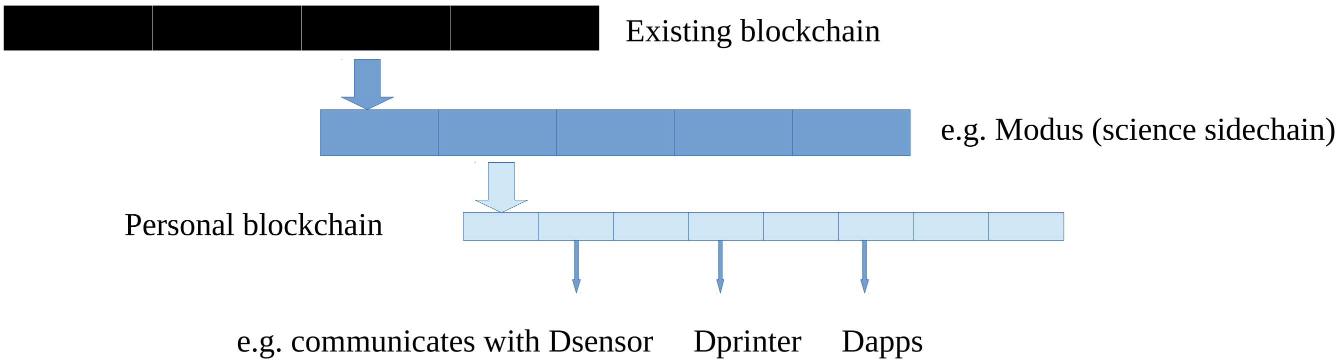
Proof of Data

1. Personal Blockchain setup from an existing blockchain

existing blockchain (secure via proof of work e.g. bitcoin or ethereum(pre mined))

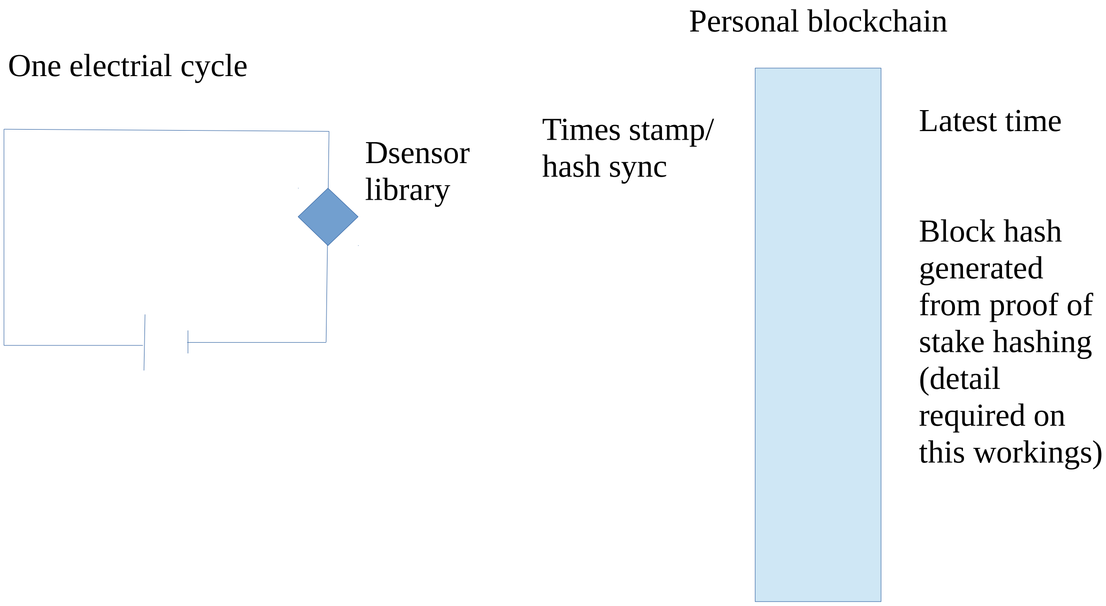

Existing blockchain
e.g. Modus (science sidechain)
Personal blockchain
e.g. communicates with Dsensor
Dprinter
Dapps

2. Firmware loader adds Dsensor library to micro-controller i.e. at electronics level

3. When the sensor starts the library automatically starts also.

4. Detail going on inside electronics

4.1 Dsensor and Personal Blockchain sync up



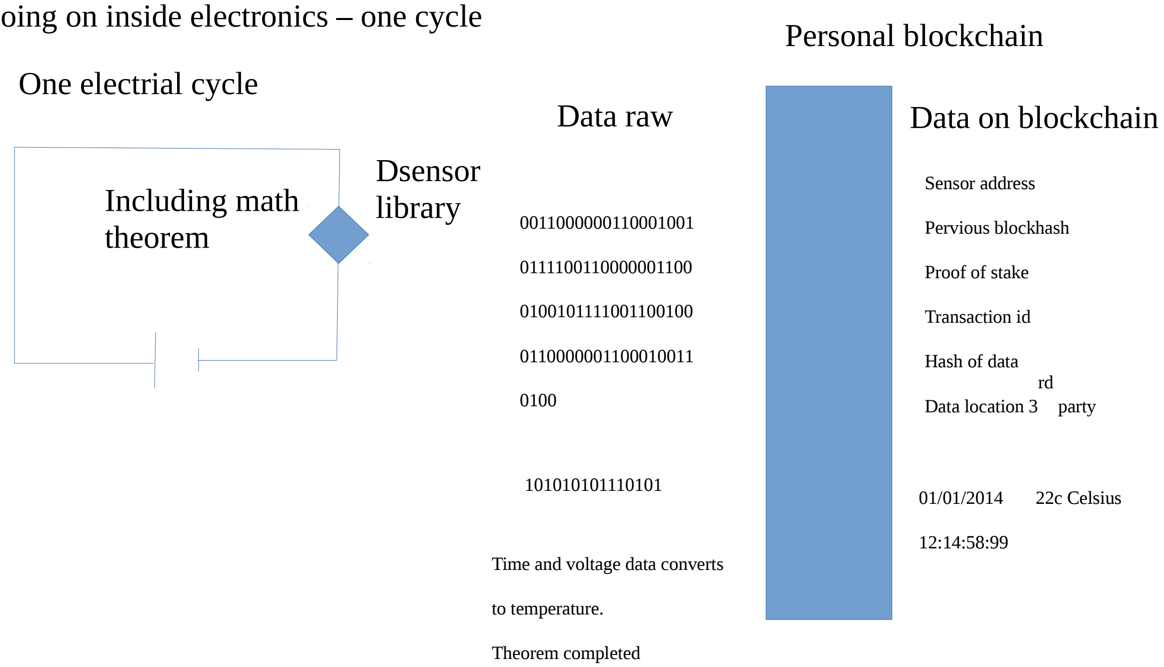
4.1.1 Public/Private Key Handshake

A normal blockchain transaction is between two peers involves the exchange of public key and a proof of work calculation to verify the necessary funds are available. The Dsensor mircocontroller library is a Peer to Sensor handshake of public keys. While the sensor is not a human, it contains a proof of data library that can only verify the authenticity of sensor data on each electronic cycle if a mathematic theorem has completed. Such mathematics are referred to as SNARK's See paper http://eprint.iacr.org/2013/507.pdf This is deeply complex mathematics combined with electronics and the goal is implement such code to make up a Dsensor firmware library.

Such work is also being researched at http://www.prismmodelchecker.org/lectures/pmc/ http://www.veriware.org/ http://www.cs.ox.ac.uk/marta.kwiatkowska/

Some of these idea will be implemented to provide analysis of the practical deployment and their success in establishing trust in the sensor data based on mathematics.

4.2 Detail going on inside electronics – one cycle



4.2.1 Successful data

When the mathematical theorem completes this will allow the second part of the Dsensor library to complete a transaction entry with the personal blockchain. This will involve creating a hash of all previous blocks and a hash of the data. The data itself will not be stored with in the personal blockchain but a storage address will be registered. However, the hash of the transaction will prove the data and the data structure was authored via a Dsensor library as the public key handshakes between the sensor and personal blockchain can only come from that process.

4.2.2 Access to Personal Blockchain

What if no access to a personal blockchain or the current personal blockchain has run out of a new personal blocks? ie. Run out of proof of stake from the sidechain?

Data will be store directly, a different proof of data path will need to be followed. See (coming soon)

5 Personal BLOCKCHAIN

5.1 Guiding principals

The personal blockchain operates its own proof of stake creation of blocks hence hashing and private/public key encryption ledger.

Every 1 minute a new transaction is created, hence 86400 new transactions per 24 hours. Each new 24 hours a new block is created for new sensors.

Proof of stake rights will be required with the pegged sidechain on a daily or more frequent basis.

5.2 Efficiency of Mekle Tree

Each daily block on a personal blockchain will be reduced to a Merkle Root number. How costly in terms of compute power, time and energy will be investigated. Sensor data can be produced a stunning volumes thus in a one minute period this can still add to many megabytes or more. Experiments will be run to provide analysis on the cost benefits of this procedure.

5.3 Time to Blockchain notes:

If the Dsensor library and the Personal Blockchain is synced to the SideChain blockchain then the time syncing between all are aligned thus in theory the data from a sensor could go straight on to the personal blockchain i.e. the sensor time stamping and personal blockchain are valid.

Could a fake Dsensor library be created to create sensor data from an imaginary sensor and still feed straight into a personal blockchain, even if all blockchains are in sync?

Yes, this would be possible but a record of this data has been published on the blockchains thus if subsequent use invalidates it as a data source then the reputation of this personal data block or the entire blockchain could be black listed across the network. It then comes a question of how many and how frequently such fake personal blochchain 'account' can be set up? The cost of setting up a new personal blockchain and its associate proof of stake will have a computation cost and history of a personal blockchain could be use to infer reuplation. ie. How often has the data been used. What is length, how regularly is it update etc. (more thinking required)

5.4 Mapping to a Smart Contract

A Smart Contract contains the terms and conditions and this will be directly linked to sensor data i.e. the smart contract will have access to monitor a Personal Blockchain. This will need to be restricted to the relevant data blocks and transactions that are relevant to the contract.

5.5. Peer to Peer Data Sharing

Given agreement has been achieved to share data via a smart contract what stops the receiving party making a copy of the data and then reselling it? At a human level, the act of making the sharing on a publicly audit-able blockchain ledger would allow traces of the sources offered to those that were listed access to the data. However, it would be completing and better to have a mathematical trust mechanism.

5.6 Peer and Peer to Peer Computation

An individual peer will hold their own data but it would be an illogical conclusion to think that peer will also have the ability and skill to create all the Dapps i.e. computations that could occur on the data. Traditionally, the data is bundled to a sensor app software program or contributed via the cloud to 'big data processing' with results being displayed back to the peer. The Dapps infrastructure will turn this model on its head. With Dapps, software computation will come to the data.

Unlocking value in data often requires the aggregation of many peers combined with a software algorithm. There is two sides to the argument, the software code owner wants the data but does not want to give access to the source code, the peers wants the software but would prefer to have control over their data.

Initial experiments will be performed to see how an enhanced Dapps VM platform can address this big problem.