# Preface

This document is the first draft meant to serve only as means for discussing various ideas and for brain storming project requirements. The requirements presented here are meant to be only indicative of what we want to build in a very abstract manner. This should not be taken as the final requirement specification document. The requirements presented in this document might not end up in the finished project because some of them might be too broad or too narrow or might not have been well defined, others might just be presented as ideas for debating different design choices to be taken at a later date.

# Securing nodes /hardware

get ideas from Filament Security white paper heading **security begins with hardware** to extrapolate general security goals you can implement in software.

for now think these

data stored on mcu or flash shold always be encrypted.

firmware on mcu or sensor should be always tamper resistant

or at the very least only specific authorized devices are able to communicate with ur iot network.

unauthrozied or reprogrammed devices should be rejected by the iot network

# running smart contracts on Devices vs running smart contracts on cell phones/special nodes

try to find a way to run microtransactions on the device i.e. some sort of store and log feature for microtransactions until the the data is presented to a special node such as cell phone to extract value into companies account. Alternatively find a way for running ethereum smart contracts directly on to the IoT device. For example filament IoT taps have on board javascipt virtual machines **read initializing devices with smart contracts** on filament security white paper. Filament uses a technique in which cryptographic credentials of an IoT device can be chained back to a root in this manner they determine authorized devices such as tablets or smart phones which are able to read data off of the IoT node. Read further **Access control in** filament security white paper.

# Centeral portal for monitoring IoT nodes

IoT nodes should have a mechanism to expose their transaction history to an organizations centeral portal i.e. all IoT devices read some special seed for the portal and present transaction and value data to the portal whenever possible. How this data is presented to the portal is largely depenedent on implementation and organizational premitives ie.e could be with the help of scaning nodes i.e. cell phones or just presented whenever came into range of special node with direct connection to the portal server.

# Micro transactions on filament

How can we easily enable microtrnasaction on our abstract IoT interface?

Filament use something close to a bitcpoin wallet on the device to enable microtransactions read **microtransactions** section of filament security white paper. Their technique builds on Json Tokens with zero knowledge proofs. They argue payement channels with both parties signing the same transaction might be too expensive for resource constrained IoT devices. I think if memory and power requirements can be dealt with i.e. for always plugged in devices payement channels can work and for truly mobile devices we might need to look into zero knowledge proof or some other solution. Implement solution 1 and leave solution 2 as further development task.

# Telehash vs MQtt

Telehash is transport agnostic, supports end to end security and node discovery. MQTT is ?

# Metering GPIO

Since all MCUs have general Inbput and output we can provide some general pins for connected external devices to our nodes which can be used to provide different services such as lights, power, wifi access etc. What is connected to these pins is not important what is important is that customers can define rates at which these pins supply energy and calculate payements in the form of microtransactions. E.g a power outlet can be connected to one of the pins the node owner has the ability to define charging rates for power delivery either one off rate for continuous use i.e. 0.1 ether for say 24 hour period or define rate based on load or time etc. the user who wishes to use or draw power will use his smart phone to request access a smart contract will be negotiated between user and device. IoT device will calculate based on payement interval/ method and rate of the service offered connected to the I/O.

# Things that an IoT blockchain interface can have

* mechanism to define company monitoring parameter i.e. define a new monitoring task and its prmitives e.g. define a class called project, tracking etc with primitves such as add sensor node to this project , remove node, display data,
* mechanism to add new sensor nodes to the system for monitoring each time a sensor node is added should its private and public keys be refreshed or should the keys stay static no matter how many times the node is remvoed or added to different projects
* projects web interface should be connected to both block chain / smart contract and sensor **nodes?**

**question: role of block chain should it be just a conflict resolution and exchange of value or much more involved?**

* chose the basic functions we need to support in our project and then decide for each function what makes more sense decentralization or centralization.
* prefer decentralization over centeralized solutions where ever possible.
* Data gathered is key and can be sold, make a mechanism for allowing users to sell their data easily I.e. generic way of reading data from devices by third parties if allowed by the user. The third parties will directly pay the user of the iot device whenever they read data.
* Selling of data should only be allowed to authorized third party entities. The authorization is obtained based on smart contract between entities. Devices should be able to be programmed in groups or across the networks with new smart contract primitives i.e. only sell pressure and light data across a route.
* Similarly preprogramed sell features for data should be removed , renewed or updated automatically and easily once the smart contract is finished or funds in the contract exhausted.
* Data can be categorized into different categories i.e. data in public can be read by one i.e. either by paying for it or for free, private data can be read by authorized personal/devices only i.e. through using some security mechanism, secret data can only be read by owner of the network and should never be disclosed to any outsiders.
* Authorization to access certain protected data can be shown by users by presenting authorization certificate signed by public key of the owner. This raises the question of weather the device will need to store private key to confirm authoprization.
* Security in hardware (mcu paired with a crypto chip filament style) vs security in software (more logical for us)
* Read Data from iot device
* Define encryption for data transfer
* Define communication channels i.e. rfid, bluetooth etc
* Cellphones can act as stable nodes of the IoT devices giving the network access to the internet and block chain at intermittent intervals or where continuous access is not possible.
* Special nodes with cellular access can sell internet access to other nodes in the networks
* Write Data
* Define Smart contract Terms
* define Payements
* Define conflict resolution mechanics
* define micro payement channels
* much more think about
* may be have something like webhooks for smart contracts to be read by web or cell interface
* Things to havce identity management, security, discoverability, digital trust, long-range wireless networks that span hundreds of miles, low-power systems, and integrating crypto-currencies
* Device discovery using telehash-native local discovery and through an organization running a notary which ties to ethereum naming service for wide area networks.

**Sensors themselves need to have security**

**Sensors job is just to report data to smart contracts on the block chain either continuously or at fixed intervals i.e. weather when shipping change hands etc. if case 1 contract will decide as soon as a violation has occurred that the violation has taken place. If case 2 sensors need to log data and securely communicate the data to the smart contract before changing hands at which point smart contract goes through entire logged data to determine if a violation has been made. Another alternative to this could be that before each hand off the data logged is cryptographically locked with each shippers key to determine who is responsible for any violation and data is communicated to the blockchain or smart contract only at the end of its journey.**

**Devise payment method for putting IoT data on the blockchain. When should the payments be made how oftern they should be made , how should disputes be resolved etc.**

**Devise Requirements weather intermediary nodes can keep information before or after putting them in the blockchain**

* **Method for modifying Ethereum or raiden network so that it supports post quantum crypto**

# Logic behind decentralizing IoT

“There are a lot of platforms and standards available today for the Internet of Things. Most of these platforms attempt to describe a high-level topology of billions of devices becoming smart and connected. Cloud computing has been nothing short of transformative, and it’s given rise to entire new fields such as predictive analytics, machine learning, and collective intelligence. Cisco estimates there were approximately 8.7 billion devices connected to the Internet in 2012, and expects that the number of connected devices could reach up to 40 billion by 2020.

Whether or not that number is correct, there will be so many devices connected that it can be argued whether the cloud will be able to keep up with it. Centralization is certainly an easier way to build out these platforms. However, the authorities in these topologies all have an influence upon the network and can be exploited. The larger a network gets, the more an incentive for bad actors.

”[1]. There are lots of good points given in [1] about why we should go in the route of decentralizing IoTs go through it again when writing motivation about your thesis and abstract interface.

Working Titles

Ganj Buksh or G-Buksh: Persian meaning unlimited treasure / moving treasure

ZANBEEL: A word derived from Persian mythology, meaning a magical pouch yielding boundless possibilities

Plutus: ancient greek god of wealth

# References

[1] https://medium.com/@FilamentHQ/a-declaration-of-device-independence-b6f83e8b6441#.flo8gr95x