

CLAIMS

1. ——— An apparatus comprising:

————— a network interface configured to receive encrypted tag data that is read by a reader from a tag associated with a physical object and signed with a key assigned to the tag; ~~by a blockchain network,~~ wherein when the reader is trusted, the reader signs the key and sends the tag data, and when the reader is untrusted, the tag sends a challenge to the blockchain network and when a correct response from the blockchain network is received, the tag passes the tag data through the reader;

————— a processor configured to determine that the signed tag data is validly signed based on a corresponding key pair of the tag which is accessible to ~~the blockchain peer, and determine, via the blockchain peer,~~ a blockchain peer, generate, via a blockchain peer of the blockchain network, a session key based on a secret value shared between the blockchain network and the tag, decrypt the encrypted tag data based on the session key, and determine whether the decrypted tag data satisfies one or more predefined conditions of the physical object; and

————— a storage configured to store the determination via a blockchain ~~database,~~ ledger.

2. ——— The apparatus of claim 1, wherein the encrypted tag data comprises sensor data that is sensed by one or more sensor devices that are coupled to the tag.

3. ——— The apparatus of claim 2, wherein the sensor data comprises a value of one or more of temperature, location, fluid flow rate, pH, velocity, acceleration, viscosity, illumination, spectral measurements, image, pressure, vibration, gravitational forces, and rotational speed.

4. ——— The apparatus of claim 2, wherein the processor is further configured to verify ~~the~~ an authenticity of the tag based on a sensor identifier that is included within the encrypted tag data.

5. ——— The apparatus of claim 1, wherein the processor is configured to determine whether the encrypted tag data violates one or more predefined conditions embedded within logic of a chaincode that runs on the blockchain peer.

6. ——— The apparatus of claim 1, wherein the network interface is further configured to transmit, via chaincode that runs on the blockchain peer, an alert to a computer device associated with the physical object.

7. — The apparatus of claim 1, wherein the tag data is further signed by a key assigned to ~~the~~a reader, and the processor is further configured to determine that the signed tag data is validly signed based on a corresponding key pair of the reader which is accessible to the blockchain peer.
8. — The apparatus of claim 1, wherein the processor is configured to store an identifier of the tag and the tag data as a key-value pair in a state database of the blockchain.
9. — A method comprising:
- retrieving sensor data from one or more hardware sensors coupled to a tag and storing the sensor data within a memory of the tag;
 - receiving a read request from a reader associated with a blockchain ~~platform;~~network, wherein when the reader is trusted, the reader signs a key and sends a tag data, and when the reader is untrusted, the tag sends a challenge to the blockchain network and when a correct response from the blockchain network is received, the tag passes the tag data through the reader;
 - verifying ~~the~~an authenticity of the blockchain ~~platform~~network based on handshake protocol between the tag and the blockchain network via the reader; ~~and~~
 - generating a session key based on a secret value shared with a blockchain platform and encrypting the sensor data based on the session key; and
- in response to a successful verification of the blockchain platform, signing the encrypted sensor data based on a private key of the tag, and transmitting the signed encrypted sensor data to the reader.
10. — The method of claim 9, further comprising checking, via a bootloader on the tag, ~~the~~an integrity of software running on the tag during a power up of the tag.
11. — The method of claim 9, wherein the verifying the authenticity of the blockchain ~~platform~~network comprises receiving data signed by the blockchain ~~platform~~network, and verifying the signed data based on a corresponding key of the blockchain ~~platform~~network stored by the tag.
12. — The method of claim 9, further comprising verifying, by the tag, ~~the~~an authenticity of the reader based on a handshake protocol with the reader.

13.——The method of claim 9, further comprising performing a key exchange with the blockchain ~~platform~~network to establish ~~a~~the secret value shared ~~key~~ between the tag and the blockchain ~~platform~~network.

~~14.——The method of claim 13, wherein the signing of the sensor data further comprises encrypting the sensor data based on the shared key with the blockchain platform prior to transmitting the signed sensor data to the reader.~~

~~15.——~~14. The method of claim 9, further comprising detecting, via the tag, that a data violation has occurred based on values of ~~the~~a decrypted sensor data ~~retrieved from the one or more hardware sensors and~~ storing the data violation within the memory.

~~16.——~~15. The method of claim 9, wherein the memory of the tag is read and write protected thereby preventing the private key from being read or modified by an external entity.

~~17.——~~16. A method comprising:

——receiving, via a blockchain peer of a blockchain network, encrypted tag data that is read by a reader from a tag associated with a physical object and signed with a key assigned to the tag;— by the blockchain network, wherein when the reader is trusted, the reader signs the key and sends the tag data, and when the reader is untrusted, the tag sends a challenge to the blockchain network and when a correct response from the blockchain network is received, the tag passes the tag data through the reader;

——determining, via a~~the~~ blockchain peer, that the signed tag data is validly signed based on a corresponding key pair of the tag which is accessible to the blockchain peer;

——generating, via a blockchain peer of the blockchain network, a session key based on a secret value shared between the blockchain network and the tag, decrypt the encrypted tag data based on the session key;

determining, via the blockchain peer, whether the tag data satisfies of one or more predefined conditions of the physical object; and

——storing the determination via a blockchain ~~database-~~ledger.

~~18.——~~17. The method of claim ~~47~~16, further comprising verifying ~~the~~an authenticity of the tag based on a sensor identifier included within the tag data.

~~19.~~—18. The method of claim ~~47~~16, wherein the determining comprises determining whether the tag data violates one or more predefined conditions embedded within logic of a chaincode running on the blockchain peer.

~~20.~~—19. The method of claim ~~47~~16, further comprising transmitting, via chaincode running on the blockchain peer, an alert to a computing device associated with the physical object.