

- 1 1. A method comprising:
2 receiving, by a validation node from an acceptance node, a transaction
3 record for a transaction conducted between the acceptance node and a user, the
4 transaction record including at least information related to the user and transaction
5 details;
6 identifying, based on the information related to the user, a blockchain
7 associated with the transaction;
8 appending the transaction record to the blockchain;
9 generating a signature by:
10 generating a first hash of at least a portion of the information
11 related to the user;
12 generating a second hash of at least a portion of the transaction
13 details;
14 combining the first hash and the second hash into a text string;
15 and
16 signing the text string, or a derivative of the text string, using a
17 private key associated with the validation node to form the signature; and
18 attaching the signature to the transaction record within the blockchain.
- 1 2. The method of claim 1, wherein combining the first hash and the
2 second hash comprises concatenating the first hash and the second hash.
- 1 3. The method of claim 1, wherein the acceptance node is a
2 computer operated by a resource provider.
- 1 4. The method of claim 1, wherein the encryption key is an RSA
2 encryption key.
- 1 5. The method of claim 1, further comprising hashing the first hash
2 and the second hash to form a third hash, the third hash being the derivative the text
3 string.

2 least a plurality of acceptance nodes.

1 7. The method of claim 1, wherein the plurality of nodes includes at
2 least a plurality of validation nodes.

1 8. A validation node server comprising:
2 one or more processors; and
3 a memory including instructions that, when executed by the one or
4 more processors, cause the validation node server to:
5 receive, from an acceptance node, a transaction information for a
6 transaction conducted between the acceptance node and a user, the transaction
7 information including at least user information and transaction details;
8 identify, based on the user information, a blockchain associated with
9 the transaction;
10 generate a transaction record based at least in part on the transaction
11 information;
12 append the transaction record to the blockchain;
13 generate a signature by:
14 generating a first hash of at least a portion of the user
15 information;
16 generating a second hash of at least a portion of the transaction
17 details;
18 combining the first hash and the second hash into a text string;
19 and
20 signing the text string, or a derivative of the text string, using a
21 private key associated with the validation node to form the signature; and
22 attach the signature to the transaction record within the blockchain.

1 9. The validation node server of claim 8, wherein the instructions
2 further cause the validation node server to distribute a public key within the
3 blockchain network.

2 further cause the validation node server to determine whether the acceptance node
3 is authorized to participate in the blockchain network prior to appending the
4 transaction record to the blockchain.

1 11. The validation node server of claim 8, wherein the first hash of
2 at least a portion of the user information comprises an electronic identifier.

1 12. The validation node server of claim 8, wherein the instructions
2 further cause the validation node server to distribute the blockchain to a client device
3 associated with the user.

1 13. The validation node server of claim 8, wherein combining the
2 first hash and the second hash comprises concatenating the first hash and the
3 second hash.

1 14. The validation node server of claim 83, wherein the instructions
2 further comprise:
3 hashing the first hash and the second hash to form a third hash, the
4 third hash being the derivative the text string.

2 one or more processors; and
3 a memory including instructions that, when executed by the one or
4 more processors, cause the resource provider computer to:
5 receive a request to complete a transaction between the
6 resource provider computer and a user, the request including at least
7 information related to the user;
8 access a user blockchain associated with the user, the user
9 blockchain generated by a validation node server and comprising a plurality of
10 transaction records;
11 verify at least one transaction record of the plurality of
12 transaction records using the information related to the user, information
13 included in the at least one transaction record, and a public key associated
14 with the validation node server;
15 determine, upon verifying the at least one transaction record, a
16 level of risk for the transaction based on the plurality of transaction records;
17 and
18 complete the transaction upon determining that the level of risk
19 for the transaction is below a threshold level of risk.

1 16. The resource provider computer of claim 15, wherein transaction
2 record of the plurality of transaction records is signed using a private key associated
3 with the validation node server.

1 17. The resource provider computer of claim 15, wherein the
2 instructions further cause the resource provider computer to determine a level of
3 trust for each transaction record of the plurality of transaction records.

1 18. The resource provider computer of claim 15, wherein the
2 instructions further cause the resource provider computer to assign a weight value to
3 at least one transaction record of the plurality of transaction records, the level of risk
4 for the transaction determined based at least in part on the assigned weight value.

- 2 value is assigned to at least one transaction record of the plurality of transaction
- 3 records based on a type of the transaction record.

- 1 20. The resource provider computer of claim 18, wherein the weight
- 2 value is assigned to at least one transaction record of the plurality of transaction
- 3 records based on an origination entity associated with the transaction record.