Politecnico di Torino

Department of Control and Computer Engineering

2021/09/14 - PHD DISSERTATION

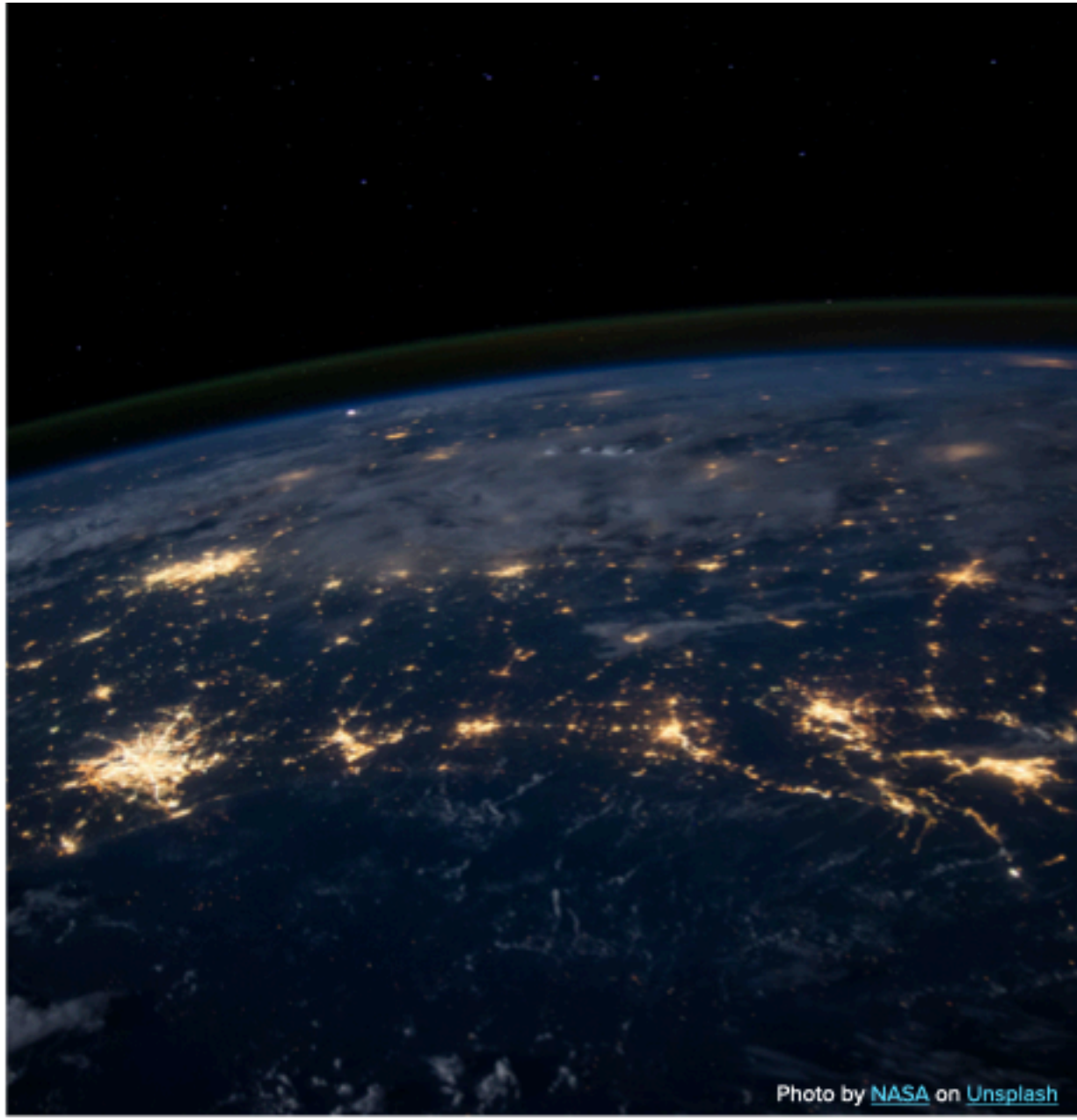
SENSOR-BASED ICT SYSTEMS FOR SMART SOCIETIES

Candidate: Edoardo Giusto

Advisor: Prof. Maurizio Rebaudengo

OUTLINE

- **Introduction**
  - IoT scopes
- **Data acquisition**
  - Air pollution monitoring
- **Data transmission**
  - Thermal monitoring
- **Data Authenticity & Safe Storage**
  - IoT + Blockchain for Food supply Chain
- **Future works**



WHAT ARE WE TALKING ABOUT?

IOT Internet of Things

IOE Internet of Everything

THE RISE OF IOT

- Term coined in 1999 by Kevin Ashton
- Applications:
  - Healthcare
  - Utilities
  - Transport
  - Home automation
  - Environmental monitoring
  - etc...
- Less desktop, more embedded:
  - Ubiquitous computing

Photo by Andres Urena on Unsplash

DATA

→ ACQUISITION → TRANSMISSION → STORAGE

QUESTIONS

Data Acquisition

- Are we sampling a certain signal at the correct frequency?
- Does the sensor we use produce scientifically valid data?
- What is the best wireless protocol to transmit sensed data?

Data Transmission

- Are these data authentic?
- Now that we were able to sample and transmit these precious data, how do we store them in a way that they cannot be tampered with/altered?

Data Authenticity and Safe Storage

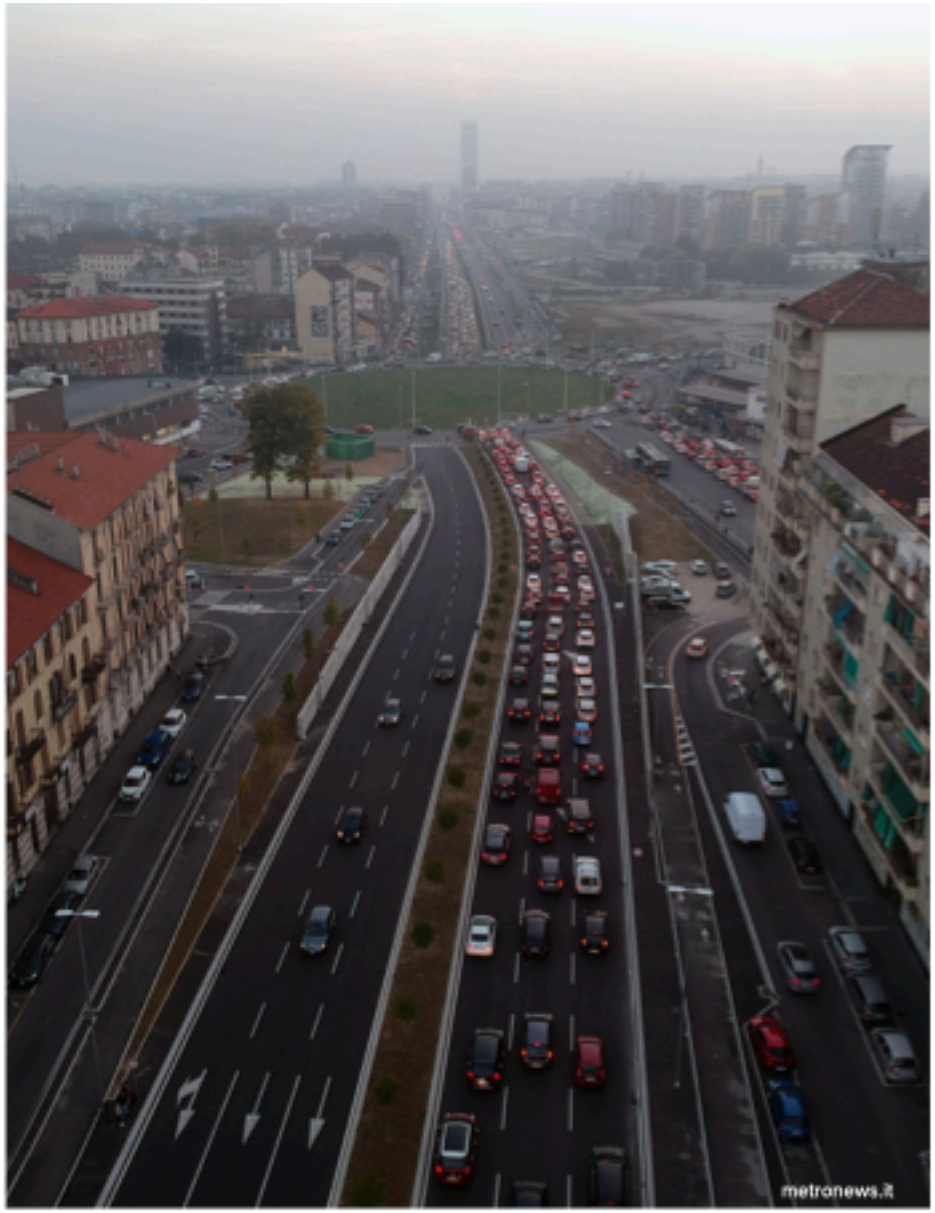
DATA ACQUISITION

FOCUS ON: AIR POLLUTION MONITORING

HOW SAFE IS THE AIR WE BREATHE?

wired.it

gomechanic.in


metronews.it

PARTICULATE MATTER

DATA ACQUISITION

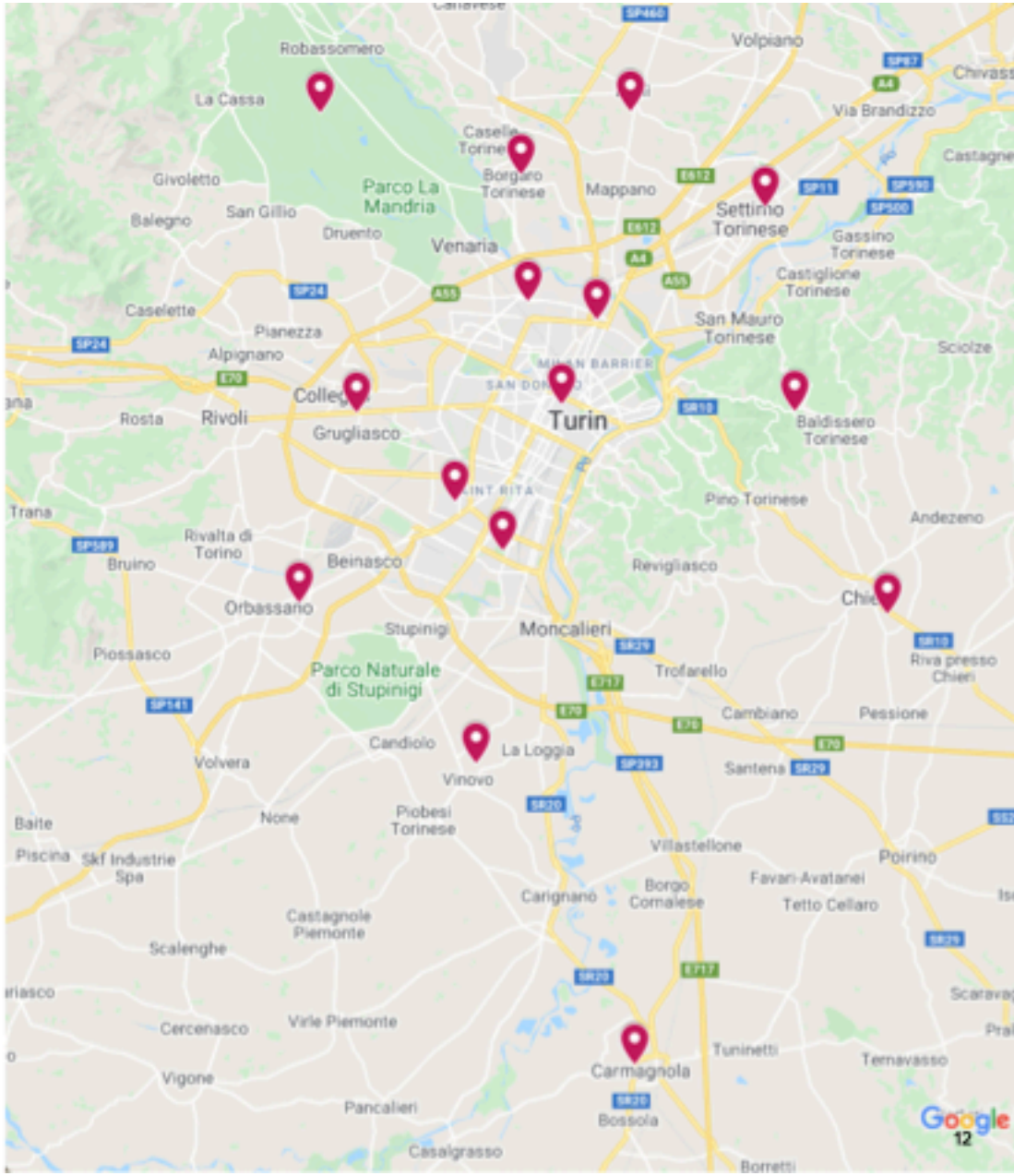
WHO IS MEASURING AIR POLLUTION IN TURIN?

- **High precision/high price sensors**
- **Crucial measurements**
  - Anti-smog operating protocol
- **Sparse network**
  - Coarse grained pollution map

DATA ACQUISITION

WHERE ARE THEY MEASURING?

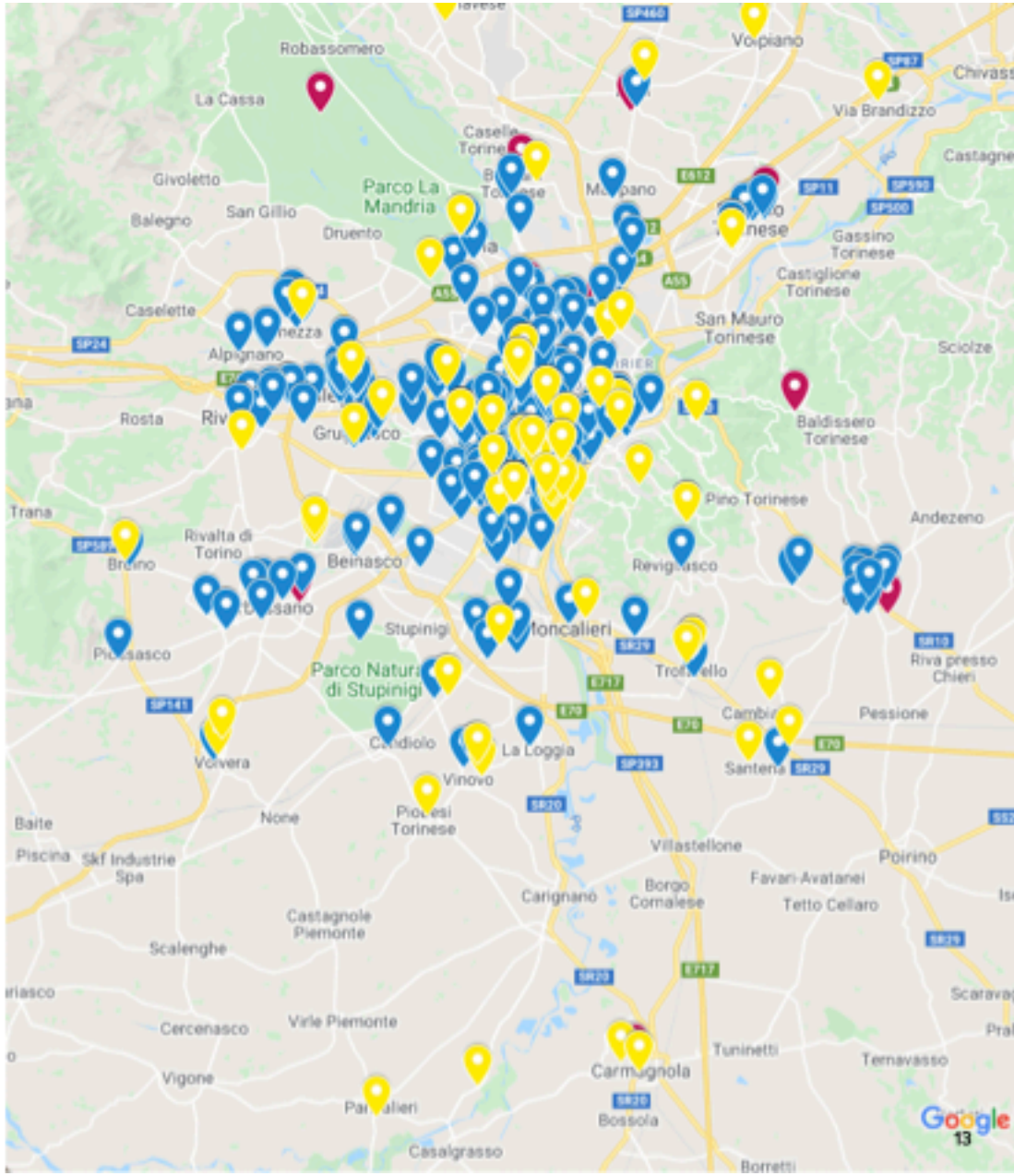
- ARPA stations



DATA ACQUISITION

WHERE ARE THEY MEASURING?

- ARPA stations
- Schools
- Hospitals/care homes



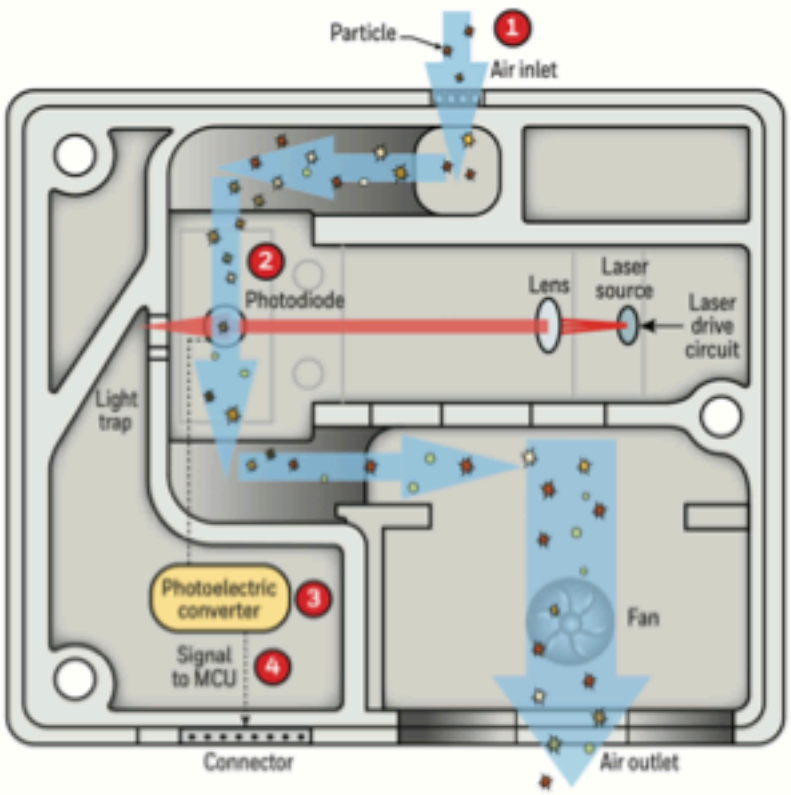
IS THERE AN ALTERNATIVE?

DENSELY DEPLOYED AND LOW-COST APPROACH

DATA ACQUISITION

LOW-COST VS CERTIFICATE METHODS

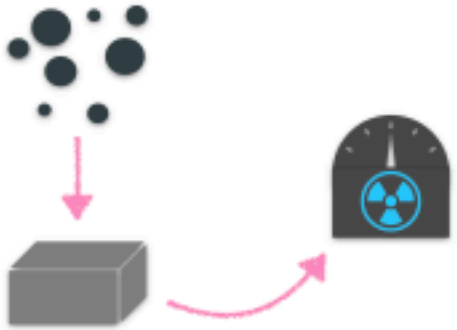
Light scattering (LS)



Credit: Honeywell

Gravimetric

β-radiation



LS ADVANTAGES

- **SIZE & WEIGHT**
  - 5cm vs 50cm side
  - 100g vs 20kg
- **LOW-COST**
  - 40€ vs 20k€
- **HIGH FREQUENCY**
  - 1*s* vs 1*h*
- **LOW-POWER**
  - 5V vs 320V

LS DISADVANTAGES

- **CERTIFICATION**
  - Not certified vs Certified
- **CALIBRATION**
  - Hard vs Easy

Compare against ARPA reference values!

DATA ACQUISITION

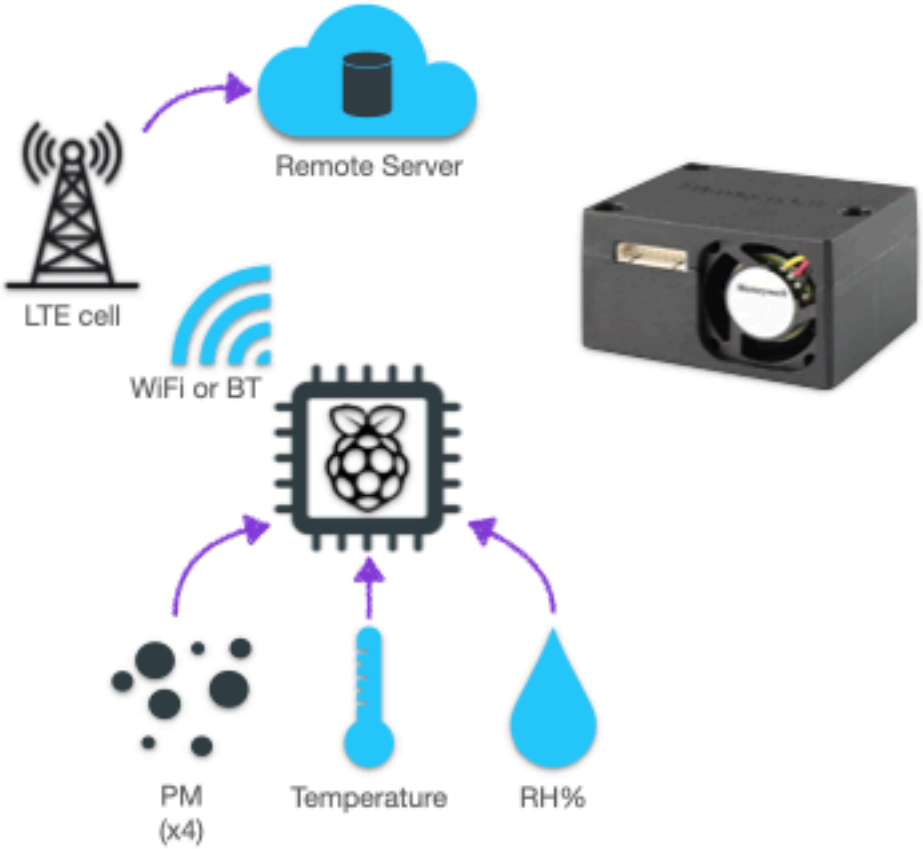
STATE OF THE ART GAPS

- Low accuracy and reliability
- Insufficient sampling
- Expensive devices
- Poor sensor testing
- Unaware of boundary conditions

DATA ACQUISITION

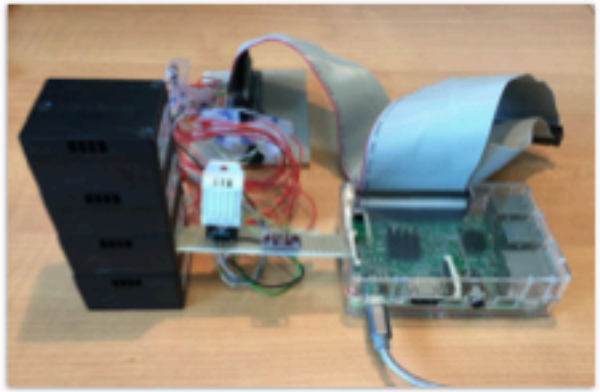
PROPOSED SOLUTION

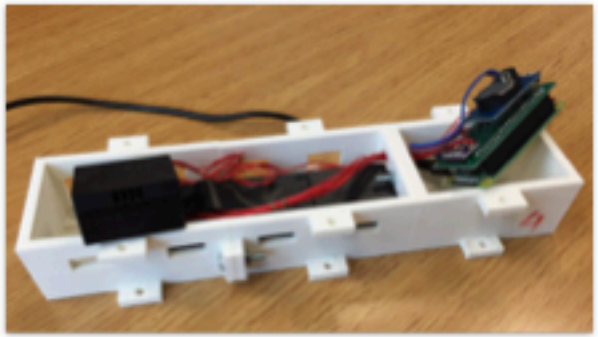
- High quality/price ratio
- PM sensor redundancy
- Boundary conditions-aware
- Open-Source SW architecture



DATA ACQUISITION

DEVELOPMENT





- **Architectural choice**
- **Components assembly**
- **Software development**
  - Sensors and other modules
- **Debugging**

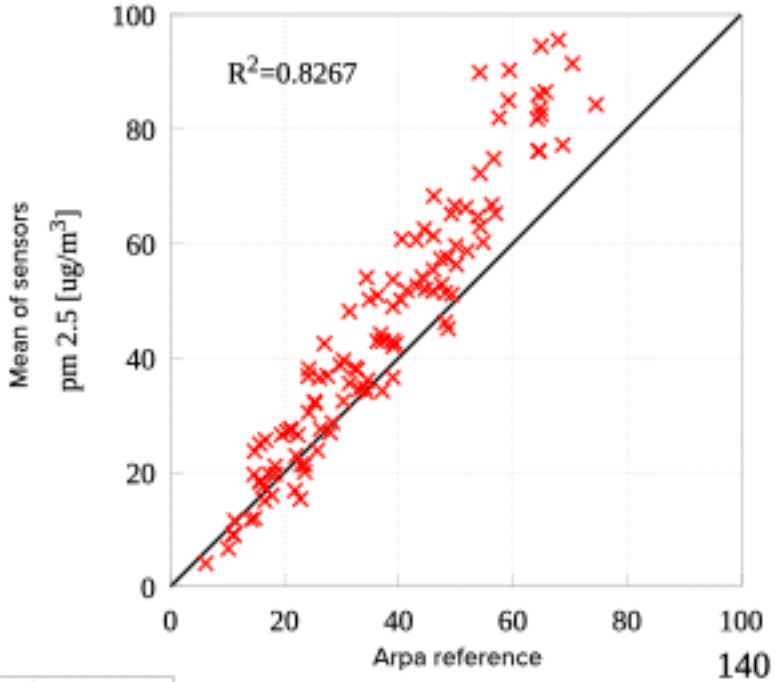
DATA ACQUISITION

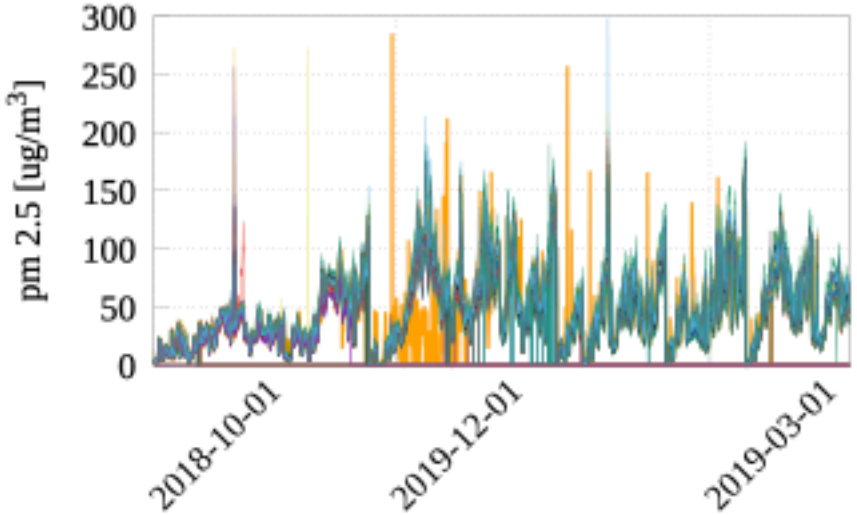
MEASUREMENT SITES AND TIMES

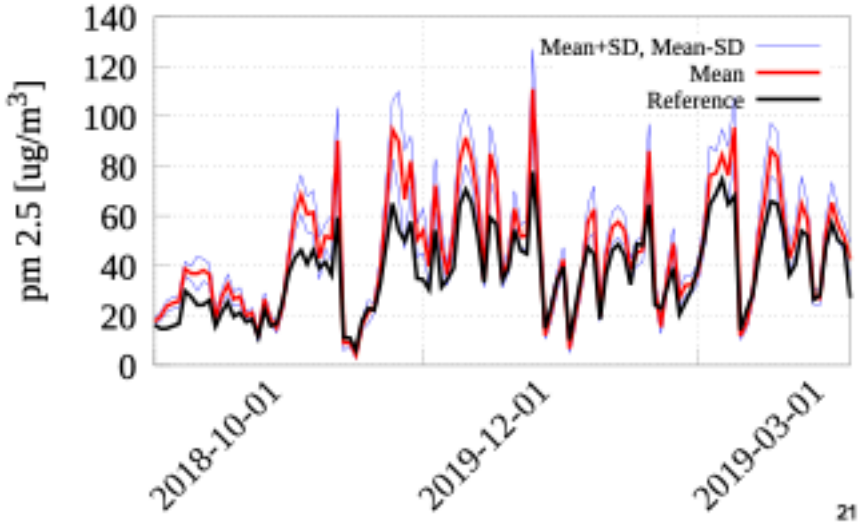
- **Long term experiment:**
  - ARPA “Rubino” reference station (red pin) 2018/10 - 2019/02
- **Spot experiments:**
  - Traffic light (orange pin) 2020/01/08
  - Multimodal path (green path) 2019/02/15
  - Limited Traffic Area (orange area, blue pins) 2018/12/03-04

DATA ACQUISITION

INITIAL EVALUATION

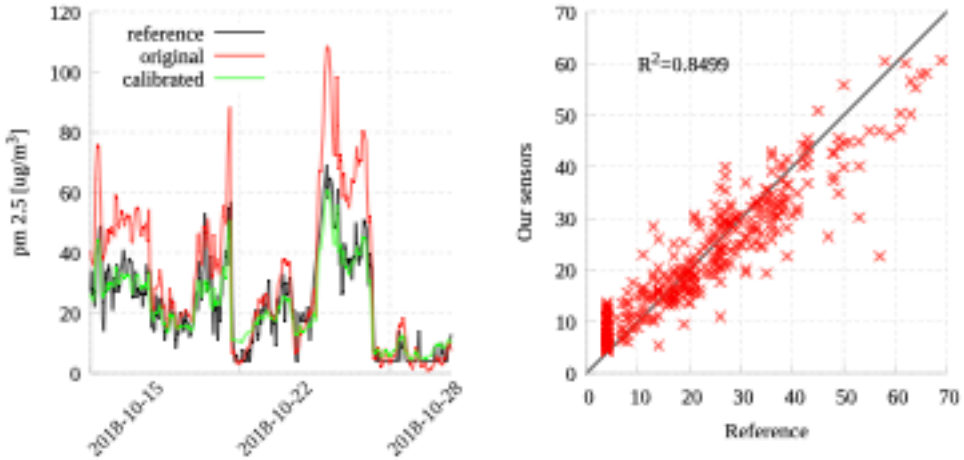




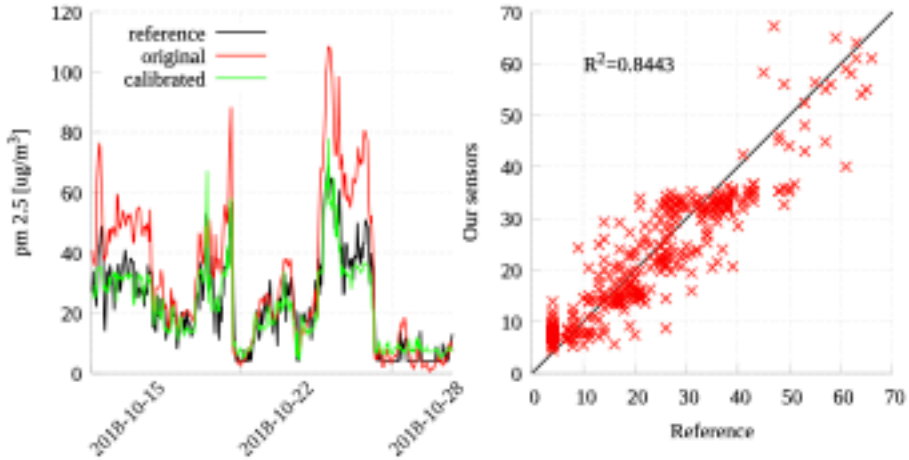


DATA ACQUISITION

CALIBRATION TECHNIQUES



Calibration using Linear Regression (sensor #34)



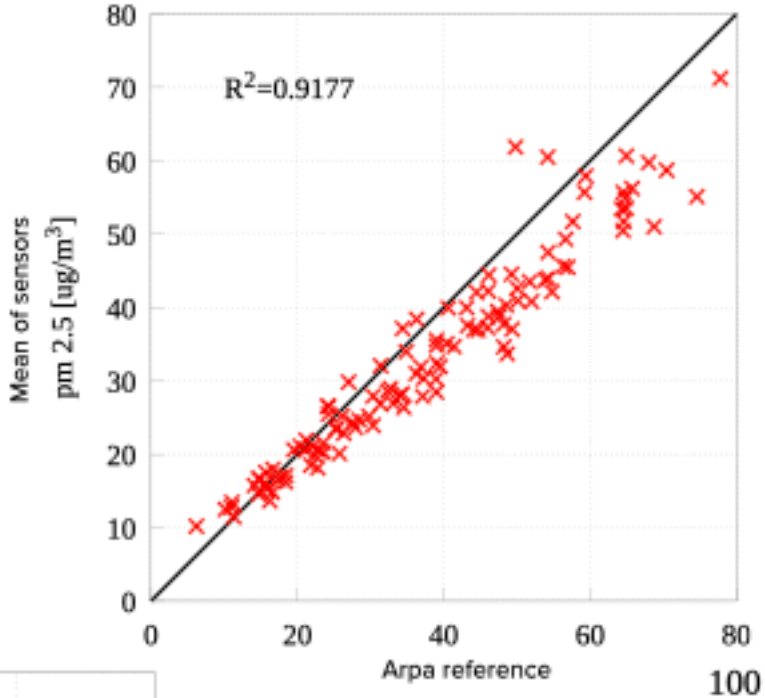
Calibration using Random Forest (sensor #34)

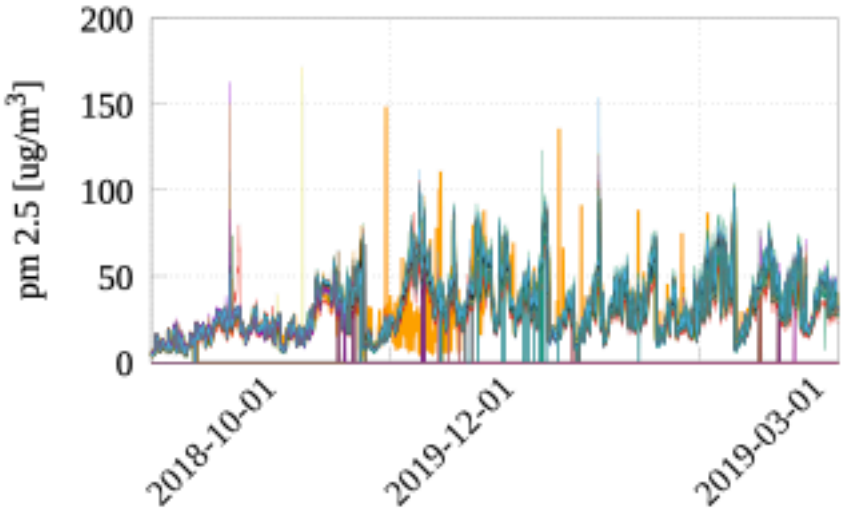
		2 weeks 323 samples			6 weeks 840 samples			12 weeks 1851 samples		
		T	H	T+H	T	H	T+H	T	H	T+H
Linear Regression	RMSE	19.03	14.17	14.42	18.96	12.58	14.70	13.49	10.04	11.66
	Correlation	0.89	0.88	0.89	0.89	0.88	0.89	0.88	0.88	0.89
Random Forest	RMSE	25.41	21.77	23.50	25.28	18.75	19.37	13.85	12.63	11.33
	Correlation	0.82	0.80	0.78	0.77	0.82	0.80	0.85	0.88	0.89

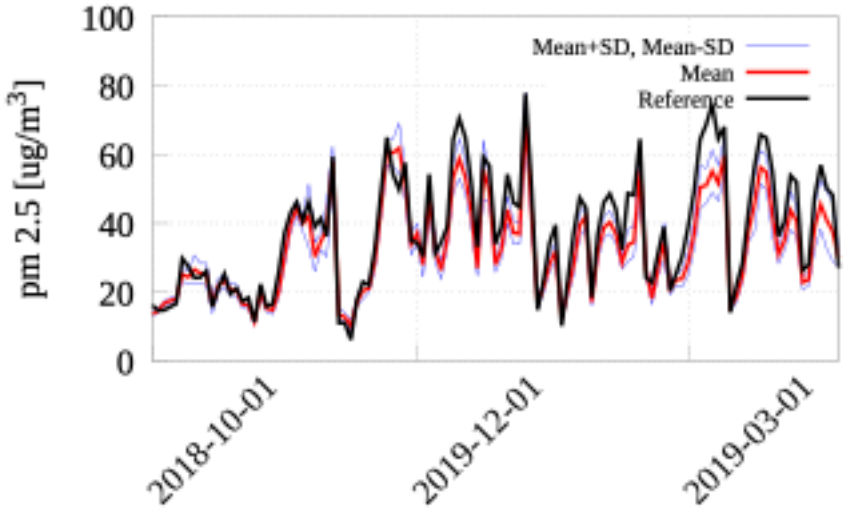
RMSE for all sensors

DATA ACQUISITION

AFTER CALIBRATION

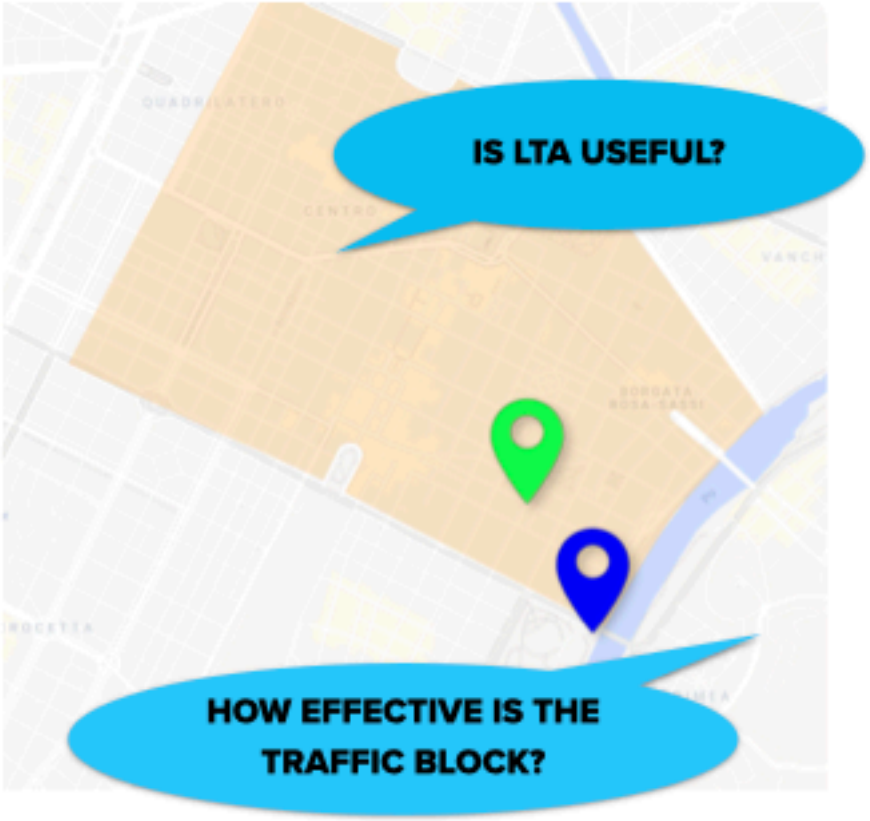


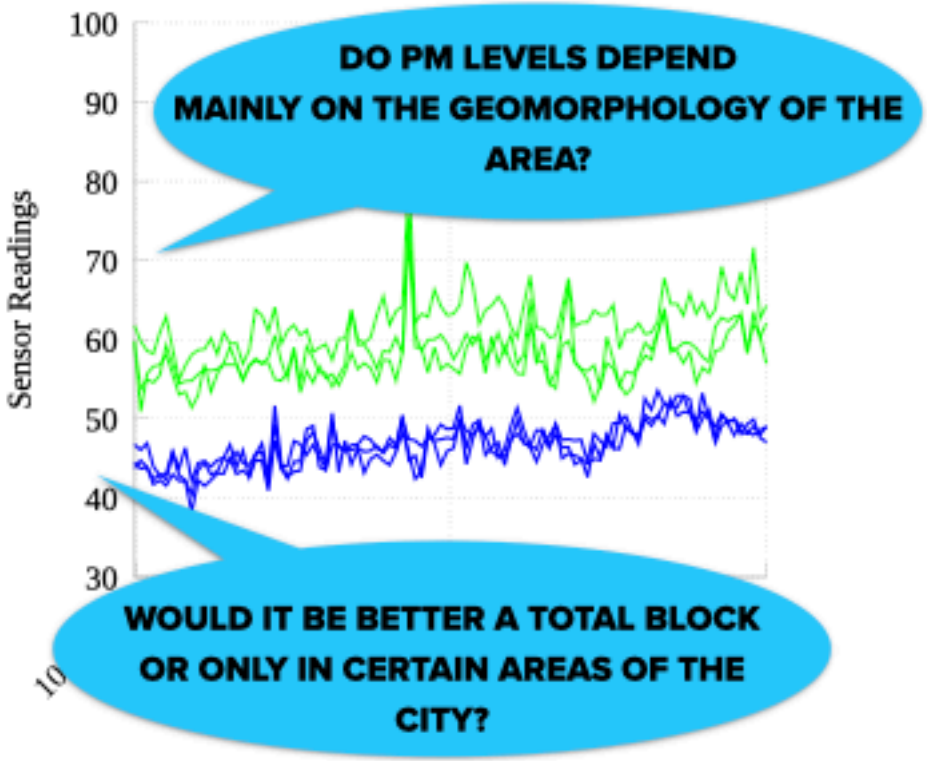




DATA ACQUISITION

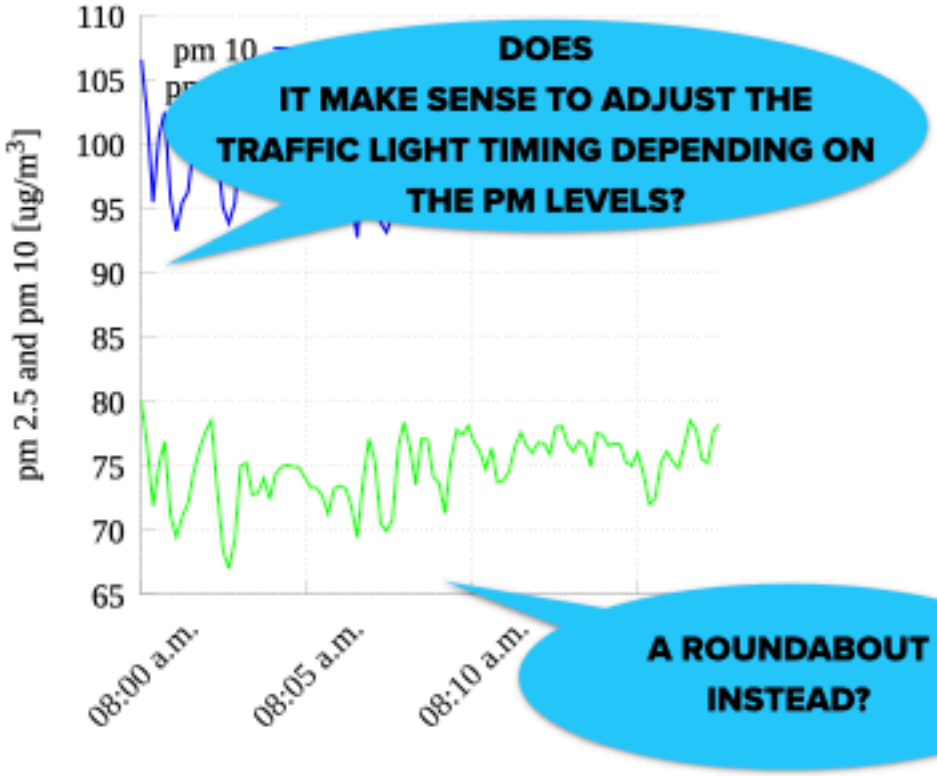
USE CASE APPLICATIONS - LIMITED TRAFFIC AREA

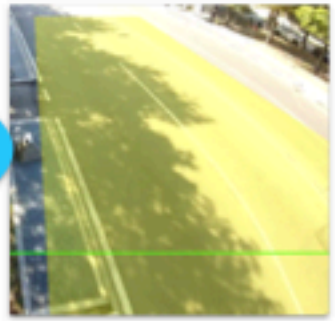




DATA ACQUISITION

USE CASE APPLICATIONS - TRAFFIC LIGHT

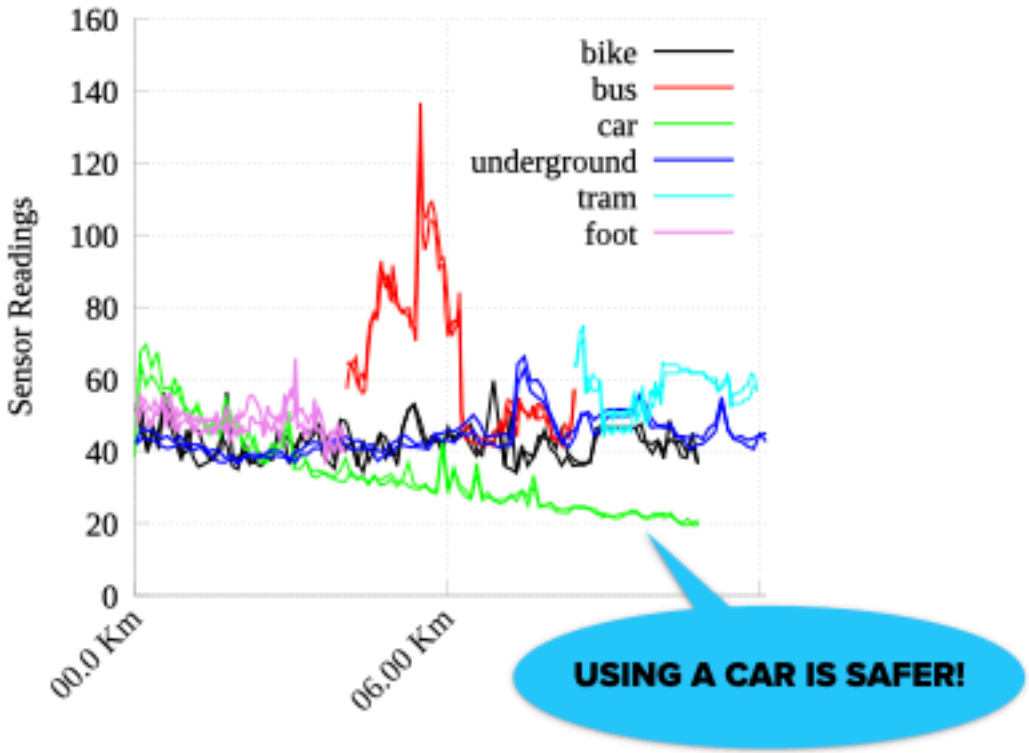




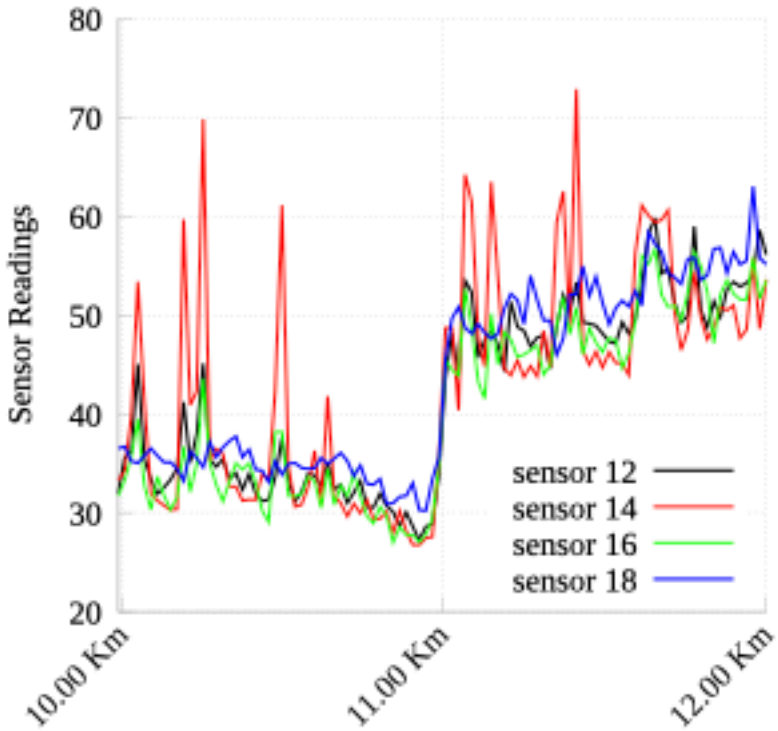
DATA ACQUISITION

USE CASE APPLICATIONS - MEANS OF TRANSPORT

WHAT TRANSPORT MEAN GUARANTEES THE LEAST EXPOSURE TO PM?



Comparison of transport means



Car window opening effect

DATA ACQUISITION

WRAP-UP

B. MONTRUCCHIO, E. GIUSTO, M. GHAZI VAKILI, S. QUER, R. FERRERO, C. FORNARO; *A DENSELY-DEPLOYED, HIGH SAMPLING RATE, OPEN-SOURCE AIR POLLUTION MONITORING WSN*. TRANSACTIONS ON VEHICULAR TECHNOLOGIES (IEEE) 2020. HTTPS://DOI.ORG/10.1109/TVT.2020.3035554

~~Replace Environment Protection Agencies~~

Work in **SYNERGY** with them

Characterise at a broad spectrum the situations happening in cities

Increase the spatial and temporal detail of PM information

Study particular phenomena

Help municipality in planning

DATA TRANSMISSION

FOCUS ON: THERMAL MONITORING FOR HOME AUTOMATION

DATA TRANSMISSION

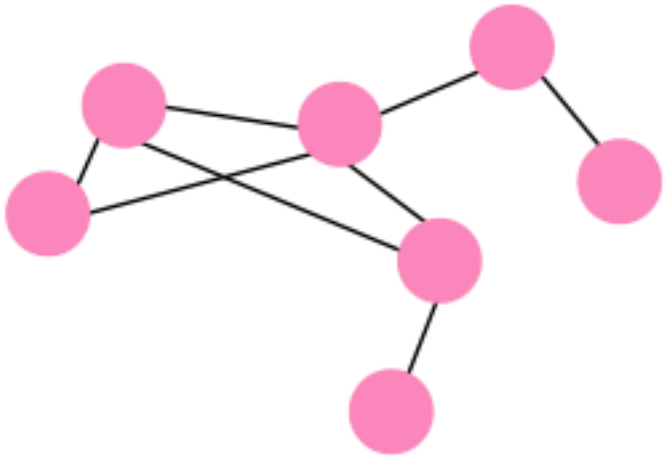
OVERVIEW

Critical:

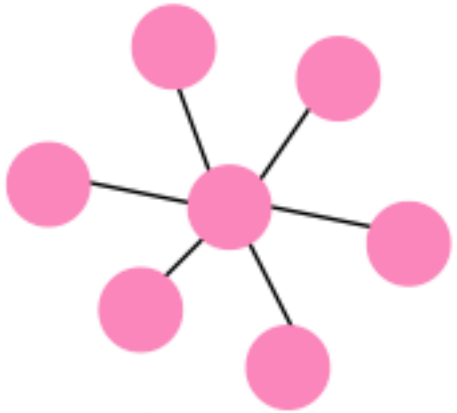
- **Power consumption**
- **Data readiness**
- **Maximum node transmission range**
- **Installation/maintenance cost**

Transmission options:

- **Copper wires**
- **Optical fibers**
- **Wireless channels**
  - WiFi
  - Bluetooth
  - RFID
  - ZigBee
  - LoRa
  - Cellular connection
  - ...



Mesh Network



Star Network

DATA TRANSMISSION

FOCUS ON: THERMAL MONITORING

Technology evaluation applied to home automation task:

- **HVAC**
  - Heating, Ventilation, Air Conditioning
    - **T+RH monitoring**

Before:

- **RFID**
  - Track perishable goods
- **Bluetooth**
  - Human occupancy of spaces

RFID & Bluetooth

DATA TRANSMISSION

RFID/BT TECHNOLOGICAL BACKGROUND

RFID

- Readers
- Tags
  - Passive
  - Semi-passive
  - Active
- Star network (strict roles)
- Different frequencies and ranges

Both

- Low energy consumption
- Moderate data rate
- Subject to interference

BT

- Mesh network (different roles)
- 2.4 MHz frequency

Hedy Lamarr

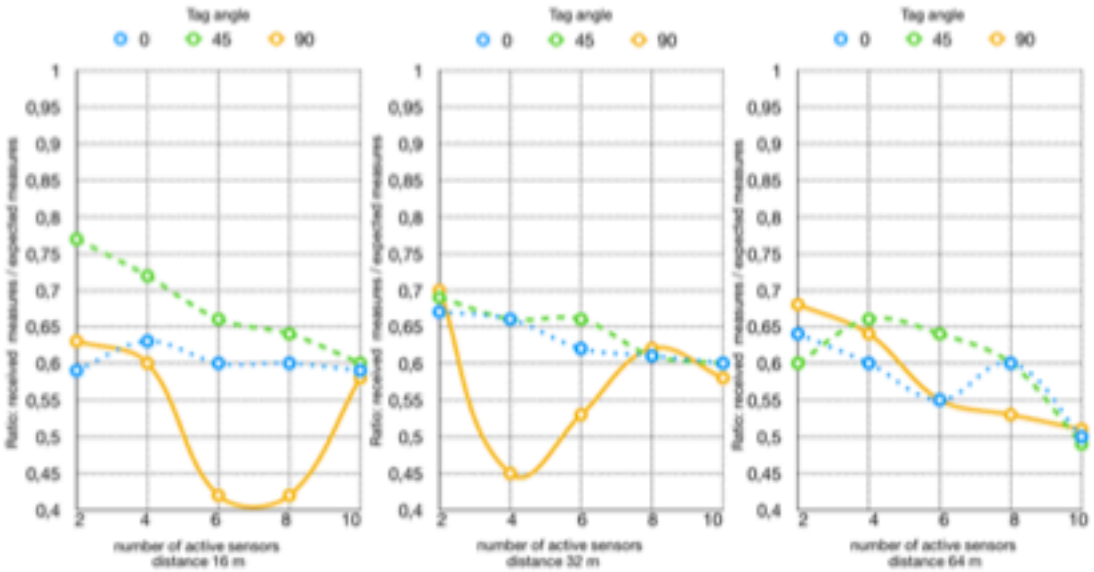
DATA TRANSMISSION

RFID/BT THEORETICAL COMPARISON

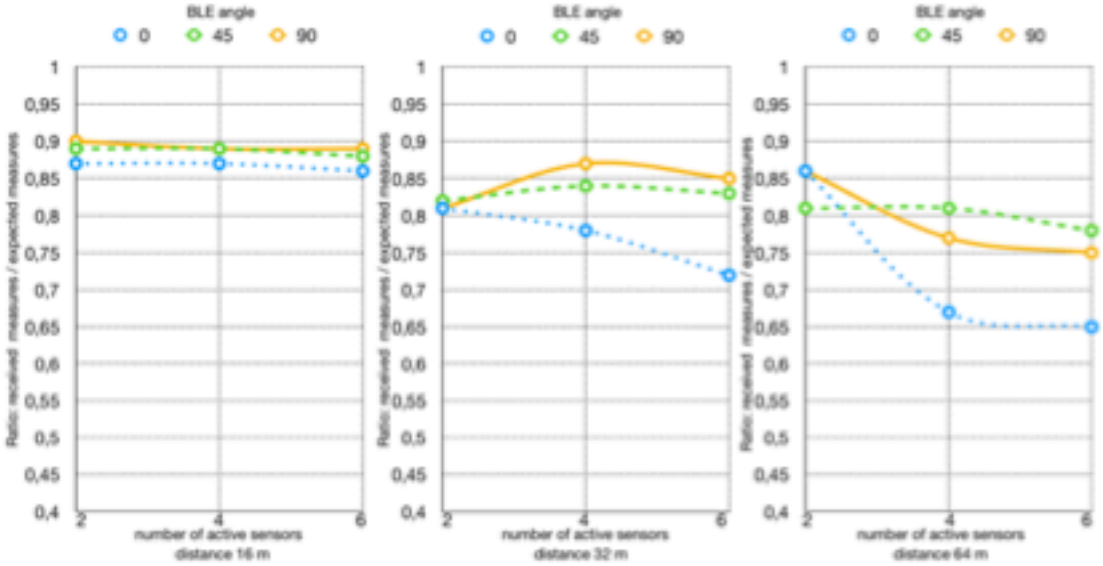
	RFID	BT
Transmission range	100m	>100m point-to-point
Scalability	Addition of reader required	Add sink nodes or reconfigure network
Interference resilience	Issues: – Collisions – Metal/water blocking	Works over congested frequency spectrum
Costs	400$ for reader, 50$ for active tag	10$ for BT tag

DATA TRANSMISSION

EXPERIMENTAL ANALYSIS - TRANSMISSION EFFICIENCY



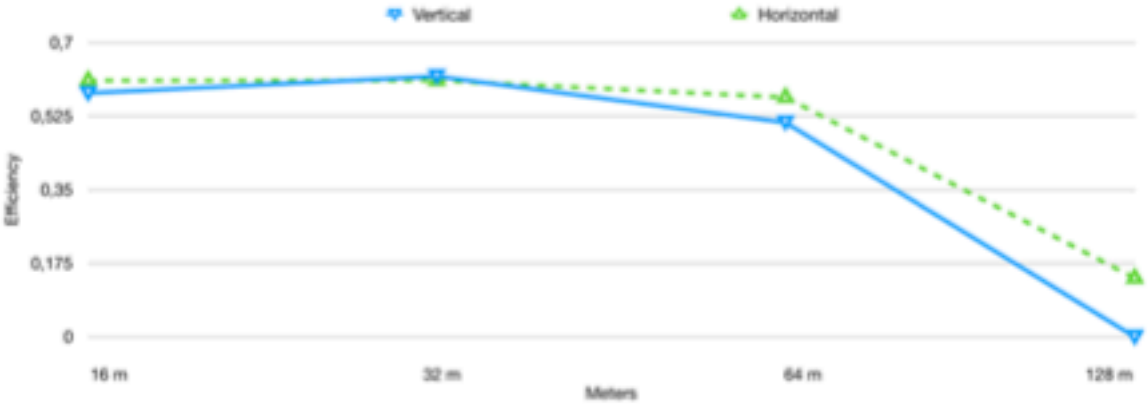
RFID



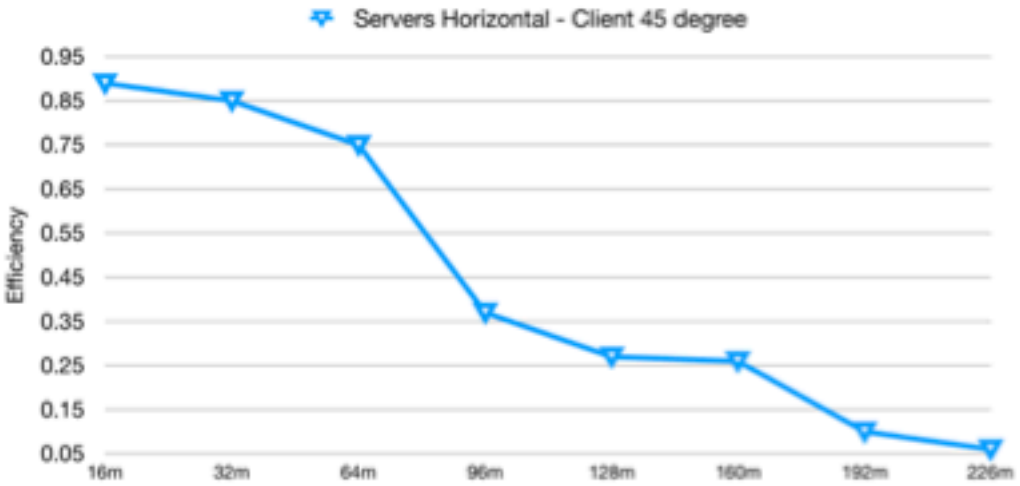
BT

DATA TRANSMISSION

EXPERIMENTAL ANALYSIS - LONG RANGE TEST



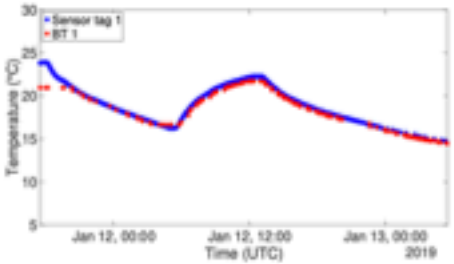
RFID



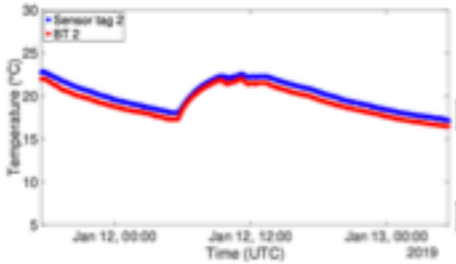
BT

DATA TRANSMISSION

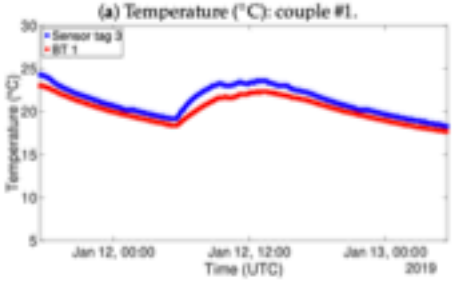
CASE STUDY



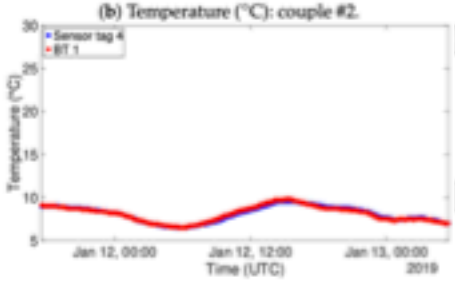
(a) Temperature (°C): couple #1.



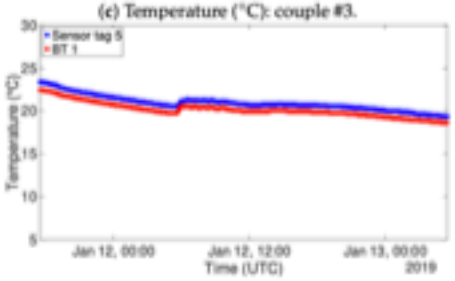
(b) Temperature (°C): couple #2.



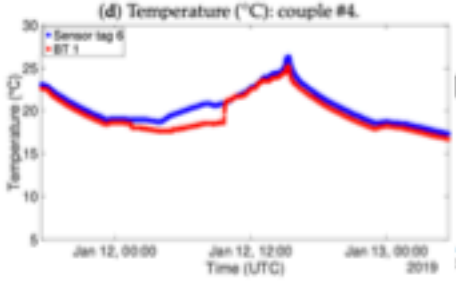
(c) Temperature (°C): couple #3.



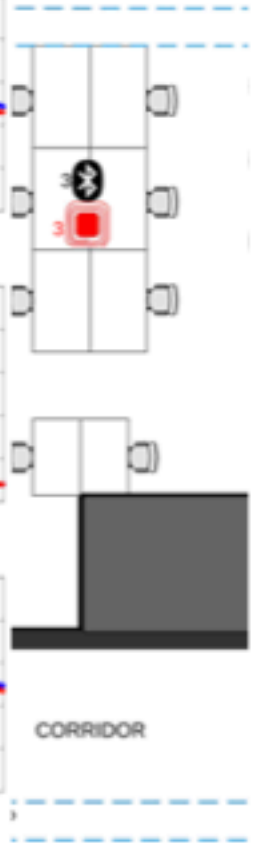
(d) Temperature (°C): couple #4.

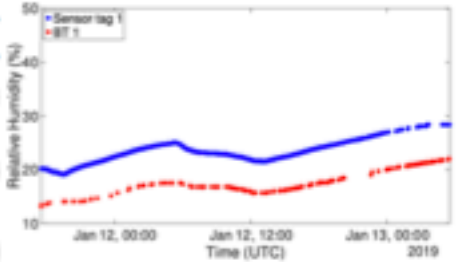


(e) Temperature (°C): couple #5.

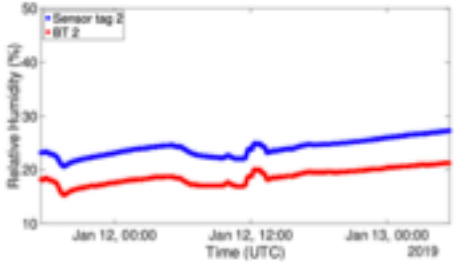


(f) Temperature (°C): couple #6.

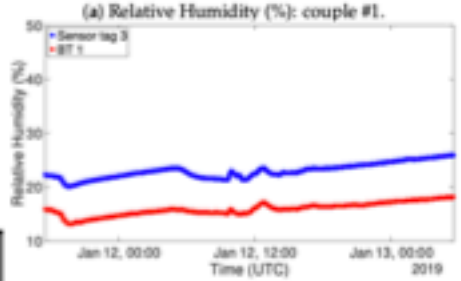




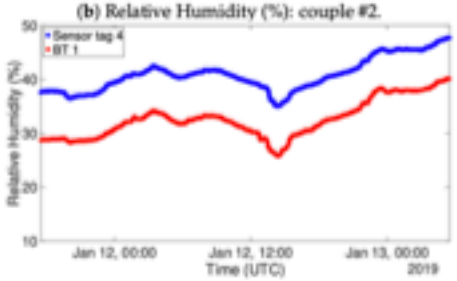
(a) Relative Humidity (%): couple #1.



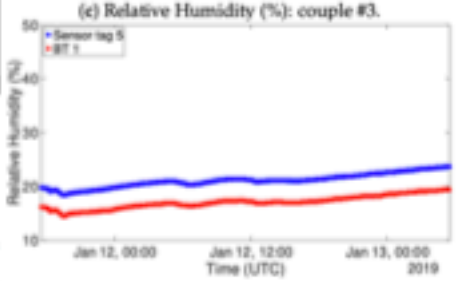
(b) Relative Humidity (%): couple #2.



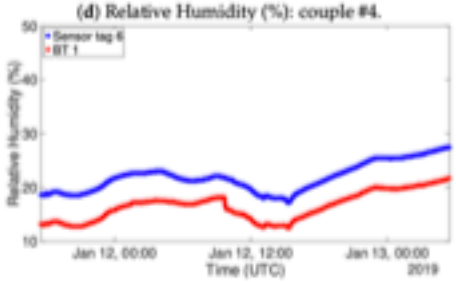
(c) Relative Humidity (%): couple #3.



(d) Relative Humidity (%): couple #4.



(e) Relative Humidity (%): couple #5.



(f) Relative Humidity (%): couple #6.

DATA TRANSMISSION

RFID VS BT WRAP-UP

E. GIUSTO, F. GANDINO, M.L. GRECO, M.GROSSO, B. MONTRUCCHIO, S. RINAUDO; *AN INVESTIGATION ON PERVASIVE TECHNOLOGIES FOR IOT-BASED THERMAL MONITORING.* SENSORS (MDPI) 2019, 19(3), 663; HTTPS://DOI.ORG/10.3390/S19030663.

Both well suited for indoor comfort monitoring

No best choice → Problem/task dependant

Tradeoff
- → **Reconfigurability**
- → **Cost**
- → **Integration**

DATA AUTHENTICITY AND SAFE STORAGE

INTEGRATION OF IOT AND BLOCKCHAIN
FOCUS ON: FOOD SUPPLY CHAIN

DATA AUTHENTICITY AND SAFE STORAGE

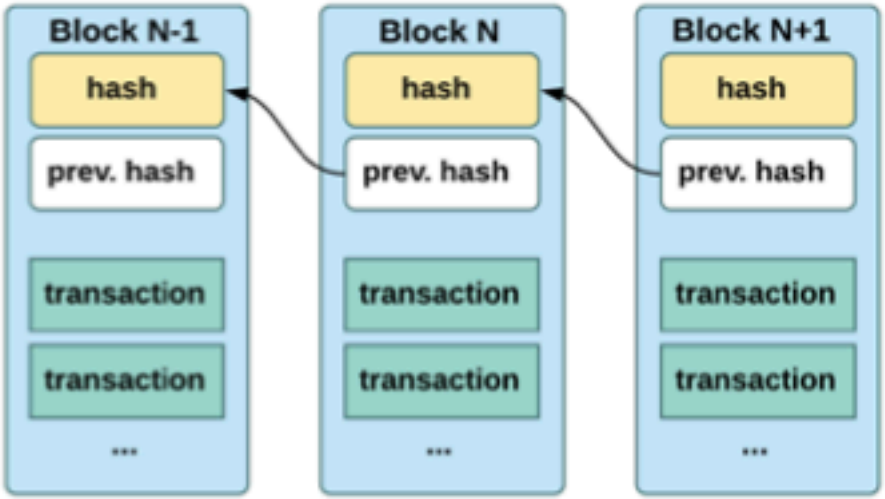
FOOD SUPPLY CHAIN ISSUES

- Paper-based documentation
- Weak certifications
- Lack of information share
- Sustainability issues
- Contamination and alterations

DATA AUTHENTICITY AND SAFE STORAGE

BLOCKCHAIN TO THE RESCUE!

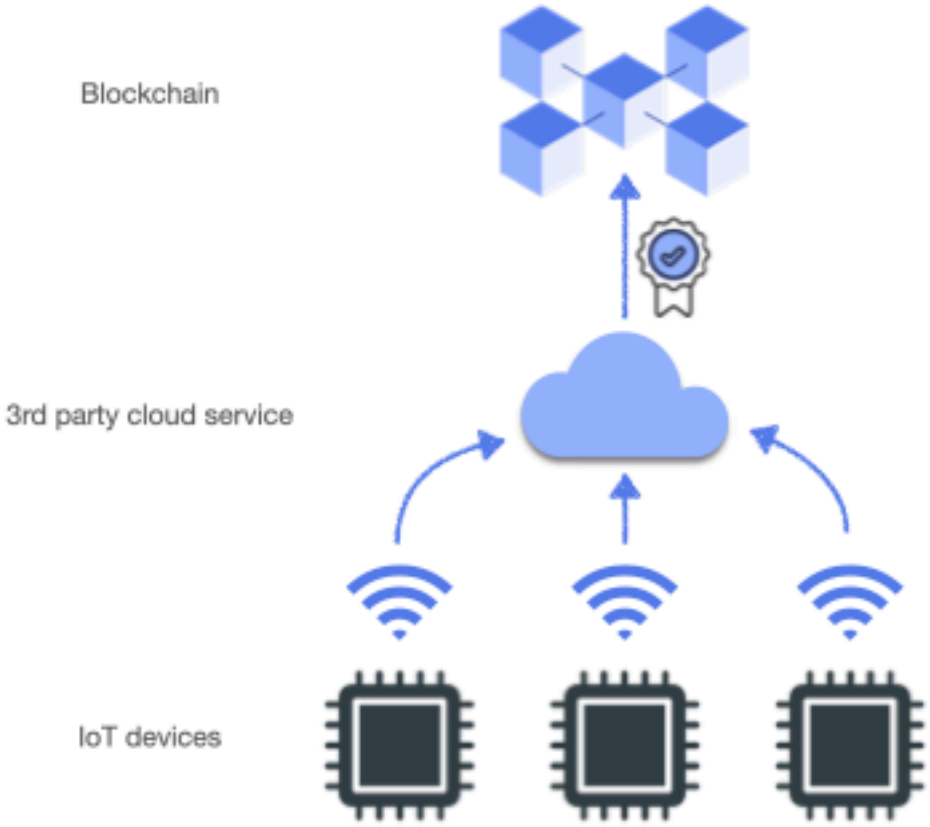
- Block hashing
- Consensus mechanism
- Asymmetric key cryptography



DATA AUTHENTICITY AND SAFE STORAGE

BLOCKCHAIN + IOT: STATE OF THE ART

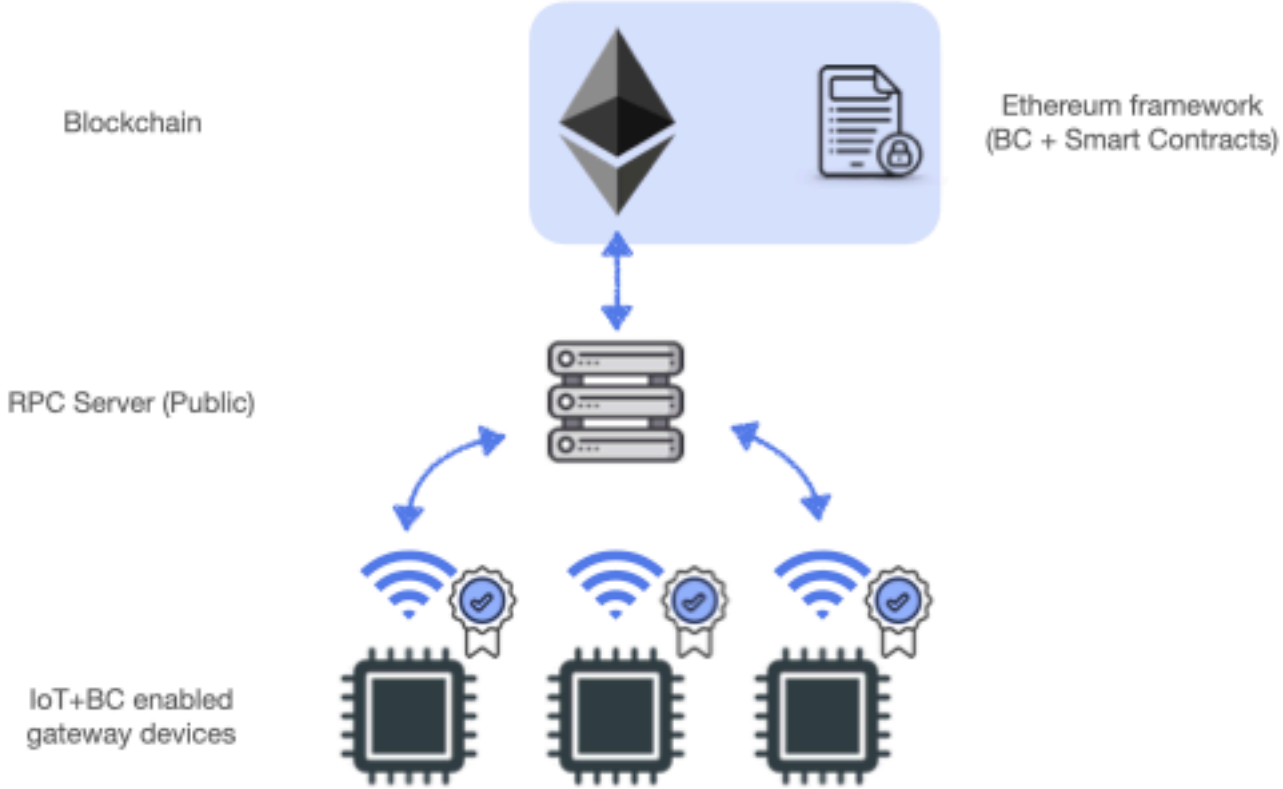
- **Client-server communication**
- **Data not signed in-place**
- **Centralisation**
  - No direct interaction
  - Single point of failure
- **High cost**



DATA AUTHENTICITY AND SAFE STORAGE

BLOCKCHAIN + IOT: PROPOSED SOLUTION

- Blockchain-enabled gateway
- In-place signature
- Remote-Procedure-Call server



Foodchain quadrans FOUNDATION

DATA AUTHENTICITY AND SAFE STORAGE

BLOCKCHAIN + IOT WRAP-UP

J. GRECUCCIO, E. GIUSTO, F. FIORI, M. REBAUDENGO; *COMBINING BLOCKCHAIN AND IOT: FOOD-CHAIN TRACEABILITY AND BEYOND*. ENERGIES (MDPI) 2020, 13 (15), 3820. HTTPS://DOI.ORG/10.3390/EN13153820

Data signed in-place

Data publicly available → Transparency

Decentralized Apps/Smart Contracts

WHAT ADVANTAGES WE GET IF WE APPLY BC TO PM MONITORING?

FUTURE WORKS

FUTURE WORKS

- **PM and thermal monitoring**
  - Automatic window opening and closing
  - Letting fresh air in without compromising thermal insulation
- **Analysis of sensor redundancy for PM monitoring**
  - Automatic re-configuration depending on status of sensors
- **Implementation of PM participate sensing**
  - BT smartphones and LoRaWAN
- **PM more tests for traffic light and LTA**
- **Exploiting BC potential in PM/Thermal monitoring**

WRAPPING UP

WRAPPING UP

- Are we sampling a certain signal at the correct frequency?
- Does the sensor we use produce scientifically valid data?
- What is the best wireless protocol to transmit sensed data?
- Are these data authentic?
- Now that we were able to sample and transmit these precious data, how do we store them in a way that they cannot be tampered with/altered?

THANK YOU

PLEASE ASK QUESTIONS

Icons by Iconscout Freebies / Alpar - Etele Meder / Raspberry Pi Icon /Rocket Icon/Apple icons.

BACKUP SLIDES

PUBLICATIONS

PUBLICATIONS

JOURNAL PAPERS

- E. Giusto, F. Gandino, M.L. Greco, M.Grosso, B. Montrucchio, S. Rinaudo; *An Investigation on Pervasive Technologies for IoT-based Thermal Monitoring*. Sensors (MDPI) 2019, 19(3), 663; https://doi.org/10.3390/s19030663.
- J. Grecuccio, E. Giusto, F. Fiori, M. Rebaudengo; *Combining Blockchain and IoT: Food-Chain Traceability and Beyond.* Energies (MDPI) 2020, 13 (15), 3820. https://doi.org/10.3390/en13153820
- E. Giusto, M. Ghazi Vakili, F. Gandino, C. Demartini, B. Montrucchio; *Quantum pliers cutting the Blockchain.* IT Professional (IEEE) 2020, Vol.22, Issue 6. https://doi.org/10.1109/MITP.2020.2974690
- B. Montrucchio, E. Giusto, M. Ghazi Vakili, S. Quer, R. Ferrero, C. Fornaro; *A Densely-Deployed, High Sampling Rate, Open-Source Air Pollution Monitoring WSN*. Transactions on Vehicular Technologies (IEEE) 2020. https://doi.org/10.1109/TVT.2020.3035554
- M. Collotta; R. Ferrero; E. Giusto; M. Ghazi Vakili; J. Grecuccio; X, Kong; ; I. You. *A Fuzzy Control System for Energy Efficient Wireless Devices in the Internet of Vehicles*. International Journal of Intelligent Systems (Wiley). https://doi.org/10.1002/int.22353

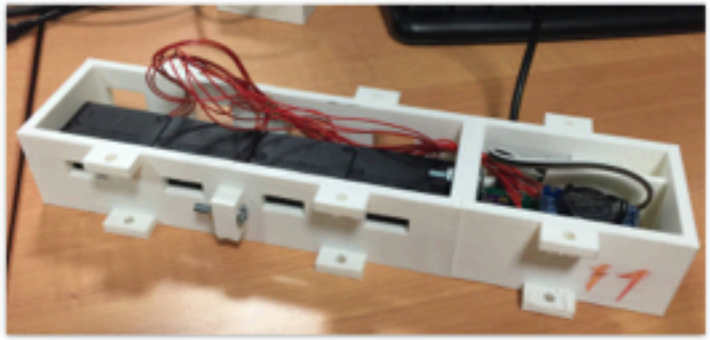
PUBLICATIONS

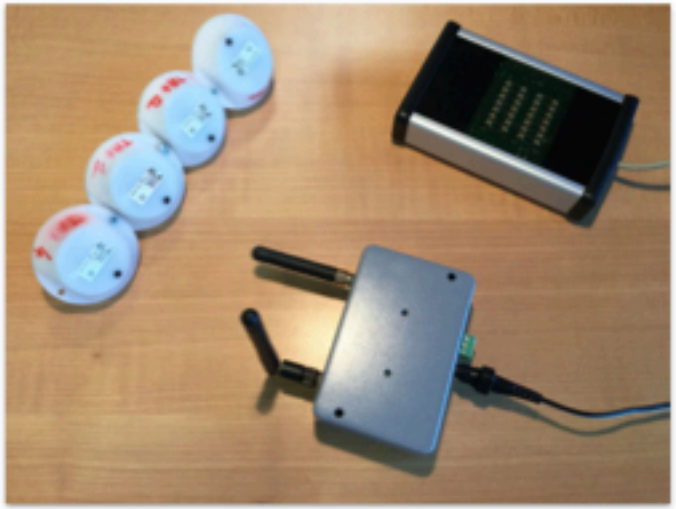
CONFERENCE PROCEEDINGS

- E. Giusto, F. Gandino, M. L. Greco, B. Montrucchio, M. Rebaudengo; *A dense RFID network for flexible Thermal Monitoring*. 2018 6th International EURASIP Workshop on RFID Technology, Brno (Czech Republic), 11-12 September 2018. (ISBN: 9781538659373). https://doi.org /10.1109/ EURFID.2018.8611649
- E. Giusto, R. Ferrero, F. Gandino, B. Montrucchio, M. Rebaudengo, M. Zhang; *Particulate matter monitoring in mixed indoor/outdoor industrial applications: a case study*. 23rd International Conference on Emerging Technologies and Factory Automation, Torino (Italy), 4-7 September 2018. (ISBN: 9781538671078). https://doi.org/10.1109/ETFA.2018.8502644
- R. Ferrero, M. Ghazi Vakili, E. Giusto, M. Guerrera, V. Randazzo; *Ubiquitous fridge with Natural Language Interaction.* 2019 IEEE International Conference on RFID Technology and Applications (RFID-TA). https://doi.org/10.1109/RFID-TA.2019.8892025
- O. Costa Hamido, G.A. Cirillo, E. Giusto; *Quantum synth: a quantum-computing-based synthesizer*. AM '20: Proceedings of the 15th International Conference on Audio Mostly, September 2020. Pages 265–268. https://doi.org/10.1145/3411109.3411135

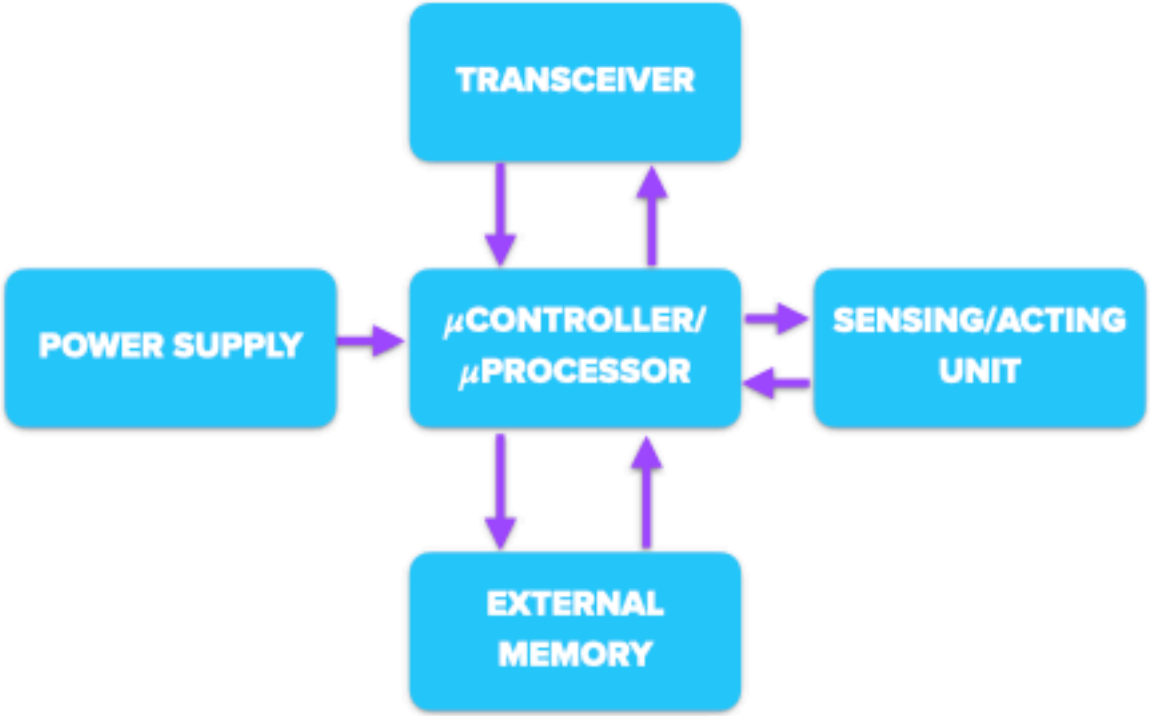
MY APPLICATIONS IN THE IOT DOMAIN

- Air Pollution Monitoring
- Thermal monitoring
- Natural Language Processing for smart fridge applications
- Food traceability
- Airplane fuselage monitoring





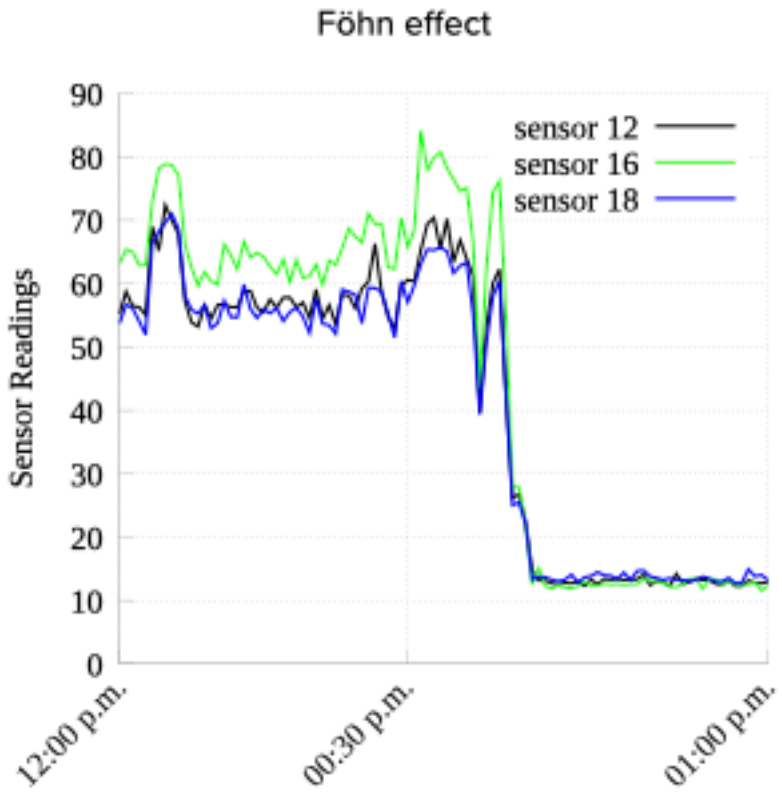
IOT NODES

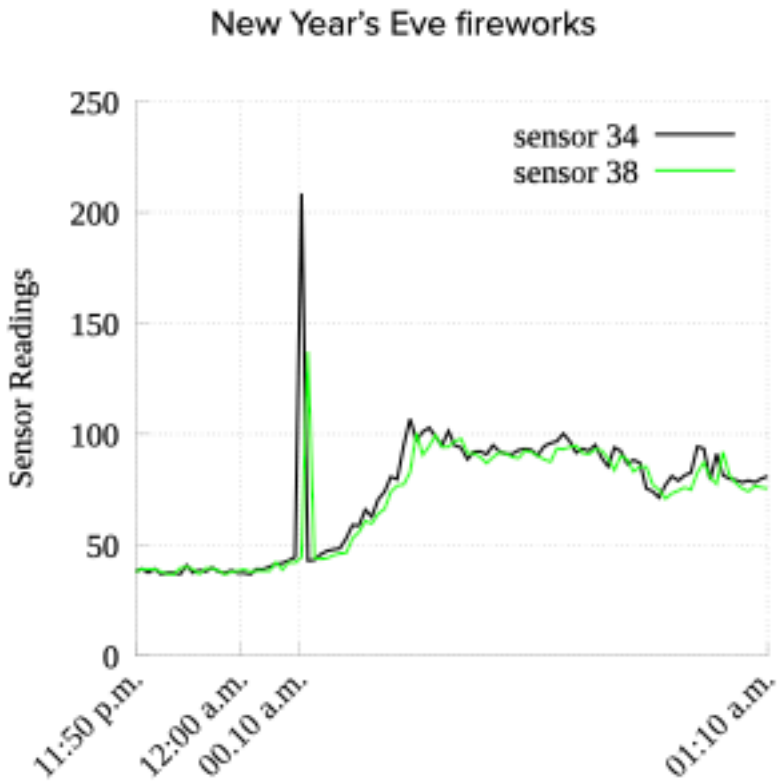


Sensing Node Architecture

DATA ACQUISITION

INTERESTING PHENOMENA

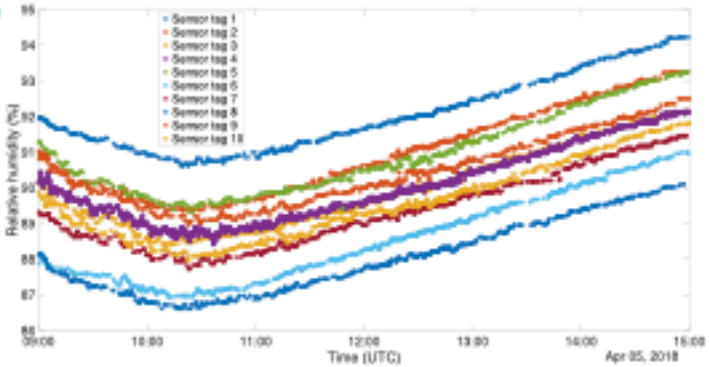


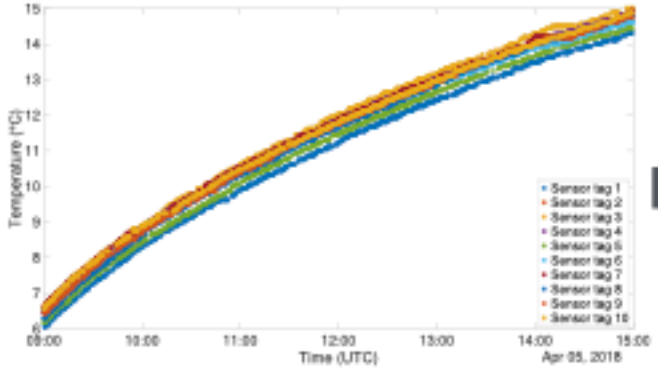


DATA TRANSMISSION

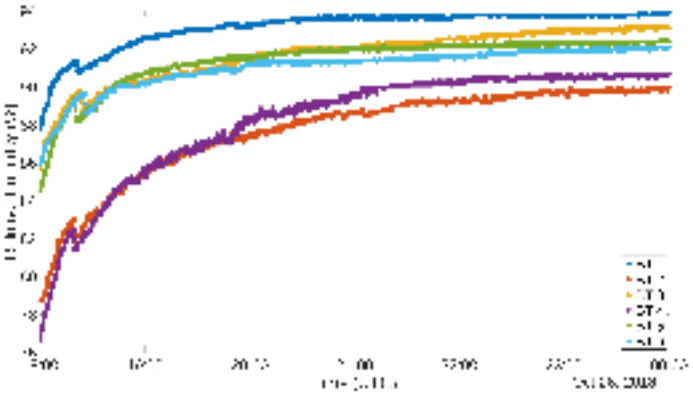
EXPERIMENTAL ANALYSIS

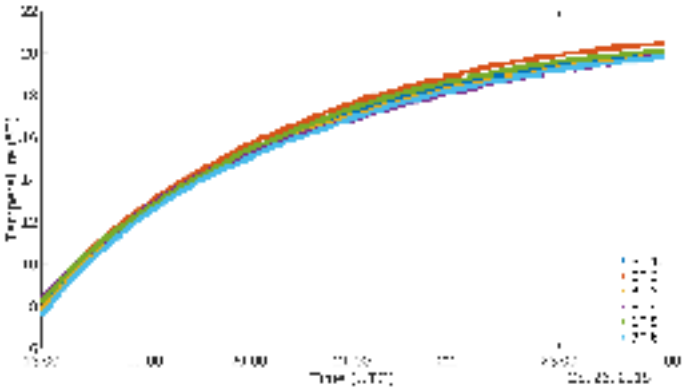
- Refrigerator test





RFID





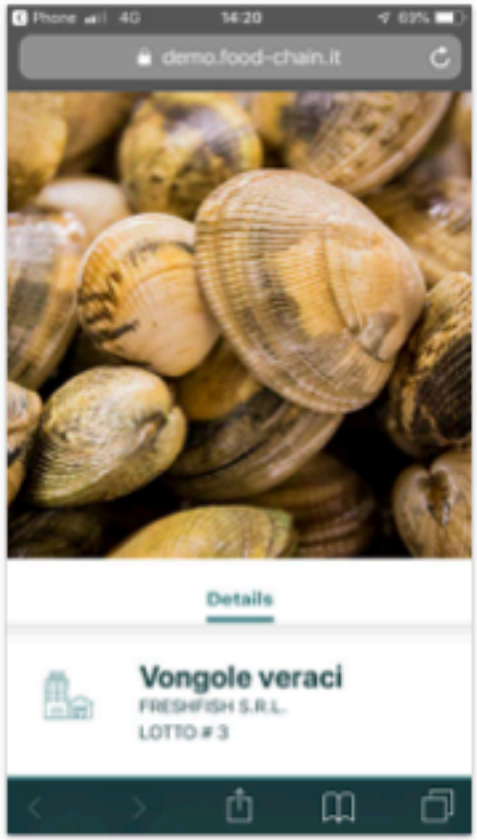
BT

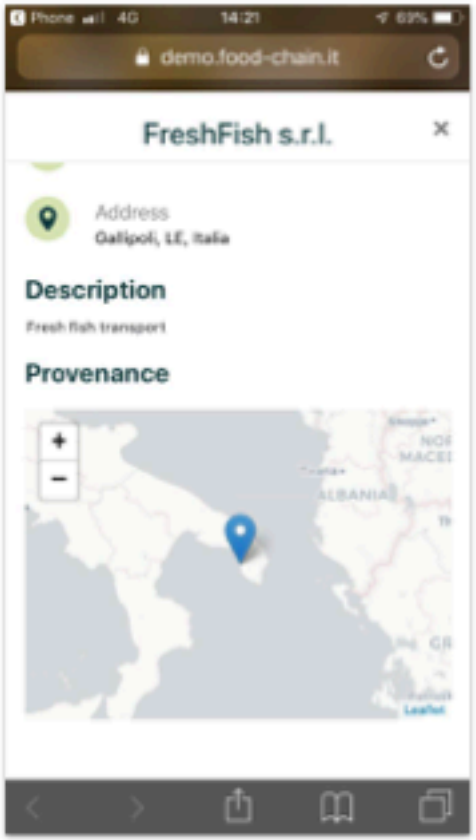
RH (%)

T(°C)

DATA AUTHENTICITY AND SAFE STORAGE

DON'T TRUST, SCAN!

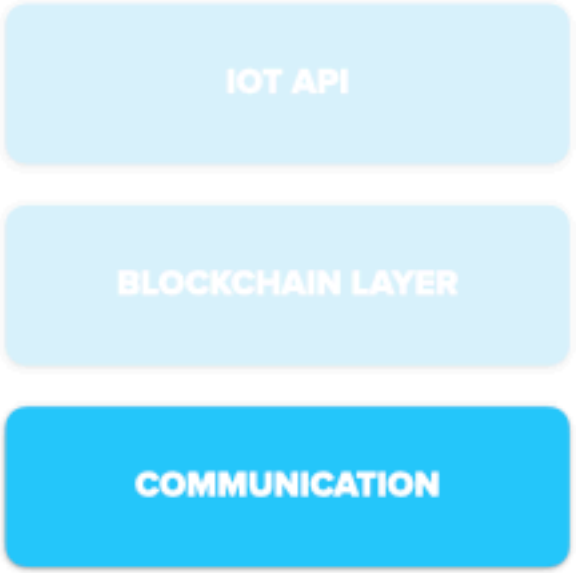




DATA AUTHENTICITY

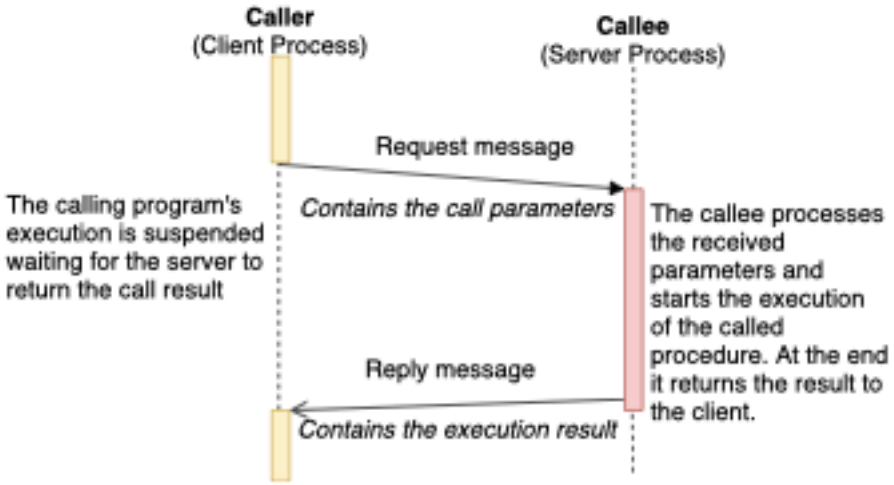
USER-FRIENDLY API - JSON-RPC LAYER

- RPC protocol over a TCP channel
- Devices remotely call procedures on other nodes
- Node executes the procedure and sends back the result

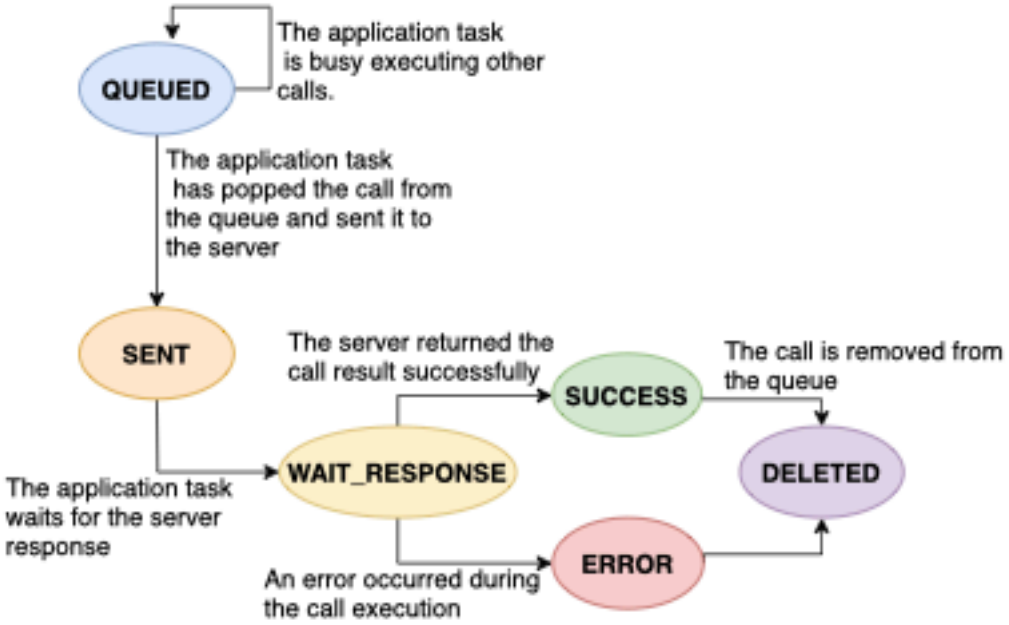


DATA AUTHENTICITY

REMOTE PROCEDURE CALL EXECUTION



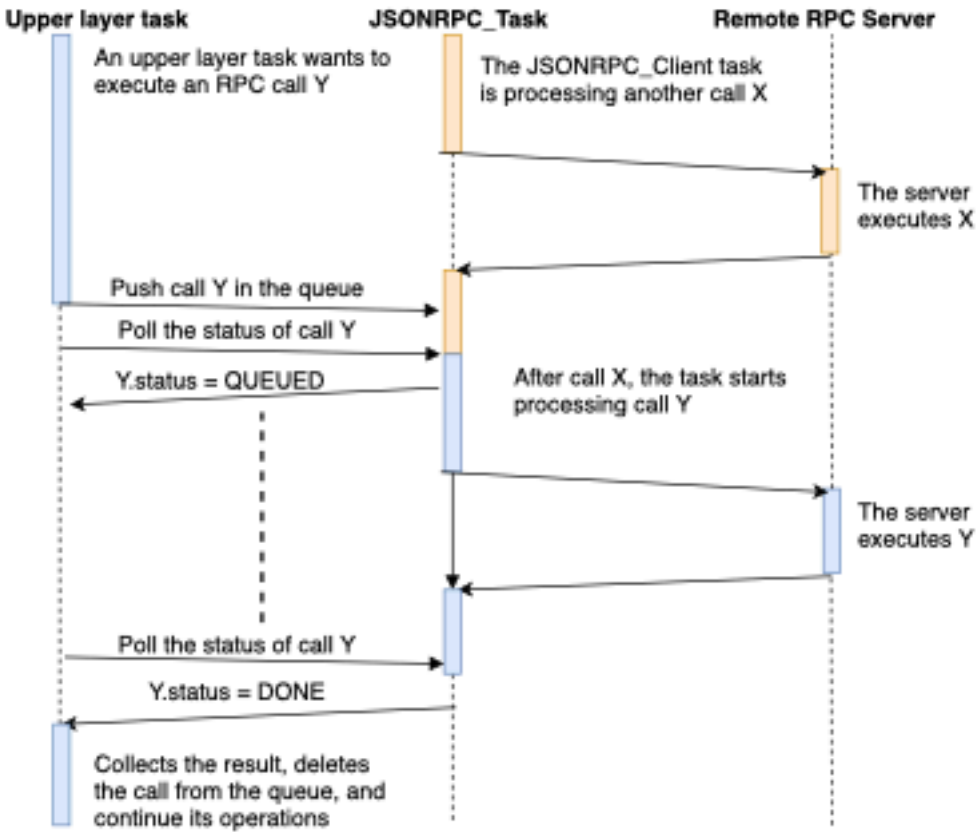
RPC execution



State-transition diagram for a call object

DATA AUTHENTICITY

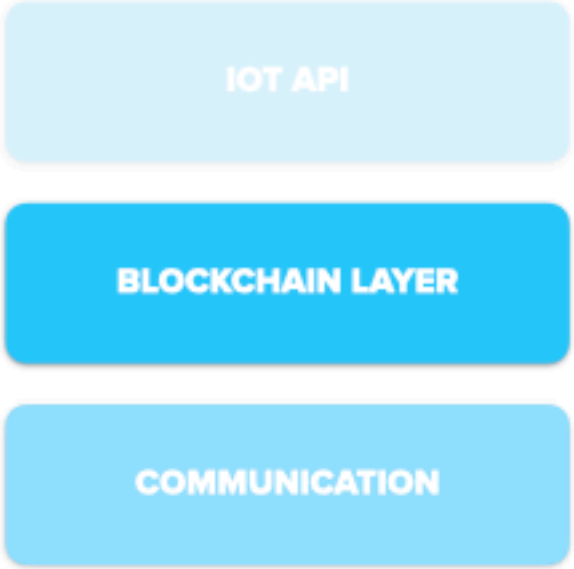
JSONRPC SEQUENCE DIAGRAM



DATA AUTHENTICITY

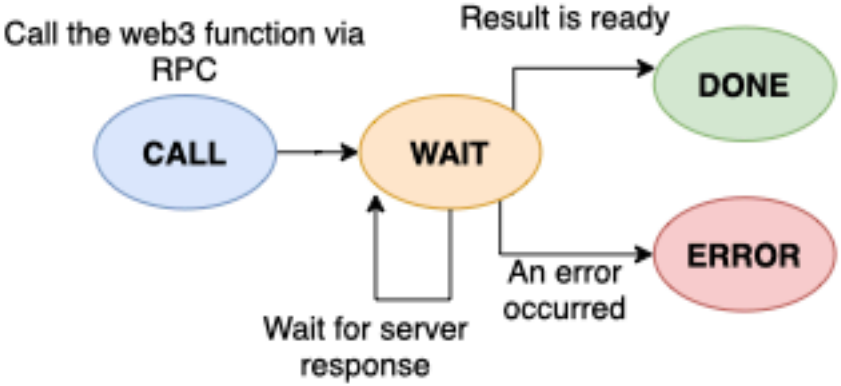
USER-FRIENDLY API

- Adapts data formats
- Sign data offline before RPC call
- Pass parameters to RPC layer and decodes the result
- Handle errors



DATA AUTHENTICITY

ETHEREUM INTERACTION BETWEEN STATES

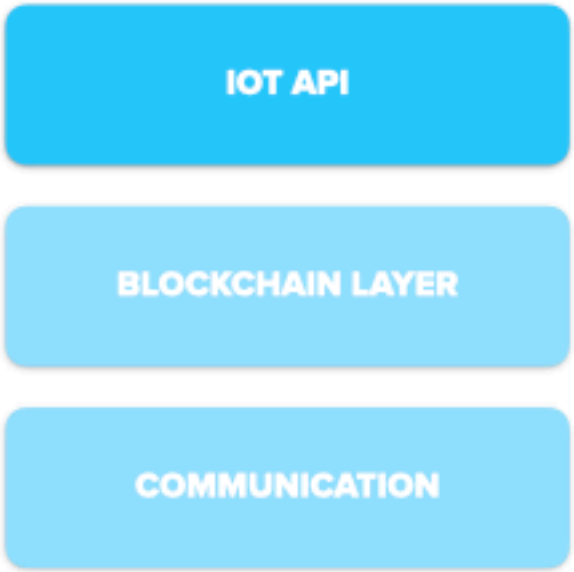


State transition diagram for a web3 call

DATA AUTHENTICITY

USER-FRIENDLY API

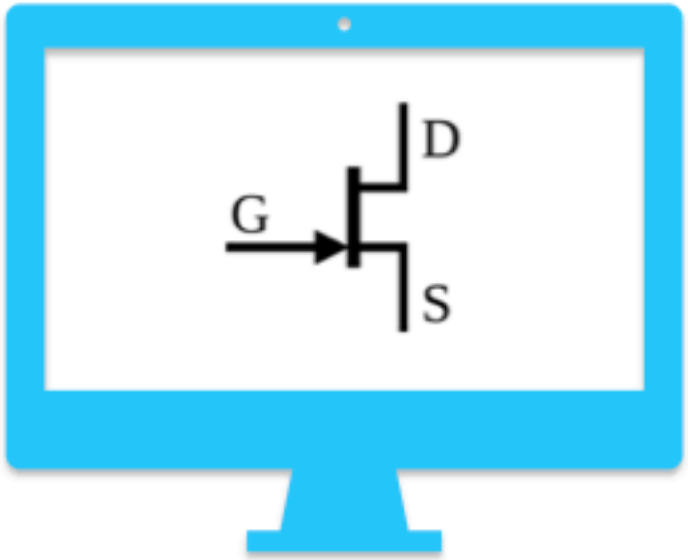
- Wraps the blockchain layer
- Hides interaction details
- Highly usable for most of IoT developers
- Allows configuration for improving portability



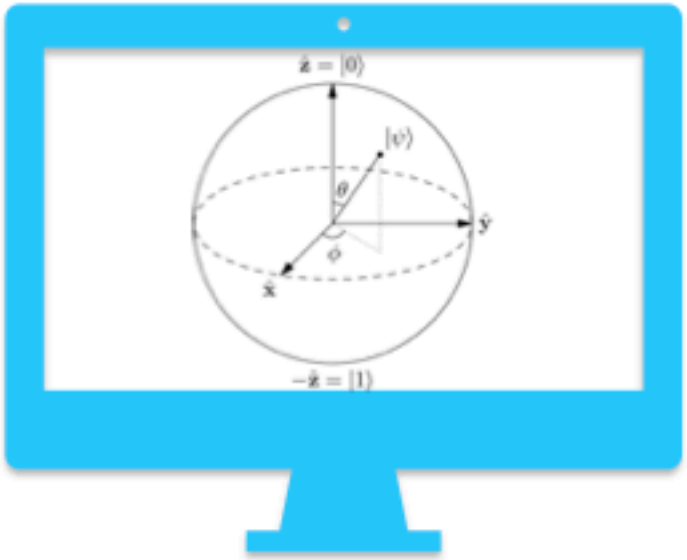
“HELLO, QUANTUM WORLD!” (...HELLO, NEW THREATS!)

"HELLO, QUANTUM WORLD!"

QUANTUM COMPUTING



Bit-based computer



Qubit-based computer

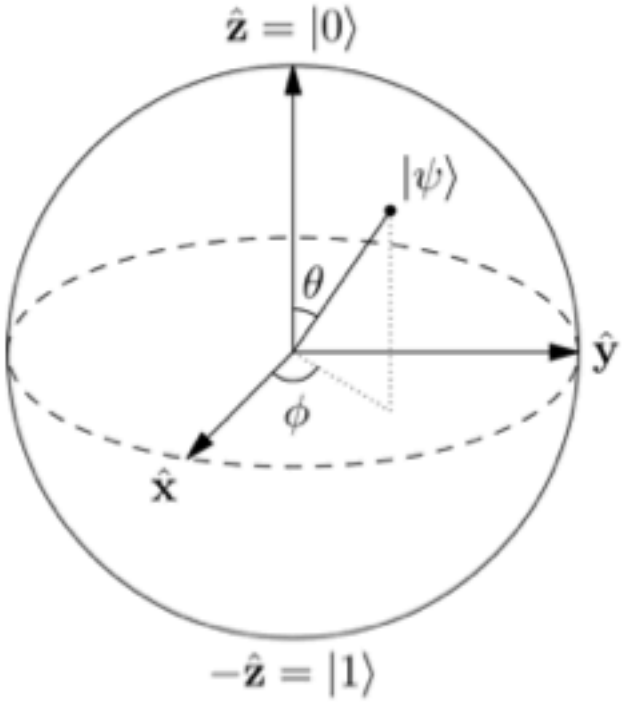
"HELLO, QUANTUM WORLD!"

QUANTUM STATES

- **Basis states**

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$



Bloch sphere

"HELLO, QUANTUM WORLD!"

QUANTUM STATES

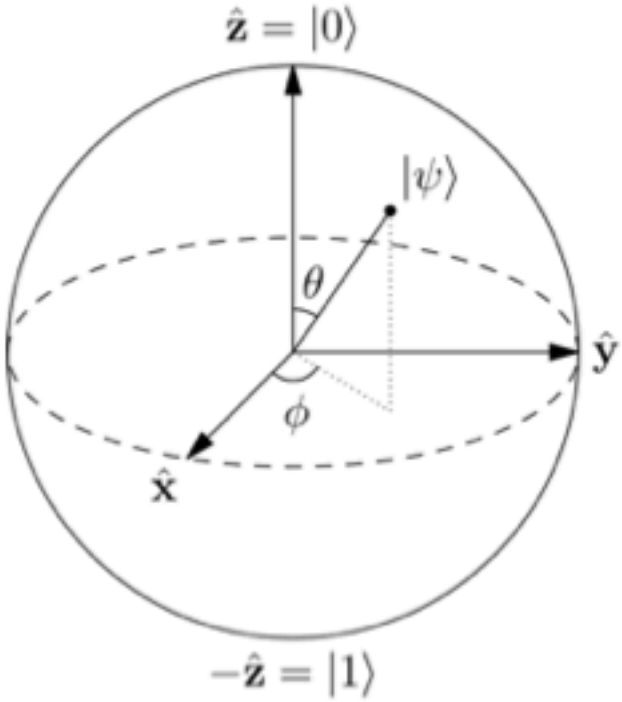
- **General state**

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

$$|\alpha|^2 + |\beta|^2 = 1$$

- **Superposition state**

$$|\psi\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$



Bloch sphere

"HELLO, QUANTUM WORLD!"

QUBIT: CHARACTERISTICS

- Superposition
  - "Both" 0 and 1 (|0> and |1>)
- Entanglement
  - Strong correlation of qubits
- Probabilistic Nature
  - Not 100% sure
- Naturally parallel
  - N qubits -> 2^N states
- Adjustable Probability Amplitudes

"HELLO, QUANTUM WORLD!"

QUBIT: ISSUES

- No-Cloning theorem
  - Cannot be copied!
- Must be kept cold
  - Around 10 mK
- Short coherence time
  - Around 100 μs
- Difficult to simulate
  - 28 qubit - 4 GB RAM
  - 56 qubit - 4.5 TB RAM
  - ...

NATURE IS QUANTUM, GODDAMN IT! SO IF WE WANT TO SIMULATE IT, WE NEED A QUANTUM COMPUTER

RICHARD FEYNMAN, CALTECH

"HELLO, QUANTUM WORLD!"

NEW POSSIBILITIES

Quantum Computation:

- Grover's algorithm
  - Search unstructured database
- Quantum annealing
  - Special purpose, optimisation of classical problems (Travelling salesperson)
- Deep Learning and Machine Learning
  - Finance, classification...

Quantum Simulation:

- Chemistry
  - Drug discovery
  - Oil and gas
  - Batteries
- Structures
  - Vehicle shape
- Systems
  - Fleet management

"HELLO, QUANTUM WORLD!"

QUANTUM THREATS TO BLOCKCHAIN

- Attacks on Proof-of-Work
  - Grover's algorithm
- Countermeasures
  - Flexibly difficult
  - Asymmetric
  - No quantum advantage
  - Shift to Proof-of-Stake
- Attacks on Signatures
  - Shor's algorithm
    - Break RSA
  - Address reuse
  - Transaction in progress
- Countermeasures
  - Size increase (keys and signatures)
  - Time to check signatures

"HELLO, QUANTUM WORLD!"

QUANTUM-PROOF DLT - REVIEW

- QRL
  - Secure signature thanks to W-OTS+
  - Public blockchain, cryptocurrency-oriented
  - Fee for transactions (mining!)
  - No Smart Contracts
- Corda
  - Secure signature thanks to W-OTS-T
  - Financial applications
  - Permissioned blockchain
  - Smart Contracts with legal prose contracts
  - No PoW
  - Cryptocurrency-agnostic
- IOTA
  - Not BC, but *tangle*
  - Suitable for IoT
    - M2M micropayments
  - Transaction issuing requires validation of 2 transactions
    - More involved, higher probability of validation
  - No mining

HELLO QUANTUM

SHOR'S ALGORITHM - PERIOD FINDING

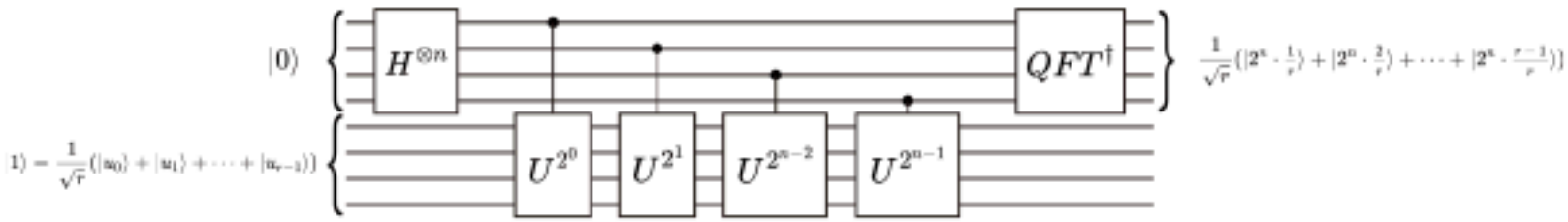
- Periodic function

$$f(x) = a^x \bmod N$$

- Period r

$$a^r \bmod N = 1$$

- Quantum Phase Estimation

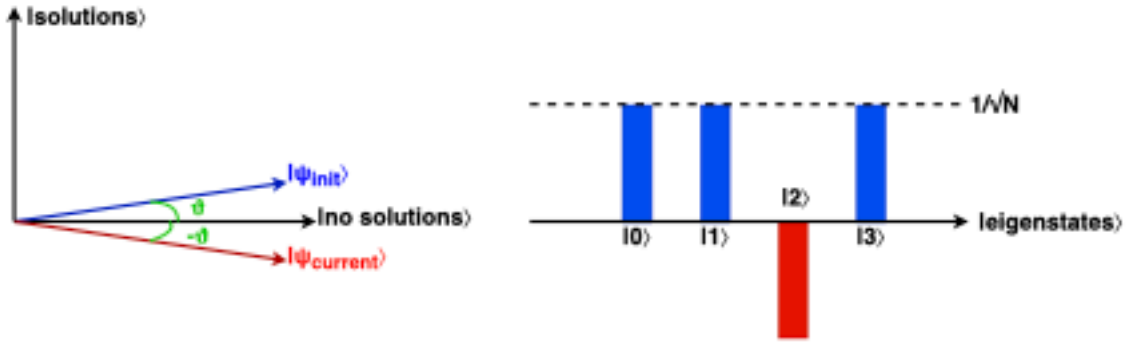


HELLO QUANTUM

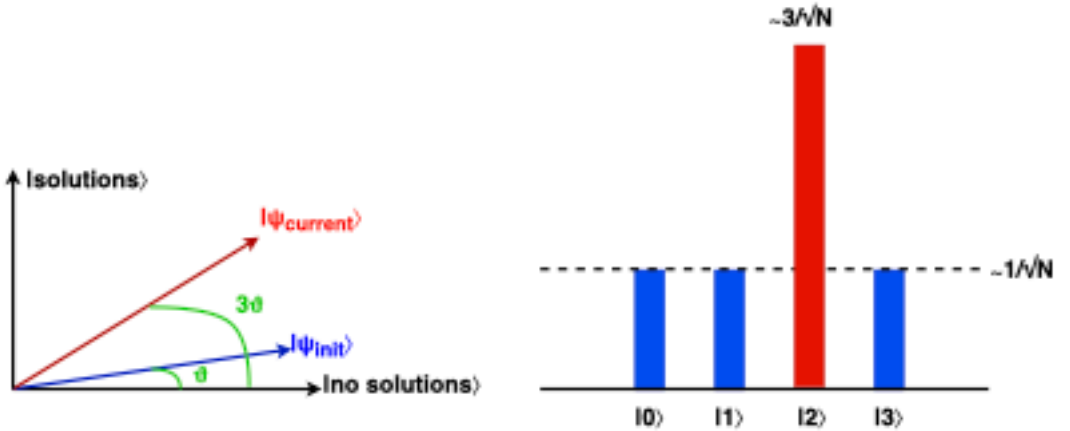
GROVER'S ALGORITHM

- Amplitude amplification
- Input: for $N = 2^n$, we are given $x \in \{0,1\}^N$
- Goal: find i s.t. $x_i = 1$ with few queries

- Classical: $O(N)$ queries
- Quantum: $O(\sqrt{N})$ queries



Phase kickback



Amplitude amplification