Dsensor – Decentralized sensors

Introduction
The majority of data generated will come from sensors. Given this volume and priority position this paper makes the case for building a Dsensor protocol element as part of the ethereum project. Contracting is backed by data and this paper proposes to get the underlying data in trustworthy state as the main contract by applying blockchain/hashing methodology to sensor data. The Internet of Things race has been characterized initially by a number of independent Maker community projects but now we see the entrance of establish tech giants to centralize the collection, storage and use applications. A Dsensor protocol within the ethereum project provides a decentralized option for the grass roots Maker and IofT communities. Sensors by their nature are at the edge of all parts of the network and value can be delivered their by Dapps, keeping the data decentralized.

Dsensor Protocol

Contract		Putting on main ethereum blockchain
Hashing		Putting on Mini blockchain
API		Communication between hardware and Dsensor
Sensor		Internet of Things and beyond data generation

Compliance over time

Sensors
The Dsensor protocol should be open and available to all sensors.

Hashing
The goal is to collect data from a sensor and turn it in to a trustworthy state. This is the primary defense against data being made up i.e. by making the sensor owner incur the cost of hashing produces a disincentive to generate fictitious data on which to trade. That that successfully enters through hashing can not still be said to accurately represent any claimed contract description but does give proof the sensor data has adhered to the protocols hashing requirements. Secondary, data integrity checks can be made with data is combined into pool. For example, google has to deal with millions of fictitious links trying to game their search engine ranking but they over whelming collective intelligence gained from aggregation can help weed out those fictitious links. A similar process can be envisioned for combined data pooling via a more advance Dsensor protocol.

Hashing ideas to search
Proof of capture: Mathematical proofs built into sensor firmware.
http://www.prismmodelchecker.org/lectures/pmc/
http://www.veriware.org/ http://www.cs.ox.ac.uk/marta.kwiatkowska/

Time limit to get sensor data on Dprotocol.
Other ideas?

API
Hardware connectivity   WIFI, Radio, BT, NF others Netmesh
Build industry strength API based on open source stack. Work with independent project e.g.
http://devices.wolfram.com/ or https://developers.ninja/libraries/nodejs.html http://cylonjs.com/

Contract
There are two main contract considerations:

1 getting sensor data on to Mini blockchain
2 two independent peers making a blockchain contract transaction to share data and monetary payments

Of these the second involved the mapping Dsensor protocol to an ethereum contract using ethereum programming tools. This involve monitoring, verifying, compliance, security and computability of the data between the two parties. When all the above are enables, the state is said to be contractable.

Note on outcomes: Two or more peers can come to agreement on a future state of being. Given an agreed sensor tracking condition are adhered the parties may exchange a monetary consideration. From a purely data point of view the data recorded is the data record.

People/skills to reach out to
Blockchain/hashing mathematics
http://www.cs.ox.ac.uk/marta.kwiatkowska/

Electronics/sensor manufacturing