CLAIMS

1. A system comprising:

(a) a first node having a key generator,

wherein the first node is an IOT component, a server, a laptop computer, a tablet PC, a smart phone, or a tablet PC; wherein the first node comprises an off-the-shelf packaged resistive random access memory (ReRAM) chip; and

wherein the ReRAM chip provides both a neuromorphic computing function for the first node and a physical unclonable function (PUF) for the key generator; and

(b) a second node configured to remotely send an attestation request to the first node, wherein the first node is configured to respond to the attestation request as part of a verification to join the network;

wherein the verification comprises using a challenge-response authentication protocol;

wherein the second node is part of a distributed ledger; and

wherein a public-private key pair is generated for the first node, wherein the private key is generated for the first node via the key generator, and the public key is registered with the distributed ledger.

2. The system of claim 1, wherein the public key is encrypted before registration with the distributed ledger.

3. The system of claim 2, wherein the security of the first node is verified through the remote attestation of the public key on the distributed ledger.

4. The system of claim 1, wherein the ReRAM chip is arranged in a crossbar array format.

5 . The system of claim 4, wherein the crossbar array format is a multi-layer crossbar array.