Sensor Library – DRAFT **NOTES** Date 16 December 2015 Thinkers: Joseph Hentz, Gregorio Reid, James Littlejohn, dsensor@dsensor.org

Introduction
The Sensor Library function is to turn sensor data into an asset in a convenient manner. The convenience comes from the ease of aggregating and managing many sensors and the automation of the storage of the data collected. While this process is undertaken the data is prepared technically to participate in mapping protocol.

Data asset
Turning sensor data into an asset is achieve by performing a merkle tree and hashing process to allow accounting entries on a blockchain to provide an immutable record of the data. While this does not prevent the creation and accounting of fraudulent sensor data it does provide a public audit trail thus any time the data is identified to be corrupt then that source can flagged to the community as being suspect. This can also be combined with a proof of work system that provides an economic disincentive on the creation of fraudulent sensor data. For truthful data sensor source this will be a minimum economic cost, CPU and time cost but to create fraudulent sensor data at an industrial scale will become vastly financially expensive.

Merkle Tree
As the sensor data is extracted from the sensor hardware and parsed out, every 1MB of data will be segmented and those segments will go though a merkle tree/ hashing processes. The root branch of the merkle tree being accounting for as an entry on a blockchain ledger.

Parser
The parser takes the raw sensor data, identifies the type of sensor and saves the data based on a publicly identifiable naming data structure.

BT sensor driver
The Bluetooth(BT) utility will allow the sensor library to communicate with a range of sensor hardware firmware.

Blockchain API
This API is the utility used to make 'mapping' accounting entries on a blockchain. These entries being used by the Mapping Protocol to provide immutable evidence of sensor data use and history.

Database API
This utility provides an automated mechanism to store data locally and to any decentralized crypto storage service or cloud computing platform. Access to data is regulated by public key cryptography and at the desecration of the local AI module in the Mapping Protocol.