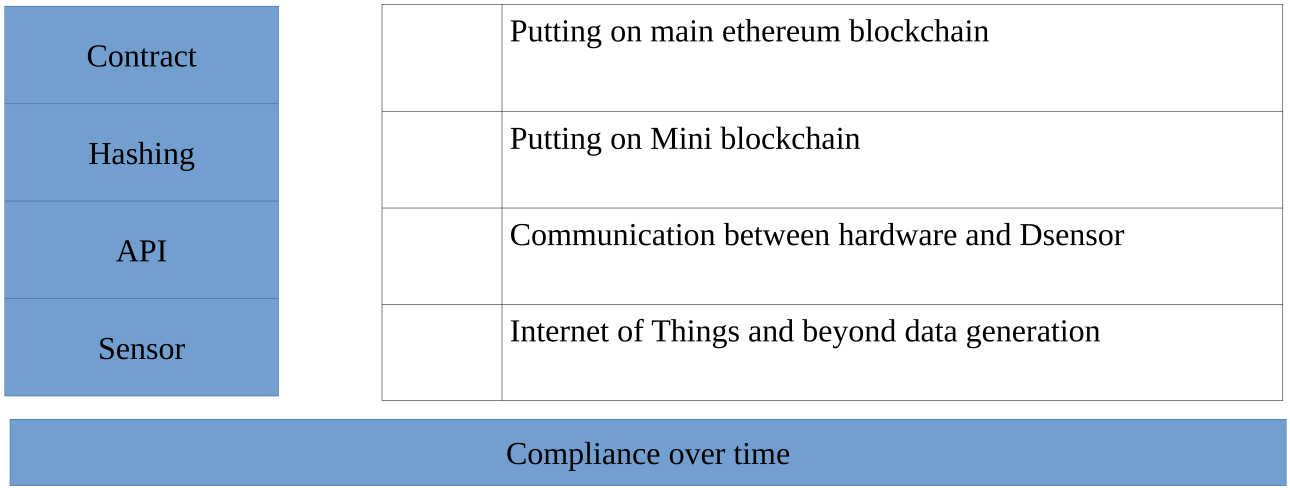
Dsensor – Decentralized sensors

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 as part of the Ethereum project. Contracts are backed by data and this paper proposes to get the underlying sensor data in trustworthy state as the main contract by applying blockchain/hashing methodologies. 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 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. Data successfully enters through hashing can not 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 when data is combined into a pool. For example, google has to deal with millions of fictitious links trying to game their search engine ranking but the 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.

Easy to get to blockchain:

The further 'distance' and time it takes for sensor data to hit a blockchain then the less certain we are on its authenticity. Direct hashing based on the electronics chip provides a close opportunity while data entering a blockchain via a third party API is much further way.

Hardware CHIP API
Every sensor will have a dedicated microcontroller chip. A hashing and blockchain library will be conceived and built. The leading hardware chip to start research around is the Arm M chipset, http://www.arm.com/images/processor/Cortex-M3-chip-diagram-LG.png Building a universal library for all chip sets will be challenge.

API
Two API data option are available:

Direct from Sensor App:
E.g. from amiigo.com developer API. Depending on how long and how open source the code making up the application will vary the trust on the state of the sensor data.

From a DATA store API:
E.g. from apple health vault. There is very little know on what happen in the secure data stores. Is the data stored exactly as recorded from a sensor? Is any tidying up of the data performed automatically? The only real way to establish trust in such data is when data pool collective intelligence can make some commentary on the data.

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/

DSapps
Decentralized Science apps are a special kind of etherum contact. The main new capability is **MAPPING** Dsensor data to contract terms in real time. This is a difficult challenge.

There are two main contract considerations:

1 getting sensor data on to Mini blockchain and reference made to a public 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 mapping, 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 conditions 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/