Dsensor – Decentralized Sensor Protocol

Date 26 December 2014
Thinkers: Joseph Hentz, Gregorio Reid, James Littlejohn, dsensor@dsensor.org

Abstract
A second major push to decentralize the Internet protocol is underway. A Dapps communication and computation infrastructure using blockchain methodologies to render trust in the logic of mathematics. This paper makes the case contributing a Dsensor (Decentralized Sensor Library) to the Dapps family to bring a 'Proof of Data' capacity to all data captured by sensors. The mathematical and computer science methods of Zero Knowledge Proofs/SNARKS will be implemented and combined with a blockchain environment that allows for infinite block creation and infinite sharing of data in a secure and trustworthy manner. The complexity of the Worlds problems are growing, be it in understanding Life, the Universe or our Environment. For example, sensor data will allow us to measure our environment like never before and with Dsensor, in a trustworthy manner, grass roots manner that allows anyone at any time or location to start contributing to solving the challenges we have before us.

1 Introduction

The majority of data generated will come from sensors. Sensors monitoring the environment, life and the Universe at large. Given this volume and priority position this paper makes the case for building a Dsensor protocol as part of the decentralized infrastructure for the Internet. Contracts are backed by data and this paper proposes to get the underlying sensor data in a 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 established tech giants to centralize the collection, storage and use applications. A Dsensor protocol provides a decentralized and secure option to those capturing sensor data and an open protocol 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 DSapps (Decentralized Sensor applications), keeping the value and data in the hands of those that own it.

2 Dsensor Protocol

Contract		DSapps Decentralized Sensor Apps, mapping contracts.
Proof of data		SNARKS to Personal blockchain
API		Communication between hardware and Dsensor
Sensor		Internet of Things and beyond data generation
Compliance over time		

3 Sensors

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

4 Connectivity API
Hardware connectivity Ethernet, WiFi, Cellular, Bluetooth, Zigbee, Netmesh
Build industry strength API based on open source stack. Work with independent projects e.g. http://devices.wolfram.com/ or https://developers.ninja/libraries/nodejs.html http://cylonjs.com/ http://www.opengeospatial.org/

5 Proof of Data – personal blockchain
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 prove a zero knowledge proof when authoring data to a personal blockchain. See the proof of data paper for more information on this process. (http://www.dsensor.org/)

Data successfully entered on a Personal Blockchain 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 peer to peer data pooling via a more advance Dsensor protocol.

5.1 Zero Knowledge Proofs
Complexity and Computer scientist are making new progress in the area of zero knowledge proofs. One such implementation are those called SNARKS, See paper http://eprint.iacr.org/2013/507.pdf This is deeply complex mathematics combined with computer science and the goal is to implement such code to make up a Dsensor firmware library.

Other such proofs are being moved from theory to practical implementation, e.g. p://www.prismmodelchecker.org/lectures/pmc/ http://www.veriware.org/ http://www.cs.ox.ac.uk/marta.kwiatkowska/

5.2 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.

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

5.2.1.2 Data API
Two API data options are available:

5.2.1.2.1 Direct from Sensor App:
E.g. from amiigo.com developer API. Depending on time taken and how open source the code of the application is will impact the trustworthy state of the sensor data.

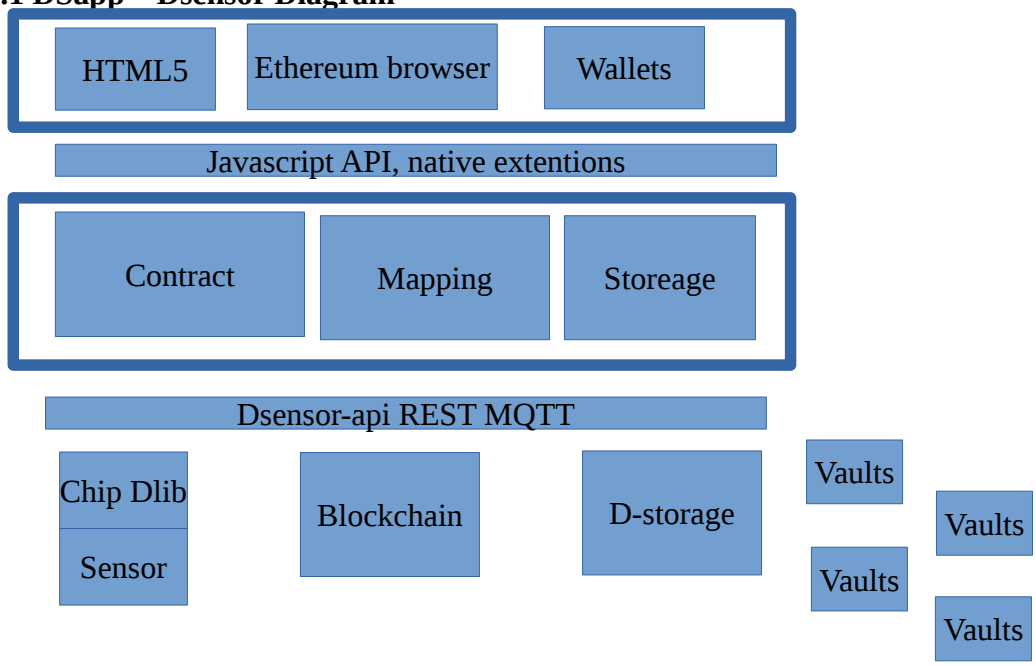
5.2.1.2.2 From a Data store API:
E.g. from apple health vault. There is very little known on what happens in these secure data stores. Is the data stored exactly as recorded from a sensor? Is any tidying up of the data performed automatically? The only real way to establish trust in such data is when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

6 DSapps

Decentralized Sensor applications (DSapps) are a special kind of smart contract. The main new capability is **MAPPING** Dsensor data to contract terms in real time. This is a difficult challenge.

MAPPING – making contracts human readable
Sensor data is brittle and human language is more grey i.e. if every tiny breach of sensor data triggers a termination event in a contract then they it may become impractical for daily use. To make contracts more robust DSapps will contain a Fuzzy Logic library in the contract builder. Developers will also be free to apply their own Fuzzy logic or other technique into the DSapp builder. See fuzz logic paper http://www.sciencedirect.com/science/article/pii/S1570870511001326

6.1 DSapp – Dsensor Diagram



6.2 There are two main contract considerations:

6.2.1 getting sensor data on to Mini blockchain and reference made to a public blockchain.

6.2.2 two independent peers making a blockchain contract transaction to share data and/or monetary payments.

Of these the second involves the mapping of data to the contract. This involves monitoring, verifying, compliance, security and computability of the data between the two parties. When all the above are enabled, 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.

6.4 EXAMPLES

6.4.1 Environment carbon blocks

Environmental sensors are becoming more readily available and more sophisticated, for example, http://arrayofthings.github.io/ Such sensor data are being fed into big data analytics, for example in Chicago, USA. However, this data could be put on a community blockchain on a geographical basis, block by block neighborhoods. Then the community can monitor their local environment. Carbon trading is becoming more established and these can now be made into 'smart contracts' and thus giving neighborhoods the ability to charge polluters in their neighborhood. This would be a new economic incentive system to build a local economy around.

6.4.2 Individual wearable data

The quantified self movement has advanced from a niche community to mainstream as tech giants have offered their own smart watches and wearables bands. These sensors work with mobile applications and data is saved to the cloud. The Dsensor protocol will allow individuals to record their own private wellbeing data on their own private blockchain and make reference to it on a public blockchain. This provides these individuals to entered into peer to peer and peer to 'computational intelligence'/ data mining applications where Smart Contract control the terms of condition of using their data i.e. release the data for use by a cancer research charity but not for advertising or insurance purposes.

6.4.3 Cosmos - Citizen Science

Humans with their sensors and intelligence as still best as some science categorization. The rise of citizen science projects like http://www.galaxyzoo.org/. These use traditional cloud based infrastructure, and the Dsensor Protocol would allow the use of a Blockchain based solution that better fits the peer to peer nature of their research.

7 Estimate of Market

As the first sentence of the document states, sensor data will be the most denominate authoring type of content. The blockchain ecosystem will require a competitive option to the status quo offerings e.g. from Xively etc. The Dsensor protocol, libraries, mapping and DSapps will require a significant developer contribution. Developers need an strong incentive to contribute. Blockchain miners and storage farmers can be paid in crypto-transaction fees. The entire MAPPING, fuzzy logic builders or verification, compliance would be offered as a service fee i.e. the two peers entering into a Dsensor based contract will also pay an amount to a verification service. This could be a fixed fee or related to the outcome.

8 People/skills to reach out to

Blockchain/hashing mathematics
Bitcoin, Ethereum, Maidsafe etc. reps associated, quarterly review.

9 The Future

With a Dsensor protocol established the foundations will have been laid for more ambitious Smart Contracts applications, namely, DScapps: Decentralised Science Application where concepts like the proof of Science can be explored.

10 Conclusions

A Dsensor Protocol will put sensor data on the blockchain in a smart and efficient way, establishing the data as trustworthy. DSapps bring the power of fuzzy logic computing to allow humans to build natural language based contract mapped to sensor data. The volume of sensors and the data they are producing will be vast and this should be acted upon at the edge of the network i.e. for each individual peer. Give peers this ability and the ability to share data peer to peer provides a new economic model of value to be established and explored.

Appendix A
Chip sets

TsmarT Embedded C WiFi
SimpleLinks Linux, Android WiFi
IMX53QSB Linux, Android Ethernet
Hitex OM13031 FreeRTOS Ethernet
Beaglebone Linux, Android Ethernet
RX62N FreeRTOS Ethernet
Raspberry Pi Linux Ethernet
Android PC 8750 Android Ethernet
LPCXpresso FreeRTOS Ethernet Optional
ARM mbed LPC1768 Embedded C/C++ Ethernet
Zolertia Z1 Embedded C 6loWPAN
PIC32 Ethernet Kit Embedded C Ethernet
Arduino Uno Arduino Ethernet, WiFi, Cellular
Arduino Due Arduino Ethernet, WiFi, Cellular
Arduino Ethernet
Arduino Ethernet
Arduino Mega 2560
Arduino
Ethernet, WiFi, Cellular
Arduino Leonardo R3
Arduino
Ethernet, WiFi, Cellular
RedBack 1.0 Arduino WiFi
DiamondBack 1.0 Arduino WiFi