 1, further comprising: identifying, with the first system, based on one or more blocks in the blockchain, one or more systems that have updated the blockchain.

7. The computer-implemented method of claim 6, further comprising: revoking, with the first system, access of the one or more systems to the shared hash map at the hash map system.

8. A system comprising at least one processor programmed and/or configured to:

store a local copy of a shared hash map stored at a hash map system, wherein the shared hash map includes a plurality of identifiers mapped to a plurality of buckets by at least one hash function, wherein one or more buckets of the plurality of buckets include at least one blockchain including a plurality of blocks corresponding to a plurality of prior transactions associated with at least one identifier of the plurality of identifiers, wherein the plurality of blocks in the at least one blockchain includes fraud data associated with the plurality of prior transactions, wherein the plurality of blocks includes a first block including an identification

of a first system that added the first block to the at least one blockchain, wherein the identification of the first system is stored in association with a first update to the at least one blockchain in the first block, wherein the plurality of blocks includes a second block including an identification of a second system that added the second block to the at least one blockchain, wherein the second system is different than the first system, wherein the identification of the second system is stored in association with a second update to the at least one block-chain in the second block, and wherein the fraud data stored in a latest block added to the at least one blockchain is determined based on the fraud data stored in the plurality of blocks including the first block and the second block;

receive transaction data associated with at least one transaction, wherein the transaction data includes at least one identifier;

access the fraud data in the at least one blockchain from the local copy of the shared hash map based on the at least one hash function and the at least one identifier;

determine authorization data associated with the at least one transaction based on the fraud data stored in the latest block added to the at least one blockchain, wherein the authorization data is associated with an authorization or a denial of the at least one transaction;

authorize or deny the at least one transaction based on the authorization data determined based on the fraud data accessed in the at least one blockchain from the local copy of the shared hash map;

determine, based on the fraud data associated with the plurality of prior transactions in the at least one block-chain and fraud data associated with the at least one transaction, updated fraud data fora further update to the at least one blockchain;

update, the at least one blockchain in the shared hash map stored at the hash map system to include a further block including the identification of the first system that added the further block to the at least one blockchain stored in association with the further update to the at least one blockchain in the further block including the updated fraud data; and

after updating the at least one blockchain in the shared hash map, refresh, based on the updated at least one blockchain in the shared hash map stored at the hash map system, the local copy of the shared hash map stored with the first system to include the at least one blockchain including the first block including the identification of the first system stored in association with the first update, the second block including the identification of the second system that added the second

block and is different than the first system stored in

association with the second update in the second block, and the further block including the identification of the first system that added the further block stored in association with the further update in the further block.

9. The system of claim 8, wherein the fraud data includes at least one of the following: an indication to automatically authorize a transaction associated with the at least one identifier, an indication to automatically deny a transaction associated with the at least one identifier, a probability that a transaction associated with the at least one identifier is a fraudulent transaction, or any combination thereof.

10. The system of claim 9, wherein the latest block in the at least one blockchain includes the probability that a transaction associated with the at least one identifier is a fraudulent transaction.

11. The system of claim 8, wherein the one or more buckets of the plurality of buckets include a plurality of blockchains, wherein a first blockchain of the plurality of blockchains includes a first plurality of blocks corresponding to a first plurality of prior transactions associated with the at least one identifier, and wherein a second blockchain of the plurality of blockchains includes a second plurality of blocks corresponding to a second plurality of prior transactions associated with the at least one identifier.

12. The system of claim 8, wherein the at least one identifier includes personally identifiable information (PII), wherein the P1 includes at least one of the following: a device fingerprint, a media access control (MAC) address, a primary account number (PAN), a bank account number, an email address, a telephone number, a social security number, an IP address, a shipping address, or any combination thereof.