

# Application of Blockchain to Secure Distributed Storage of the SAFecast Open Sensor Network Data

## Pieter Franken

Senior Visiting Researcher, Blockchain Lab, Keio University SFC  
Research Affiliate, Center for Civic Media, MIT Media Lab  
Representative Director, SAFecast Japan 一般社団法人

## Richard Rowland

Senior Student, Keio University SFC

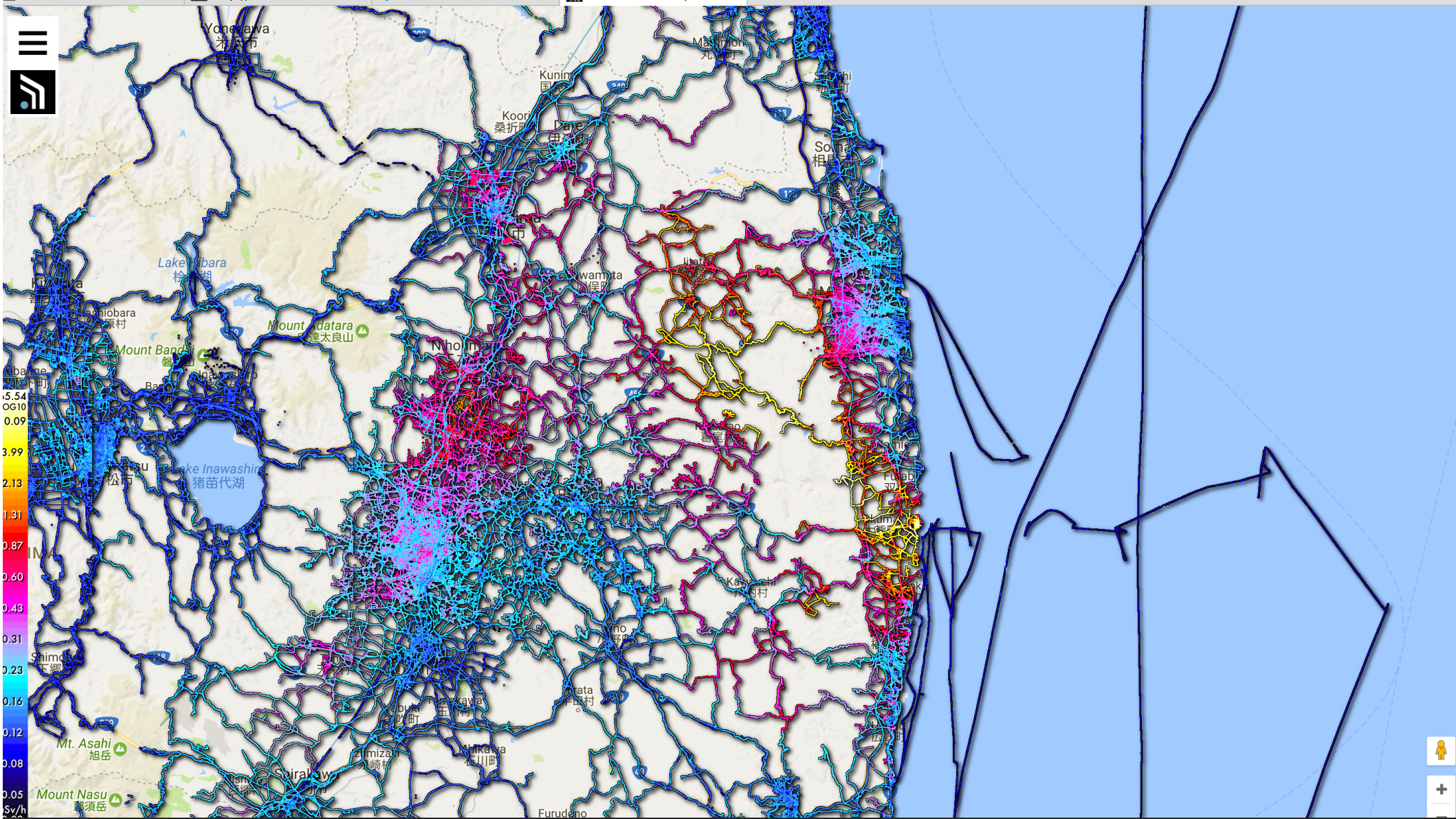


# The Safecast Project Today

- Collected over 85,000,000 measurements, adding ~2,000,000 new measurements each month with contribution from over 100 countries
- Mobile and stationary sensors measuring radiation and air pollution
- Fully open data set (CC-0)

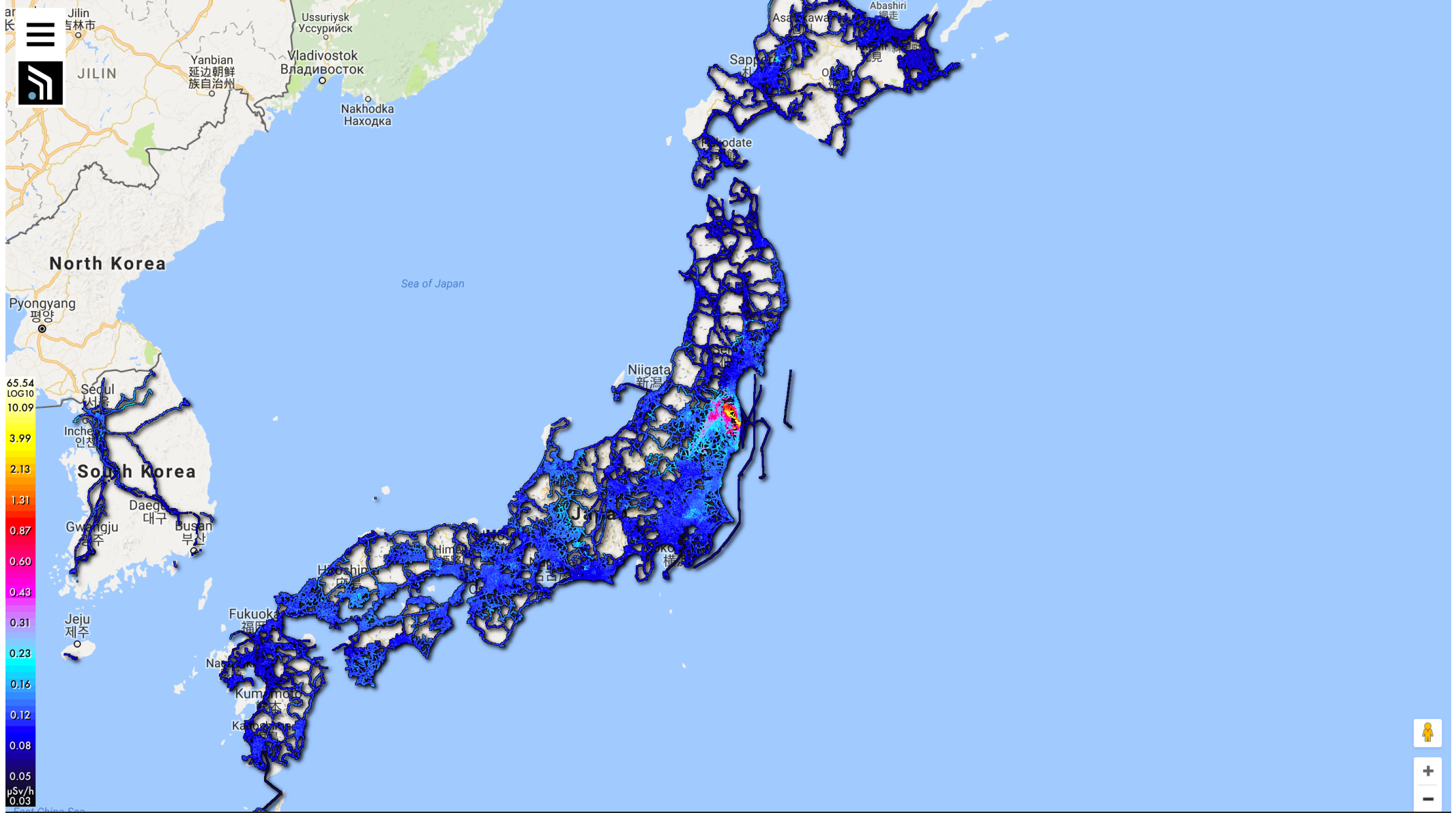
<http://map.safecast.org>

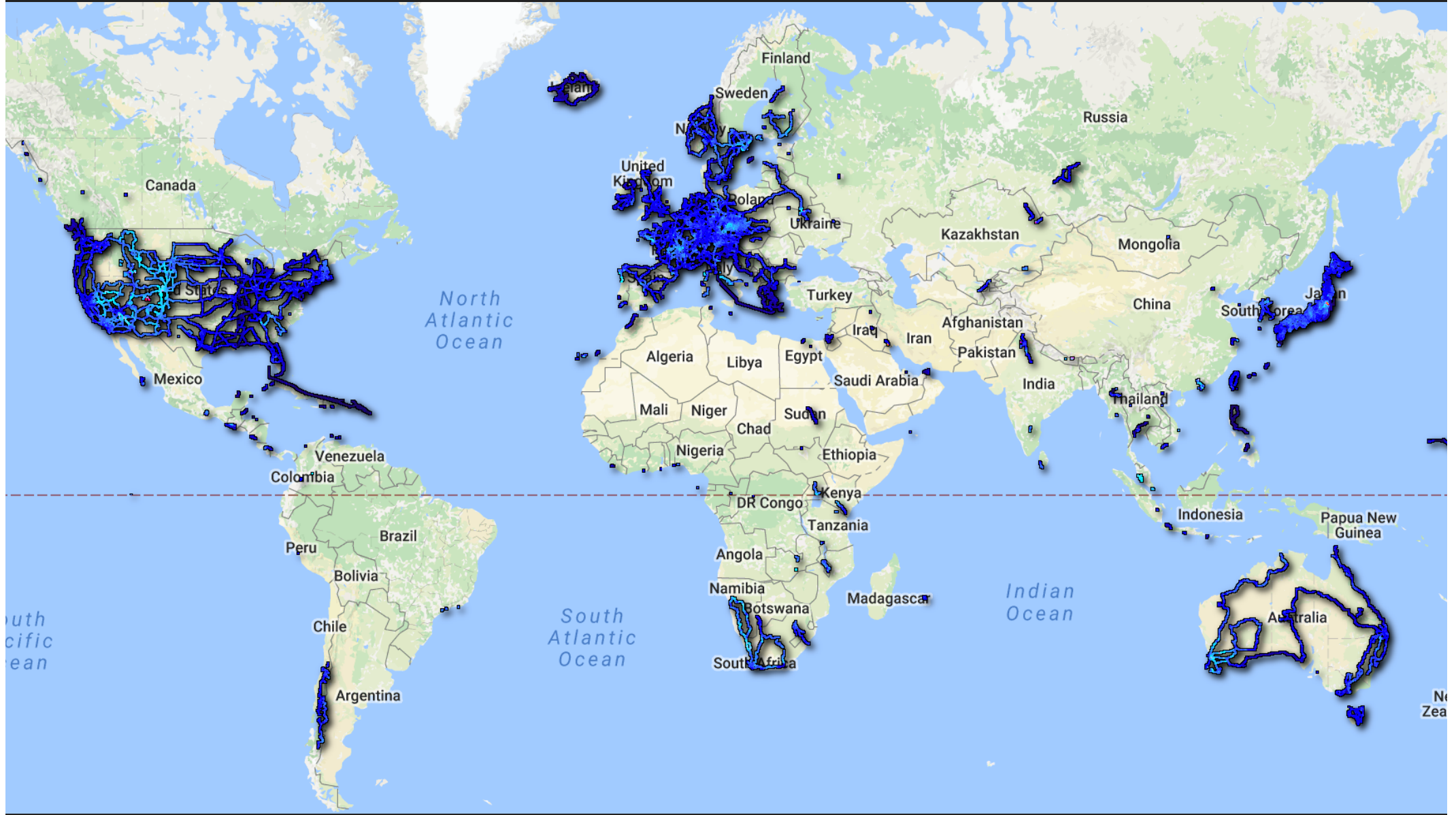




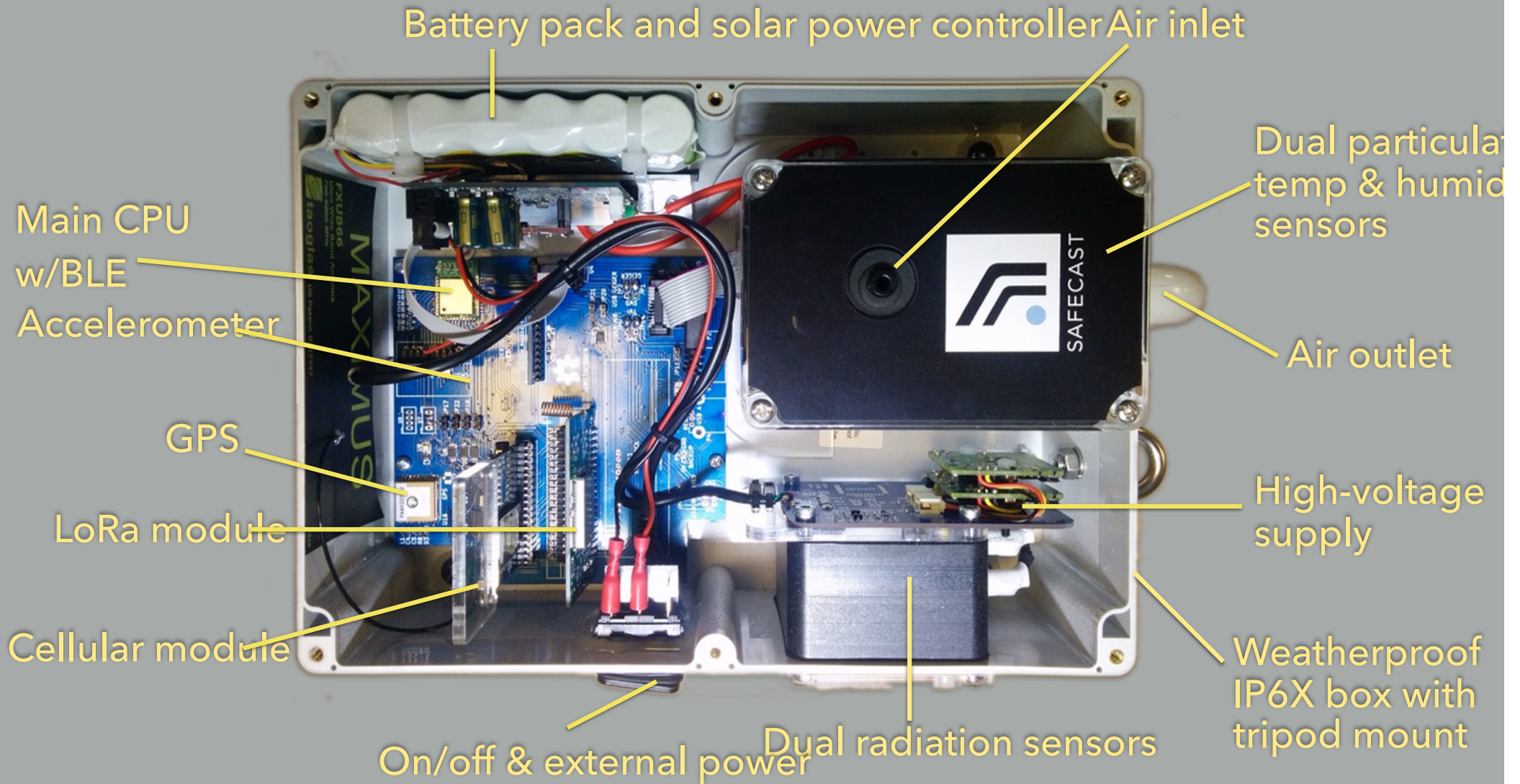
5.54  
3.99  
2.13  
1.31  
0.87  
0.60  
0.43  
0.31  
0.23  
0.16  
0.12  
0.08  
0.05  
sw/h















# Research Paper

IOPscience

Journals ▾

Books

Publishing Support

Login ▾

Search IOPscience content

Search

Article Lookup ▾

Journal of Radiological Protection



Official journal of  
the Society for  
Radiological Protection

PAPER • OPEN ACCESS

## Safecast: successful citizen-science for radiation measurement and communication after Fukushima

Azby Brown<sup>1,3</sup>, Pieter Franken<sup>2,3</sup>, Sean Bonner<sup>2,3</sup>, Nick Dolezal<sup>3</sup> and Joe Moross<sup>3</sup>

Published 6 June 2016 • © 2016 IOP Publishing Ltd

[Journal of Radiological Protection, Volume 36, Number 2](#)

 Article PDF

[Figures ▾](#) [References ▾](#) [Citations ▾](#)

### + Article information

#### Abstract

The Fukushima Daichi Nuclear Power Plant disaster, which began on 11 March 2011, provided a crucial opportunity to evaluate the state of preparation on the part the powerplant operator (TEPCO), relevant Japanese government agencies, and international oversight bodies, to gather necessary information on radiation risks quickly and to share it with those tasked with emergency response as well as with the general public. The inadequacy of this preparation and the chaotic nature of inter-agency and inter-governmental communication has been well noted in several official reports on the disaster. In response, Safecast, an international, volunteer-based organization devoted to monitoring and openly sharing information on environmental radiation and other pollutants, was initiated on 12 March 2011, one day following the start of the accident. Since then the group has

6904 Total downloads

Cited by 5 articles



Turn on MathJax

Share this article



Abstract

1. Introduction

2. Method

3. Results

4. Conclusions

Acknowledgments

References

Citations

#### Related content

##### JOURNAL ARTICLES

[Improved communication, understanding of risk perception and ethics related to ionising radiation](#)

[The limits of public communication coordination in a nuclear emergency: lessons from media reporting on the Fukushima case](#)

[The state of radiological protection; views of the radiation protection profession: IRPA13, Glasgow, May 2012](#)

[Looking for citizen-centered communication: dialogues between radiological protection or nuclear safety specialists and media professionals](#)

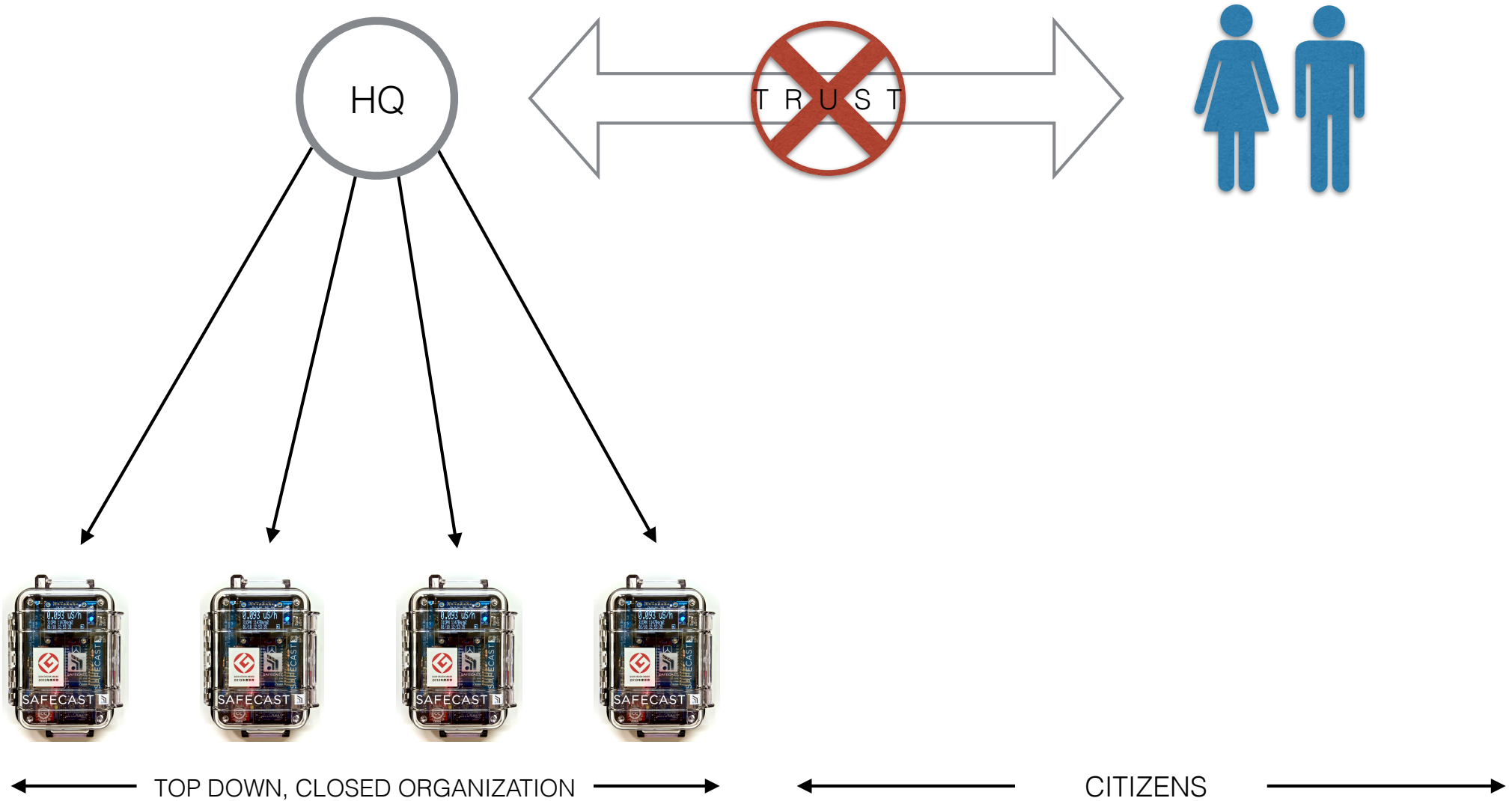
[How did media present the radiation risks after the Fukushima accident: a content analysis of newspapers in Europe](#)

[Radiological protection issues arising during and](#)

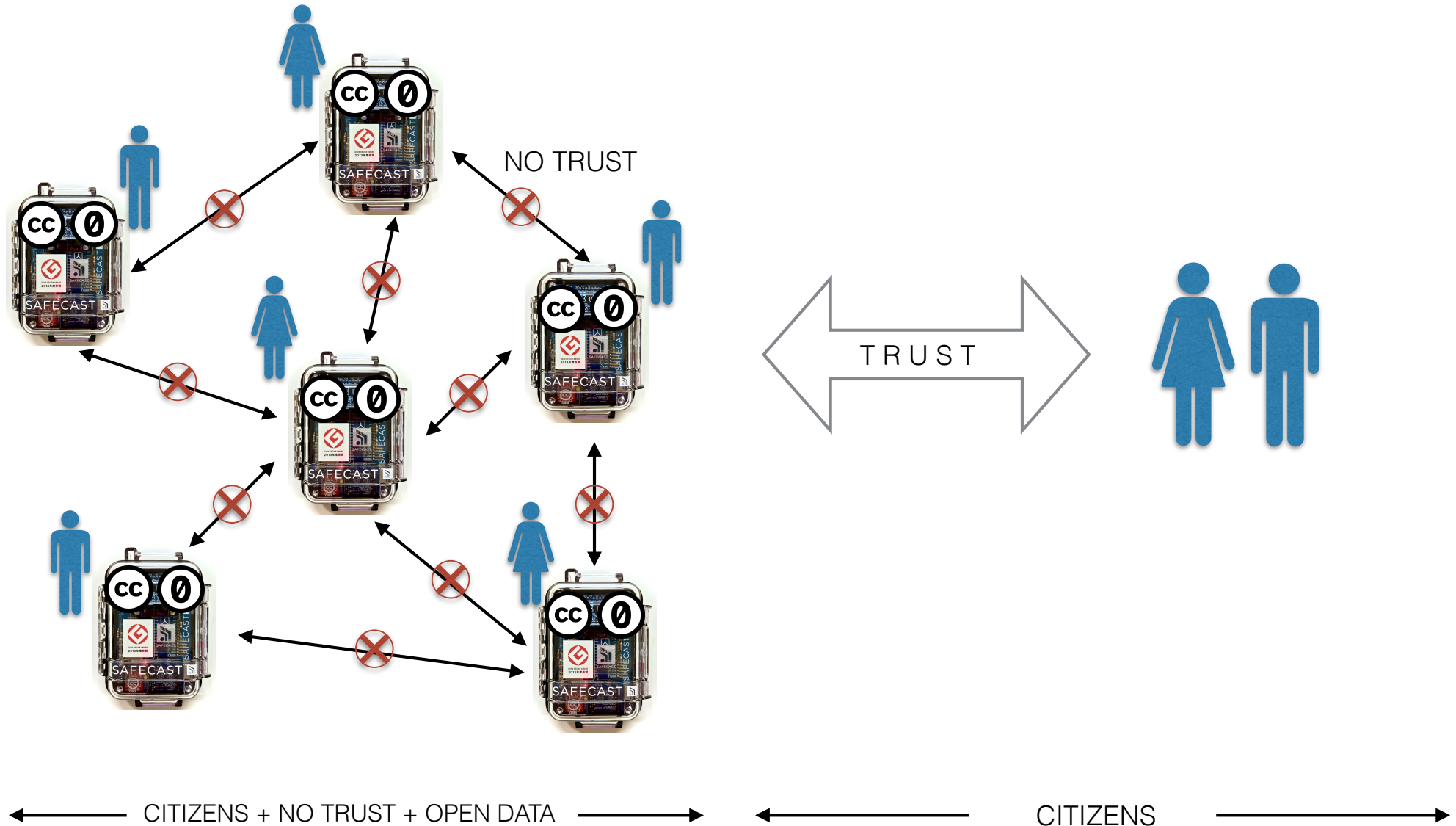
TRUST NO ONE

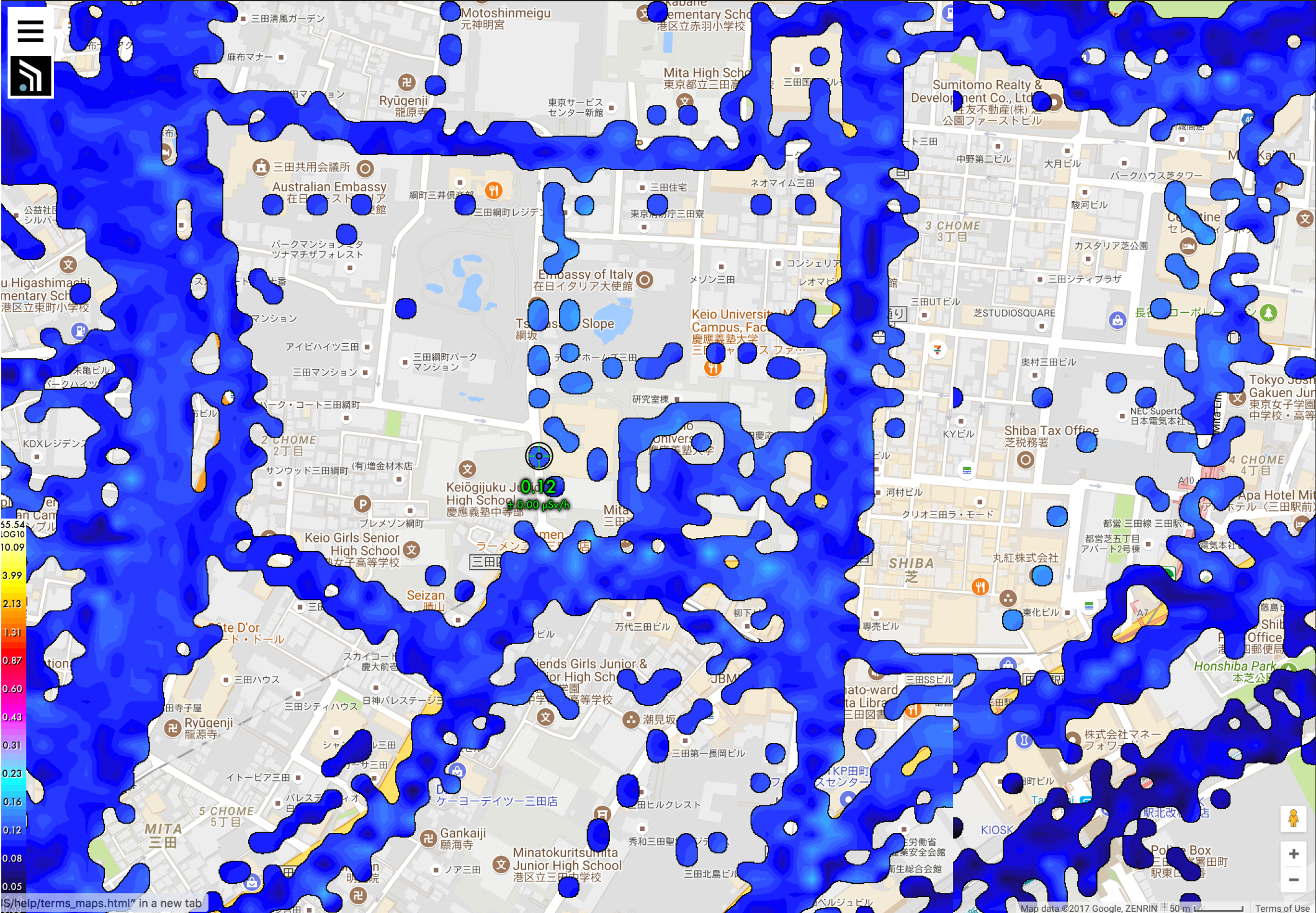
The background of the image is a dark, atmospheric landscape. The sky is a deep, dark blue with some lighter, wispy clouds. The foreground and middle ground are dominated by dark, silhouetted hills and mountains. The overall mood is somber and mysterious.

# Top-Down, Closed Organizations Lost Citizens Trust

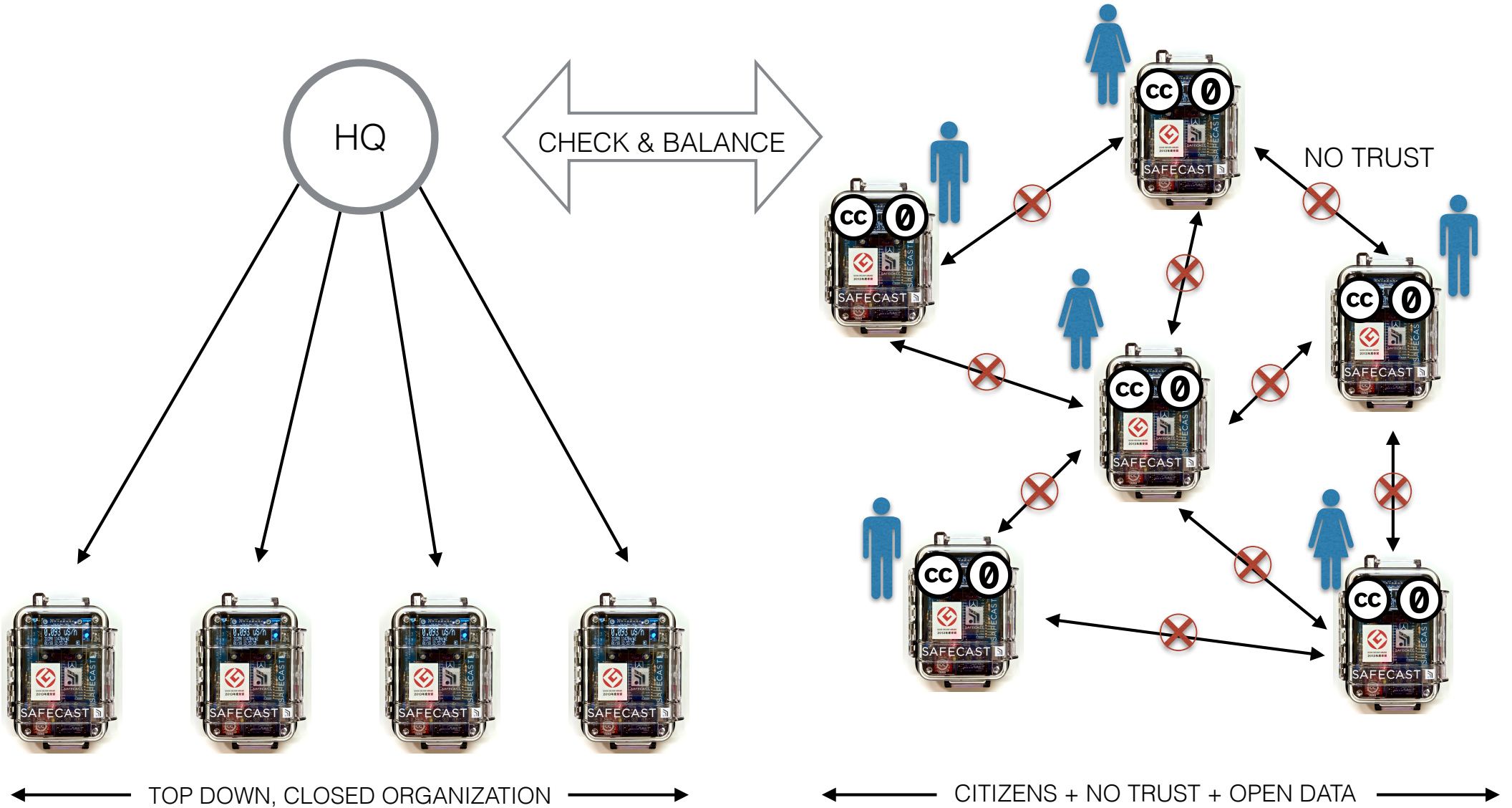


# Power of the Crowd: Building *Trust* out of *No Trust*





# Bring Check and Balance



# Today's Challenges in Open Sensor Networks

- How to detect broken sensors
- How to detect “rogue/fake” sensors
- How to prevent “bricked” devices
- How to ensure network is autonomous and fully decentralized
- How to ensure provenance of data collected - preserve history
- How to have no dependency on a central database



# Apply Blockchain Principles

- Distributed Trust
- Distributed Database
- Provenance
- Decentralized control
- Autonomous network
- Public, Non-permisioned

# Blockchain Principles across the Safecast Ecosystem

← SENSORS →      ← NETWORK →      ← CLOUD →



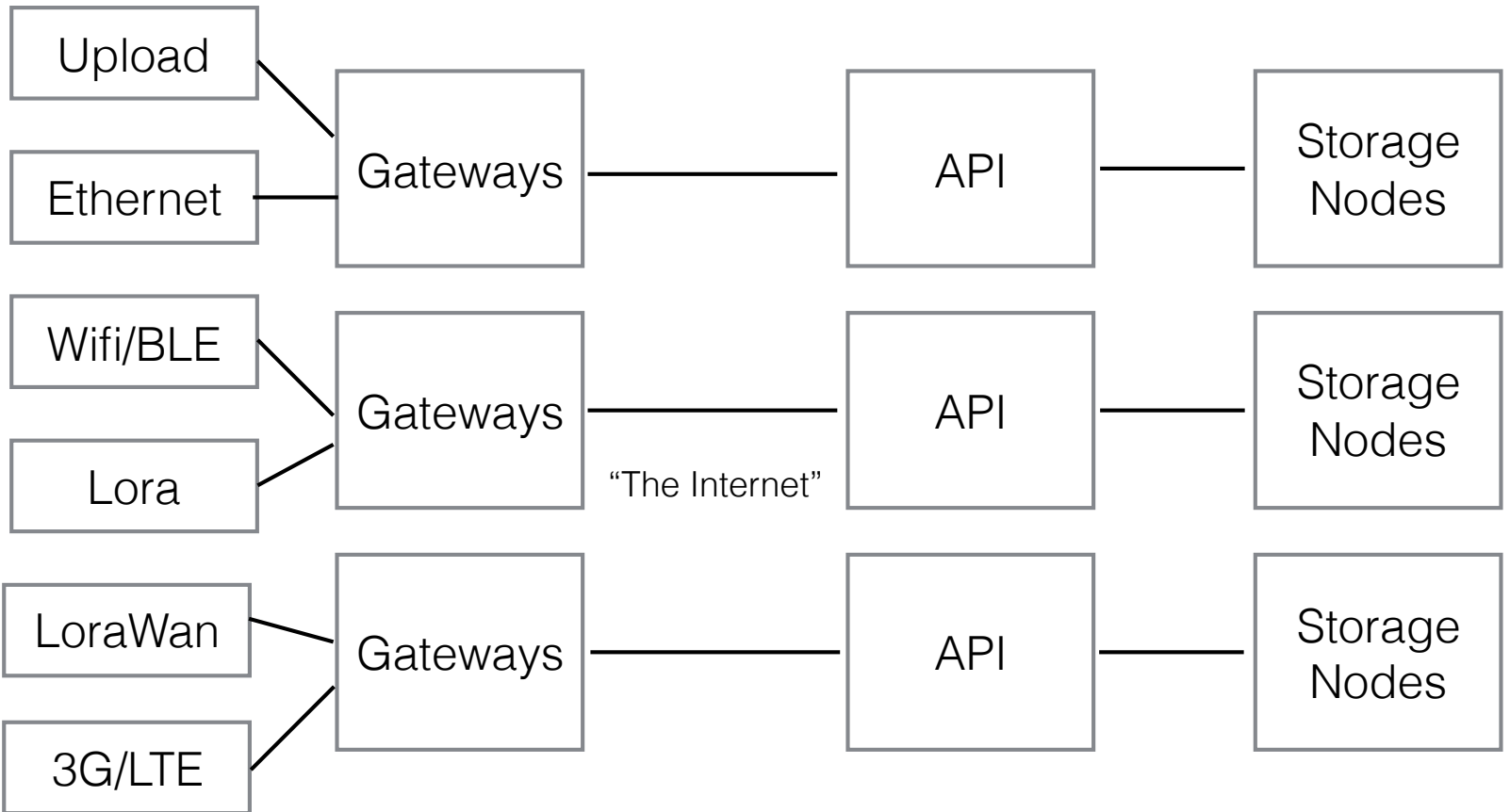
Mobile



Stationary  
(powered)



Autonomous  
Ultra low power



← DISTRIBUTED, AUTONOMOUS, DECENTRALIZED, PROVENANCE, PUBLIC, NONPERMISIONED →

# Research Solution Space

- (lightweight) digital signature for integrity
- excluding irregular data from malicious sensor
- strength and weakness of each approach (including non blockchain, centralized solutions, consensus based, byzantine, public/private key)
- Provenance between sensor and CPU in end point (e.g. bGeigie)
- how to deal with (lack of) trust in the network
- how to handle amendments
- how to leverage citizen driven network (no single owner, openness, distributed trust, detect rogues)
- Reputation management for each sensor / participant
- algorithms that work with super low power CPU's
- Trusted Execution Environments
- how to handle broken sensors, offline data (store and forward), corrections, fault tolerant
- hack sensors - try to break the system from outside / Bsafe.network
- economic incentive across network to enable autonomous processing (at endpoint, nodes)

# Applicability of Research

- IoT
- Big Data
- large, open data sets
- self governance
- autonomous systems
- News / Social Media

# Immutability of Open Data through Distributed Storage

**Richard Rowland**  
Keio University SFC

# Blockchain Principles across the Safecast Ecosystem

← SENSORS →      ← NETWORK →      ← CLOUD →



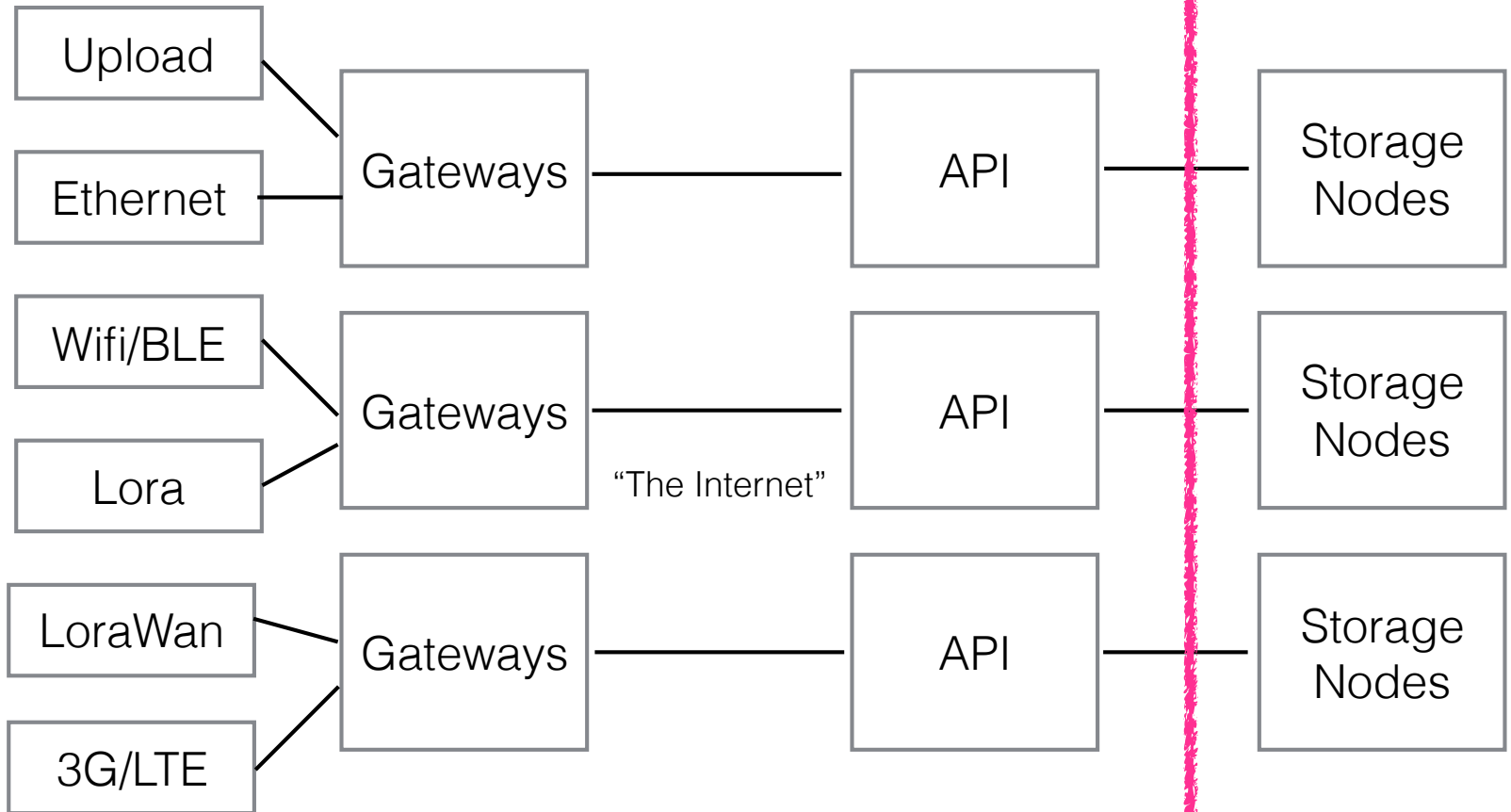
Mobile



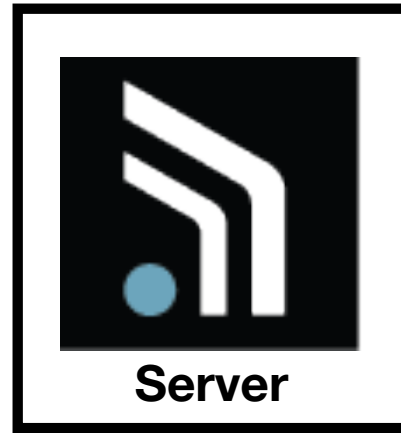
Stationary  
(powered)



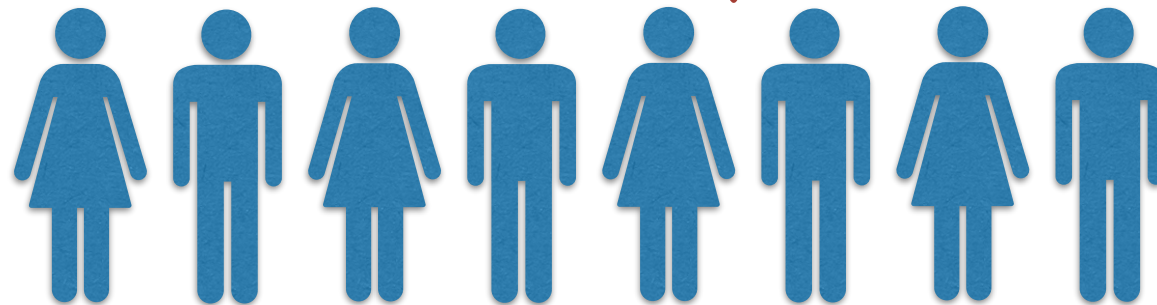
Autonomous  
Ultra low power



← DISTRIBUTED, AUTONOMOUS, DECENTRALIZED, PROVENANCE, PUBLIC, NONPERMISIONED →



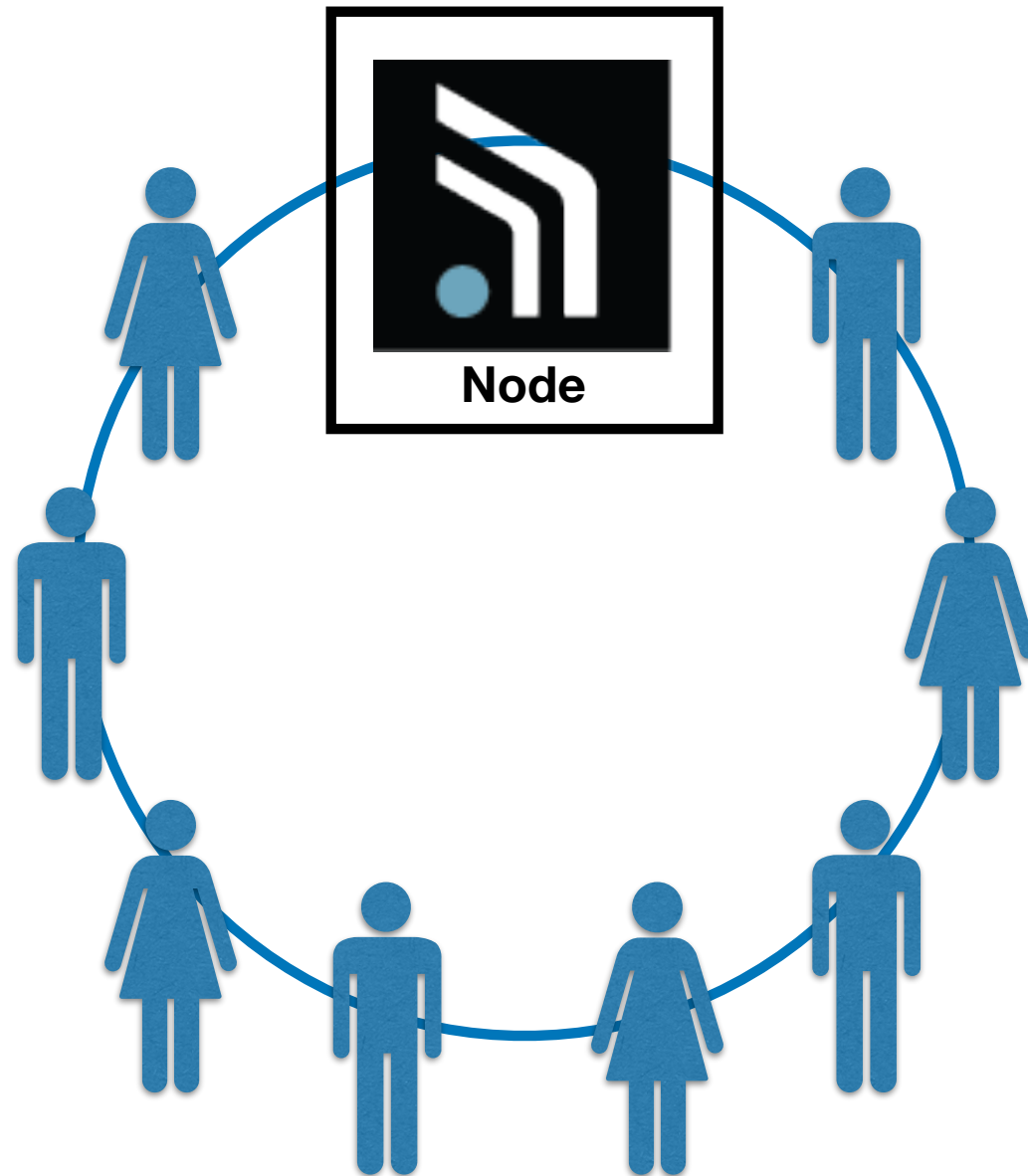
Trust ~~X~~



# Centralized Hosting

**Problem:**  
*How to Remove  
Need for Trust?*





# Decentralized Hosting

## **Solution:**

- Distribute data of replicated nodes**
- Timestamp and sign data to ensure provenance**
- Base timestamp on public blockchain that offers a verifiable “notary” stamp**



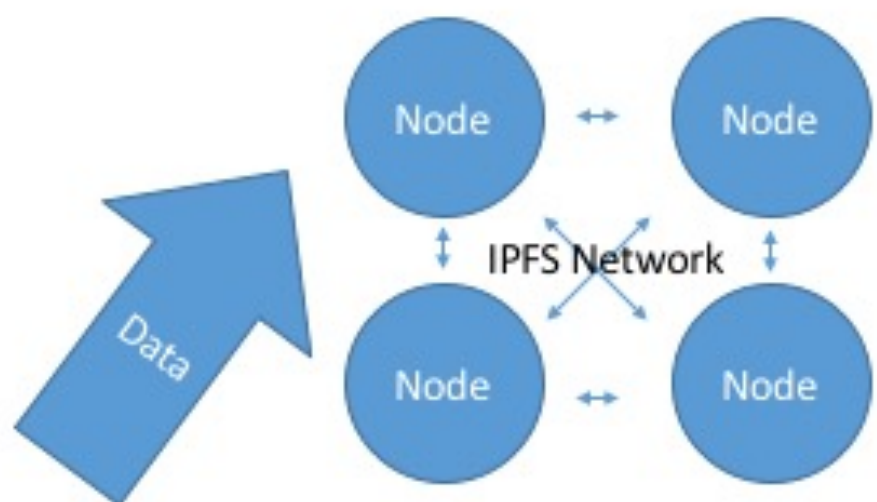
HTTP

CSV DATA  
entry...  
entry...  
entry...  
entry...  
entry...



IPFS

CSV DATA  
entry...  
entry...  
entry...  
entry...  
entry...



**Implementation:**

**IPFS**

**OpenTimestamps**

**Bitcoin**

# IPFS

- A suite of P2P technologies enabling distributed web
- Participants seed the data
- Routing: DHT
- Data Exchange: BitTorrent

# OpenTimestamps

- Timestamp on Bitcoin Blockchain
- Prove that document existed by that date
- Aggregates hashes of documents into a merkle tree
- As trustable as Bitcoin Blockchain

# Bitcoin

- Bitcoin is based on a public, non-permissioned blockchain
- Open, trusted project
- Blockchain provides trusted timestamp
- Alternates Public Blockchain: Ethereum



HTTP

CSV DATA  
entry...  
entry...  
entry...  
entry...  
entry...

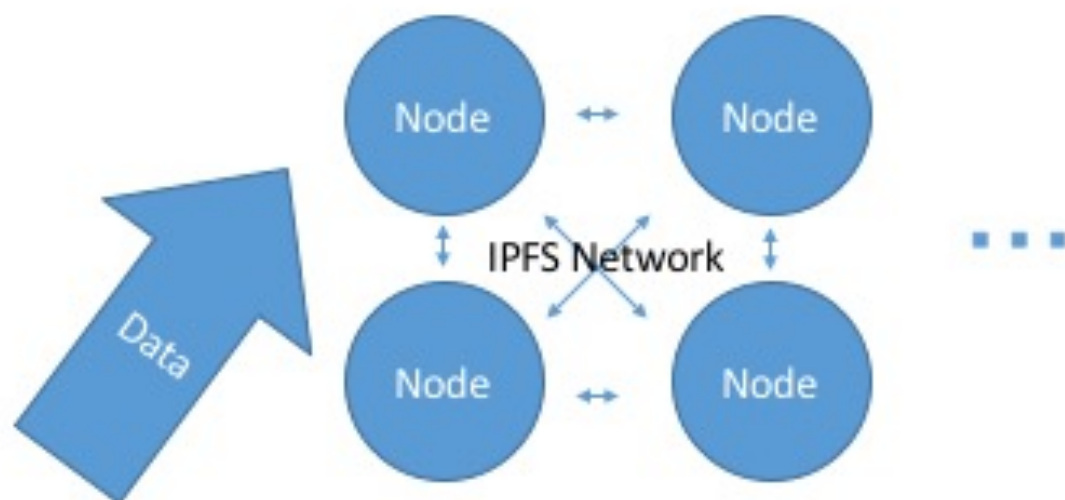


IPFS

CSV DATA  
entry...  
entry...  
entry...  
entry...  
entry...



Hash



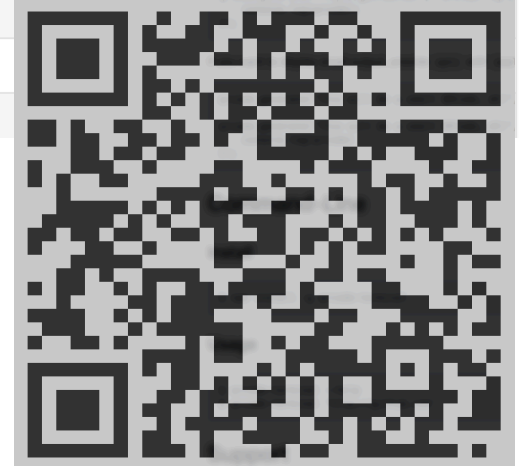


**DEMO**

## Index of /ipfs/QmdZBrNhMTGNB7XQkMB4S3igzxhJzcPPriUSeXyYf6BV8J

	..	
	<a href="#">000407.csv</a>	191 B
	<a href="#">000603.csv</a>	309 B
	<a href="#">000605.csv</a>	310 B
	<a href="#">001107.csv</a>	136 B
	<a href="#">001201.csv</a>	214 B
	<a href="#">020103.csv</a>	245 B
	<a href="#">196912.csv</a>	11 kB
	<a href="#">197001.csv</a>	246 kB
	<a href="#">197002.csv</a>	1.1 kB
	<a href="#">197006.csv</a>	142 B
	<a href="#">198110.csv</a>	17 kB
	<a href="#">198310.csv</a>	402 B
	<a href="#">200011.csv</a>	405 B
	<a href="#">200304.csv</a>	2.9 kB
	<a href="#">200306.csv</a>	258 B
	<a href="#">200404.csv</a>	177 B
	<a href="#">200606.csv</a>	33 kB
	<a href="#">201009.csv</a>	214 B

[https://ipfs.io/ipfs/  
QmdZBrNhMTGNB7XQkMB4S3igzxhJzcPPriUSeXyYf6BV8J](https://ipfs.io/ipfs/QmdZBrNhMTGNB7XQkMB4S3igzxhJzcPPriUSeXyYf6BV8J)



# Actual Time stamp receipt

```
→ dataset ots verify 201711.csv.ots  
Assuming target filename is '201711.csv'  
Got 1 attestation(s) from https://finney.calendar.eternitywall.com  
Got 1 attestation(s) from https://bob.btc.calendar.opentimestamps.org  
Got 1 attestation(s) from https://alice.btc.calendar.opentimestamps.org  
Success! Bitcoin attests data existed as of Sat Dec 16 03:52:24 2017 JST
```

# Thank you!

[pieter@safecast.org](mailto:pieter@safecast.org)  
[r1cky@sfc.wide.ad.jp](mailto:r1cky@sfc.wide.ad.jp)



**SFC**  
KEIO UNIVERSITY



**BASE**  
ALLIANCE



mit  
media  
lab



SAFECAST