

WHAT IS CLAIMED IS:

- 1 1. A method comprising, the following steps:
 - 2 a) posting, by a user device to a blockchain, a deposit transaction
 - 3 comprising a deposit value and conditions;
 - 4 b) updating, by the user device, a state according to a transaction
 - 5 amount;
 - 6 c) transmitting, by the user device, a state update of the state to a
 - 7 server computer;
 - 8 d) responsive to step c), receiving, by the user device, a payment
 - 9 complete message comprising a tuple from the server computer;
 - 10 e) verifying, by the user device, the conditions; and
 - 11 f) processing, by the user device, a server deposit transaction on the
 - 12 blockchain in response to verifying.
- 1 2. The method of claim 1, wherein the user device is a first user
- 2 device, the payment complete message is a second payment complete message,
- 3 and the tuple is a certificate tuple, and wherein the method further comprises the
- 4 following steps between steps a) and b):
 - 5 transmitting, by the first user device, a payer authorization message to
 - 6 a second user device, the payer authorization message comprising the certificate
 - 7 tuple comprising a transaction identifier, the transaction amount, and a validity time;
 - 8 transmitting, by the first user device, the payer authorization message
 - 9 to the server computer;
 - 10 receiving, by the first user device, a first server authorization message
 - 11 comprising the tuple from the server computer;
 - 12 receiving, by the first user device, a second authorization complete
 - 13 message comprising the tuple from the second user device;
 - 14 transmitting, by the first user device, a payment initiation message
 - 15 comprising the transaction identifier to the second user device and the server
 - 16 computer; and
 - 17 receiving, by the first user device, a first payment complete message
 - 18 comprising the tuple from the second user device.

1 3. The method of claim 2, wherein prior to verifying the conditions,
2 the method comprises:

3 verifying that the first payment complete message and the second
4 payment complete message were received before the validity time.

1 4. The method of claim 1, wherein verifying the conditions further
2 comprises:

3 constructing, by the user device, a witness comprising the state;
4 evaluating, by the user device, the conditions with the witness to output
5 a value; and
6 verifying, by the user device, the conditions if the value is greater than
7 a threshold.

1 5. The method of claim 4, wherein processing the server deposit
2 transaction comprises claiming the value from the deposit value, and wherein the
3 difference between the deposit value and the value is refunded to the server
4 computer.

1 6. The method of claim 1, wherein the deposit transaction is a first
2 deposit transaction and the conditions are first conditions, the method further
3 comprising:

4 posting, by the user device to the blockchain, a second deposit
5 transaction comprising the deposit value and second conditions.

1 7. The method of claim 6, wherein the transaction is a first
2 transaction and the verification of the first conditions is a first verification, and
3 wherein the method further comprises:

4 verifying, by the user device, the second conditions; and
5 posting, by the user device, a second transaction to the blockchain
6 based on the verification of the second conditions.

1 8. The method of claim 6, wherein the second conditions depend
2 on the first conditions.

1 9. A user device comprising:

2 a processor; and
3 a non-transitory computer-readable medium comprising code,
4 executable by the processor, for implementing a method comprising at least the
5 steps of:
6 a) posting, to a blockchain, a deposit transaction comprising a deposit
7 value and conditions;
8 b) updating a state according to a transaction amount;
9 c) transmitting a state update of the state to a server computer;
10 d) responsive to step c), receiving a payment complete message
11 comprising a tuple from the server computer;
12 e) verifying the conditions; and
13 f) processing a server deposit transaction on the blockchain in
14 response to verifying.

1 10. The user device of claim 9, wherein the user device is a first
2 user device, the payment complete message is a second payment complete
3 message, wherein the tuple is a certificate tuple, and wherein the method further
4 comprises the following steps between steps a) and b):
5 transmitting a payer authorization message to a second user device,
6 the payer authorization message comprising the certificate tuple comprising a
7 transaction identifier, the transaction amount, and a validity time;
8 transmitting the payer authorization message to the server computer;
9 receiving a first server authorization message comprising the tuple
10 from the server computer;
11 receiving a second authorization complete message comprising the
12 tuple from the second user device;
13 transmitting a payment initiation message comprising the transaction
14 identifier to the second user device and the server computer; and
15 receiving a first payment complete message comprising the tuple from
16 the second user device.

1 11. The user device of claim 10, wherein the method further
2 comprises:
3 determining a current time; and
4 aborting the method if the current time is greater than the validity time.

1 12. The user device of claim 10, wherein the method further
2 comprises, prior to transmitting the payer authorization message:
3 computing a hash of a random string;
4 generating an authorization initiation message comprising the hash, the
5 transaction identifier, the transaction amount, and the validity time;
6 transmitting the authorization initiation message to the second user
7 device; and
8 receiving, from the second user device, a payee authorization message
9 comprising the tuple.

1 13. The user device of claim 9, wherein if the conditions are not
2 verified, processing the server deposit transaction comprises refunding the server
3 deposit transaction to the server computer.

1 14. The user device of claim 9, wherein if the method is aborted, the
2 deposit transaction is refunded to the user device.

1 15. The user device of claim 9, wherein the state comprises an
2 identifier, a user device balance, and a server balance and wherein updating the
3 state comprises:
4 incrementing the identifier;
5 decreasing the user device balance by the transaction amount; and
6 increasing the server balance by the transaction amount.

1 16. A method comprising at least the steps of:
2 a) posting, by a server computer to a blockchain, a deposit transaction
3 comprising a deposit value and conditions;
4 b) receiving, by the server computer from a user device, a state
5 update;
6 c) updating, by the server computer, a state according to a transaction
7 amount;
8 d) transmitting, by the server computer to the user device, a payment
9 complete message;
10 e) verifying, by the server computer, the conditions; and

11 f) processing, by the server computer, a server deposit transaction on
12 the blockchain in response to verifying.

1 17. The method of claim 16, wherein the user device is a first user
2 device, wherein the blockchain is a first blockchain, the deposit transaction is a first
3 deposit transaction, and the conditions are first conditions, and wherein the payment
4 complete message is a second payment complete message, the method further
5 comprising between steps a) and b):

6 posting, by the server computer to a second blockchain, a second
7 deposit transaction comprising the deposit value and second conditions;

8 receiving, by the server computer from a second user device, a payee
9 authorization message, the payee authorization message comprising a tuple
10 comprising a transaction identifier, a transaction amount, and a validity time by which
11 a transaction response is to be received;

12 receiving, by the server computer from a first user device, a payer
13 authorization message comprising the tuple;

14 comparing, by the server computer, the tuple in the payee authorization
15 message and the tuple in the payer authorization message;

16 transmitting, by the server computer to the first user device, a first
17 server authorization response message comprising the tuple;

18 transmitting, by the server computer to the second user device, a
19 second server authorization message comprising the tuple;

20 receiving, by the server computer from the first user device, a payment
21 initiation message comprising the transaction identifier; and

22 receiving, by the server computer from the second user device, a first
23 payment complete message comprising the transaction identifier.

1 18. The method of claim 17, further comprising:

2 setting, by the server computer, a flag to zero in response to receiving
3 the payer authorization message; and

4 setting, by the server computer, the flag to one in response to receiving
5 the state update.

1 19. The method of claim 17, wherein the state is a first state,
2 wherein the first state comprises a first identifier, a first user device balance, and a

3 first server balance, and a second state comprising a second identifier, a second
4 user device balance, and a second server balance.

1 20. The method of claim 19, further comprising:
2 updating, by the server computer, the first state in response to
3 receiving the payment initiation message by incrementing the first identifier,
4 decreasing the first user device balance by the transaction amount, and increasing
5 the first server balance by the transaction amount; and
6 updating, by the server computer, the second state in response to
7 receiving the first payment complete message by incrementing the second identifier,
8 decreasing the second server balance by the transaction amount, and increasing the
9 second user device balance by the transaction amount.