WHAT IS CLAIMED IS:

1. A method comprising:

receiving, by a validation node from an acceptance node, a transaction record for a transaction conducted between the acceptance node and a user, the transaction record including at least information related to the user and transaction details;

identifying, based on the information related to the user, a blockchain associated with the transaction;

appending the transaction record to the blockchain;

generating a signature by:

generating a first hash of at least a portion of the information related to the user;

generating a second hash of at least a portion of the transaction details;

combining the first hash and the second hash into a text string, wherein combining the first hash and the second hash comprises concatenating the first hash and the second hash;

hashing the first hash and the second hash to form a third hash, the third hash being a derivative of the text string;

signing the derivative of the text string, using a private key associated with the validation node to form the signature; and

attaching the signature to the transaction record within the blockchain.

2. The method of claim 1, wherein the acceptance node is a computer operated by a resource provider.

3. The method of claim 1, wherein the private key is an RSA encryption key.

4. A validation node server comprising:

one or more processors; and

a memory including instructions that, when executed by the one or more processors, cause the validation node server to:

receive, from an acceptance node, a transaction information for a transaction conducted between the acceptance node and a user, the transaction information including at least user information and transaction details;

identify, based on the user information, a blockchain associated with the transaction;

generate a transaction record based at least in part on the transaction information;

append the transaction record to the blockchain;

generate a signature by:

generating a first hash of at least a portion of the user information;

generating a second hash of at least a portion of the transaction details;

combining the first hash and the second hash into a text string, wherein combining the first hash and the second hash comprises concatenating the first hash and the second hash;

hashing the first hash and the second hash to form a third hash, the third hash being a derivative of the text string;

signing the derivative of the text string, using a private key associated with the validation node to form the signature; and

attach the signature to the transaction record within the blockchain.

5. The validation node server of claim 4, wherein the instructions further cause the validation node server to distribute a public key within a blockchain network.

6. The validation node server of claim 4, wherein the instructions further cause the validation node server to determine whether the acceptance node is authorized to participate in a blockchain network prior to appending the transaction record to the blockchain.

7. The validation node server of claim 4, wherein the first hash of at least a portion of the user information comprises an electronic identifier.

8. The validation node server of claim 4, wherein the instructions further cause the validation node server to distribute the blockchain to a client device associated with the user.

9. A resource provider computer comprising:

one or more processors; and

a memory including instructions that, when executed by the one or more processors, cause the resource provider computer to:

receive a request to complete a transaction between the resource provider computer and a user, the request including at least information related to the user;

access a user blockchain associated with the user, the user blockchain generated by a validation node server according to claim 4, and comprising a plurality of transaction records;

verify at least one transaction record of the plurality of transaction records using the information related to the user, information included in the at least one transaction record, and a public key associated with the validation node server;

determine, upon verifying the at least one transaction record, a level of risk for the transaction based on the plurality of transaction records; and

complete the transaction upon determining that the level of risk for the transaction is below a threshold level of risk.

10. The resource provider computer of claim 9, wherein the instructions further cause the resource provider computer to determine a level of trust for each transaction record of the plurality of transaction records.

11. The resource provider computer of claim 9, wherein the instructions further cause the resource provider computer to assign a weight value to at least one transaction record of the plurality of transaction records, the level of risk for the transaction determined based at least in part on the assigned weight value.

12. The resource provider computer of claim 11, wherein the weight value is assigned to at least one transaction record of the plurality of transaction records based on a type of the transaction record.

13. The resource provider computer of claim 11, wherein the weight value is assigned to at least one transaction record of the plurality of transaction records based on an origination entity associated with the transaction record.