

WHAT IS CLAIMED IS:

1. ~~A computer-implemented method comprising:~~
 - ~~receiving, with a transaction processing system, a transaction request initiated by at least one of a first computing device associated with a first user and a second computing device associated with a second user, the transaction request comprising:~~
 - ~~a first user token comprising a first token identifier and a first account balance, the first account balance encrypted with a public key of a public/private key pair associated with the first user;~~
 - ~~a second user token comprising a second token identifier and a second account balance, the second account balance encrypted with a public key of a public/private key pair associated with the second user; and~~
 - ~~a transaction value;~~
 - ~~in response to verifying the transaction request, generating, with the transaction processing system using a zero-knowledge computation, a new first account balance and a new second account balance based on the first account balance, the second account balance, and the transaction value;~~
 - ~~generating, with the transaction processing system, a new first user token comprising the new first account balance, the new first account balance encrypted with the public key of the public/private key pair associated with the first user; and~~
 - ~~generating, with the transaction processing system, a new second user token comprising the new second account balance, the new second account balance encrypted with the public key of the public/private key pair associated with the second user.~~
2. ~~The computer-implemented method of claim 1, further comprising, in response to receiving, from an issuer system associated with the first user, a first initial account balance encrypted with the public key of the public/private key pair associated with the first user:~~
 - ~~generating, with the transaction processing system, the first user token;~~
 - ~~and~~
 - ~~communicating, with the transaction processing system, the first user token to the first computing device associated with the first user.~~

~~3. The computer-implemented method of claim 2, further comprising, in response to receiving, from an issuer system associated with the second user, a second initial account balance encrypted with the public key of the public/private key pair associated with the second user:~~

~~generating with the transaction processing system, the second user token; and~~

~~communicating, with the transaction processing system, the second user token to the second computing device associated with the second user.~~

~~4. The computer-implemented method of claim 1, wherein the transaction value is encrypted with the public key of the public/private key pair associated with the first user.~~

~~5. The computer-implemented method of claim 4, wherein generating the new first account balance comprises executing, by the transaction processing system, a zero-knowledge subtraction of the transaction value from the first account balance, and wherein the new first user token is digitally signed by the transaction processing system.~~

~~6. The computer-implemented method of claim 5, wherein generating the new second account balance comprises executing, by the transaction processing system, a zero-knowledge addition of the transaction value to the second account balance, and wherein the new second user token is digitally signed by the transaction processing system.~~

~~7. The computer-implemented method of claim 1, wherein the transaction request is digitally signed with a private key of the public/private key pair associated with the first user, and wherein verifying the transaction request comprises decrypting, by the transaction processing system, the transaction request using the public key of the public/private key pair associated with the first user.~~

~~8. The computer-implemented method of claim 7, wherein the transaction request is further digitally signed with a private key of the public/private~~

~~key pair associated with the second user, and wherein verifying the transaction request further comprises decrypting, by the transaction processing system, the transaction request using the public key of the public/private key pair associated with the second user.~~

~~9. A system comprising at least one transaction processing server including at least one processor, the at least one transaction processing server programmed or configured to:~~

~~receive a transaction request initiated by at least one of a first computing device associated with a first user and a second computing device associated with a second user, the transaction request comprising:~~

~~a first user token comprising a first token identifier and a first account balance, the first account balance encrypted with a public key of a public/private key pair associated with the first user;~~

~~a second user token comprising a second token identifier and a second account balance, the second account balance encrypted with a public key of a public/private key pair associated with the second user; and~~

~~a transaction value;~~

~~in response to verifying the transaction request, generate, using a zero-knowledge computation, a new first account balance and a new second account balance based on the first account balance, the second account balance, and the transaction value;~~

~~generate a new first user token comprising the new first account balance, the new first account balance encrypted with the public key of the public/private key pair associated with the first user; and~~

~~generate a new second user token comprising the new second account balance, the new second account balance encrypted with the public key of the public/private key pair associated with the second user.~~

~~10. The system of claim 9, wherein the at least one transaction processing server is further programmed or configured to:~~

~~in response to receiving, from an issuer system associated with the first user, a first initial account balance encrypted with the public key of the public/private key pair associated with the first user;~~

~~_____ generate the first user token; and~~
~~_____ communicate the first user token to the first computing device associated with the first user; and~~
~~_____ in response to receiving, from an issuer system associated with the second user, a second initial account balance encrypted with the public key of the public/private key pair associated with the second user:~~
~~_____ generate the second user token; and~~
~~_____ communicate the second user token to the second computing device associated with the second user.~~

~~_____ 11. The system of claim 9, wherein the transaction value is encrypted with the public key of the public/private key pair associated with the first user.~~

~~_____ 12. The system of claim 11, wherein generating the new first account balance comprises executing a zero-knowledge subtraction of the transaction value from the first account balance, wherein generating the new second account balance comprises executing a zero-knowledge addition of the transaction value to the second account balance, and wherein the new first user token and the new second user token are digitally signed by the at least one transaction processing server.~~

~~_____ 13. The system of claim 9, wherein the transaction request is digitally signed with a private key of the public/private key pair associated with the first user, and wherein verifying the transaction request comprises decrypting the transaction request using the public key of the public/private key pair associated with the first user.~~

~~_____ 14. The system of claim 13, wherein the transaction request is further digitally signed with a private key of the public/private key pair associated with the second user, and wherein verifying the transaction request further comprises decrypting the transaction request using the public key of the public/private key pair associated with the second user.~~

~~_____ 15. A computer program product comprising at least one non-transitory computer-readable medium including program instructions that, when executed by at least one processor, cause the at least one processor to:~~

_____ receive a transaction request initiated by at least one of a first computing device associated with a first user and a second computing device associated with a second user, the transaction request comprising:

_____ a first user token comprising a first token identifier and a first account balance, the first account balance encrypted with a public key of a public/private key pair associated with the first user;

_____ a second user token comprising a second token identifier and a second account balance, the second account balance encrypted with a public key of a public/private key pair associated with the second user; and

_____ a transaction value;

_____ in response to verifying the transaction request, generate, using a zero-knowledge computation, a new first account balance and a new second account balance based on the first account balance, the second account balance, and the transaction value;

_____ generate a new first user token comprising the new first account balance, the new first account balance encrypted with the public key of the public/private key pair associated with the first user; and

_____ generate a new second user token comprising the new second account balance, the new second account balance encrypted with the public key of the public/private key pair associated with the second user.

_____ 16. The computer program product of claim 15, wherein the program instructions further cause the at least one processor to:

_____ in response to receiving, from an issuer system associated with the first user, a first initial account balance encrypted with the public key of the public/private key pair associated with the first user:

_____ generate the first user token; and

_____ communicate the first user token to the first computing device associated with the first user; and

_____ in response to receiving, from an issuer system associated with the second user, a second initial account balance encrypted with the public key of the public/private key pair associated with the second user:

_____ generate the second user token; and

~~communicate the second user token to the second computing device associated with the second user.~~

~~17. The computer program product of claim 15, wherein the transaction value is encrypted with the public key of the public/private key pair associated with the first user.~~

~~18. The computer program product of claim 17, wherein generating the new first account balance comprises executing a zero-knowledge subtraction of the transaction value from the first account balance, wherein generating the new second account balance comprises executing a zero-knowledge addition of the transaction value to the second account balance, and wherein the new first user token and the new second user token are digitally signed by the at least one transaction processing server.~~

~~19. The computer program product of claim 15, wherein the transaction request is digitally signed with a private key of the public/private key pair associated with the first user, and wherein verifying the transaction request comprises decrypting the transaction request using the public key of the public/private key pair associated with the first user.~~

~~20. The computer program product of claim 19, wherein the transaction request is further digitally signed with a private key of the public/private key pair associated with the second user, and wherein verifying the transaction request further comprises decrypting the transaction request using the public key of the public/private key pair associated with the second user.~~

1. A computer-implemented method comprising:

receiving, with a transaction processing system, a transaction request initiated by at least one of a first computing device associated with a first user and a second computing device associated with a second user, the transaction request comprising:

a first user token comprising a first token identifier and a first account balance, the first account balance encrypted with a public key of a

public/private key pair associated with the first user;
a second user token comprising a second token identifier and a second
account balance, the second account balance encrypted with a public
key of a public/private key pair associated with the second user; and
a transaction value;

in response to receiving the transaction request, verifying, with the transaction
processing system, the transaction request; and

in response to verifying the transaction request:

generating, with the transaction processing system, a new first account
balance by executing a zero-knowledge subtraction of the transaction
value from the first account balance;

generating, with the transaction processing system, a new first user
token comprising the new first account balance, the new first account
balance encrypted with the public key of the public/private key pair
associated with the first user;

digitally signing, with the transaction processing system, the new first
user token;

transmitting, with the transaction processing system, the new first user
token to the first computing device for storage on the first computing
device as a current first user token of the first user and for use in future
transactions by the first user;

generating, with the transaction processing system, a new second
account balance by executing a zero-knowledge addition of the
transaction value to the second account balance;

generating, with the transaction processing system, a new second user
token comprising the new second account balance, the new second
account balance encrypted with the public key of the public/private key
pair associated with the second user;

digitally signing, with the transaction processing system, the new second
user token; and

transmitting, with the transaction processing system, the new second
user token to the second computing device for storage on the second

computing device as a current second user token of the second user and for use in future transactions by the second user.

2. The computer-implemented method of claim 1, further comprising, in response to receiving from an issuer system associated with the first user, a first initial account balance encrypted with the public key of the public/private key pair associated with the first user:

generating, with the transaction processing system, the first user token; and communicating, with the transaction processing system, the first user token to the first computing device associated with the first user.

3. The computer-implemented method of claim 2, further comprising, in response to receiving, from an issuer system associated with the second user, a second initial account balance encrypted with the public key of the public/private key pair associated with the second user:

generating with the transaction processing system, the second user token; and communicating with the transaction processing system, the second user token to the second computing device associated with the second user.

4. The computer-implemented method of claim 1, wherein the transaction value is encrypted with the public key of the public/private key pair associated with the first user.

5. The computer-implemented method of claim 1, wherein the transaction request is digitally signed with a private key of the public/private key pair associated with the first user, and wherein verifying the transaction request comprises decrypting, by the transaction processing system, the transaction request using the public key of the public/private key pair associated with the first user.

6. The computer-implemented method of claim 5, wherein the transaction request is further digitally signed with a private key of the public/private key pair associated with the second user, and wherein verifying the transaction request further comprises decrypting, by the transaction processing system, the transaction request using the public key of the public/private key pair associated with the second user.

7. A system comprising at least one transaction processing server including at least one processor, the at least one transaction processing server programmed or configured to:

receive a transaction request initiated by at least one of a first computing device associated with a first user and a second computing device associated with a second user, the transaction request comprising:

a first user token comprising a first token identifier and a first account balance, the first account balance encrypted with a public key of a public/private key pair associated with the first user;

a second user token comprising a second token identifier and a second account balance, the second account balance encrypted with a public key of a public/private key pair associated with the second user; and

a transaction value;

in response to receiving the transaction request, verify the transaction request; and

in response to verifying the transaction request:

generate a new first account balance by executing a zero-knowledge subtraction of the transaction value from the first account balance;

generate a new first user token comprising the new first account balance, the new first account balance encrypted with the public key of the public/private key pair associated with the first user;

digitally sign the new first user token;

transmit the new first user token to the first computing device for storage on the first computing device as a current first user token of the first user and for use in future transactions by the first user;

generate a new second account balance by executing a zero-knowledge addition of the transaction value to the second account balance;

generate a new second user token comprising the new second account balance, the new second account balance encrypted with the public key of the public/private key pair associated with the second user;

digitally sign the new second user token; and

transmit the new second user token to the second computing device for storage on the second computing device as a current second user token of the second user and for use in future transactions by the second user.

8. The system of claim 7, wherein the at least one transaction processing server is further programmed or configured to:

in response to receiving, from an issuer system associated with the first user, a first initial account balance encrypted with the public key of the public/private key pair associated with the first user:

generate the first user token; and

communicate the first user token to the first computing device associated with the first user; and

in response to receiving, from an issuer system associated with the second user, a second initial account balance encrypted with the public key of the public/private key pair associated with the second user:

generate the second user token; and

communicate the second user token to the second computing device associated with the second user.

9. The system of claim 7, wherein the transaction value is encrypted with the public key of the public/private key pair associated with the first user.

10. The system of claim 7, wherein the transaction request is digitally signed with a private key of the public/private key pair associated with the first user, and wherein verifying the transaction request comprises decrypting the transaction request using the public key of the public/private key pair associated with the first user.

11. The system of claim 10, wherein the transaction request is further digitally signed with a private key of the public/private key pair associated with the second user, and wherein verifying the transaction request further comprises decrypting the transaction request using the public key of the public/private key pair associated with the second user.

12. A computer program product comprising at least one non-transitory computer-readable medium including program instructions that, when executed by at least one processor, cause the at least one processor to:

receive a transaction request initiated by at least one of a first computing device associated with a first user and a second computing device associated with a second user, the transaction request comprising:

a first user token comprising a first token identifier and a first account balance, the first account balance encrypted with a public key of a public/private key pair associated with the first user;

a second user token comprising a second token identifier and a second account balance, the second account balance encrypted with a public key of a public/private key pair associated with the second user; and
a transaction value;

in response to receiving the transaction request, verify the transaction request;
and

in response to verifying the transaction request:

generate a new first account balance by executing a zero-knowledge subtraction of the transaction value from the first account balance;

generate a new first user token comprising the new first account balance, the new first account balance encrypted with the public key of the public/private key pair associated with the first user;

digitally sign the new first user token;

transmit the new first user token to the first computing device for storage on the first computing device as a current first user token of the first user and for use in future transactions by the first user;

generate a new second account balance by executing a zero-knowledge addition of the transaction value to the second account balance;

generate a new second user token comprising the new second account balance, the new second account balance encrypted with the public key of the public/private key pair associated with the second user;

digitally sign the new second user token; and

transmit the new second user token to the second computing device for storage on the second computing device as a current second user token of the second user and for use in future transactions by the second user.

13. The computer program product of claim 12, wherein the program instructions further cause the at least one processor to:

in response to receiving, from an issuer system associated with the first user, a first initial account balance encrypted with the public key of the public/private key pair associated with the first user:

generate the first user token; and

communicate the first user token to the first computing device associated with the first user; and

in response to receiving, from an issuer system associated with the second user, a second initial account balance encrypted with the public key of the public/private key pair associated with the second user:

generate the second user token; and

communicate the second user token to the second computing device associated with the second user.

14. The computer program product of claim 12, wherein the transaction value is encrypted with the public key of the public/private key pair associated with the first user.

15. The computer program product of claim 12, wherein the transaction request is digitally signed with a private key of the public/private key pair associated with the first user, and wherein verifying the transaction request comprises decrypting the transaction request using the public key of the public/private key pair associated with the first user.

16. The computer program product of claim 15, wherein the transaction request is further digitally signed with a private key of the public/private key pair associated with the second user, and wherein verifying the transaction request further comprises decrypting the transaction request using the public key of the public/private key pair associated with the second user.