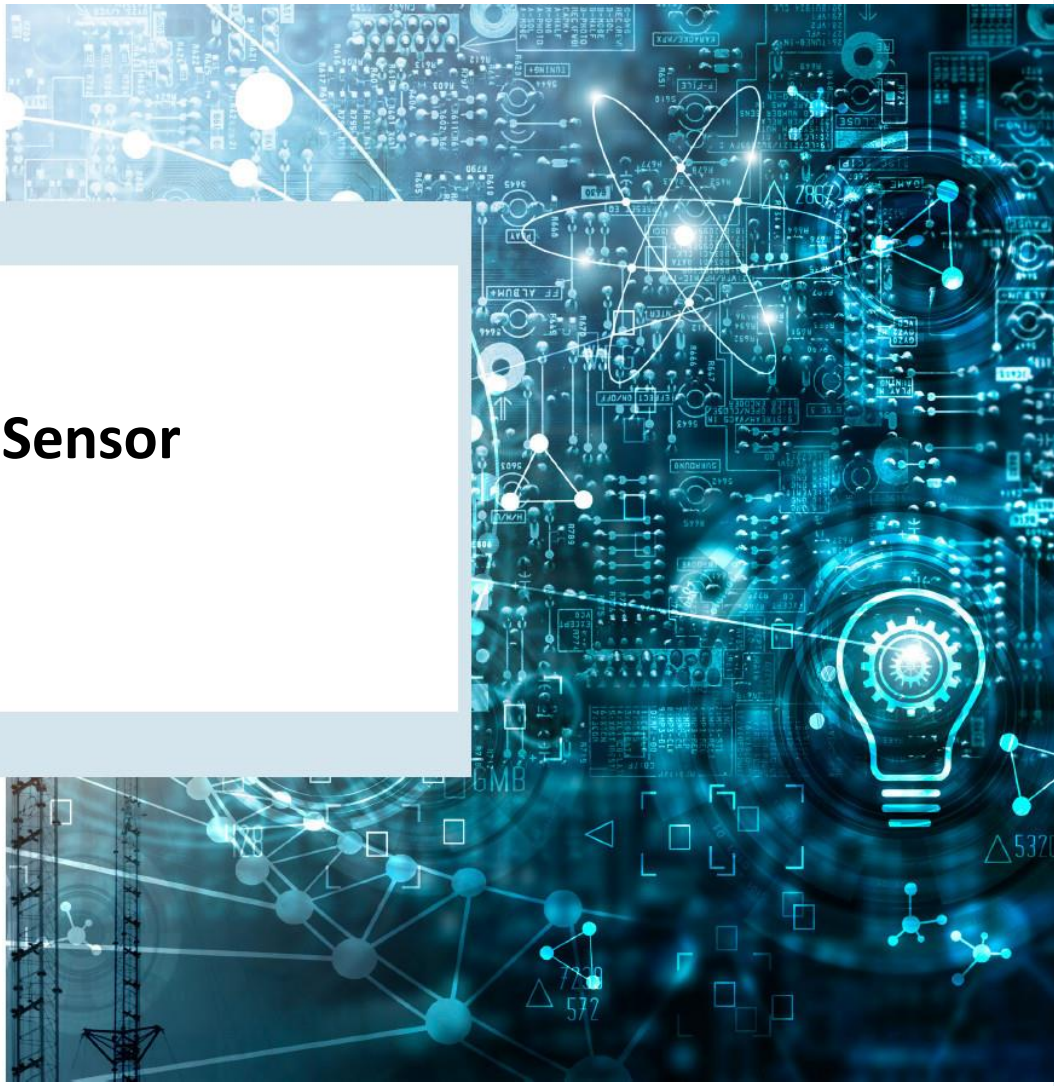
CHIPKIN



Brochure

Secure Block Chain Sensor

Overview

The Secure Block Chain Sensor addresses the critical issue of trust in downstream supply chains by providing a tamper-proof and immutable system for monitoring and verifying production data. This innovative technology ensures the integrity of components supplied by downstream suppliers, thereby safeguarding the quality of products and services.

Can you trust your downstream suppliers?

The quality of your products and services is dependent on the quality of the components supplied by your downstream supply chain. How do you know you can trust the quality and production data they provide? The fact is you can't.


Food | October 20, 2017 | By Kate Dwyer

Trader Joe's Recalls Salad for Possible Listeria Contamination

The bacteria can cause serious illness.

That is where the Secure Block Chain Sensor comes in. These sensors are deployed in your supplier's production facilities. You choose the measurements that are meaningful to you. The sensors have wireless capability, so they can be easily deployed and installed at minimal cost. The sensors are tamper proof. The Secure Block Chain Sensor knows its location, knows if the sensor has been tampered with, knows the sensor readings. This data is encrypted and sent to the Secure Block Chain Sensor Network of block chain servers. Now the data is cast in concrete and cannot be altered. Now that is a basis for trust.


THE WALL STREET JOURNAL.

Subscribe | Sign In

Uber Breach and Response Draw Global Regulatory Scrutiny

Facebook Plans to Let Users Know if They Followed Russian Pages

RISK & COMPLIANCE JOURNAL. | COMMENTARY

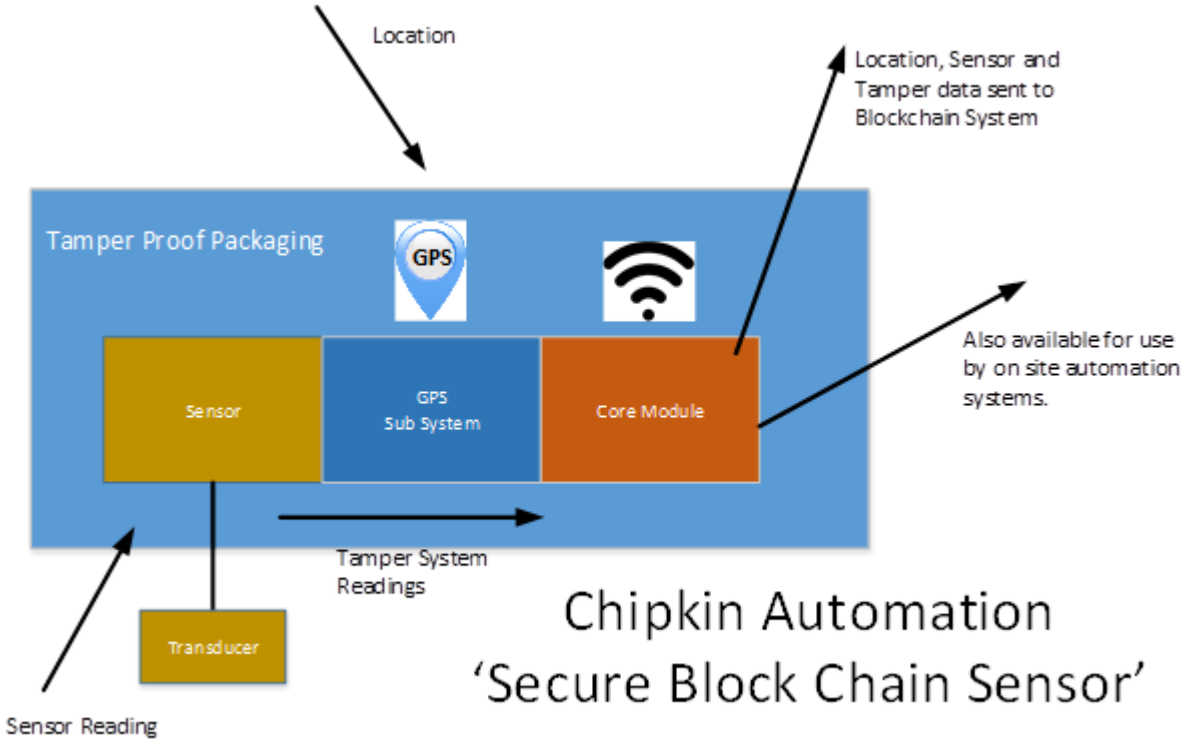
Crisis of the Week: Doctored Data Thrusts Kobe Steel Into Scandal

By Ben DiPietro

Oct 30, 2017 1:34 pm ET

How the 'Secure Block chain Sensor' works

The integration of block chaining technology into sensor data ensures the integrity and security of information gathered by the sensors. This approach prevents any alteration, movement, offline status, or tampering with the data, as it becomes an immutable part of the block chained record.



Data from the sensor is block chained. Meaning that it cannot be altered after the fact. Nor can it be moved, taken offline or tampered with because this additional data is also part of the block chained record.

- Packaging – Secure packaging designed to damage the unit if tampered with. You can tell if the sensor goes offline and can demand an explanation.

- Tamper Sensing – Short circuit and Open Circuit protection systems using technologies from the Fire Alarm and Detection industry. Also includes monitoring of the electrical load of the sensor at a micro level to sense changes. Also includes other internal sensors like temperature providing additional data that can be used to detect tampering.

- Location Sensing – GPS unit is integral. Wireless is integral. Location is determined using GOS and local wireless modules. This means the sensor cannot be moved without this being reported.

- Block chaining – The Sensor, Tamper, Location and other internal data is sent to the cloud – via wireless and/or wired connections. Sent direct to the Secure Sensor Block chain Network where it is recorded in the immutable ledgers of the block chain. The Block chain servers are run by trusted 3rd party or combination of corporate and other servers.

Agricultural Application – Does your organic crop grower cheat and use pesticides and prohibited chemical fertilizers?