

CLAIMS

What is claimed is:

1. A method, comprising:

5 executing, by at least one blockchain computing device in a blockchain network, a zero-knowledge proof (ZKP) smart contract in response to receiving a proof, a customer hash, a merchant hash, and a purchase amount from a merchant computing device during a payment process;

10 executing, by the at least one blockchain computing device via the ZKP smart contract, a validate function, wherein the validate function is executed by inputting a verification key, the proof, and the customer hash into the validate function, ~~and~~ wherein the validate function is associated with a zero-knowledge proof algorithm, the proof having been generated by a customer computing device based at least in part on a proof function associated with the ZKP algorithm, and the proof function having been executed by inputting a proving key, the customer hash, and a payment hash into the proof algorithm;

15 adjusting, by the at least one blockchain computing device via the ZKP smart contract, a customer account balance associated with the customer hash in response to the validate function passing, wherein the customer account balance is adjusted based on the purchase amount, for the customer account balance to be maintained on the blockchain network;

20 adjusting, by the at least one computing device via the ZKP smart contract, a merchant account balance associated with the merchant hash, wherein the merchant account balance is adjusted based on the purchase amount, for the merchant account balance to be maintained on the blockchain network; and

25 generating, by the at least one blockchain computing device via the ZKP smart contract, a success notification for writing to the blockchain network, wherein the success notification comprises data indicating that the payment process was successfully completed.

30 ~~2. The method of claim 1, the proof having been generated by a customer computing device based at least in part on a proof function associated with the zero-knowledge proof algorithm; and~~

the proof function having been executed by inputting a proving key, the customer hash, and a payment hash into the proof algorithm.

5 23. The method of claim 12, the proof having been generated in response to a payment purchase being initiated with the merchant computing device, and the payment hash having been generated by inputting customer identifying data and a customer nonce into a hashing algorithm.

10 34. The method of any of claims 1 and 2-3, the zero-knowledge proof algorithm having been created by an issuer computing device, wherein the zero-knowledge proof algorithm comprises a key generator function, the proof function, and the validate function, the proving key and the verification key having been generated based at least in part on an execution of the key generator function, 15 the key generator function having been executed by inputting a random number into the key generator function, and wherein the ZKP smart contract is generated to comprise the validate function.

20 45. The method of any of claims 1-34, the merchant hash having been generated by an issuer computing device based at least in part on a merchant registration request associated with the merchant computing device, and the merchant hash having been generated by inputting merchant identifying data and 25 the merchant nonce into a hashing algorithm.

30 56. The method of claim 45, further comprising generating, by the at least one blockchain computing device via the ZKP smart contract, the merchant hash and the merchant account balance for writing to the blockchain network.

67. The method of any of claims 1-56,

the customer hash having been generated based at least in part on receiving a customer registration request from the customer computing device, and

the customer hash having been generated by inputting the customer identifying data
5 and the customer nonce into the hashing algorithm.

78. The method of claim 67, further comprising generating, by the at least one blockchain computing device via the ZKP smart contract, the customer hash and the customer account balance for writing to the blockchain network.

10

89. A computer-based system, comprising:

a processor; and

a tangible, non-transitory memory configured to communicate with the processor, the tangible, non-transitory memory having instructions stored thereon that, in response to
15 execution by the processor, cause the processor to perform operations comprising:

executing a zero-knowledge proof (ZKP) smart contract in response to receiving a proof, a customer hash, a merchant hash, and a purchase amount from a merchant computing device during a payment process;

executing, by the ZKP smart contract, a validate function, wherein the
20 validate function is configured to be executed by inputting a verification key, the proof, and the customer hash into the validate function, ~~and~~ wherein the validate function is associated with a zero-knowledge proof algorithm, the proof having been generated by a customer computing device based at least in part on a proof function associated with the zero-knowledge proof algorithm, and the proof function having been executed by inputting a
25 proving key, the customer hash, and a payment hash into the proof algorithm;

adjusting, by the ZKP smart contract, a customer account balance associated with the customer hash in response to the validate function passing, wherein the customer account balance is adjusted based on the purchase amount, and for the customer account balance to be maintained on a blockchain network;

adjusting, by the ZKP smart contract, a merchant account balance associated with the merchant hash, wherein the merchant account balance is adjusted based on the purchase amount, for the merchant account balance to be maintained on the blockchain network; and
generating, by the ZKP smart contract, a success notification for writing to the
5 blockchain network, wherein the success notification comprises data indicating that the payment process was successfully completed.

~~10. The computer-based system of claim 9,~~
the proof having been generated by a customer computing device based at least in
10 part on a proof function associated with the zero knowledge proof algorithm; and
the proof function having been executed by inputting a proving key, the customer hash, and a payment hash into the proof algorithm.

~~911. The computer-based system of claim 810,~~
15 the proof having been generated by the customer computing device in response to the payment purchase being initiated with the merchant computing device, and
the payment hash having been generated by inputting customer identifying data and a customer nonce into a hashing algorithm.

~~102. The computer-based system of any of claims 8 and 911,~~
20 the zero-knowledge proof algorithm having been created by an issuer computing device,
wherein the zero-knowledge proof algorithm comprises a key generator function, the proof function, and the validate function;
25 the proving key and the verification key having been generated based at least in part on an execution of the key generator function,
the key generator function having been executed by inputting a random number into the key generator function, and
wherein the ZKP smart contract is generated to comprise the validate function.

30

113. The computer-based system of any of claims 89-102,
the merchant hash having been generated by an issuer computing device based at
least in part on a merchant registration request associated with the merchant computing
device, and

5 the merchant hash having been generated by inputting merchant identifying data and
the merchant nonce into a hashing algorithm.

124. The computer-based system of claim 113, wherein the operations further
comprise generating, by the ZKP smart contract, the merchant hash and the merchant account
10 balance for writing to the blockchain network.

135. The computer-based system of any of claims 89-124,
the customer hash having been generated by an issuer computing device in response
to the issuer computing device receiving a customer registration request from a customer
15 computing device, and

the customer hash having been generated by inputting the customer identifying data
and the customer nonce into the hashing algorithm.