WHAT IS CLAIMED IS:

1. A method using a node managing a blockchain in a blockchain network, the blockchain comprising an entry point smart contract, a first smart contract, a second smart contract, and a plurality of blocks, the method comprising:

receiving, by the node, a blockchain transaction request comprising transaction parameters associated with a blockchain transaction, the transaction parameters including a master computer digital signature;

verifying, by the entry point smart contract with the second smart contract, at least some of the transaction parameters;

providing, by the entry point smart contract to the first smart contract, a signature validation request comprising the master computer digital signature;

verifying, by the first smart contract, the master computer digital signature;

receiving, by the entry point smart contract from the first smart contract, a signature validation response from the first smart contract;

communicating, by the entry point smart contract with the second smart contract to execute the blockchain transaction request; and

calling, by the second smart contract, the first smart contract to request blockchain tokens to complete the blockchain transaction, wherein the first smart contract acquires and provides the blockchain tokens to an account associated with the second smart contract.

2. The method of claim 1, wherein the first smart contract acquires the blockchain tokens via a token exchange.

3. The method of claim 1, wherein the blockchain transaction transfers an amount of the blockchain tokens from a first user associated with the second smart contract to a second user, wherein the method further comprises:

transmitting, by the second smart contract to a third smart contract, which completes the blockchain transaction.

4. The method of claim 1, wherein the master computer digital signature is received from a master computer that generated the master computer digital signature.

5. The method of claim 4, wherein the master computer stores a master computer private key of a master computer public-private key pair, and produces the master computer digital signature with the master computer private key.

6. The method of claim 1, wherein the master computer digital signature is generated by a master computer, after the master computer initiates an authorization request message with a gateway computer in communication with an authorizing entity computer.

7. The method of claim 6, wherein the authorization request message has an off-chain value.

8. The method of claim 1, wherein the blockchain transaction request is received from an interaction application on a communication device.

9. The method of claim 8, wherein the transaction parameters are generated using the communication device.

10. The method of claim 9, wherein the communication device is a mobile phone.

11. The method of claim 1, wherein the blockchain transaction request is received from a master computer, wherein the master computer generates the master computer digital signature after the master computer initiates an authorization request message with a gateway computer in communication with an authorizing entity computer.

12. The method of claim 11, The method of claim 12, wherein before initiating the authorization request message, the master computer receives an off-

chain transaction request comprising the transaction parameters and a credential or credential from an access device that interacts with a user device comprising a user device private key, wherein the user device does not have remote communication capabilities.

13. The method of claim 12, and wherein the user device is in the form of a card.

14. A computer node for managing a blockchain comprising an entry point smart contract, a first smart contract, a second smart contract, and a plurality of blocks comprising:

a processor;

and a non-transitory computer readable medium, the non-transitory computer readable medium comprising code, executable by the processor for performing operations comprising:

receiving by the computer node, a blockchain transaction request comprising transaction parameters associated with a blockchain transaction, the transaction parameters including a master computer digital signature;

verifying, by the entry point smart contract with the second smart contract, at least some of the transaction parameters;

providing, by the entry point smart contract to the first smart contract, a signature validation request comprising the master computer digital signature;

verifying, by the first smart contract, the master computer digital signature;

receiving, by the entry point smart contract from the first smart contract, a signature validation response from the first smart contract;

communicating, by the entry point smart contract with the second smart contract to execute the blockchain transaction request; and

calling, by the second smart contract, the first smart contract to request blockchain tokens to complete the blockchain transaction, wherein the first smart contract acquires and provides the blockchain tokens to an account associated with the second smart contract.

15. A method comprising:

transmitting, by a communication device to a master computer, an off-chain transaction request comprising a credential or an off-chain token for an off-chain transaction in association with a blockchain transaction, wherein the master computer initiates an authorization request message with a gateway computer in communication with an authorizing entity computer;

receiving, by the communication device, an off-chain transaction response from the master computer, the off-chain transaction response comprising a master computer digital signature, the master computer digital signature indicating approval of the authorization request message; and

transmitting, by the communication device to a node in a blockchain network managing a blockchain, a blockchain transaction request comprising

transaction parameters associated with the blockchain transaction, the transaction parameters including the master computer digital signature, wherein the node verifies the transaction parameters with a second smart contract, and provides a signature validation request comprising the master computer digital signature to a first smart contract using a first smart contract address and receives a signature validation response from the first smart contract, and executes the blockchain transaction by communicating with the second smart contract, wherein second smart contract calls the first smart contract to request funds from first smart contract, which acquires and provides blockchain tokens to a second smart contract account.