



Paul Pinault

Blog/contact : www.disk91.com

Twitter : @disk_91

YouTube: <https://www.youtube.com/c/PaulPinault>

The Internet Of Things

Introduction to what is the Internet of Things, why does it change the world where we live, what are the technologies behind the scene ?
How des it apply to your domain ?



ISIMA ENGINEER

17 years  **MICHELIN** IT, IoT

VP Product & Market Strategy

We make manufacturing more efficient, less impacting environment through the data analysis.



IoT Expert



- <https://www.disk91.com>
- <https://youtube.disk91.com>
- <https://github.com/disk91/stm32-it-sdk>



DEVICE MAKER & STARTUP
FOUNDER 

TEACHER and SPEAKER



What do you think IoT is ?



Is IoT...

Useless IoT ?



COUNT EGGS

Know on your smartphone the number of eggs you still have in your fridge



TOOTHBRUSH

Make tooth wash a game for children, even if exposing your smartphone to the worst conditions



FRIDGE

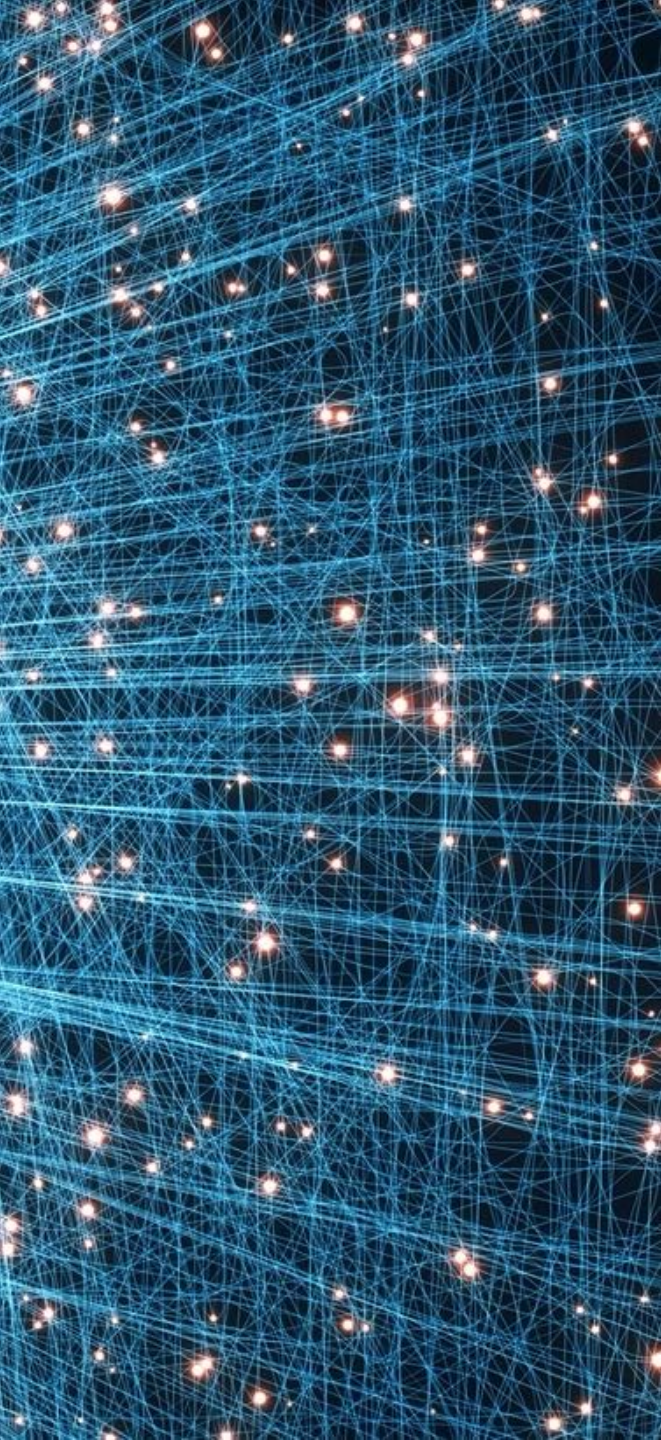
Make your fridge doing shopping for you



FEEDING BOTTLE

Measure the quantity of milk your baby has drunk

Is IoT... Evil ?



LINKY

Supposed to emit terrible radio waves, spy on you



CAMERA

Identify you, spy on you, source of the largest ddos attack on Internet infrastructures

5G

Supposed to emit radio waves that can kill us all shortly, activating nanoparticles injected with covid vaccines...

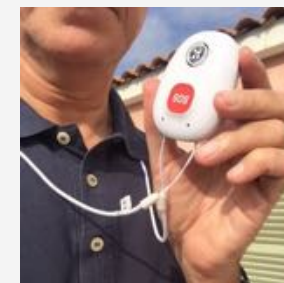
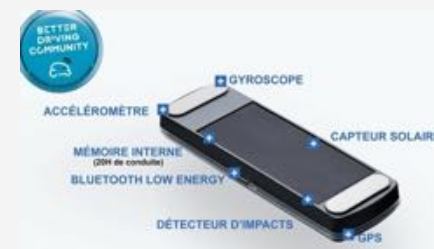


CAR

Car could be controlled remotely by a third party. Could be stolen with digital intrusion. Manufacturer could disable features, use remotely

Is IoT...

Saving life ?



BALANCE

Measures the increase in weight sign of a near cardiovascular risk in certain diseases

GLASS

Make sure that the elderly drink enough water and do not become dehydrated

VEHICLE

Understand your driver behavior and provide advice to improve your driving safety

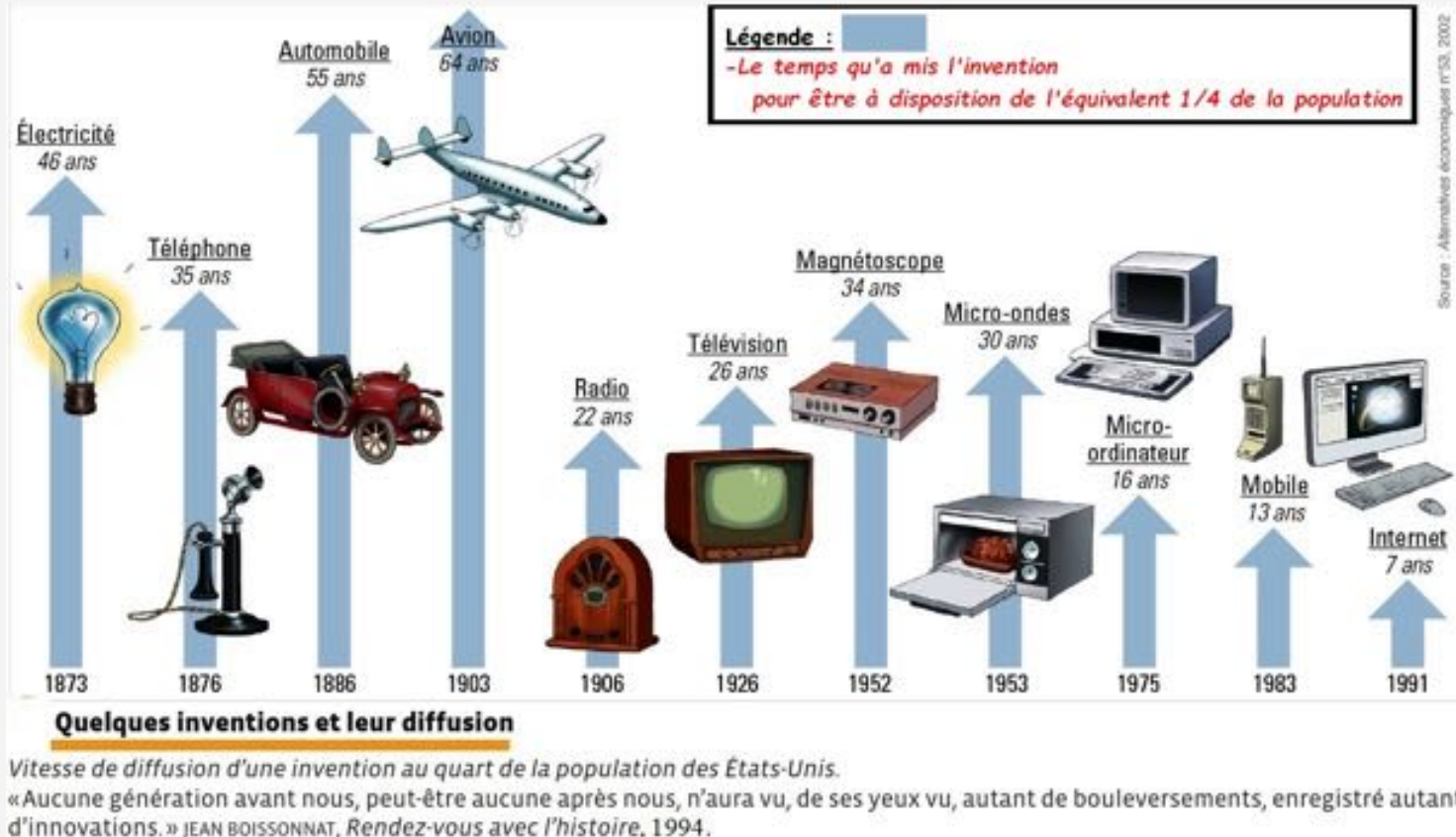
EMERGENCY CALL

Emergency call for elderly in the event of a fall



IoT is a revolution changing the way industries are going to execute their processes

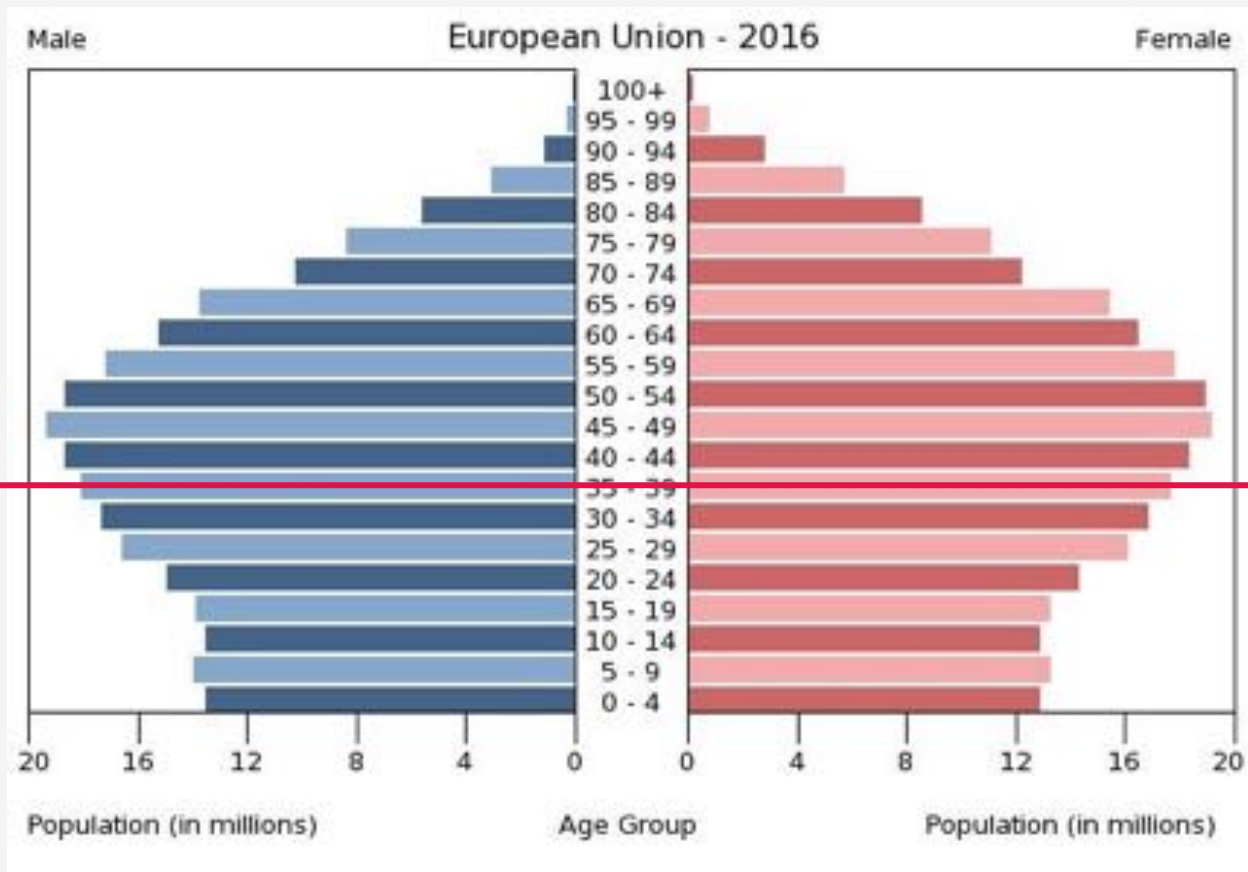




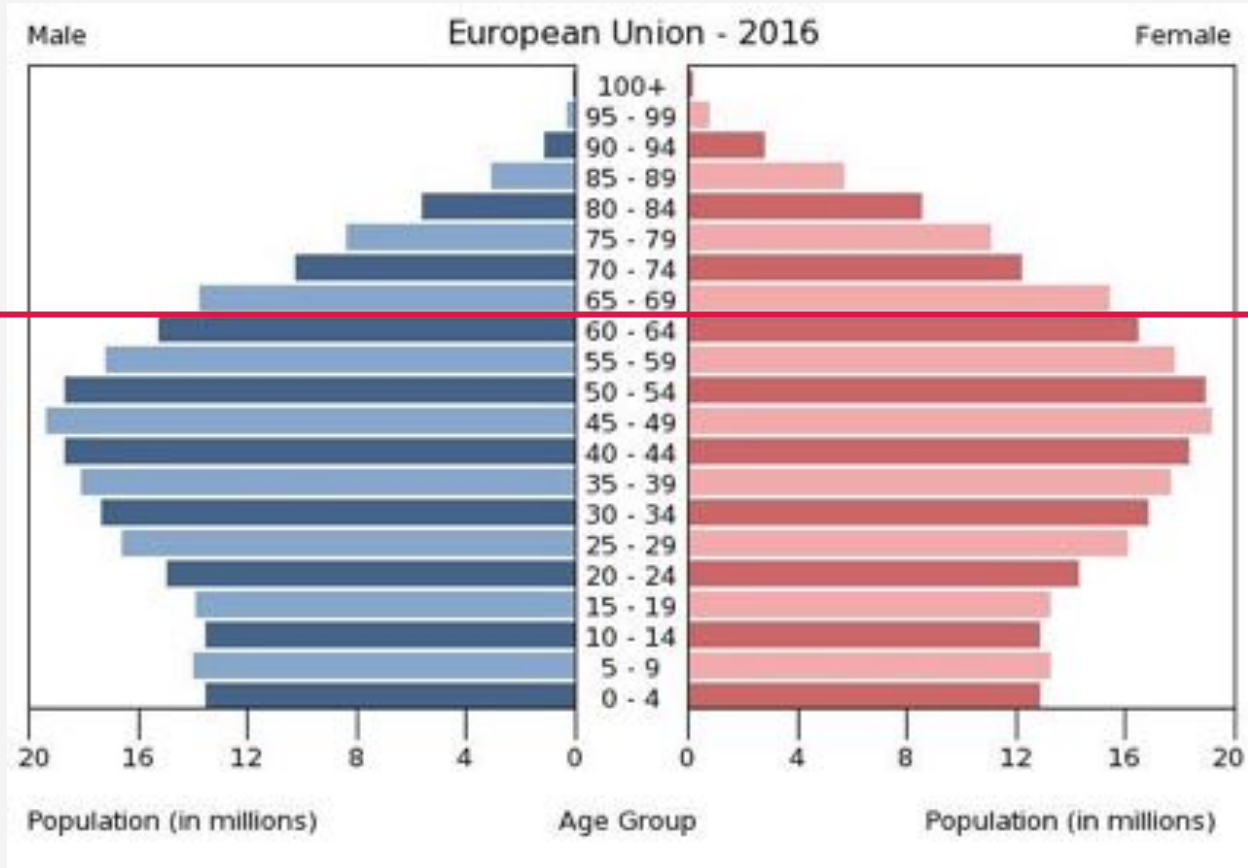
In the past 20 years the digitalization has transformed our world but it has made it really more complex.

SIMPLE USER INTERFACE

COMPLEX USER INTERFACE



About 60% of European population has to learn computers / smartphone / Internet after school age (> 20 year old)



Most of these people never had to use a computer / smartphone in their professional life

20%

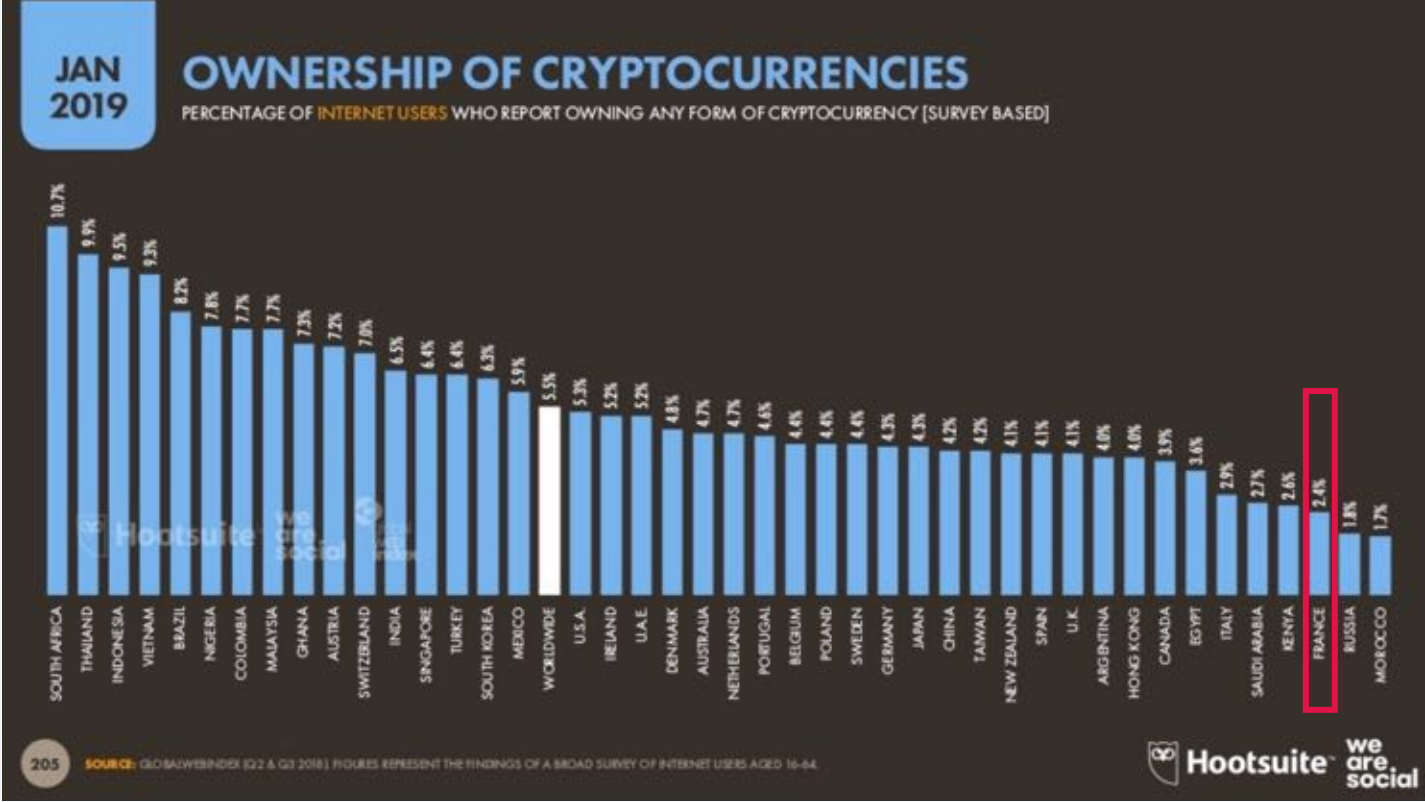


Helium deployment density



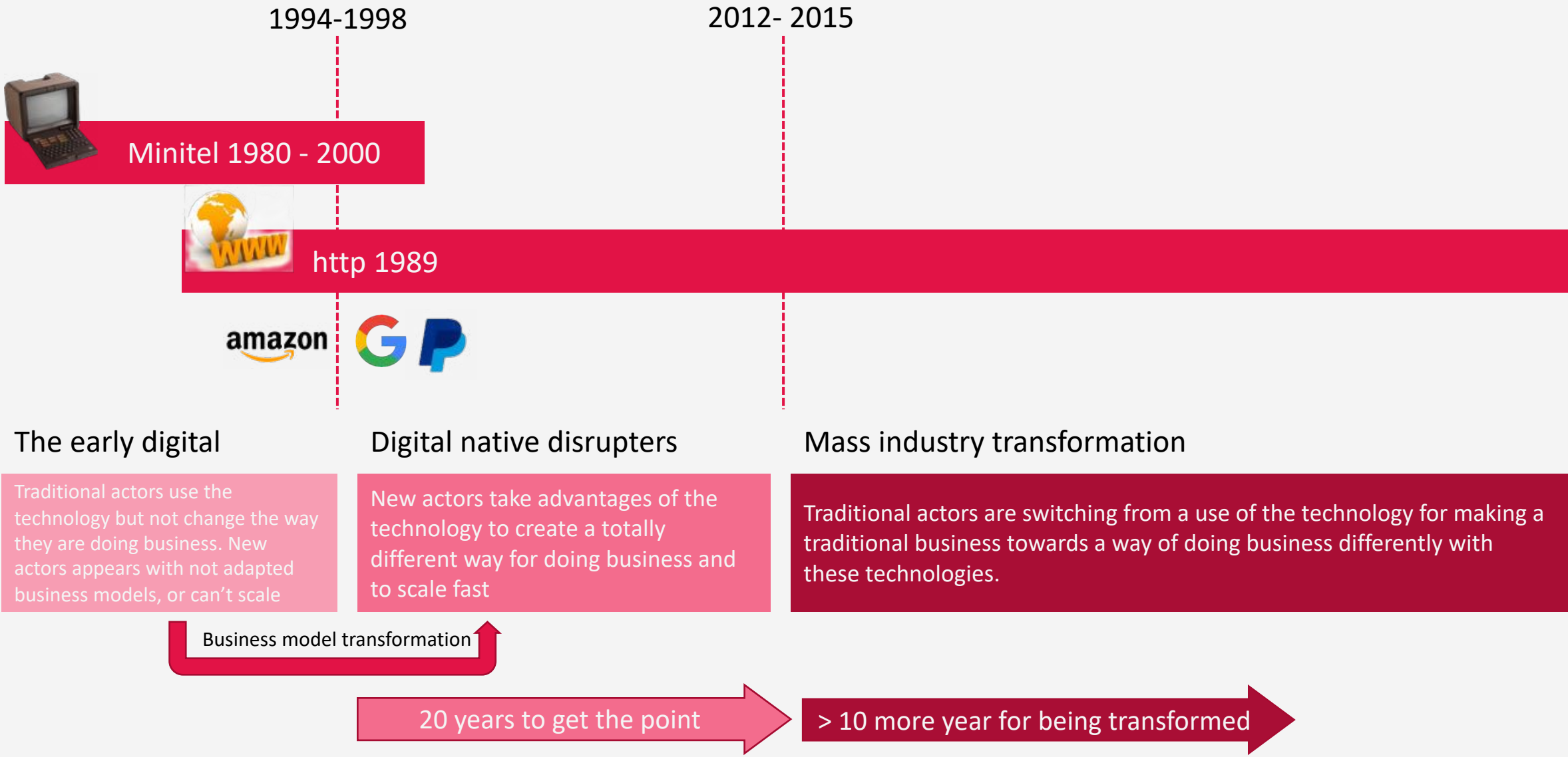
Planet watch adoption (French project)

” Our ability in France to adopt change and technology is lower than others European around



” Our ability in France to adopt change and technology is lower than others European around

Industrial processes transformation takes time



DIGITAL / IoT

Transformation are ways to make existing business in a totally different way

1 Customer change management takes time

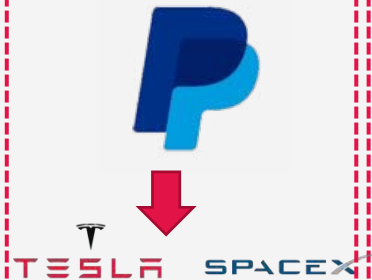
2 Traditional business transformation takes longer time

Winners are the one able to use the technology to embrace a transformation quicker than the others

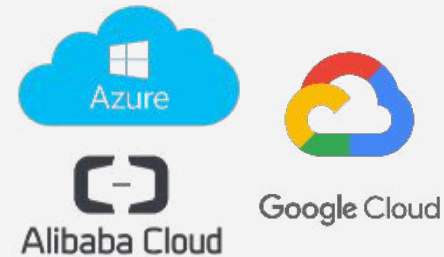
Pre-existing



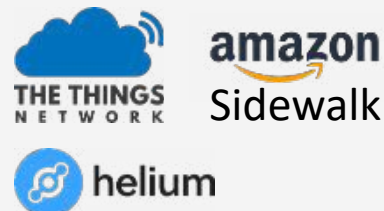
Disrupter



Transformation

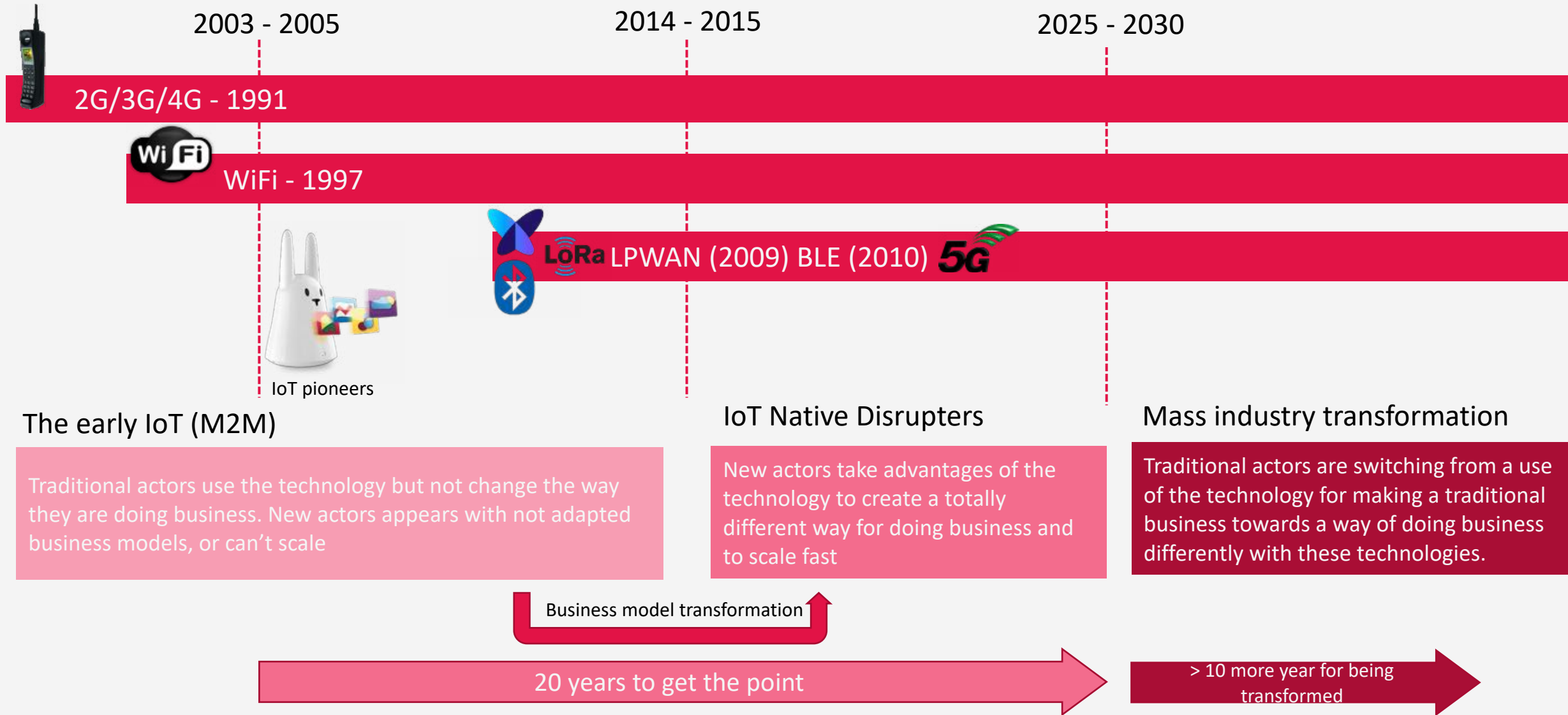


Next step



The different phases of the IoT transformation

Industrial processes transformation takes time



The background features a central globe with a network of white lines and dots. Surrounding the globe are several white gears of varying sizes, each containing a different icon: a briefcase, a person in a suit, a target, a dollar sign, a camera, a document, a magnifying glass, and a bar chart. The scene is set against a dark blue background with bright blue and purple light streaks and starburst effects.

IoT is one of the next “digital transformation”

It basically create a new opportunity to transform the industrial processes by issuing new data from the real world. It transforms the relationship between providers, customers and products.

**DECISION
TAKEN FROM
NEVER SEEN,
MASSIVE DATA**

IoT Data will fulfill a new set of IA to pilot industrial processes, sustainability ...

**DATA GENERATION
FROM RAW
MATERIAL TO
FINISHED PRODUCT
END OF LIFE**

Industrial processes get benefit of seamless data access from any stage of the product and its components

**FROM PRODUCT
APPROACH TO
SERVICES
ORIENTATION**

Any connected product can be a source of new value creation in a service-oriented approach

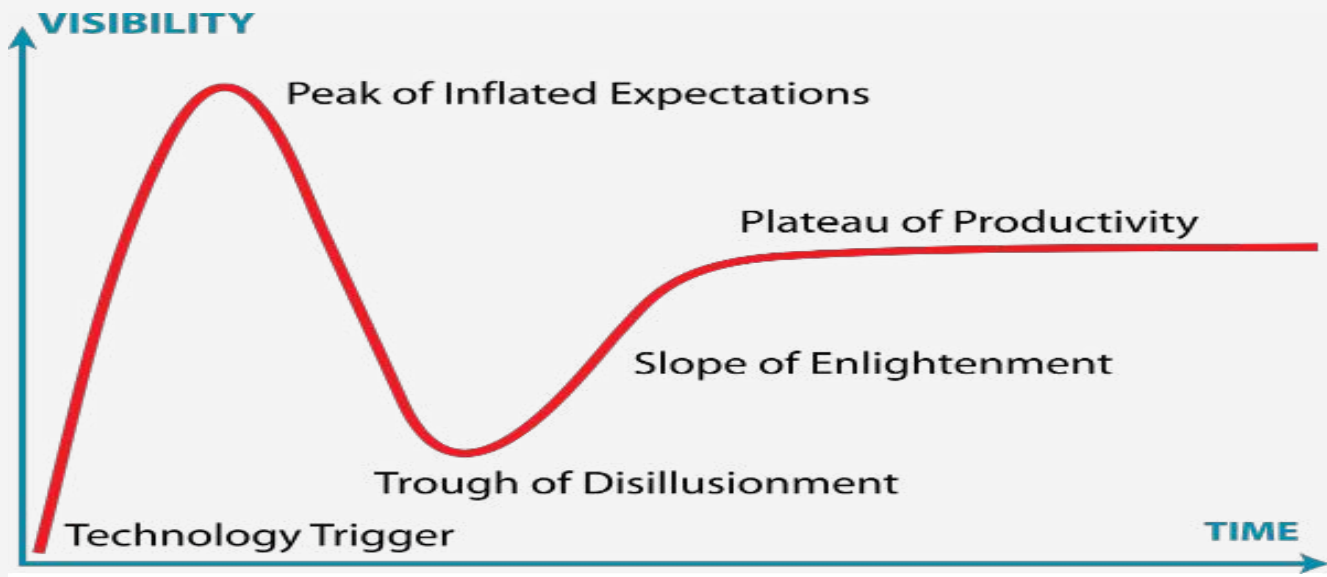
Why new technologies are so long for being adopted ?

Any new technology is a strong change for each of the individuals. The rate of change is going faster since the last 20 years.

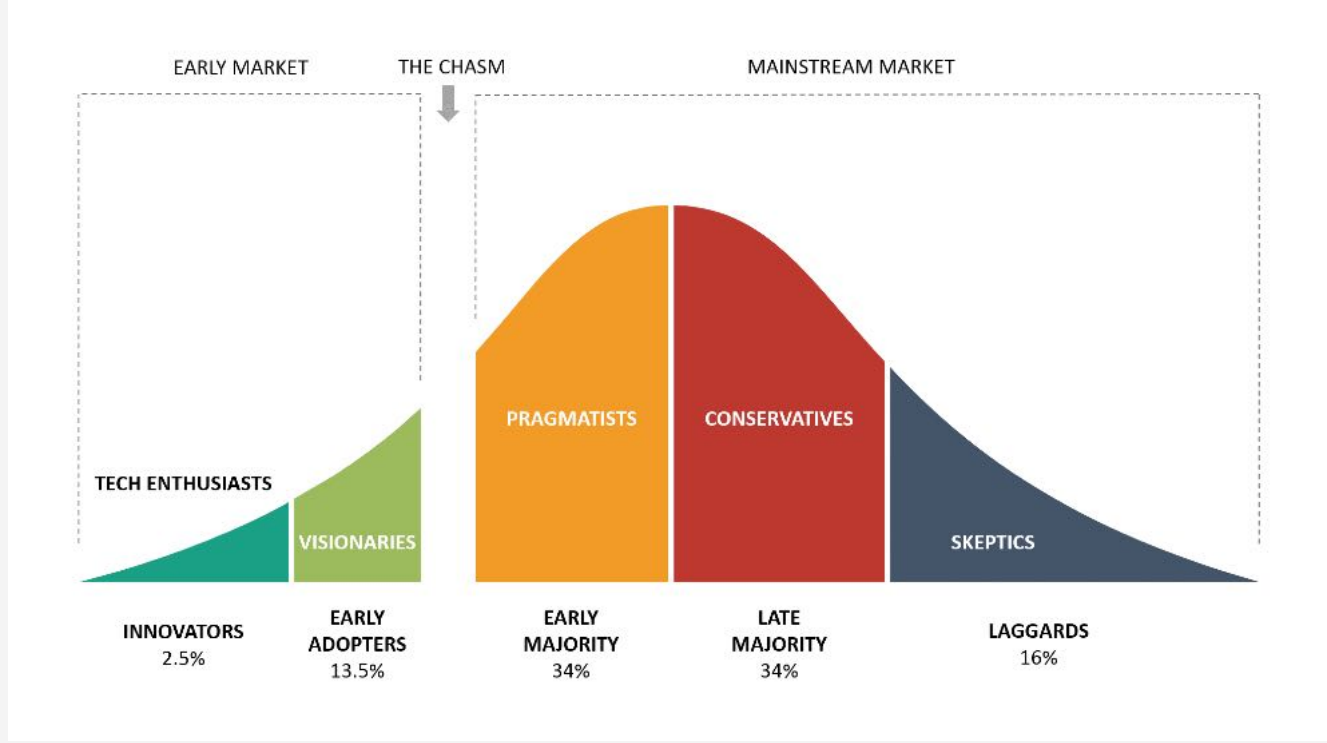
The whole society is changing with new ways of work, new way of interacting, new ways of making politics.

We have to fight against large challenge changing our 100 year old model about climate, world governance and equilibrium

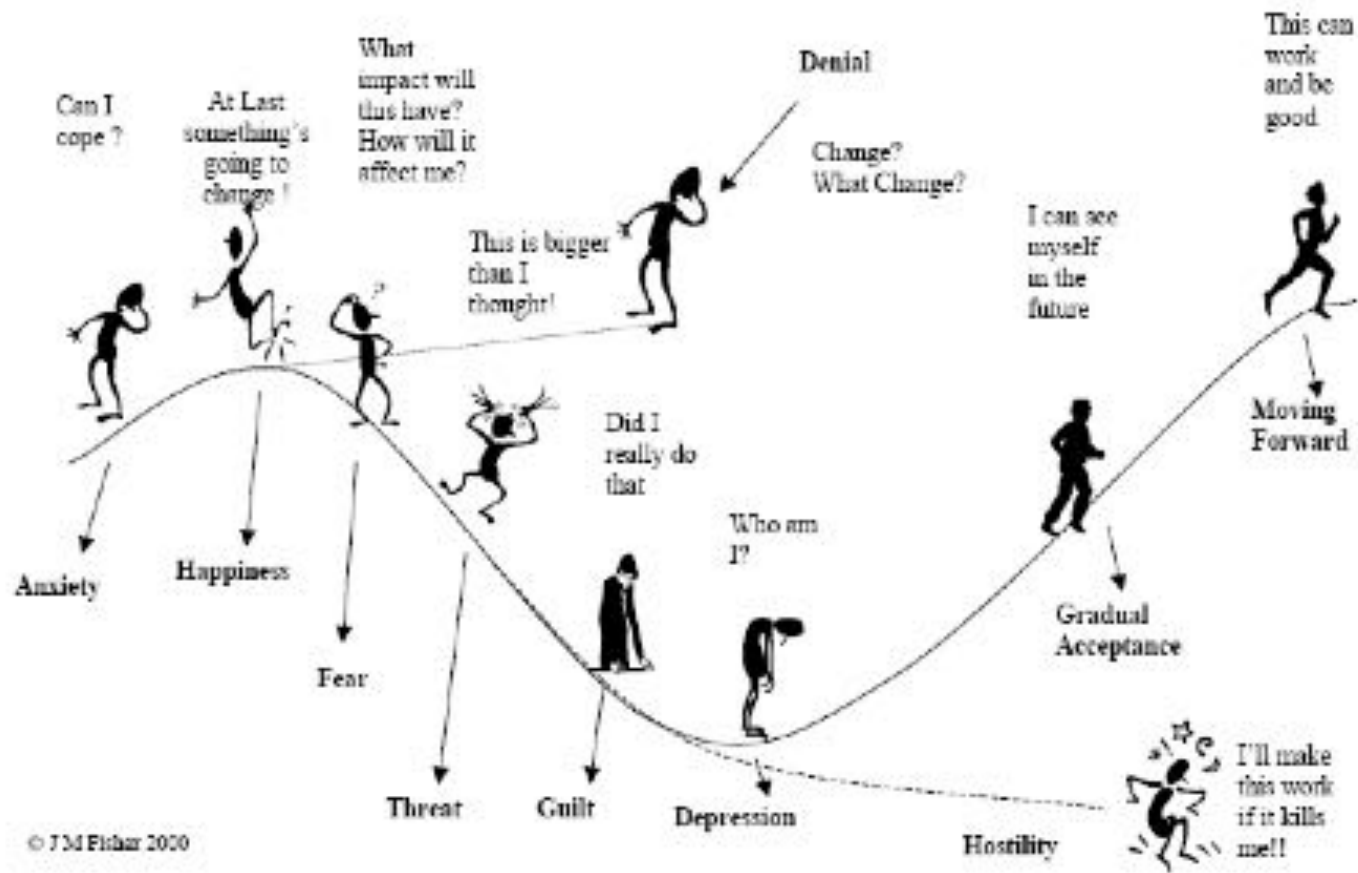




” Adoption follows the hype cycle pattern, related to the ability of humans to embrace change



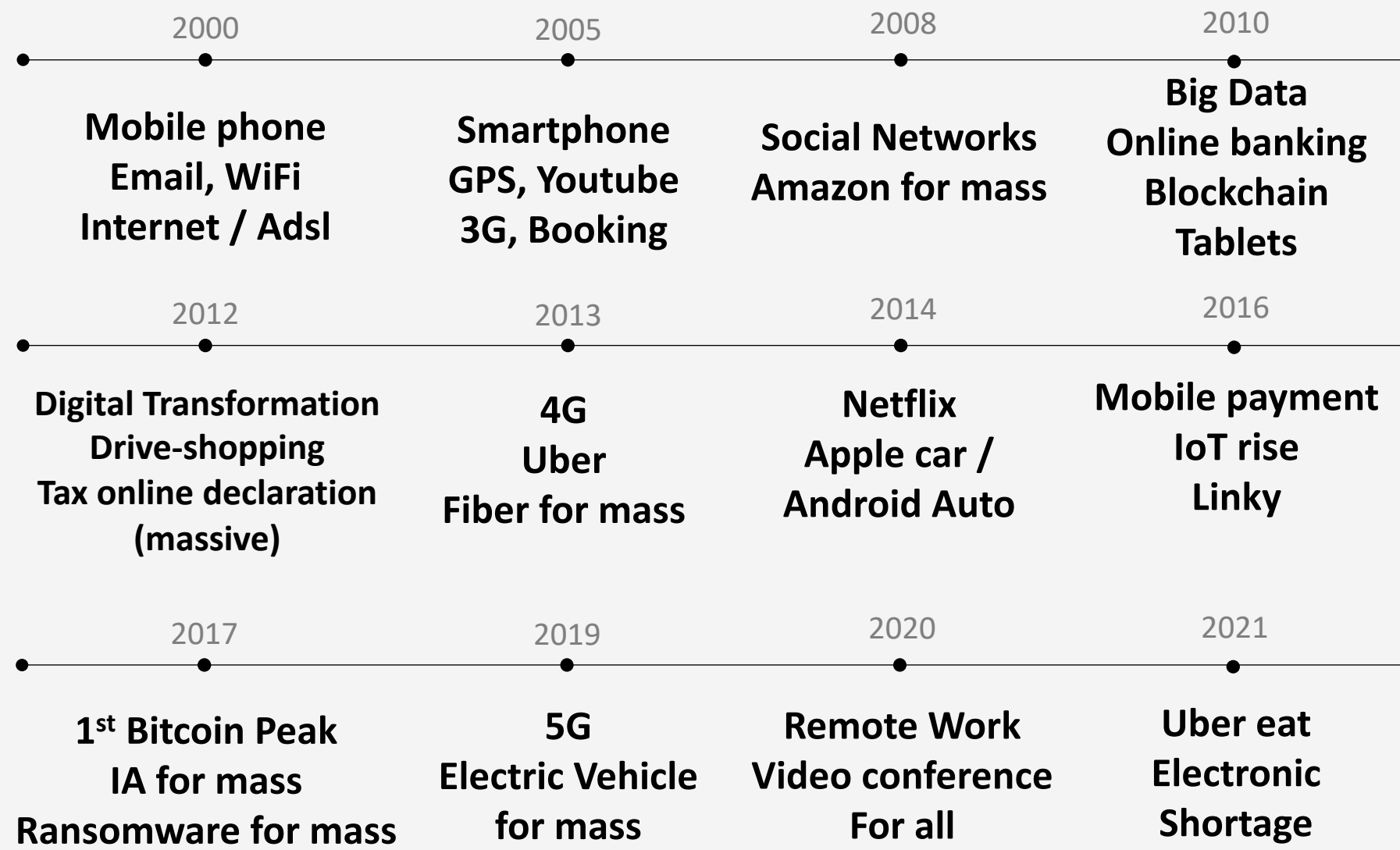
The Process of Transition



People adoption is a long process and the multitude of new technologies to adopt generate a large community of people rejecting novelty

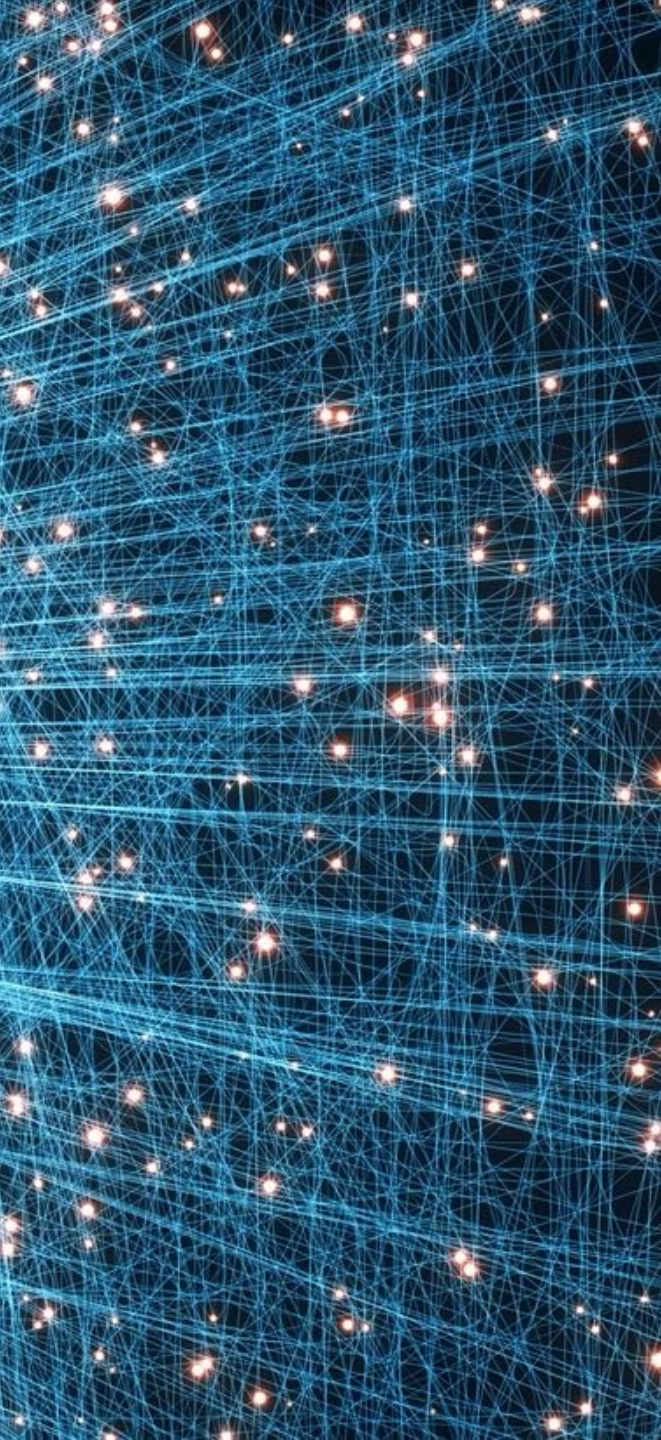
Recent technologies to be adopted

In the past 20 years



It has some consequences

Schizophrenic society



LCI @LCI · 05/07/2020

Éric Piolle (EELV) moque la #5G, une technologie "qui sert à regarder du porno dans l'ascenseur en HD" bit.ly/38qYvnt

458 607 228

Éric Piolle @EricPiolle

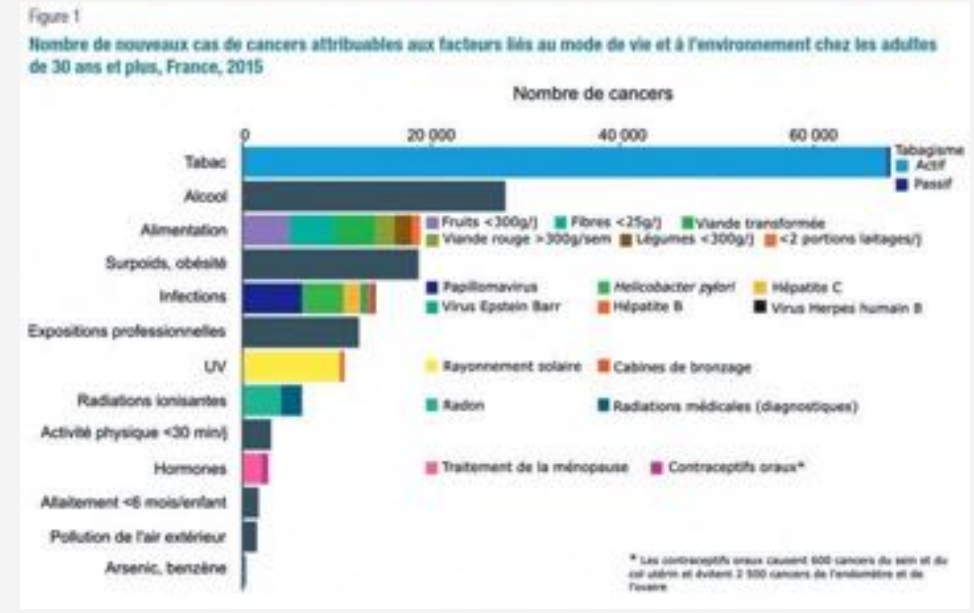
Plus de monde sur le terrain que sur l'autoroute... #Marseille #FRAGER

21:43 · 15/06/2021 · Twitter Media Studio

13 Retweets 116 Tweets cités 100 J'aime

It has some consequences

Crazy consequences



It has some consequences

But nothing really new

Lien entre l'utilisation des téléphones mobiles et les tumeurs cérébrales 11^e législature

Question écrite n° 05599 de M. Emmanuel Hamel (Rhône - RPR)
 publiée dans le JO Sénat du 22/01/1998 - page 204

M. Emmanuel Hamel attire l'attention de M. le secrétaire d'Etat à la santé sur l'information parue à la page 13 du quotidien Le Figaro du 5 janvier dernier selon laquelle " une étude australienne >...> fait état d'une augmentation des tumeurs du cerveau ". D'après un médecin australien " cette augmentation de 50 % observée chez les hommes et de 62,5 % chez les femmes depuis 1982 pourrait être liée au développement du téléphone mobile au cours de cette décennie ". Il lui demande quelle est sa réaction face à cette information.

Réponse du ministère : Santé
 publiée dans le JO Sénat du 12/11/1998 - page 3655

Réponse. - Le docteur Davidson de l'hôpital de Fremantle a publié une étude, il y a quelques mois, dans le Medical Journal of Australia, mettant en parallèle, d'une part, une augmentation de la fréquence des cancers du cerveau en Australie durant la période 1982-1992, de 50 % chez l'homme et de 62,5 % chez la femme et, d'autre part, une augmentation du nombre de téléphones portables dans ce pays durant la même période, sans toutefois prétendre établir de relation entre ces événements. Cette étude est critiquable sur le plan méthodologique, notamment en raison de l'absence de prise en compte du type de tumeurs, dont certaines sont en relation avec l'augmentation de la durée de vie ou surviennent chez le très jeune enfant. De plus, aucune information concernant les caractéristiques des téléphones mobiles utilisés en Australie (dont les standards sont différents des réseaux français) n'est donnée. Par ailleurs, lorsqu'un agent physique ou chimique exerce un effet cancérigène, on observe constamment un délai de l'ordre de dix à trente ans entre l'exposition et l'apparition d'une tumeur. Si un lien existait entre l'utilisation des téléphones mobiles et les cancers du cerveau, un accroissement sensible de ces cancers ne devrait pas être observé avant une dizaine d'années au minimum. En France, durant la période 1985-1995, le taux de survenue de décès par cancers primitifs du cerveau a également augmenté de 16,3 % chez les hommes et de 31 % chez les femmes. Une analyse fine des résultats montre que cette évolution est liée à une augmentation de la fréquence dans les classes d'âge supérieures, c'est-à-dire supérieures à soixante-quatre ans, ainsi que dans les classes d'âges inférieures, c'est-à-dire de moins de quatre ans. Ces populations sont peu portées naturellement à utiliser des téléphones portables. On constate en revanche une stabilité, voire une diminution, de la fréquence des cancers du cerveau dans les autres classes d'âge, c'est-à-dire de cinq à cinquante-cinq ans, alors que ce sont précisément ces classes d'âge qui sont susceptibles d'utiliser des téléphones portables. Cependant, il est nécessaire de poursuivre l'étude épidémiologique et les recherches sur les facteurs pouvant expliquer l'augmentation de la fréquence de tels cancers.

CANCER

Cancer du cerveau : les téléphones portables disculpés

Par **Lise Loumé** le 10.05.2016 à 15h18, mis à jour le 10.05.2016 à 15h18
 Lecture 4 min.

Une vaste étude rapporte que ces trente dernières années, l'usage croissant du téléphone portable n'a pas entraîné une augmentation du nombre de cancers du cerveau en Australie.

PLUS - COMMENTER - PART.

Question de la semaine: on en jette dans la pelure de fruit ?

L'astronaute allemand Maurer s'apprête à re... l'ISS

Time for science to conduct studies and get a clear result. Even if the original response gave the final direction.

During that time it has been recommended to use headphone. Still ?

1998



2016

It has some consequences

But nothing really new



<https://www.futura-sciences.com> · [Translate this page](#)

Le four à micro-ondes est-il dangereux pour la santé ?
 2 days ago — Ainsi le risque d'apparition de composés cancérogènes est bien plus limité qu'avec d'autres modes de cuisson. On ne peut que déconseiller les ...

<https://www.lci.fr> · [Toute l'info](#) · [Santé](#) · [Translate this page](#)

Le four micro-ondes est-il oui ou non néfaste pour la santé - LCI
 Sep 10, 2018 — Aucun danger non plus de la part des ondes qui ont servi à chauffer votre plat une fois celui-ci sorti, assure Jean-Michel Courty. "Quand l' ...

<https://www.cchst.ca> · [phys_agents](#) · [Translate this page](#)

Fours à micro-ondes et leurs dangers : Réponses SST
 Les fours à micro-ondes peuvent-ils présenter des rayonnements de fuite? ... Un usage abusif, une accumulation de poussières ou l'usure normale attribuable à une ...

<https://www.medisite.fr> · [a-la-maison...](#) · [Translate this page](#)

Micro-ondes : connaissez-vous vraiment les dangers ?
 Sep 10, 2020 — Vous êtes également nombreux à craindre le potentiel risque de cancer : alors que certains scientifiques craignent la formation de composés ...

1955



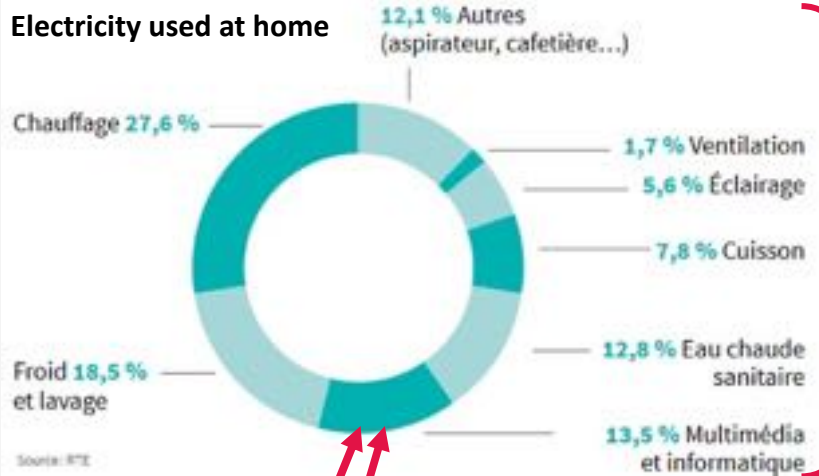
2021



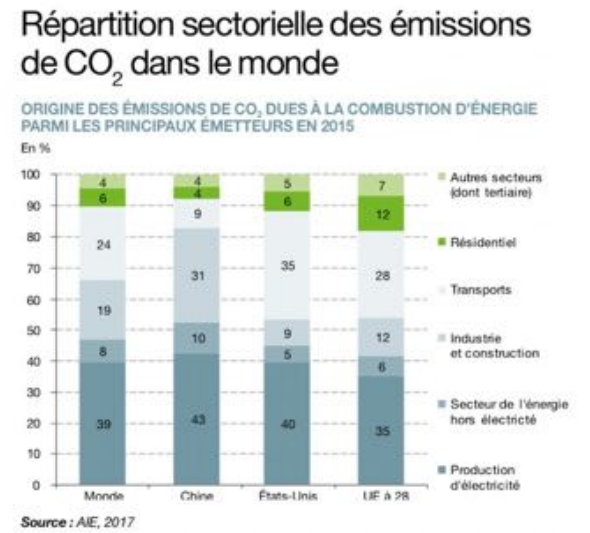
IoT / Digital transformation and Climate / Planet impact



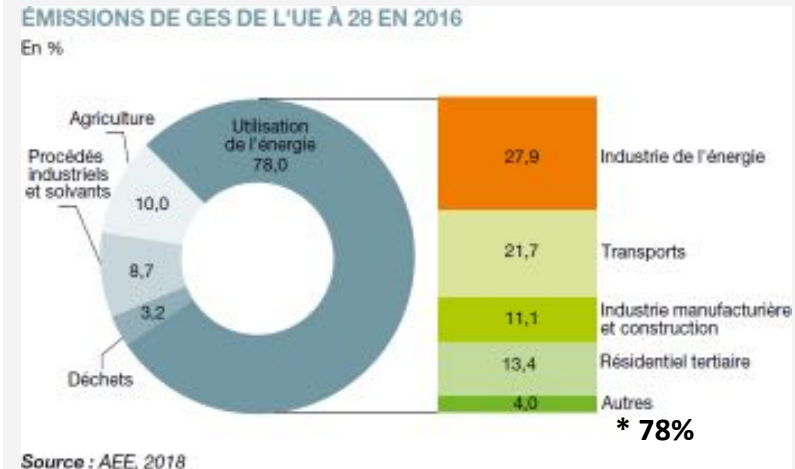
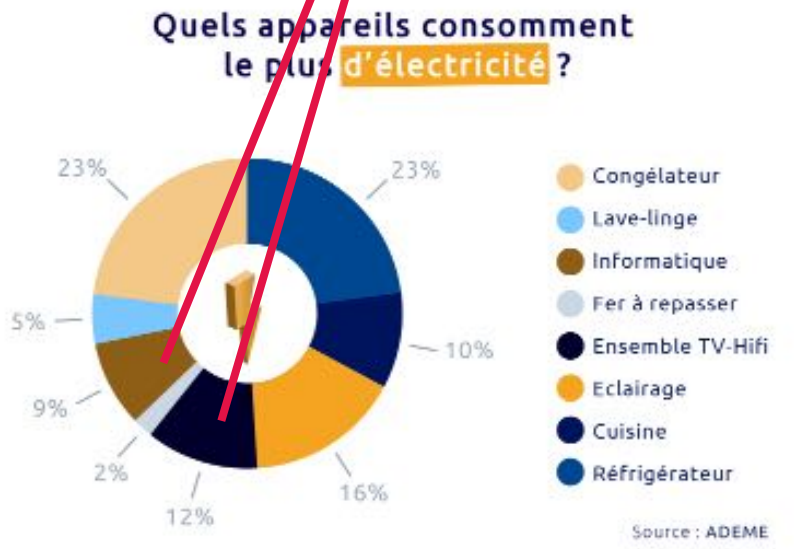
IT is requiring energy



6% * 27%



* 35%

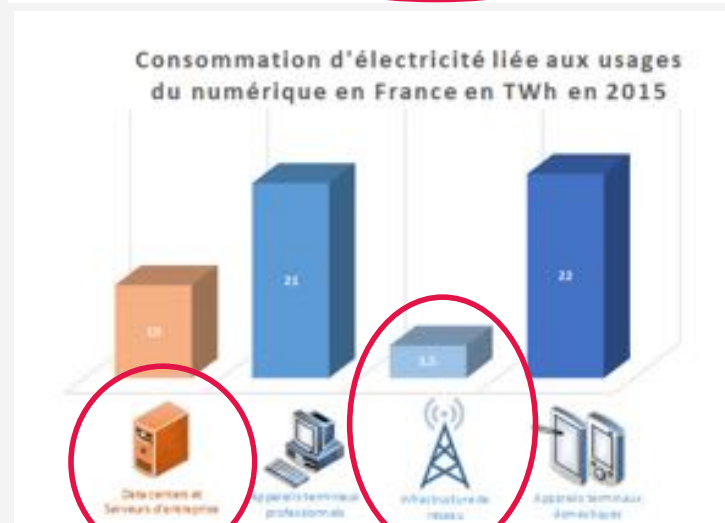
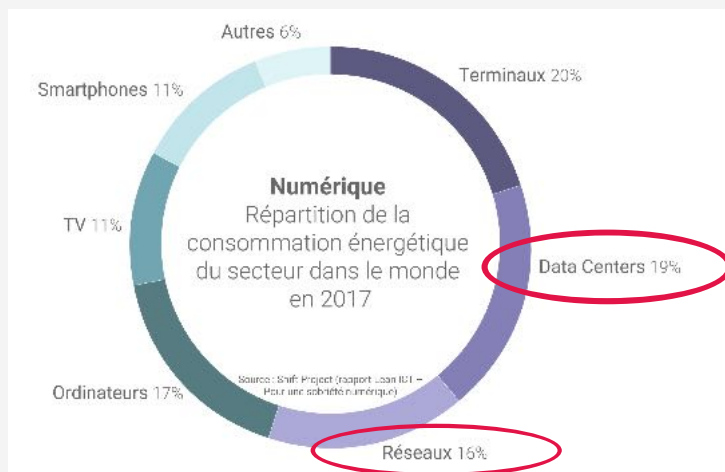


* 78%

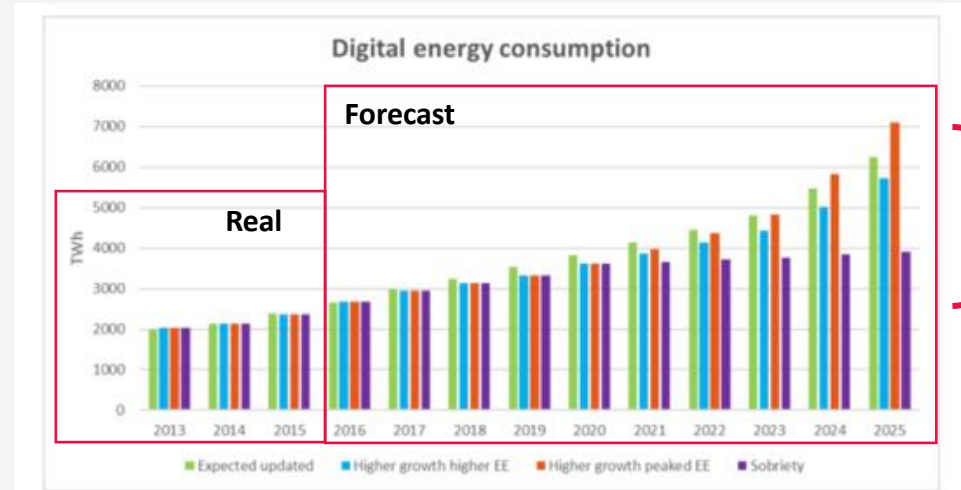
Home
IT
0.44%
GES

Not necessarily at home

Electricity used at home



Bilan GES		Fabrication	Utilisation	Total
Terminaux		40%	26%	66%
Réseau		3%	16%	19%
Data Centers		1%	14%	15%
		44%	56%	



According to Forecast digital GES should be 4% total in 2020

Mostly for construction

Making IT is 44% of GES according to previous slide source:

- Steel 10kWh / kg
- Aluminum 60 kWh / kg
- Copper 20kWh / kg
- Plastic 20kWh / kg
- Paint 30kWh / kg
- Electronic 3.5MWh / kg

- Intel i7 about 0,3g -> 1.05kWh / processor
- Estimate total in a computer : 2g-5g -> 7kWh – 17,5kWh

- Rare earths – about 2g / computer (Led Display-sound)



2000 – 15kg

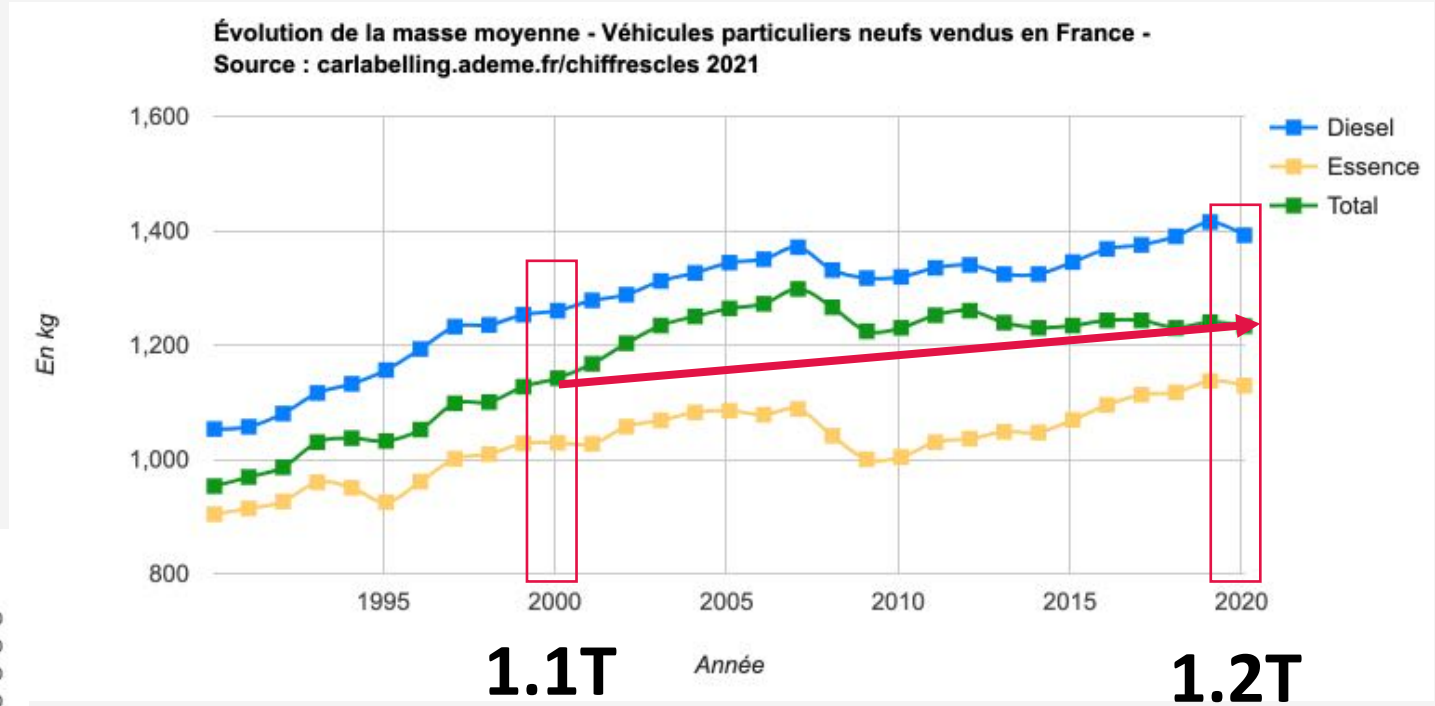
15x less →



2020 – 1kg

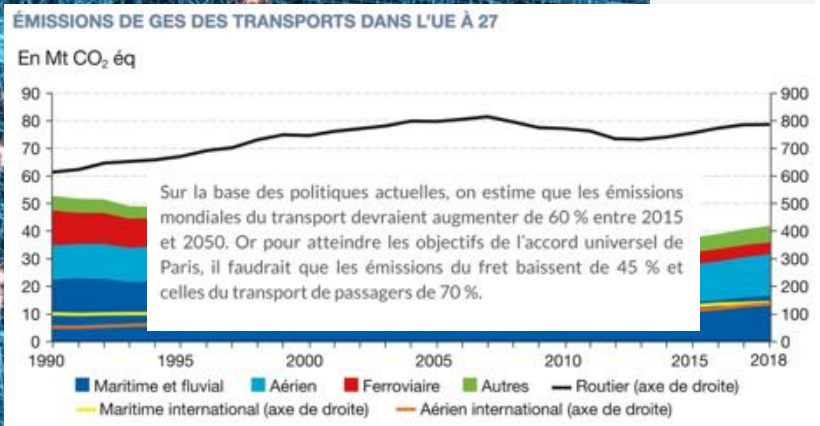
Mostly for construction

Let's compare to car's market



1.1T
Equivalent to 73 computers

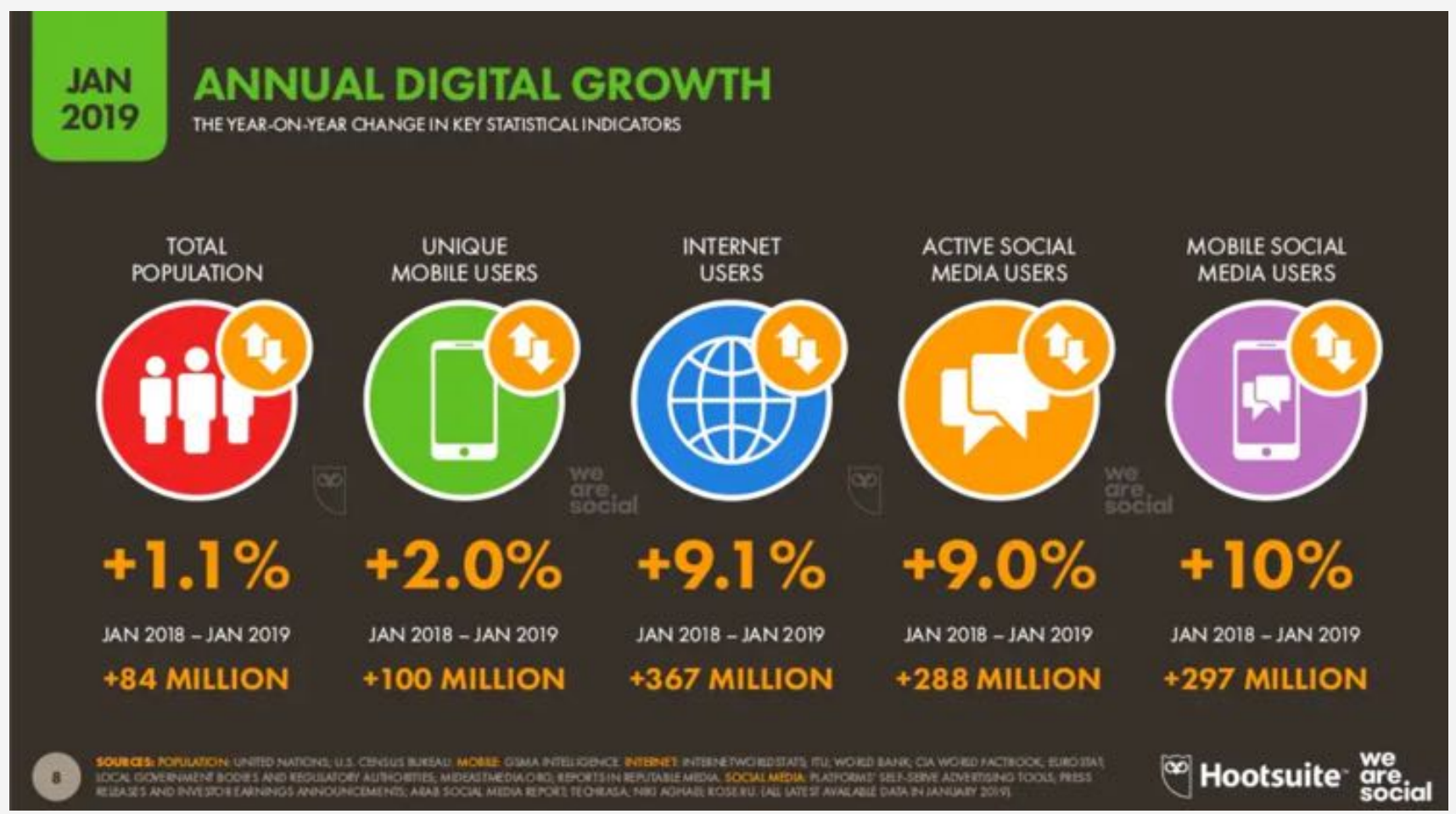
1.2T
Equivalent to 1200 computers



So... where is the growth ?



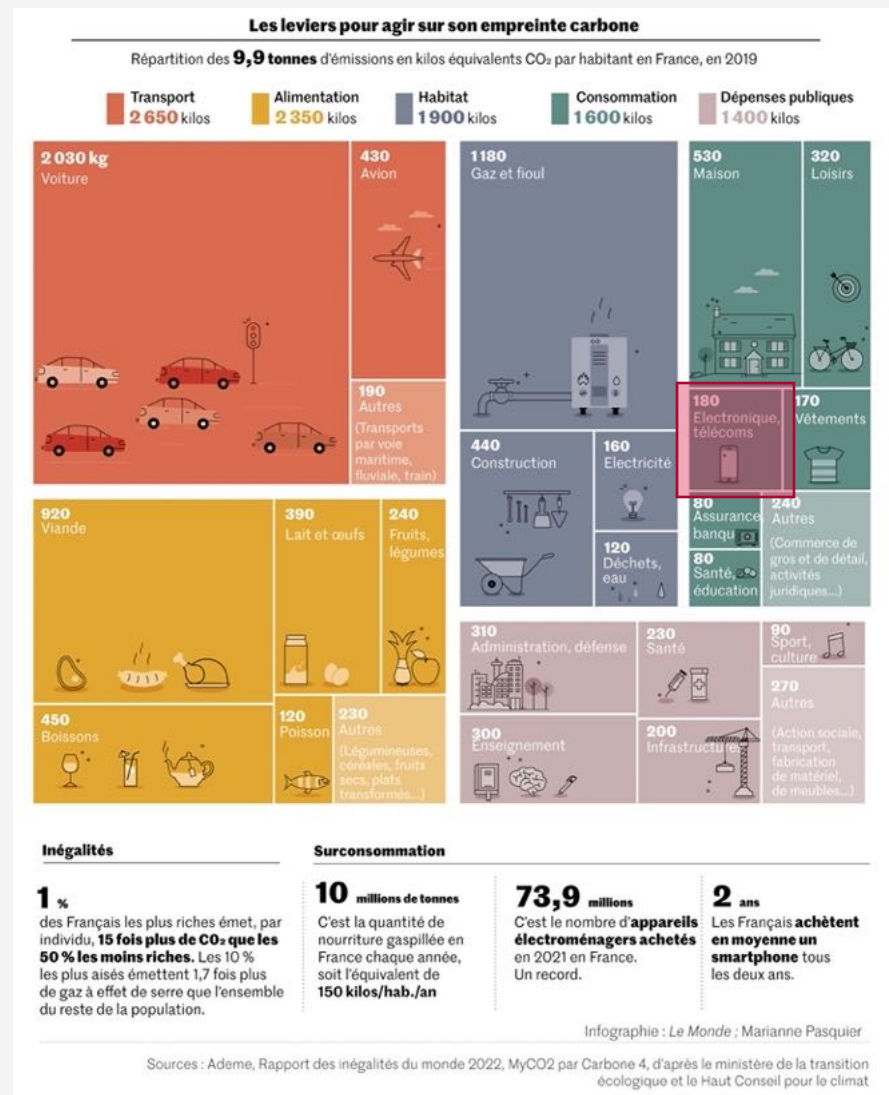
So... where is the growth ?



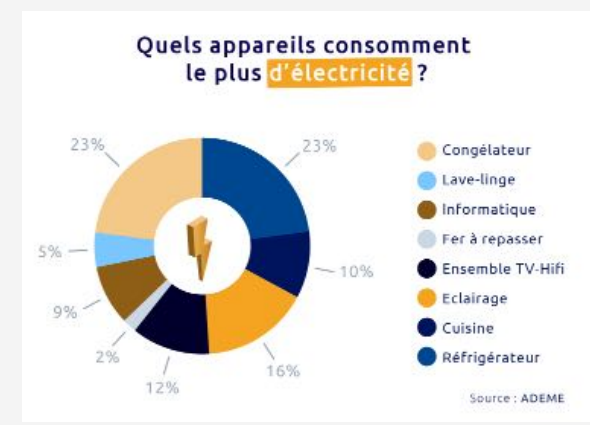
Author – Paul Pinault / Disk91.com

IT Energy consumption and Climate impact

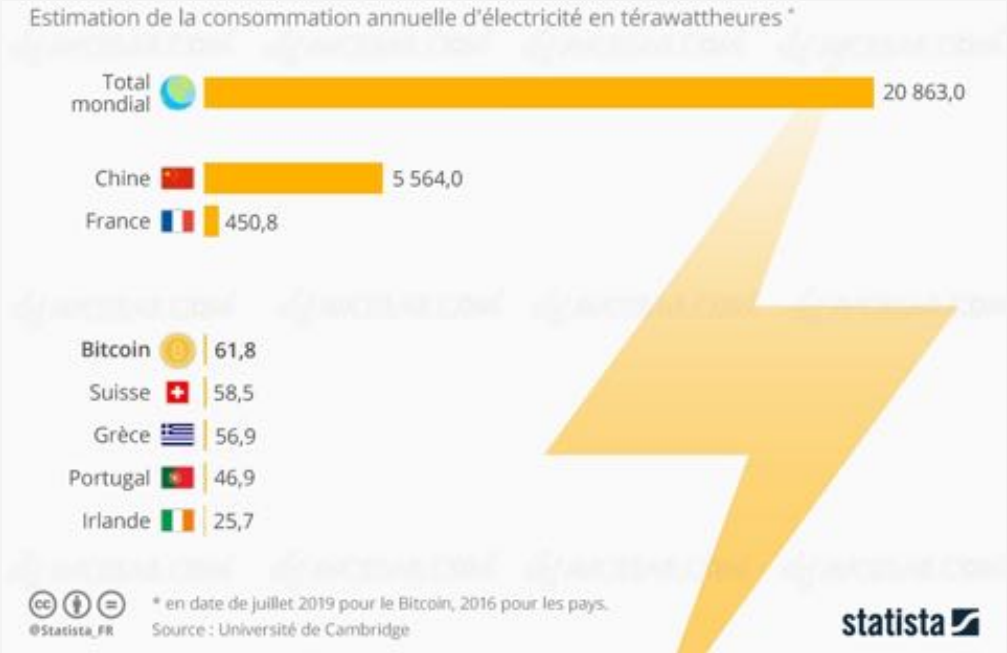
But the previous technologies are 96% of the problem



Citizen technologies, including all the consumer electronic (not the smartphone but TV, washing machine ...) are the 1.8%



New technologies source of waste

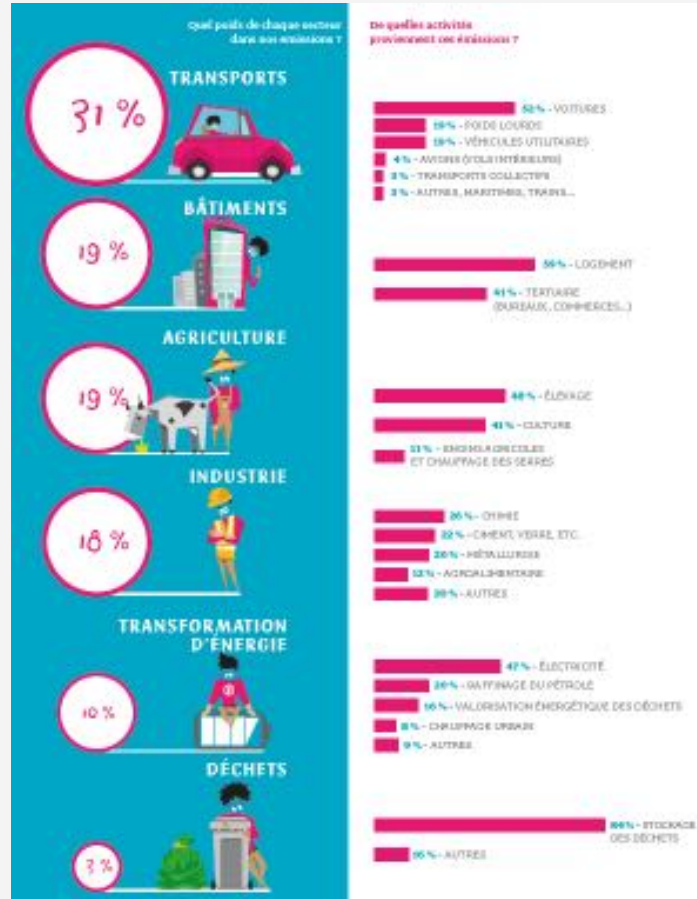


2021 BTC estimate 140TWh
2022 should be around 79TWh

Estimation 3.4M ATM machine
worldwide at 2.5KWh each = 8.6TWh

IT Energy consumption and Climate impact

But the previous technologies are 96% of the problem



Netflix episode is 400m equivalent car driving

By going at work with your bicycle you can watch a full season every day of the year.

Going to theater with your car is worst than watching 10 movies on Netflix (just for the drive)

What is **France** theater energy consumption ?

Average 95kW for 2000 seats and 10 rooms

5000 theater's rooms in France

About 47MW (412GWh / an)

What is Netflix **global** energy consumption ?

Average 400W per server (cold included)

17000 servers WW

About 6.8MW (60GWh / an)

What about TV ?

- > 13000 radio emitter in France
- > 200kW to 700 kW radio

	T2 2015	T2 2017	T2 2018
Nombre moyen d'écrans par foyer permettant de regarder la vidéo	5,4	5,5	5,6
Téléviseur	1,7	1,6	1,5
Ordinateur	1,4	1,4	1,6
Téléphone mobile (dont smartphone)	1,8	1,9	1,9
Tablette tactile	0,5	0,6	0,6

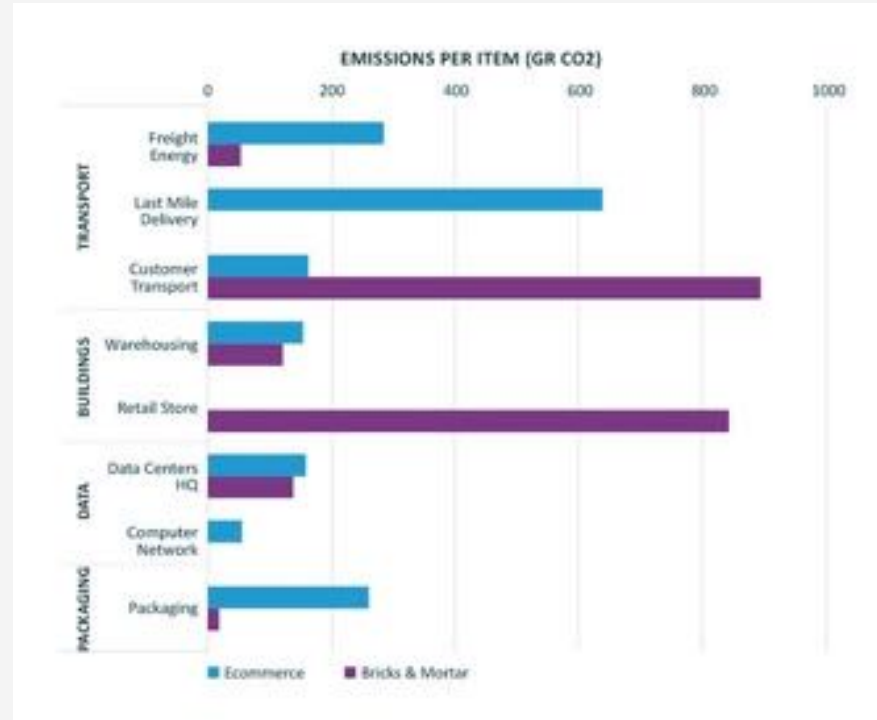
La télévision par internet est le premier mode de réception de la télévision sur le poste principal

Comme sur l'ensemble du foyer, la réception hertzienne terrestre connaît une légère hausse sur le poste principal début 2018, réduisant l'écart la séparant de la réception par internet (de 8,2 points fin 2017 à 7,3 points au 2^{ème} trimestre 2018). Ces chiffres révèlent en creux que la réception hertzienne est plutôt utilisée sur poste secondaire, probablement en raison de sa gratuité.



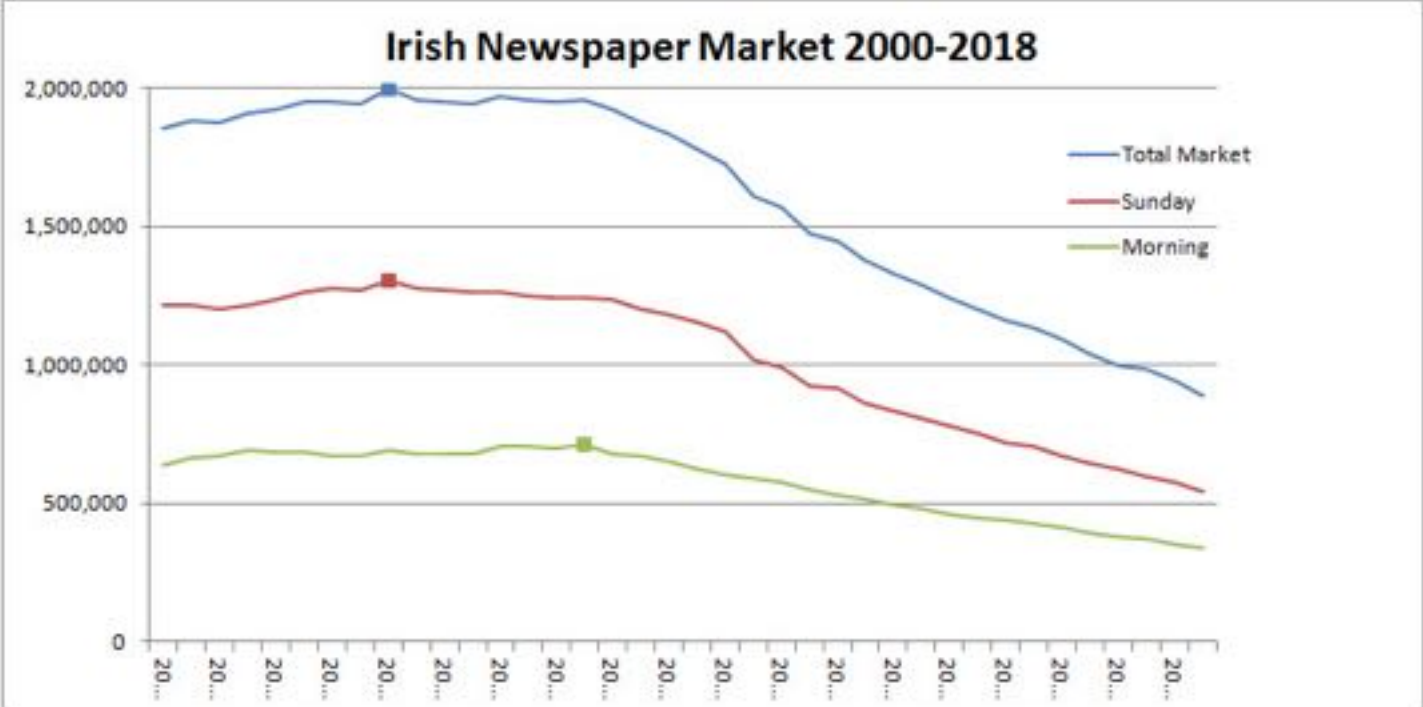
Technology is also the solution

GES on retail



17% positive savings

Technology is also the solution



>50%

- less paper
- less print
- less transport

Technology is also the solution



830.000 tons of physical mailbox spam in France for a year

4kWh / kg
157Wh / unit (0.03€)

3.3TWh / an

CO2 effort 1,5km elec vehic / j
216m thermal vehic / j
Per people



511Md total email in FRANCE for a year

Wh / email	Total Yearly energy	Vehicle eq m / day CO2
Ademe 2011 avg 81kb / email 2Wh	1TWh	Eq elec : 480m Eq thermic : 65m
Real size 70% spam & 5kb + 30% legit @75kb (avg 26Kb) 0.64Wh	0,32TWh	Eq elec : 153m Eq thermic : 20m
Applying more's low /2 every 18 months 0.01Wh	0,005TWh	Eq elec: 2m Eq thermic: 32cm

Email is not



“30 emails are equivalent to 1 day of a light bulb”



**→ 1.6Wh / email
X
306.4Md email /d**



490GWh / j



122M servers



means

Every servers sold by the last 10 years are only doing email

Email is not

“email for a 100 employees is 136Kg CO2 per employee per year = 1.4 CDG<->NY”



13T/y = 130MWh/y
= 14kW



35 Servers



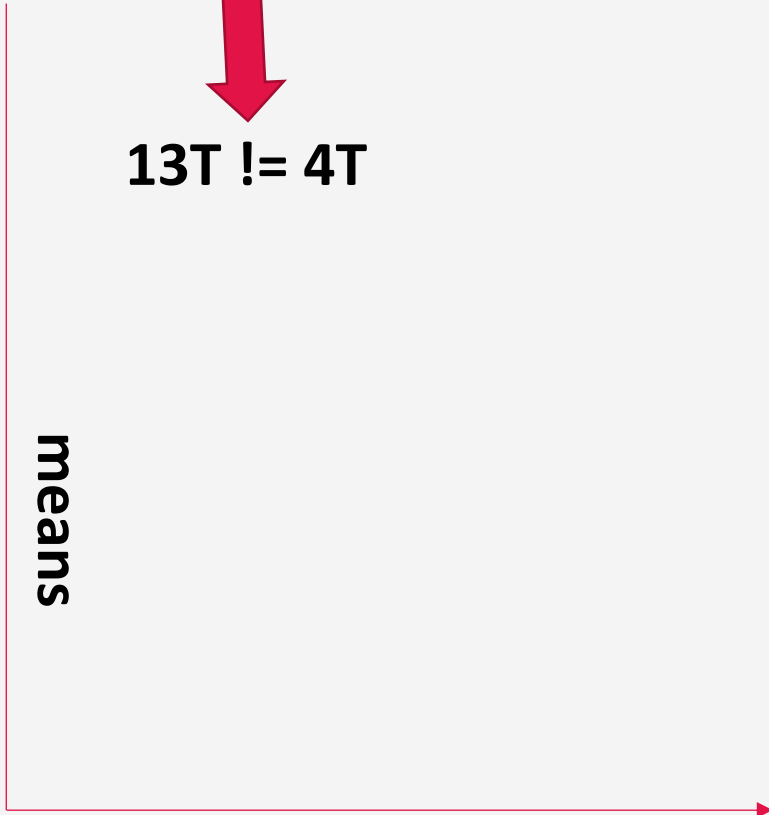
2000 cores
17TB RAM



500 macbook
32GB RAM

13T != 4T

means



Remote Office

Energy reduction plan in 2022 in **France**, includes a potential 9.1TWh gas energy reduction by increasing the remote office.

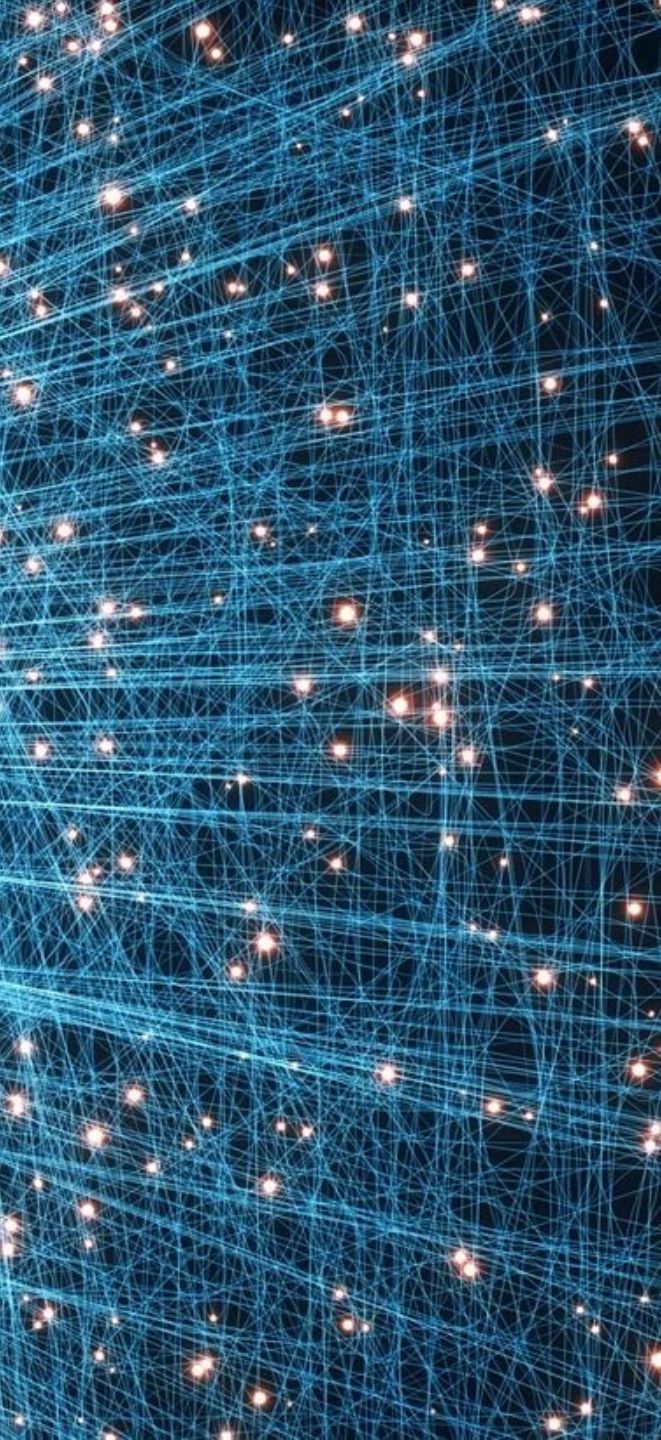
The associated transport reduction is estimated to 2.8TWh

This is equivalent to 3,4M physical cooled servers.



This is more than Google Amazon Facebook, Apple and Microsoft all over the world (estimation around 2,5M)

Technology also provide a new approach



↳ Wi6Labs a retweeté

 **Laurent Riéra** @LaurentRiera · 5 h

Vers une ville climato-intelligente ? Quand l'#IOT se met au service de l'identification et du suivi des îlots de chaleur urbains. Article technique ET passionnant sur le déploiement de capteurs connectés à @metropolerennes utilisant le réseau #LoRaWAN wi6labs.com/2021/04/28/ver...



Alkante et 8 autres

🗨️ 6 ❤️ 11 ↗️



**IoT is a solution,
based on data collected
from physical world,
directly, by things**

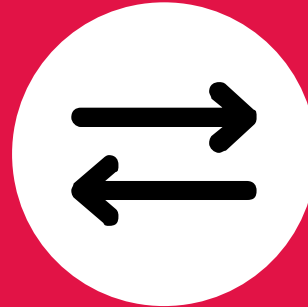


**IoT has 3 layers
to compose a
solution.**



DEVICES

To capture the data from the physical world
Devices are numerous. Larger the fleet is and larger the value created by the platform will be.



COMMUNICATION

To transmit, autonomously, the captured data from the fields to the consumers.
Communication key feature is not to be fast; it is to be energy efficient.



PLATFORM

Makes the data meaningful and accessible to the end-user.
Process large set of data. Mix different source of data. Create individual and aggregated value.
Manage the device fleet



FITBIT USE CASE

Get personal activity & health data from million of different people world-wide. Process them and propose:

- Individual feedback
- Global data studies and partnership programs



MULTIPLE DEVICES

Collecting the same type of Data



USING BLUETOOTH

And the customer smartphone as a Gateway to internet



WITH APP AND BIG DATA

To propose a valuable customer experience and B2B services like health insurances

NETATMO USE CASE

Get home environmental information – Temperature, Hygro, Sound...

- Individual feedback
- Global data studies and partnership programs



MULTIPLE DEVICES

Collecting the different type of data all related to your home



USING Wi-Fi

And the customer Internet connectivity to reach the backend services



WITH APP AND BIG DATA

To propose a valuable customer experience and B2B services like city map of environmental noise



Let's make a short break

LEARNING AT THIS STEP



IoT is a Solution

Composed by Hardware, Network and Software.
It needs maintenance and the associated business model is a service



Belonging on multiple technologies

The communication layer uses different technologies depends on the context.



With a two sides source of value

A direct benefit for the end-user (the reason why he buy it) and a B2B source of revenue obtained thanks to the massification of the collected data

IoT solutions have a complex cost model

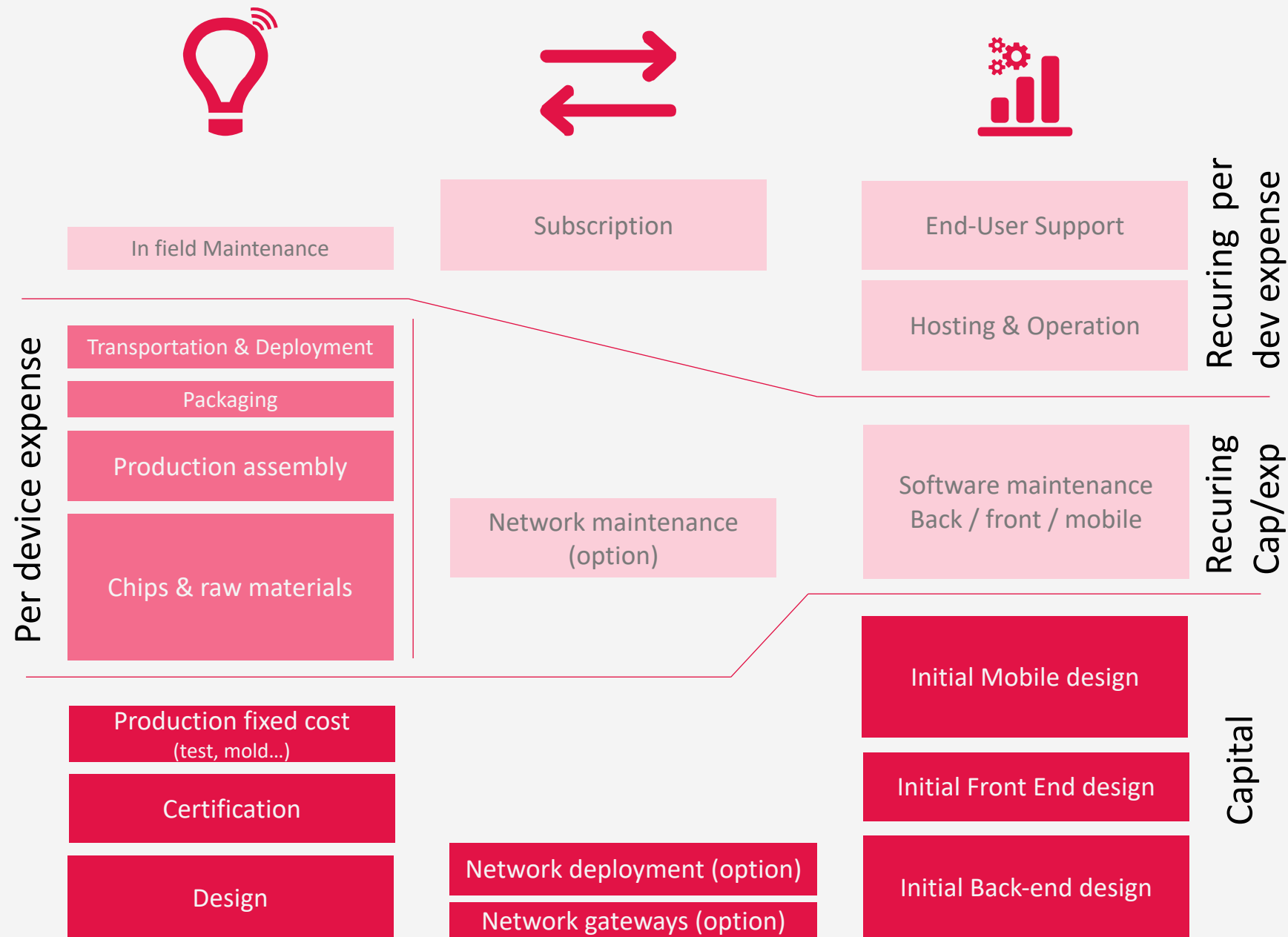
Mixing

- Capital to produce the software / hardware and industrialization design
- Per devices costs related to production and distribution
- Recuring investment to maintain the software stack
- Recuring cost for supporting maintenance, communications, platform run and end-user-support

1 Volume of devices is a key factor

2 Longer the service is delivered and higher the cost per device is

IoT solution business model differ from commodity product standard





HARDWARE ONLY

Xiaomi -Caméra de Sécurité Domestique 360° 1080P- Blanc

[Visiter la boutique Xiaomi](#)

★★★★☆ 2 442 évaluations | 177 questions avec réponses

Prix conseillé : ~~39,99 €~~

Prix : **33,98 €**

Économisez : **6,01 € (15 %)**

Tous les prix incluent la TVA.

[Assistance produit Amazon gratuite incluse](#)

Livraison GRATUITE (0,01€ pour les livres) **en point retrait.** [Détails](#)

Neufs (9) à partir de **33,98 €** + Livraison GRATUITE



IoT ORIENTED SOLUTION

Arlo Pro 3 | Pack de 2 caméras de surveillance 2K HDR, Batterie rechargeable Alarme Grand angle 160°, Audio Bi-directionnel Eclairage spotlight intégré (VMS4240P)

[Visiter la boutique Arlo](#)

★★★★☆ 82 évaluations

| 8 questions avec réponses

Prix : **599,00 €**

Tous les prix incluent la TVA.

Payez: 149,75 € x 4 (-13,48 0 € de frais inclus) [Voir conditions et plus de facilité de paiement](#)

[Assistance produit Amazon gratuite incluse](#)



IoT needs recurring revenue or needs to include future costs in the initial price

HARDWARE ONLY



Hangang Traceur GPS Magnétique
 90 Jours Longue Veille IP65 étanche
 Suivi en Temps Réel, Tracker GPS
 pour Voiture Camion Moto Véhicule
 Outo TKMARS905

Marque : HanGang
 ★★★★★ 125 évaluations
 | 104 questions avec réponses

Prix : 52,99 €
 Tous les prix incluent la TVA.

Coupon Utiliser le coupon de 5% Détails

Payez en 4 fois dès 75 € d'achats Voir détails et conditions

Message promotionnel Promo... 3 promotions

Assistance produit Amazon gratuite incluse
 Livraison GRATUITE (0.01€ pour les livres) en point



IoT ORIENTED SOLUTION



Passez la souris sur l'image pour zoomer



Tractive Collier Gps pour Chien - Traceur Gps avec
 Portée Illimitée, Blanc

Visiter la boutique Tractive
 ★★★★★ 3 540 évaluations | 43 questions avec réponses

Prix conseillé : 49,00€ De quoi s'agit-il?
 Prix de l'offre : 19,19 €
 Économisez : 29,81 € (61 %)
 Tous les prix incluent la TVA.

Livraison GRATUITE (0,01€ pour les livres) en point retrait. Détails

Neufs & occasions (7) 18,81 € et livraison GRATUITE pour les commandes d'un montant supérieur à 25,00 €

- **ABONNEMENT REQUIS** : à partir de 3,75 € par mois (pour abonnement biennal payable à l'avance), plusieurs options disponibles. L'appareil fonctionne grâce à une carte SIM déjà intégrée, et nécessite donc un abonnement Tractive couvrant la connexion mobile.
- **TRACEUR GPS** : Appareil de suivi GPS léger (35 g) et étanche, recommandé pour les chiens de plus de 4,5 kg. Le traceur Tractive GPS s'attache facilement à tout collier ou harnais. Contrairement aux GPS Bluetooth, le traceur Tractive a une portée illimitée.



Recurring revenue is
 a warranty for
 platform evolutions
 and data safety.

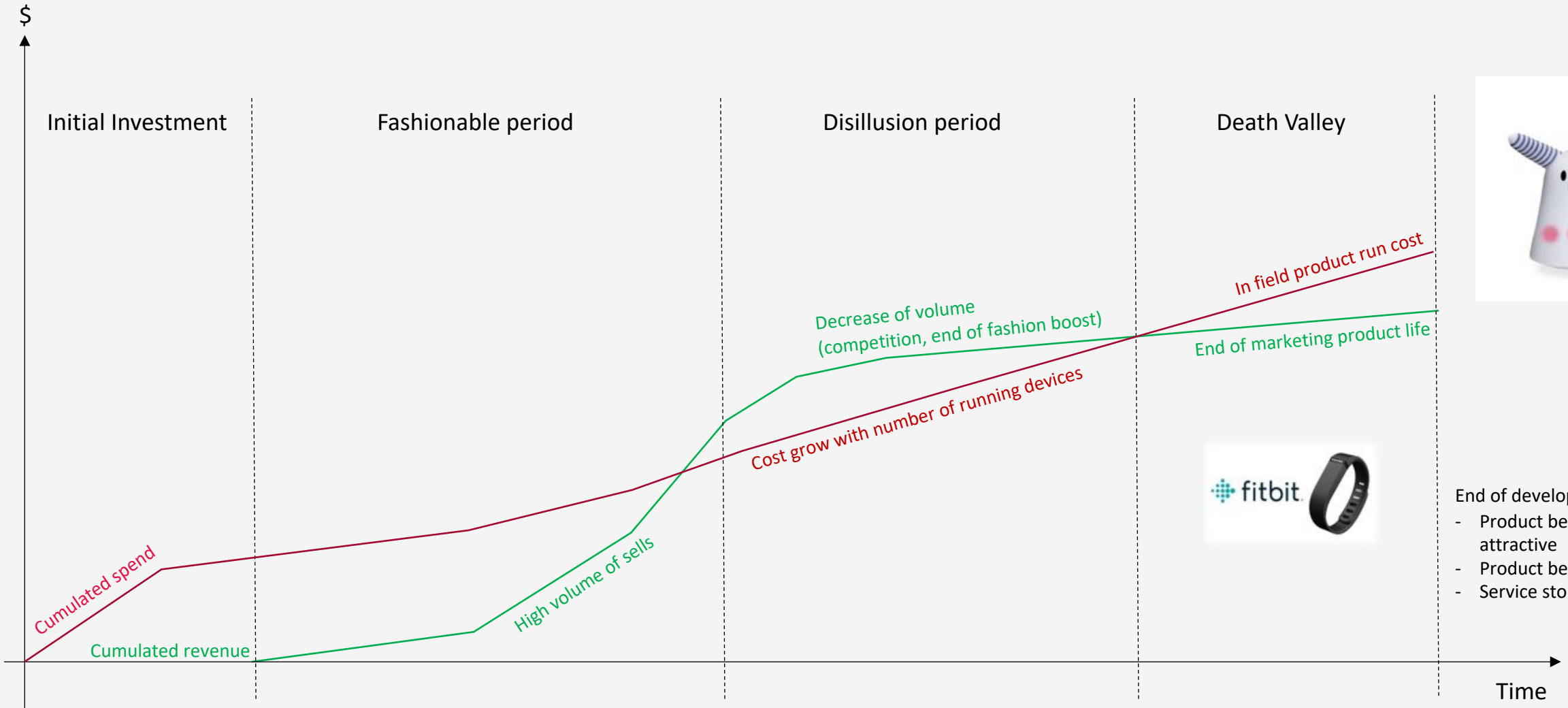
Tractive GPS nécessite un abonnement afin de pouvoir suivre votre chien

BASIC			PREMIUM	
à partir de € 3.75 / mois			à partir de € 4.16 / mois	
Mensuel	Annuel	7 ans	Annuel	2 ans
€ 7.99	€ 49.90	€ 89.90	€ 59.90	€ 99.90
€ 7.99 / mois	€ 4.16 / mois	€ 3.75 / mois	€ 4.99 / mois	€ 4.16 / mois

- | | |
|--|--|
| <ul style="list-style-type: none"> ✓ Suivi GPS (intervalles de 2 à 60 minutes) ✓ LIVE Tracking illimité (intervalles de 2-3 secondes) ✗ Couverture mondiale (pays d'origine uniquement) ✗ Historique de localisation illimité ✗ Exportation de l'historique de localisation (fichiers gpx et kmf) ✗ Accès depuis plusieurs comptes ✗ Service Client PREMIUM | <ul style="list-style-type: none"> ✓ Suivi GPS (intervalles de 2 à 60 minutes) ✓ LIVE Tracking illimité (intervalles de 2-3 secondes) ✓ Couverture mondiale ✓ Historique de localisation illimité ✓ Exportation de l'historique de localisation (fichiers gpx et kmf) ✓ Accès depuis plusieurs comptes ✓ Service Client PREMIUM |
|--|--|



Selling IoT as a Product leads to slow death



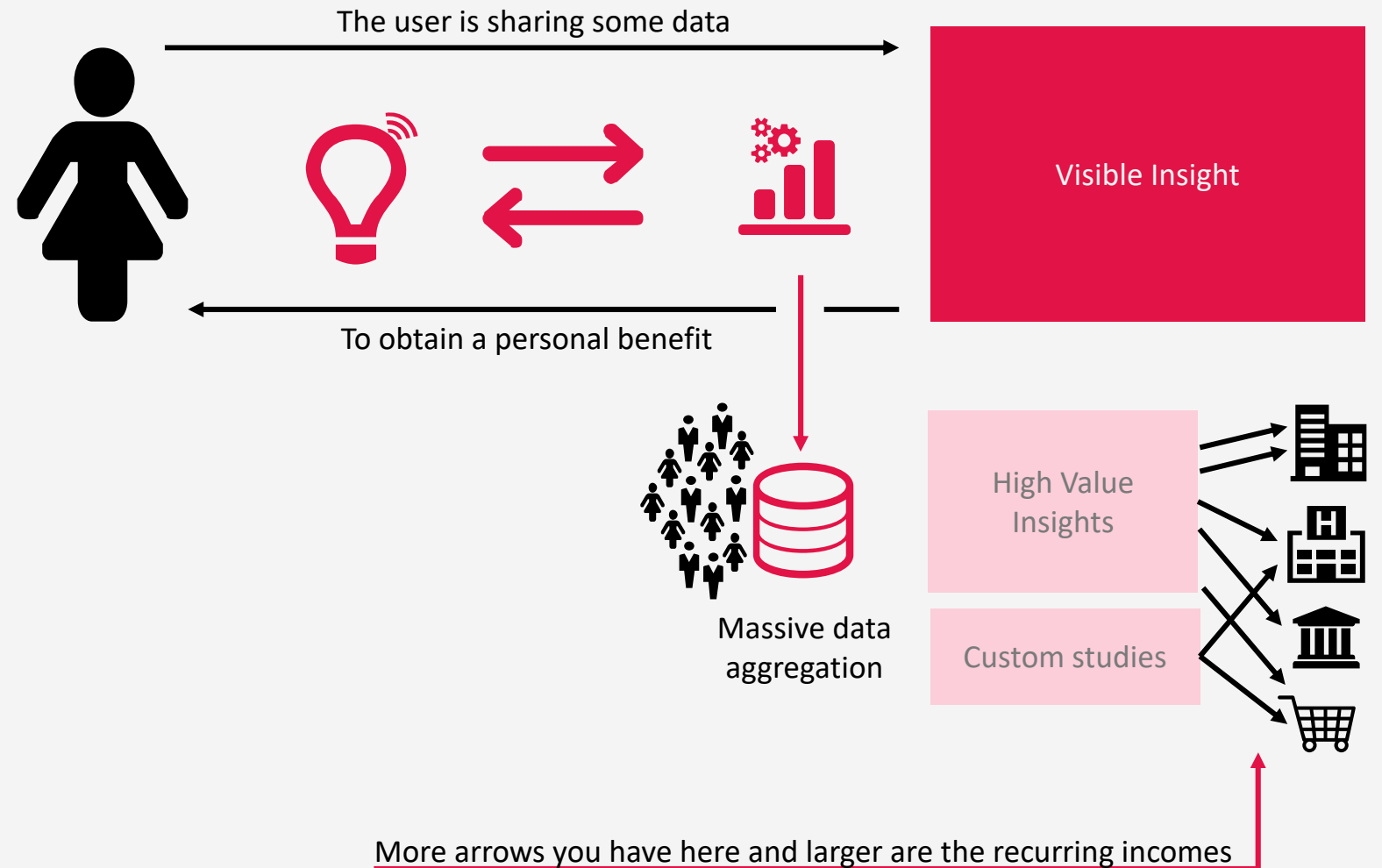
- End of developments
- Product becomes less attractive
 - Product becomes insecure
 - Service stops working

IoT revenue model

There are many revenue model, an illustration here is on B2C direct solution with indirect B2B markets

- 1 There is the reason why you accept / want the solution.
- 2 There are the market where the solution creates value, sometime the reason why the solution has been created.

This is a win-win deal for human generated data



**“DATA IS THE NEW OIL”
is a wrong assumption !
However, data is **Ore** .**



MORE DATA YOU HAVE HIGHER ITS VALUE IS.

With larger data set you can extract more value, touch larger indirect businesses.



THE VALUE OF DATA IS ONLY DUE TO ITS UNIQUENESS

As the data can be sold without reducing your stock of Data, its value comes to a non existing competition or its value tends toward 0.



The rules of the DATA ORE

Mining data let you make a stock; the stock values comes from the number of markets/customers you can reach with unique Insights. This is related to the volume of data you have and the lack of competition. Selling you raw data is making new competitors.



DATA MINING HAS A COST



DATA CAN BE REUSE INDEFINITELY



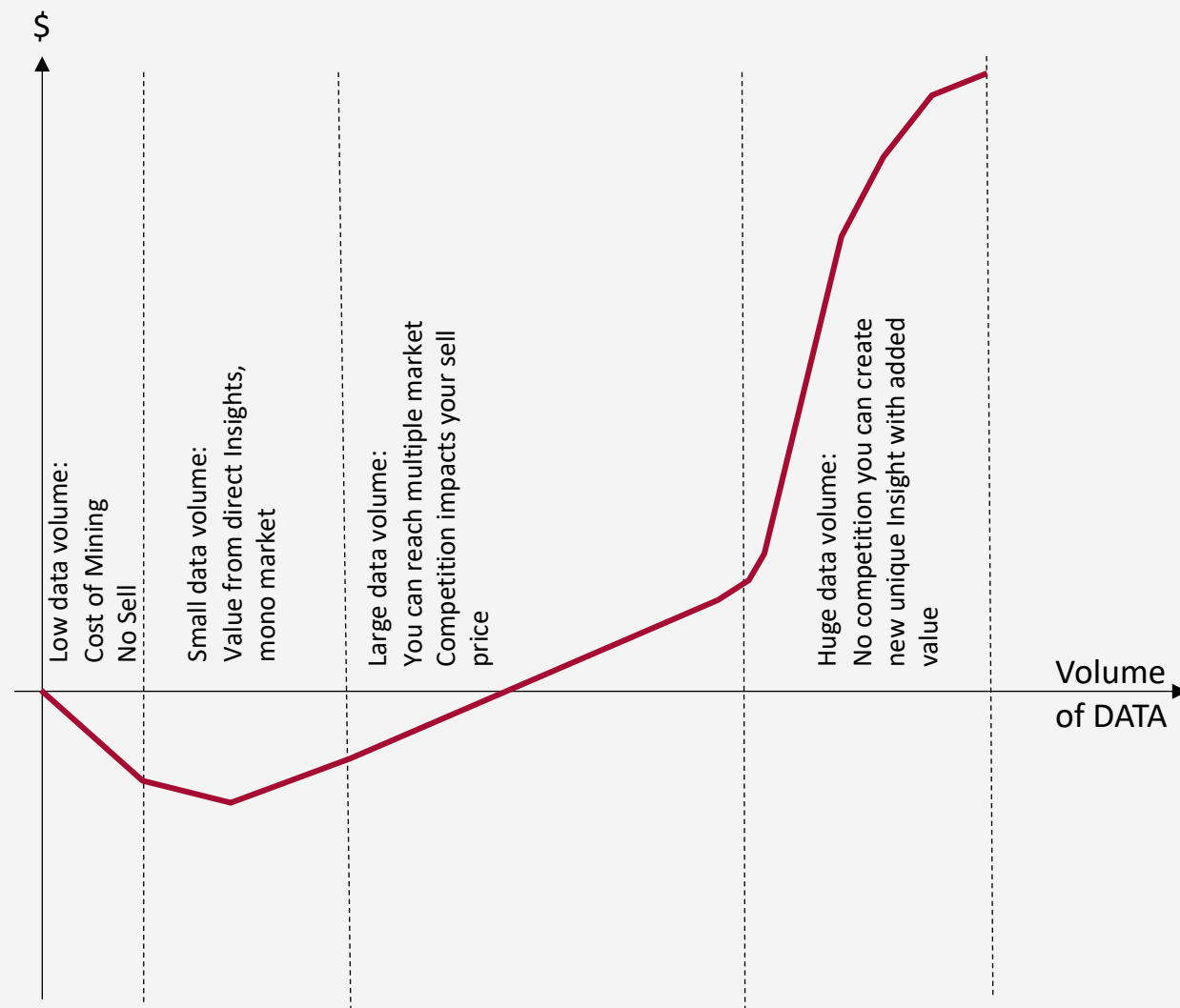
SELLING RAW DATA DESTROY ITS VALUE



DATA VALUE COMES FROM YOUR STOCK OR RAW DATA

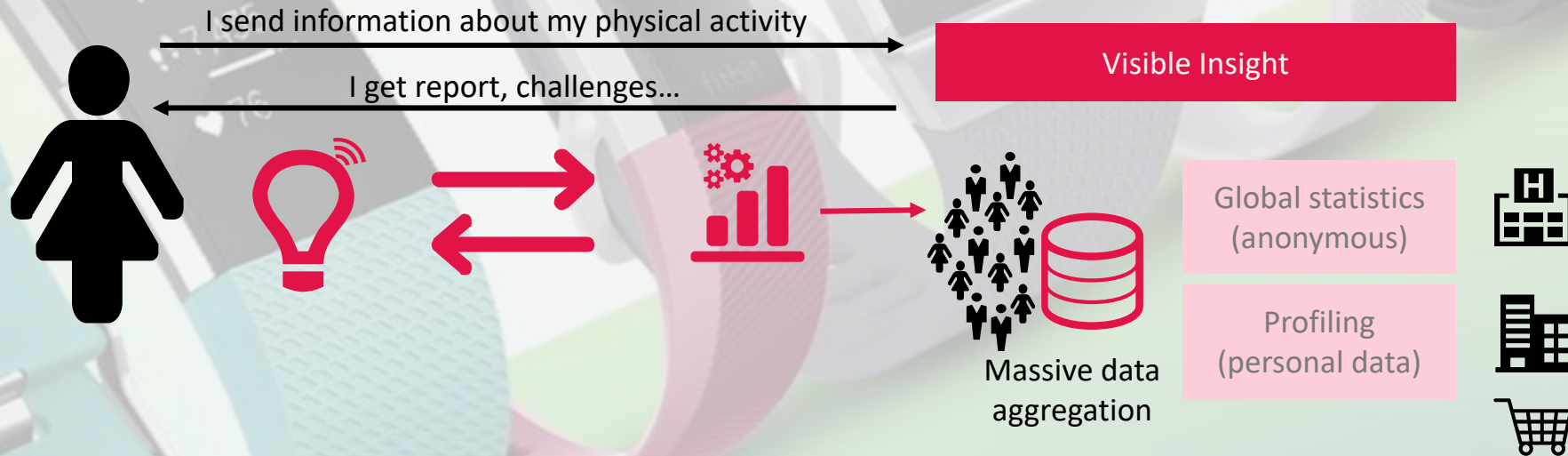


ANY COMPETITOR HAVING MORE DATA THAN YOU DESTROY YOUR DATA VALUE



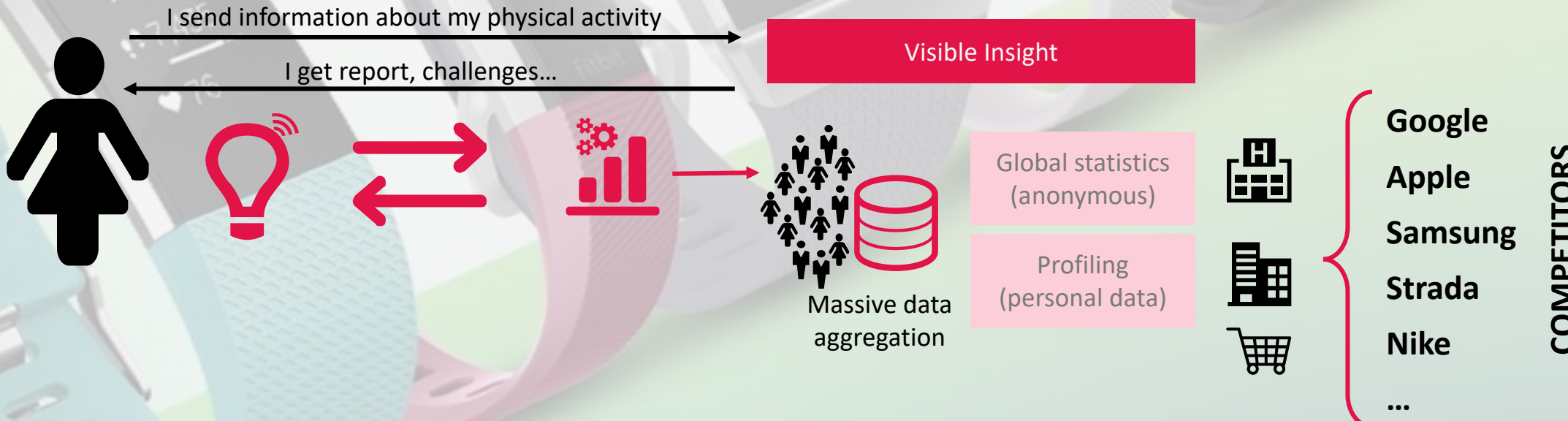
FITBIT USE CASE

Fitbit was the first to capture the human activity at a scale never obtained before. They have been able to propose unique Insights to health research, insurance market and much more. They were expecting a significant revenue from it to support the run costs.



FITBIT USE CASE

The activity sensors have been deployed in cellphone, watches and many competitor's activity trackers making the activity data value tending toward zero today.



BLOCKCHAIN CAN FIX THIS

By proposing a reward mechanism based on a digital asset produced for no-value, you can kickstart the deployment of a fleet of devices



PlanetWatch®



PlanetWatch has quickly reached 60.000 sensors

- **Token distributed to miners for gathering data**
- **Token needed to enter the PlanetWatch game (ponzi like)**
- **Token value is growing due to demand push**
- **1-2 week return on invest during the first months**
- **... Later years ...**
- **The fleet is in place, 72.000 sensor 1 year after start**

B2B Logistic Use-Case

With a tracker deployed in the element of the logistic chain, many companies are looking to improve the supply-chain cost by reducing the transport duration and reducing the stock size and associated cost.



Visible Supply Chain Insight

Global statistics

Transporter profiling

What the project targets with a sufficient value to finance it (build+run)

In most of the case, nothing is done here, and value is lost

Let's make a short break

LEARNING AT THIS STEP



IoT has recurring costs

Longer the service is delivered, higher the cost is per device.



Business model includes recurring cost

In the initial price (device will have a programmed obsolescence) or within a subscription



Multi-side business can be a solution

By targeting different market and extracting more value from the data you can balance the recurring cost issue



IoT is an opportunity to innovate like Internet or smartphones transformed our environment



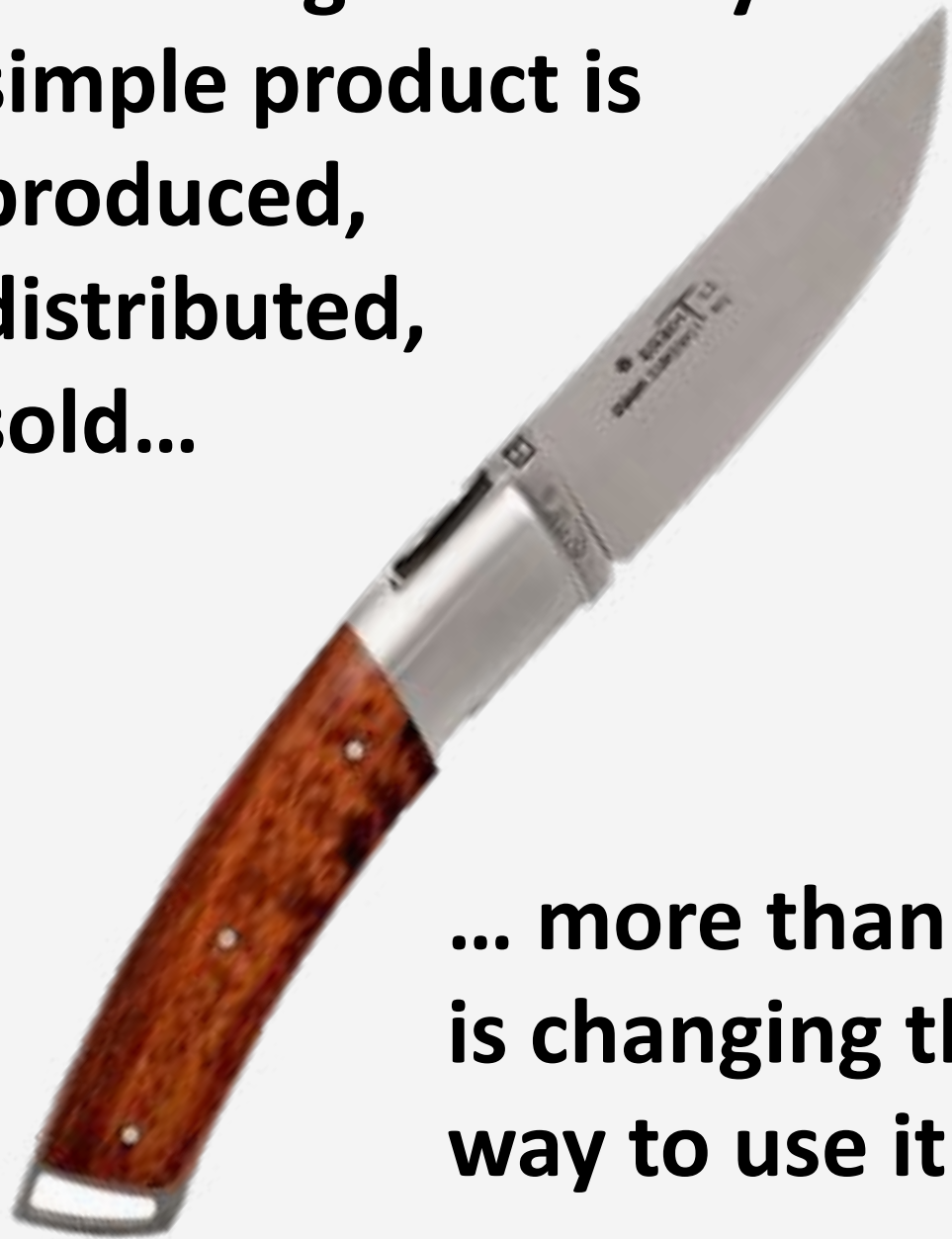


”

Adding a connectivity feature on an existing things does not make innovation happen.

Innovation transforms an existing market or create new markets

IoT changes the way a simple product is produced, distributed, sold...



... more than it is changing the way to use it

Understand the use of product

Propose maintenance based on use

Unlock special blade

Track product in distribution circuit

Propose renewal right on time

Per use billing

Allow opening

Fight against counterfeiting

Why connecting tables ?

- Would it be for the end-user to master its dinner habits ?
 - Are your ready to pay for it ?

NO !

- Would it be for the manufacturing process ?
 - Can we save money ?

YES !



Manufacturers needs to forecast future order with accuracy to plan raw material purchase and flatten manufacturing process.



IoT can give them a real time view of the distribution stocks and move away from forecast to real-time market data.

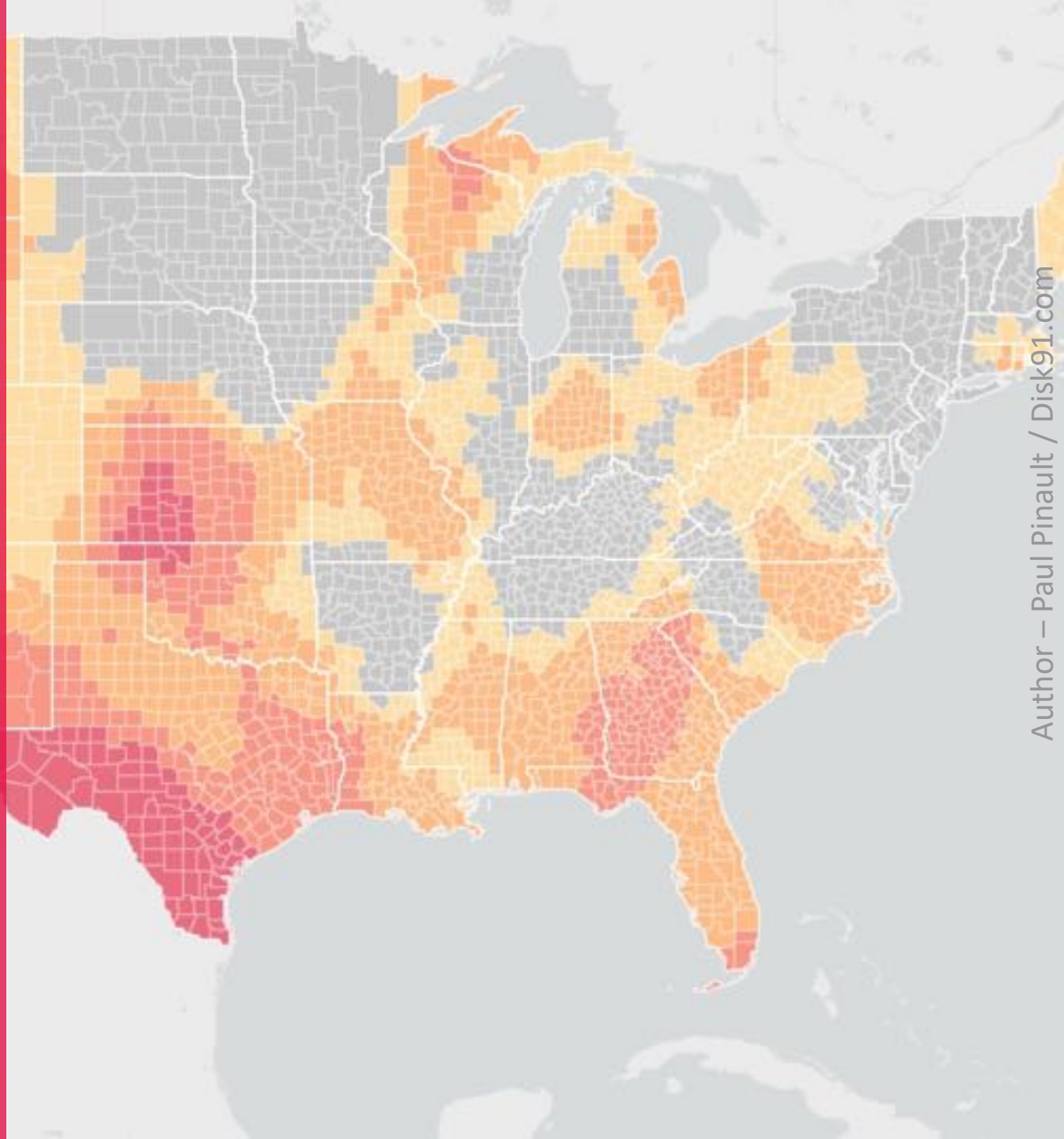


IoT can fight against pandemics

Here is a Map of Covid evolution within the USA made by Kinsa connected thermometer. This is precious visualization obtained with \$30-\$50 thermometers, complex to use. It is like a satellite watching hearth with a 100km x 100km definition.

How this could be with IoT at Scale providing a 100m x 100m definition, thanks to \$3 connected thermometers ?

- It could predict any pandemic movements.
- Gives immediate results even before test.
- It could give transparency all over the world.
- Allow to confine small area instead of whole countries.
- It could protect the personal data more than the existing solutions.

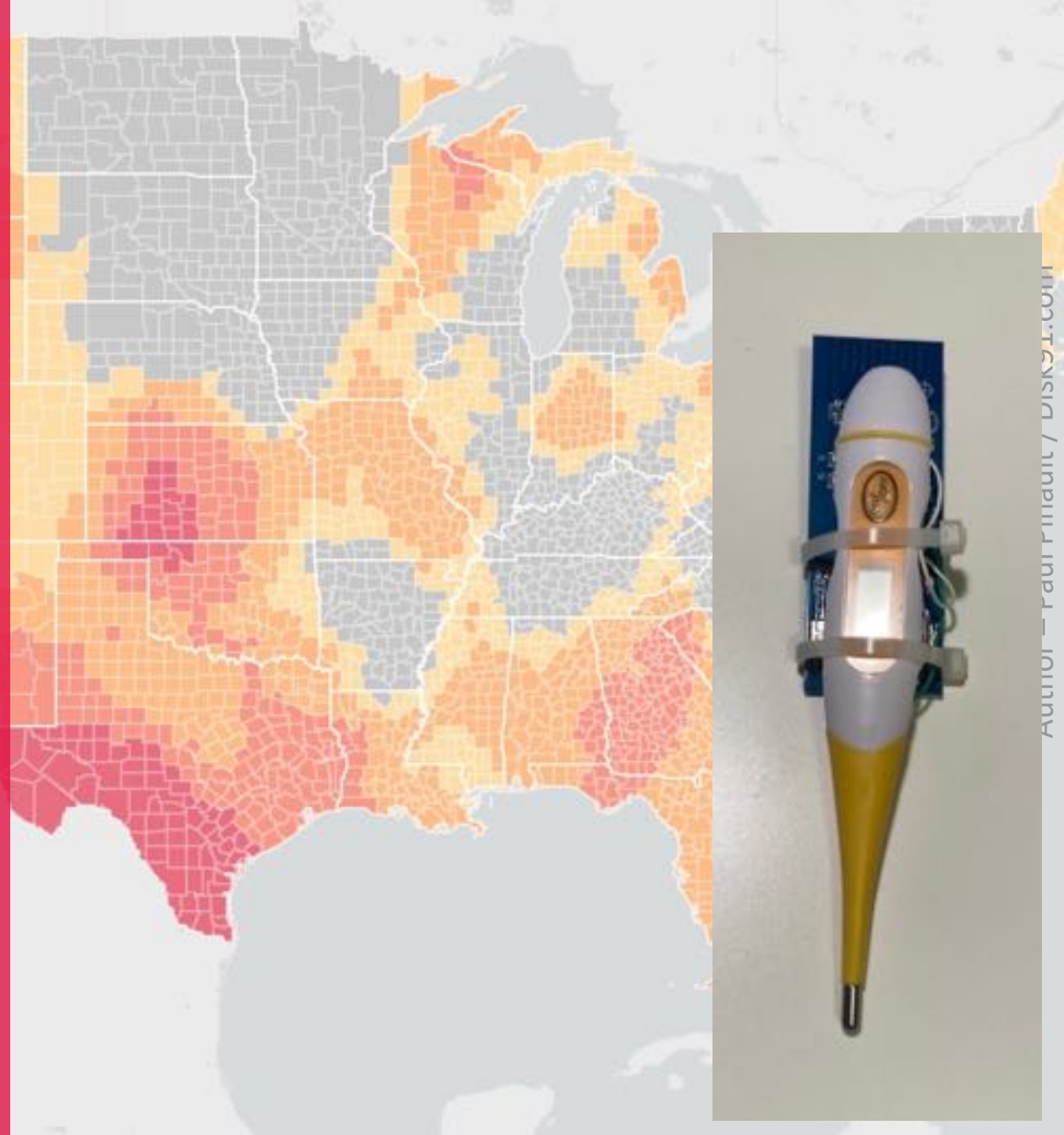


IoT can fight against pandemics

Here is a Map of Covid evolution within the USA made by Kinsa connected thermometer. This is precious visualization obtained with \$30-\$50 thermometers, complex to use. It is like a satellite watching hearth with a 100km x 100km definition.

How this could be with IoT at Scale providing a 100m x 100m definition, thanks to \$3 connected thermometers ?

- It could predict any pandemic movements.
- Gives immediate results even before test.
- It could give transparency all over the world.
- Allow to confine small area instead of whole countries.
- It could protect the personal data more than the existing solutions.



IoT for public led problem to service

Public lights are fails and detection is usually made manually on regular basis.

- It has a detection cost
- It implies a bad quality of service

Connected lights can reduce the detection cost, allow to get an immediate detection and maintenance offering a high quality of service.

But it is also an opportunity to transform this kind of maintenance as a service, being able to do predictive maintenance.

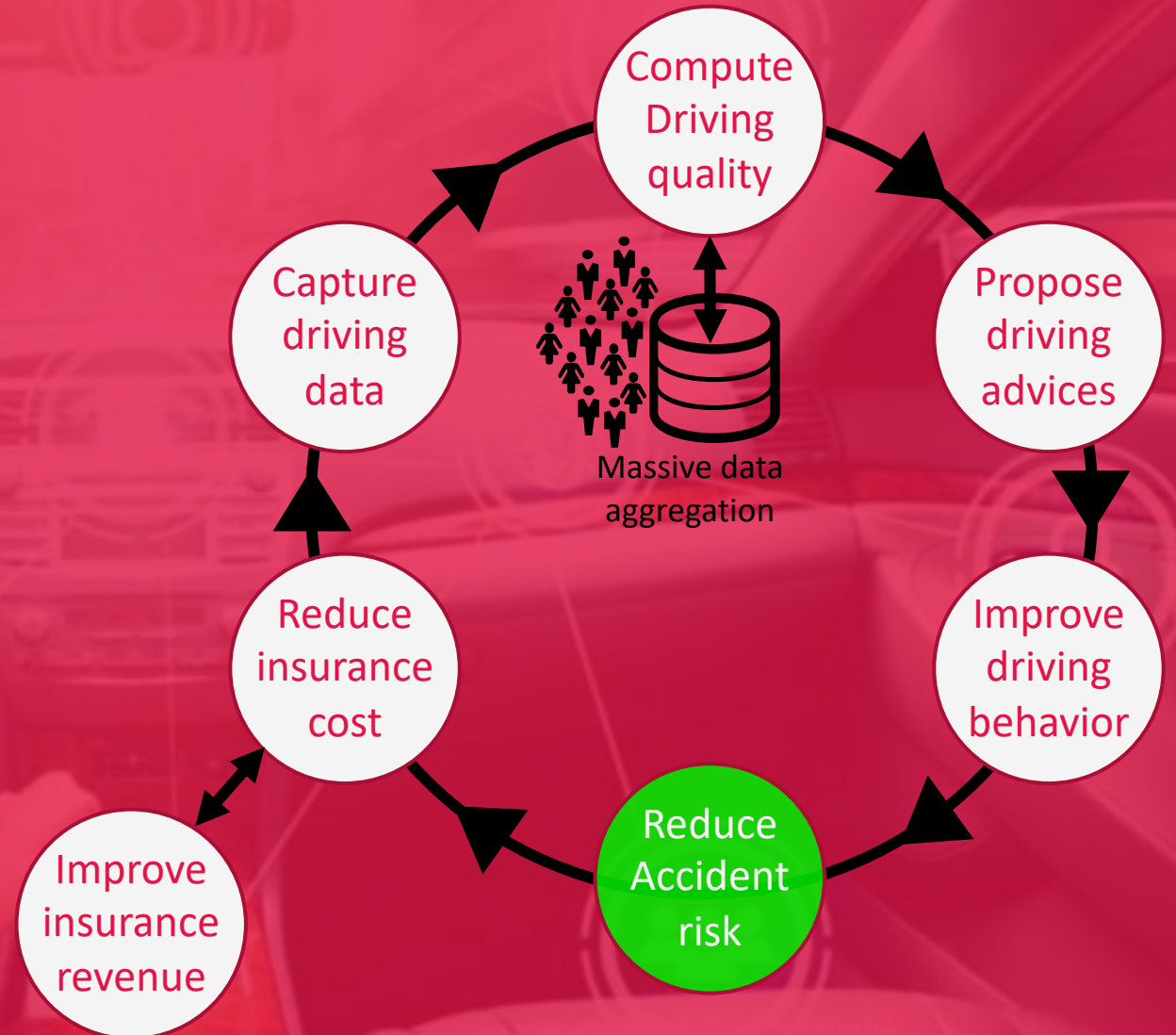
It's also an opportunity to change the way the city lights are managed and to save a lot of energy with a higher service level for the citizens.

Connecting a light today is less than \$2 hardware.



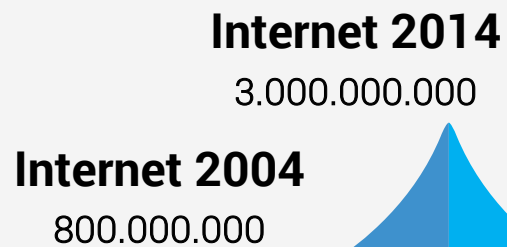


IoT for safer mobility



IoT makes technologies reaching a new scale

Family scale



Humanity scale



Things scale



IoT at scale

What makes the difference and innovation with IoT is the ability to **make it at scale**. The ability to **deploy millions of devices in the field**.

\$1

ULTRA-LOW-COST DEVICES

In 2020 we reached under \$1 IoT devices first condition to support at scale deployment

X

IN FIELD COST TENDING TO ZERO

The second condition to support at scale deployments.



IoT as the source of physical world AI



**IoT CAPTURES THE
ENVIRONMENTAL
DATA
DATA FEED THE AI.**

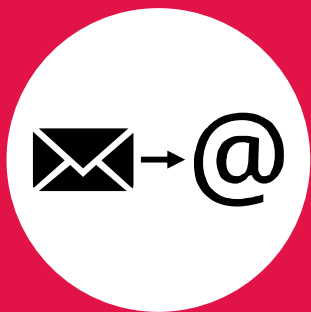


AI main domains of implementation is **digital world** (images, video, sounds, voice, social network, books ...)
The AI capabilities in the physical world is huge (car driving, industrial maintenance, pollution, energy consumption reduction, climate prediction, health & pandemic...)

Currently, **physical world AI** is limited by the small number of data we have for training the neuronal networks.
IoT, by massively gathering physical world data is **enabling new AI capabilities**.

Let's make a short break

LEARNING AT THIS STEP



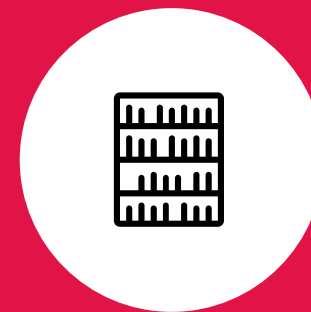
IoT is transforming a market

Making things communicating, automate reporting is not enough



It allows to get data from Things anywhere

It gives the solution provider to grab data from any of the things at scale



IoT scale is Things scale

IoT revolution will make sense at scale, therefore the most important things for a breakthrough is the solution TCO per Things



IoT have multiple faces for addressing all the Thing's contexts.

New networks made IoT to come alive.



Wearable – human data capture



- 1 day to 1-week autonomy
- Small
- Not expensive
- Subscription challenge

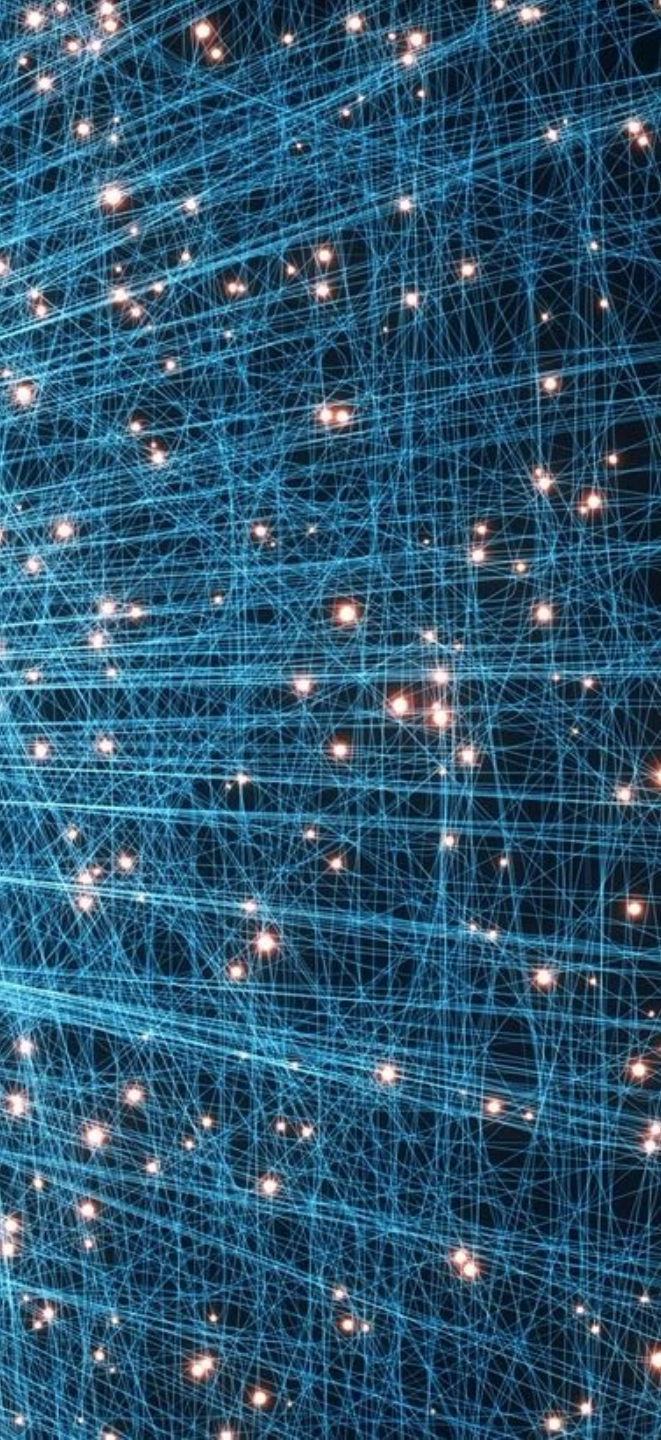


- Get benefit of the human smartphone
- 5m coverage
- Free large bandwidth*



- Focus on user experience
- Belongs on personal data

* This perspective is a market size limiter...



Network characteristics for

Wearables



BLUETOOTH

For customers with a smartphone AND data.

This is basically limiting the target population

Target Geeks

CELULAR TECHNOLOGIES

Enable access for all with a constraints on communication costs

Reduce autonomy

Target elderly, non geeks

Smart home – control, save, protect



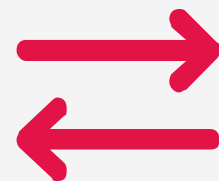
- 6-month to 2 years autonomy
- Small & Design
- Not expensive
- Subscription against savings



- Get benefit of the home Internet access
- Home wide coverage (300m)



- Focus on user experience
- Belongs on personal data
- Smart home is not home automation



Network characteristics for

Smart Home



ZIGBEE

With a gateway connected to home Internet

Low energy communication solution including mesh capabilities



WiFi

Already existing every-where with coverage limitation.

Configuration is complex



LoRa

With a gateway connected to home Internet

Low energy communication solution with large coverage



Bluetooth

With a gateway connected to home Internet

Mesh or long range for smart home. Easy to connect with smartphone

Smart city – optimize, greenify...



- 5-years to 30 years autonomy
- No maintenance



- Low cost
- Small bandwidth
- City wide network (10 - 100km)



- High level of insight
- Massive data processing
- Money/Energy saving oriented
- Subscription

Network characteristics for Smart Cities

0G



MESHED NETWORK

City wide meshed network like Amazon Sidewalk are promising for B2C and could be used for Smart Cities

Industrial IoT – reduce costs, improve quality, secure investments



- 1-years to 30 years autonomy
- Reduced maintenance



- Take benefit of existing networks (M2M)
- Autonomous in private network (or public)







- Difficulty on multi-tenant added value.
- Massive data processing
- Money/Energy saving/Risk reduction oriented

Network characteristics for

Industrial IoT

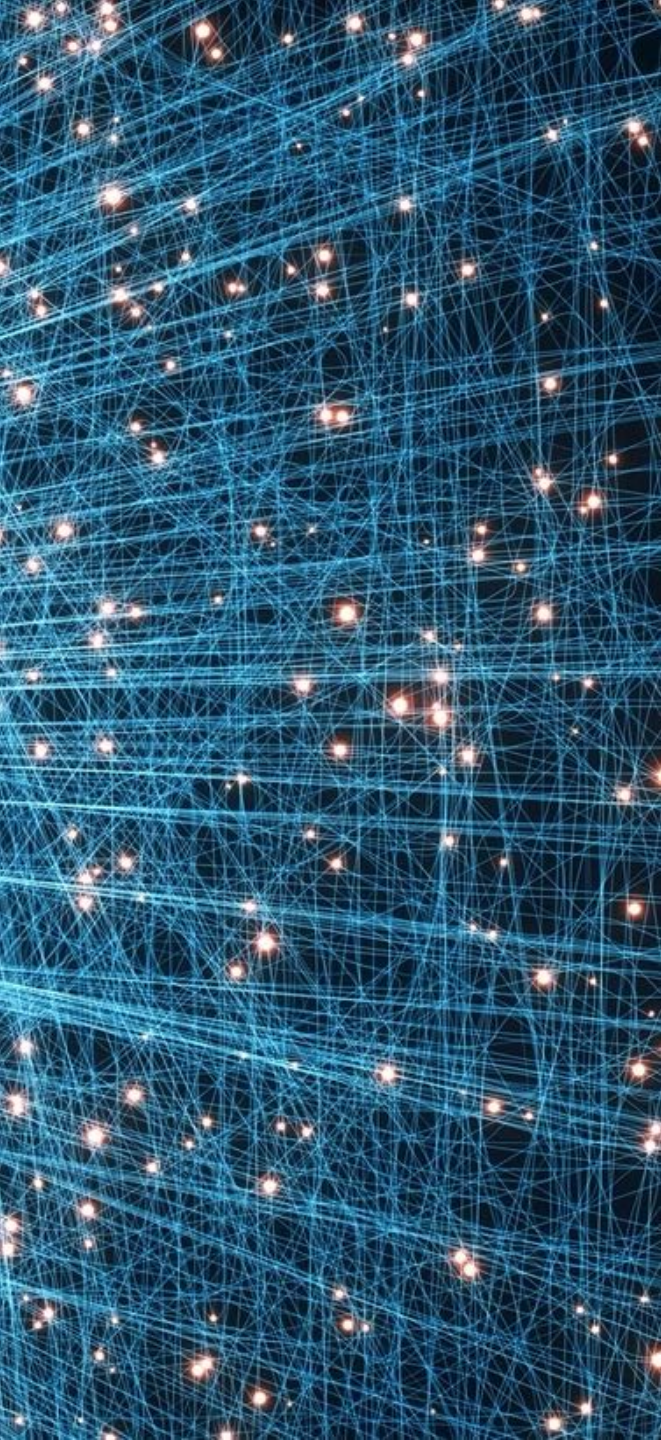


			
ETHERNET	WiFi	LoRaWAN	Sigfox
<p>Old M2M technology already in place.</p>	<p>Already in most of factories and warehouse</p>	<p>Allows to deploy private network at low cost.</p>	<p>No investment, public network can be extended locally.</p>
<p>Reliable and secured but costly for massive deployment</p>	<p>Configuration is complex</p>	<p>Industrial site coverage with 1-3 gateways only.</p>	<p>No maintenance cost, subscription cost.</p>
<p>Reduced maintenance, not mobile</p>	<p>Reduced autonomy</p>	<p>Reduced maintenance</p>	<p>Long Autonomy Ultra low-cost devices</p>
		<p>Long Autonomy</p>	



IoT / IoT4i / IIoT

IoT	Locations 10.000+	Sensors 10.000+	Frequency Low	Data Similarity
IoT4i	Locations 100+	Sensors 1000+	Frequency Low	Data Variety
IIoT	Locations 100+	Sensors 10.000+	Frequency High	Data Variety



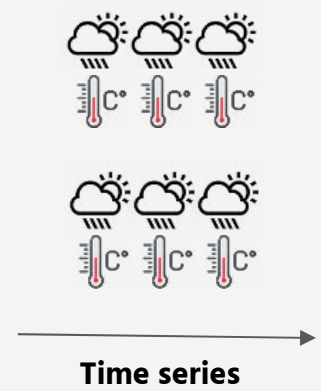
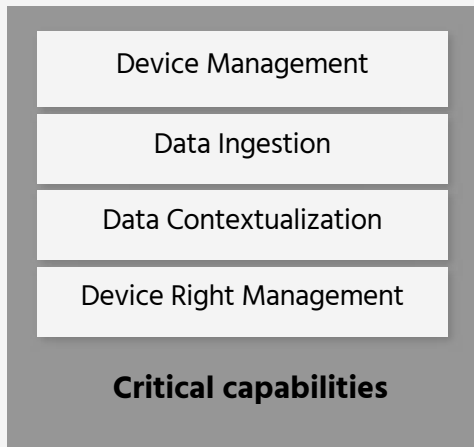
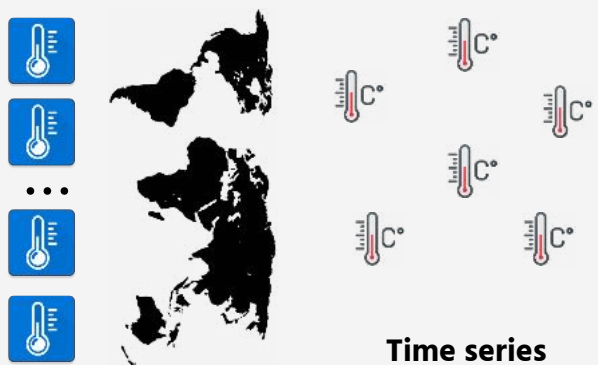
IoT / IoT4i / IIoT

IoT	Locations 10.000+	Sensors 10.000+	Frequency Low	Data Similarity	
	Device Management				
IoT4i	Locations 100+	Sensors 1000+	Frequency Low	Data Variety	
IIoT	Locations 100+	Sensors 10.000+	Frequency High	Data Variety	BIG DATA
	Volume		Velocity		

IIoT vs IoT

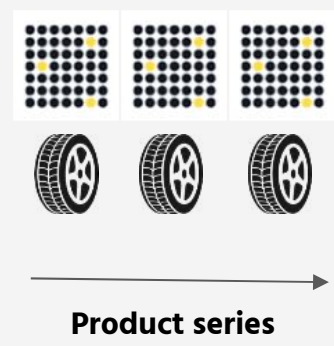
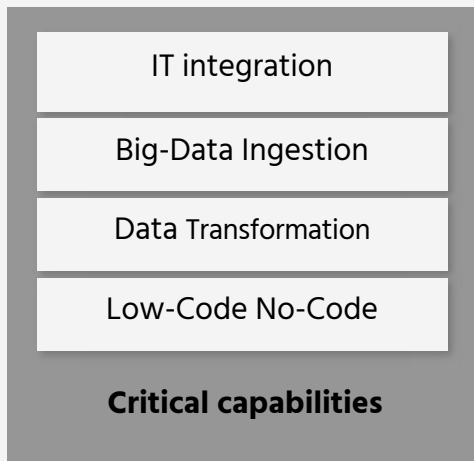
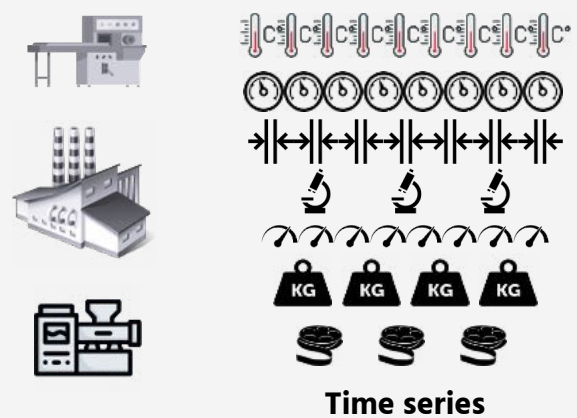
IoT

Thousands of devices, in **many locations**, delivering **homogeneous** data at a **low rate**



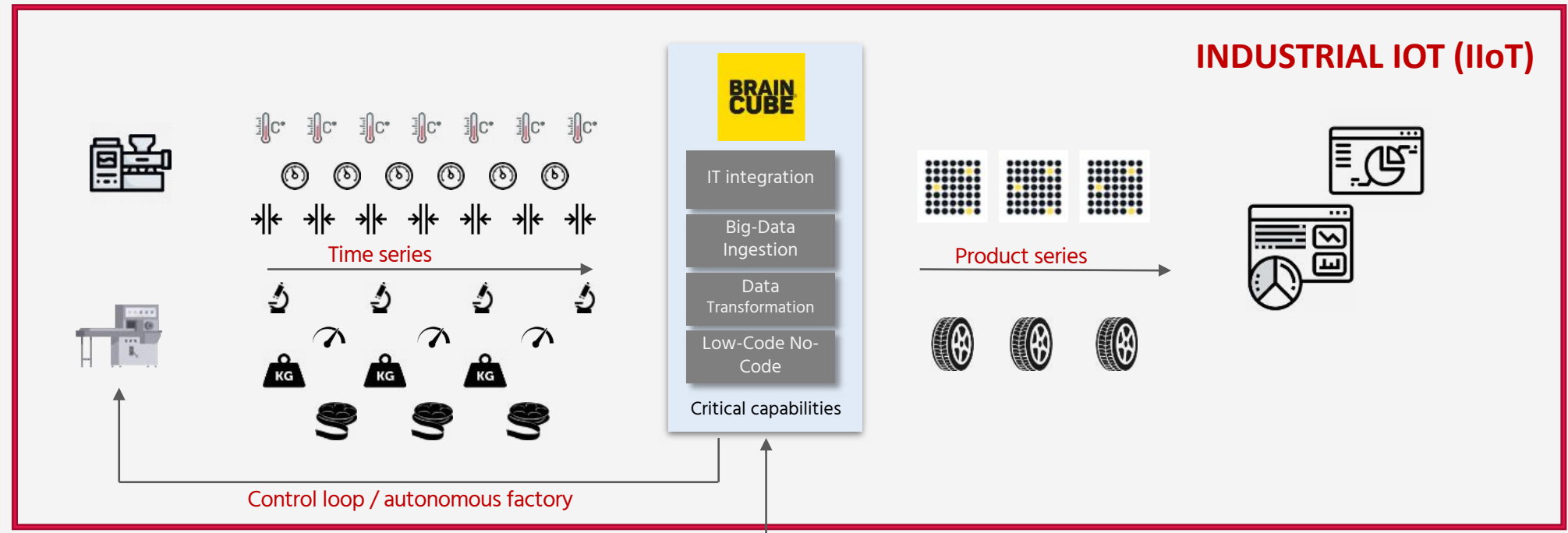
IIoT

Thousands of sensors, in a **single location**, delivering **heterogeneous** data at **high rate**



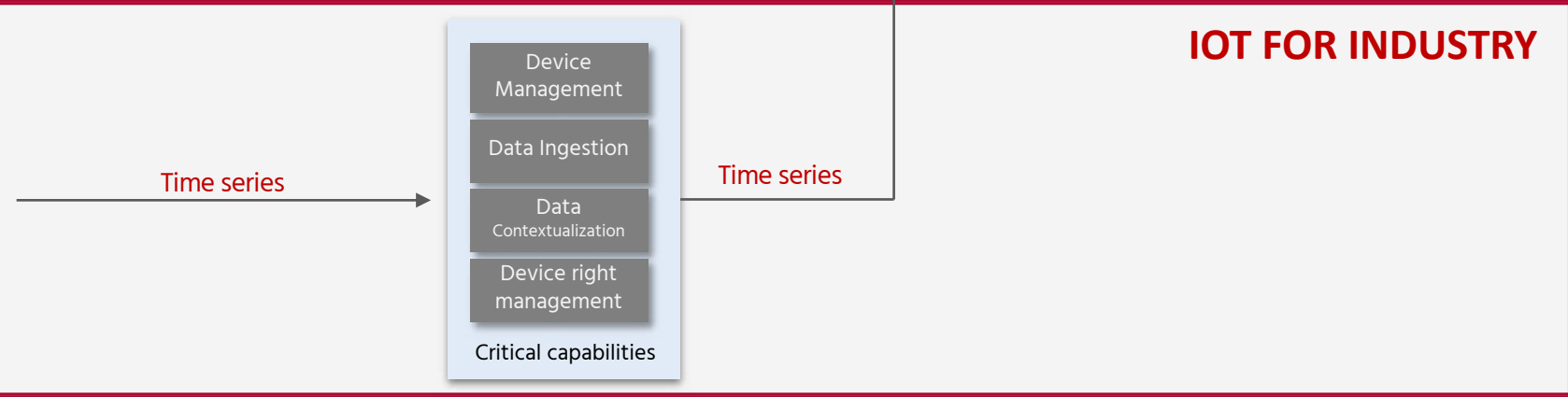
Both IIoT and IoT4i works together

0
 1
 1
 1
 1
 0
 0
 1
 1



1
 1
 1
 1

Environmental and additional Data



Author – Paul Pinault / Disk91.com

Agricultural IoT – optimize production, reduce inputs



- 1-years to 10 years autonomy
- No maintenance
- Accept aggressive environmental situations



- Run where the network never is.
- Low bandwidth data

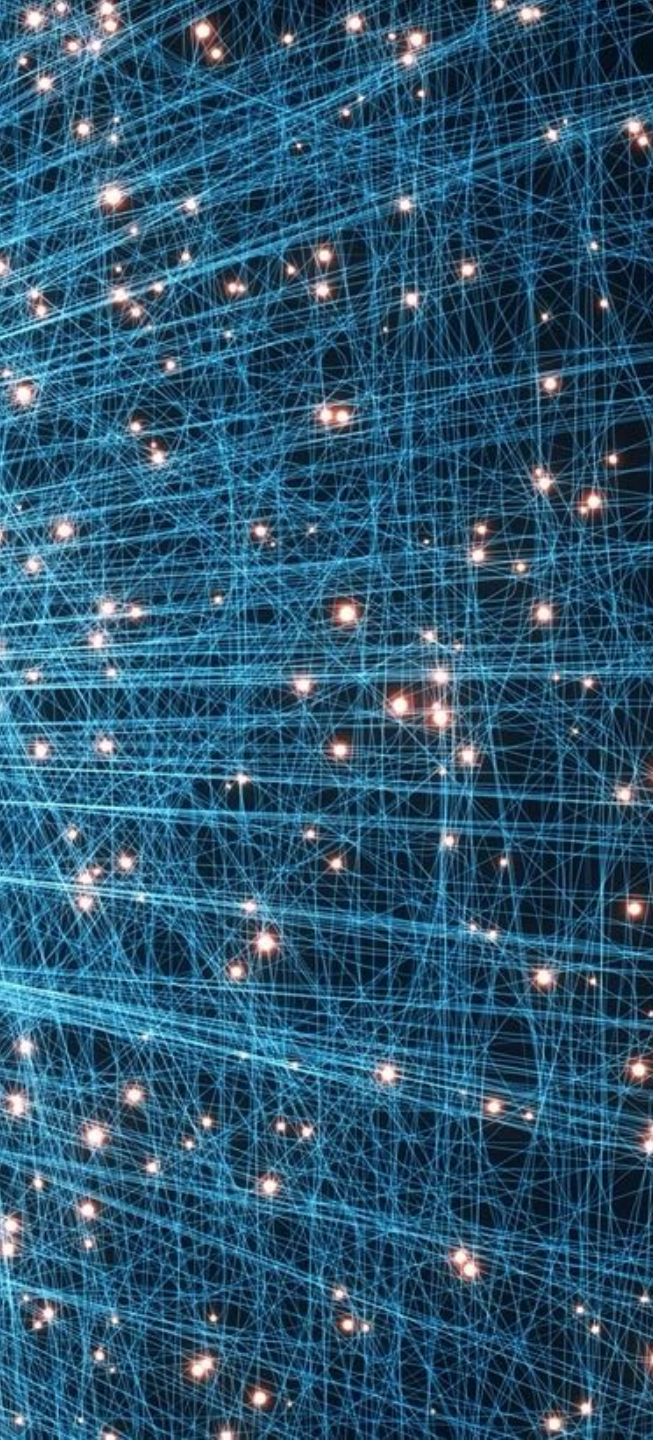


- Must be simple / low tech
- Massive data aggregation ready
- Subscription challenge vs investments



Network characteristics for

Agricultural IoT



CELULAR

Usually deployed far after cities, countryside will mostly rely on 2G / 4G technologies.

Allows when needed large data transfer



LoRaWAN

Allows to deploy private network at low cost.

Agricultural site coverage with 1-5 gateways only.

Reduced maintenance

Long Autonomy



Sigfox

No investment, public network can be extended locally.

No maintenance cost, subscription cost.

Long Autonomy
Ultra low-cost devices



Kinéis

Satellites
No investment, public network.

No maintenance cost, subscription cost.

Long Autonomy

Supply chain / Logistic IoT – optimize, track



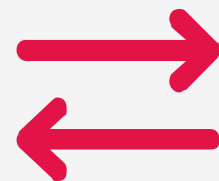
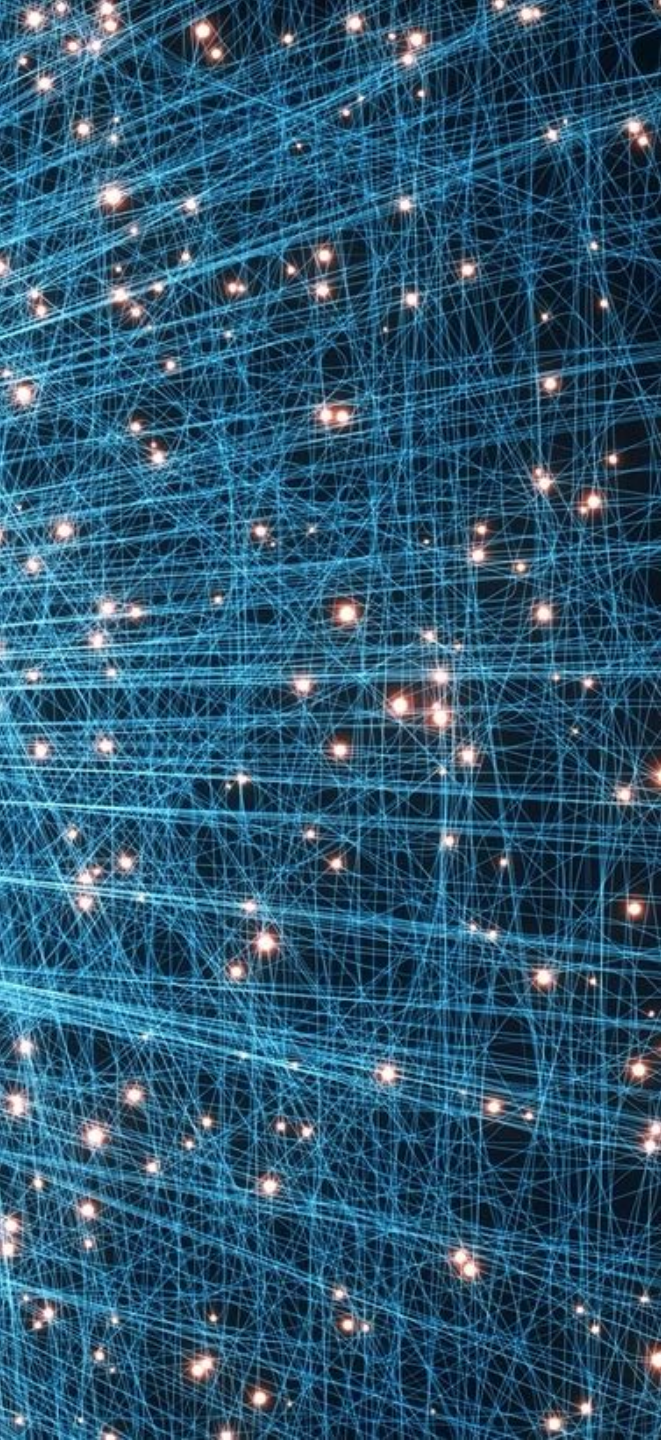
- 1-years to 3 years autonomy
- Low maintenance
- Low cost
- Vs Precision dilemma



- Nation-wide to world-wide
- Low bandwidth data



- Cost challenge
- Integration challenge
- Multiplicity of solution providers
- From the truck to the things.



Network characteristics for

Supply & Logistic IoT



CELULAR

Need world-wide coverage, well deployed networks.

4G, sometime 4G LTE-M with fallback.

Energy consuming but having a large historical footprint



Sigfox

The growing network covering many countries as a single one.

Simple to use. Low power consumption

Ultra Low Cost

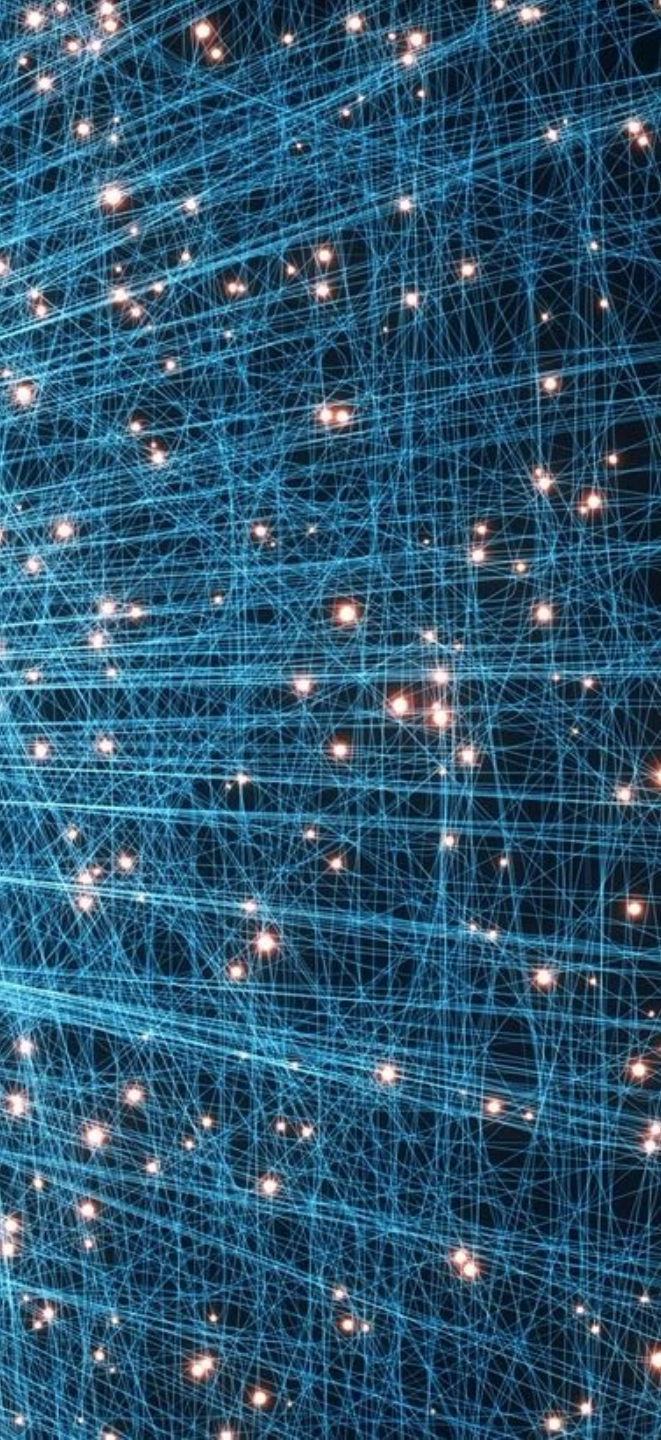


Kinéis

Satellites
No investment, public network.

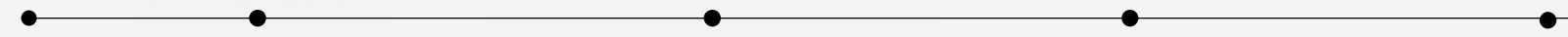
No maintenance cost, subscription cost.

Long Autonomy



Network characteristics for

Connected cars



4G

5G

For the next 5 to 10 years the networks will remain 4G in certain area.

With low latency the 5G will improve autonomous vehicle by connecting cars each others.

Let's make a short break

LEARNING AT THIS STEP



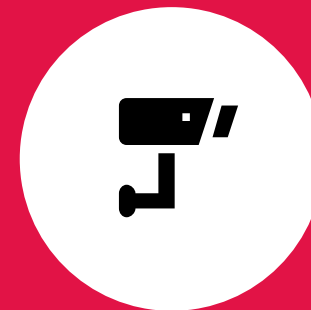
IoT has many faces

There is not one IoT but different domains where IoT applies with different targets, different constraints



Many technologies are covering these faces

To solve the different constraints, we have a large set of technologies. IoT revolution comes with the arrival with these technologies as enablers



Data access vary

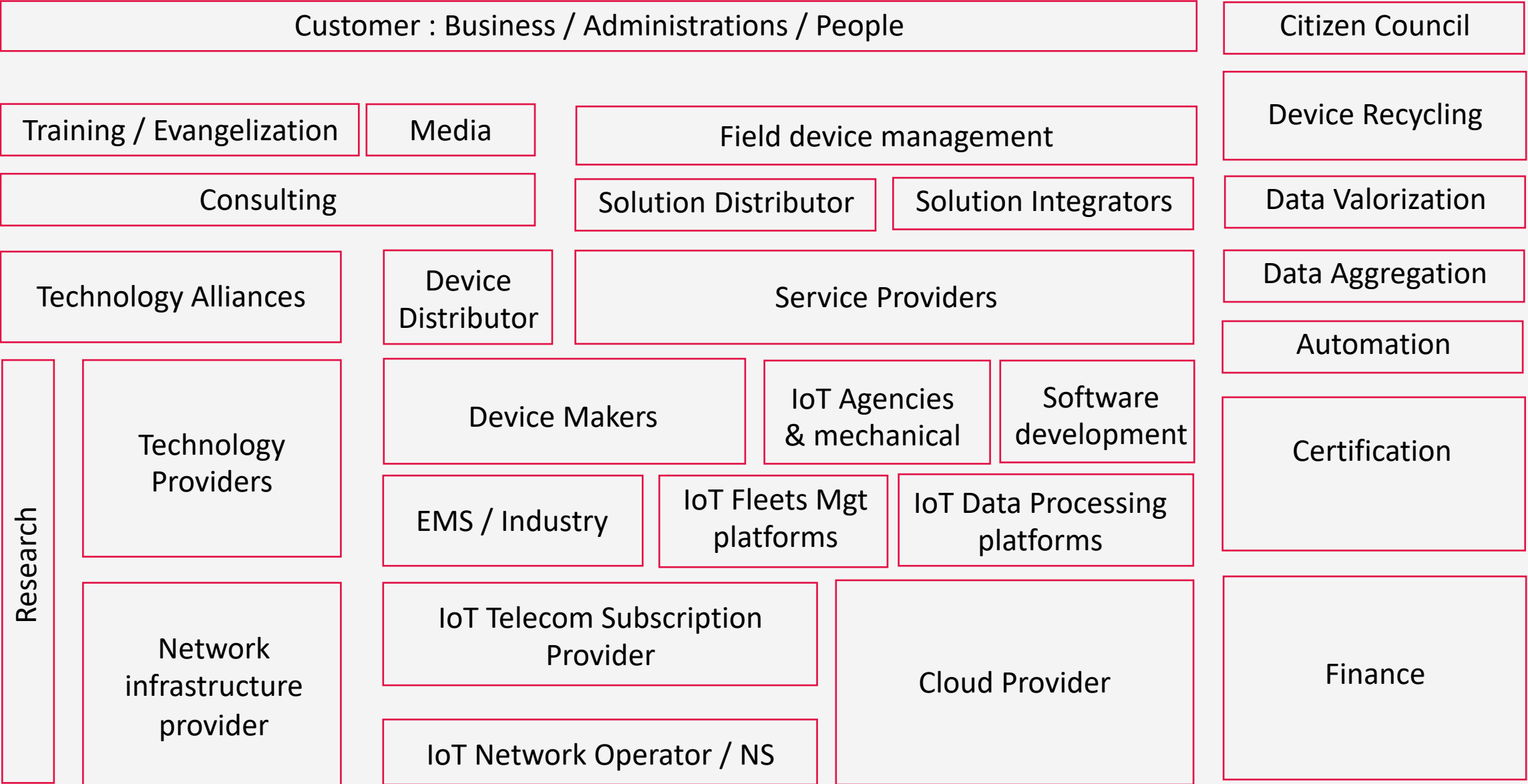
Depending on the execution context, data sensitivity vary and the ability to manipulate it of makes added value with massification vary.



The IoT Ecosystem is rich of many players with different roles in the value chain.



IoT's rich ecosystem overview



Technology Actors

They are creating the technologies enabling the innovation

Main domains:

- Telecom
- Energy
- Harvesting
- Silicon
- Protocols
- Encryption
- Sensors
- IA
- Platforms

Make the next generation of IoT technologies, low power, harvesting, batteries...
Like Sigfox, Saft , Universities...

Research

Technology Alliances

Define norms.
Like LoRaAlliance, Wize Aliance, DeWi

Technology Providers

Provide dedicated solution for IoT like low power MCU, radio chip, batteries, sensors, gateways ...
Like, ST Micro, Saft, Semtech, Bosh, Sigfox, Kerlink, RAK Wireless ...

Network infrastructure provider

Provide network infrastructure to support IoT communications. They are deploying the communication towers, the network radio equipment and maintain it. Like Sigfox, Objenious, TDF, Orange, SFR, Suez, Kineis, Lacuna Space, amazon...

Cloud Providers

Provide Hosting and processing power for IoT data and services.
Like Amazon, Azure, Google, Alibaba, OVH, be ys Cloud.

IoT Fleets Mgt platforms

Manage fleets of device, health monitoring, life-cycle, updates.. Like balena.io

IoT Data processing Pf

Provide Software solution to store and process IoT data. Like Aws, Azure, myDevices, Datacake, TheThings.io, Ubidot ...

Device life cycle

They are participating to the creation and production of the IoT devices, then to the maintenance and end-of-life management .

This is including the service ecosystem for developing HW / FW / SW for the IoT solutions.

Device Makers

Make devices for selling them as device, they are not providing service based on data produced by devices. Like Adeunis, Draguino

IoT Agencies

Make device's engineering for customers. Sell services not devices. Make electronic design and firmware design, Also mechanical design. Like Exotic Systems, Rtone ...

Software development

This category includes specialists of mobile applications and backend / frontend application for IoT. Like Sigfox IoT Agency, Openium, most of the consulting companies like Accenture, CGI ...

EMS / Industry

Produce devices, many actors like EMS producing boards, plastic injector producing enclosure, packaging production ...

Device Recycling

Manage the end of life for electronic devices.

Certification

Certify electronic systems for CE, FCC... regulation. Certify radio protocols and performance like for LoRaWan and Sigfox. Certify security, quality in the service process and data management.

Communication providers

They are providing network server and subscriptions for the devices

IoT Telecom Subscription Provider

Provide subscription on owned networks or networks owned by other company. Like Sigfox, Objenious, TheThingsIndustry, Helium, Soracom, Orange, SFR, ...

IoT Network Operator / NS

Provide network server, software on the physical telecom infrastructure where devices are registered and relaying device data to customer application. Like Helium, TheThingsNetwork, TheThingsIndustry, Sigfox, Objenious, Lorient, Actility, Helium-lot.eu ...

Automation

Provide services for automation / integration. Platform to send email, sms, hosting Mqtt broker ... like twilio, ifttt, HiveMQ ... It also includes iPaaS and Api Management solution used to expose data.

Device and Data commerce

**They are selling the IoT solutions and devices.
They can also just process data to create added value.**

Device Distributor

They sell IoT devices like any other electronic product. Like Darty, Leroy-Merlin, myDevices.

Service Providers

They sell Insights to customers with, usually, a subscription fee. The device is the way to provide the service. Like Flipr, IngeniousThings, Michelin DDI ...

Solution Distributor

Distribute existing solutions as B2B2B or B2B2C. Usually manage the customer relationship, sales, deploy, support.

Solution Integrators

Integrate existing IoT solution in company information system.

Field device management

Manage in field IoT device fleets, on large territories. Deployment, maintenance, upgrade, removal ...

Data Valorization

Buy existing IoT data to process them and create new added value. Company own IP for data processing algorithm but not capture IoT Data on it own.

Data Aggregation

Aggregate different IoT data in the same domain but from different solutions, including Open Data. Format them and sell access to them for data valorization.

IoT eco-system transformation

They are accelerating or slowing down the IoT transformation.

Consulting

They are pushing use-cases to industries and administration, expose the value creation for these solution. Support the industry and administration in the IoT transformation. Like KPMG, Accenture, CGI ...

Training / Evangelization

They are explaining the IoT transformation, usually to push the technology they develop. It also includes the universities training students on new technologies. Like Sigfox, LoRaAlliance, TheThingsConference, disk91.com

Media

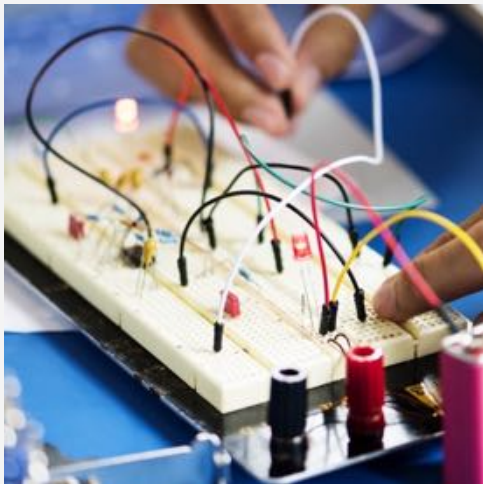
They mostly create IoT phantasm in the society mind for the best and the worst. They directly influence the IoT adoption.

Citizen Council

As a response of the media IoT phantasms, council of citizen impacts / influence the deployment and decision takers. They usually works for citizen privacy protection.

Finance

Startup ecosystem, on the early stage of every new technology and transformation need to be financed. On top of this, the transformation from a device-based business model (capex) to service-based business model (opex) needs financing supports for small size business.



What is an IoT project ? Main steps, technologies involved, associated investments



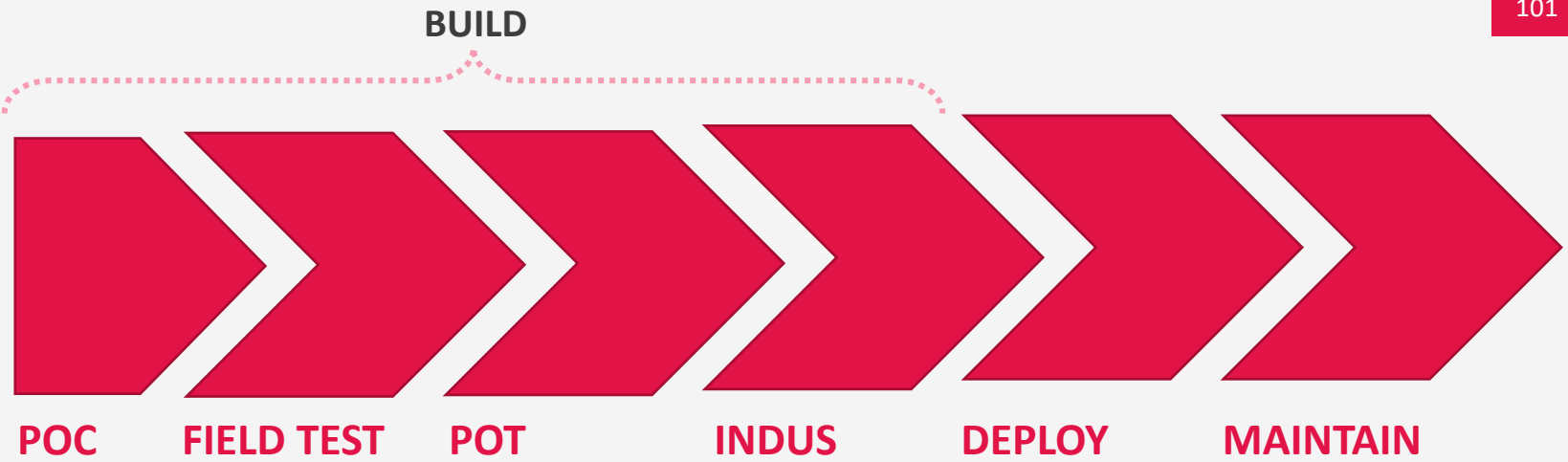
Typical IoT Project timeline

Successful IoT projects are the one getting the best Field experience in the early stages.

Do not make the large investment needed in the industrialization phase until making them.

18 Months – usual duration for an IoT build project

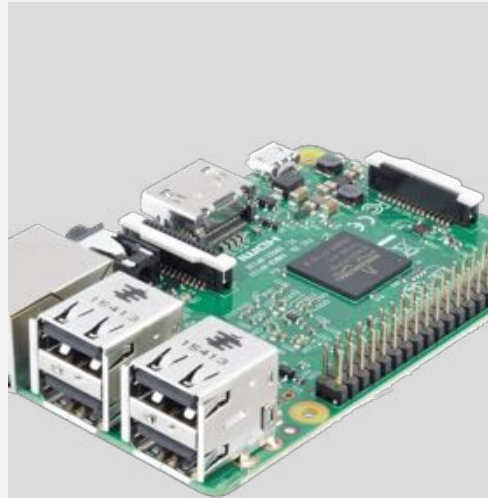
80 % Share of build investment spent in INDUS Phase



2-3 weeks timed-boxed

1 POC phase

Create a quick & dirty solution able to determine the main fields issues solution, get the first set of data and prove the business model ; imagine business model extension.
We are using out of the box building blocks.



AIM ON THE FASTEST

Autonomy, cost, size, design are not the problem to solve at this step. Use existing elements, buy/hack existing devices. Multiply sensors, use local storage if needed.



SELECT THE RIGHT NETWORK

Network will be a major field constraint impacting the business model. It's better but not mandatory to select the right one.



USE OF MARKET IOT PLATFORM

Do not invest on UI, Excel is good enough, but there are many IoT platform on the market you can connect your prototypes.



10-30 weeks

2 Field test

Deploy 20 to 100 POC devices on the field, in the real conditions, measuring the expected data + a maximum of environmental data. You need to be sure to understand the input impacting the business model.



ACCEPT TO LOST DEVICES

Any destroyed device is an opportunity to understand an unexpected situation. Ensure you have a diversity of context corresponding to the target situations.



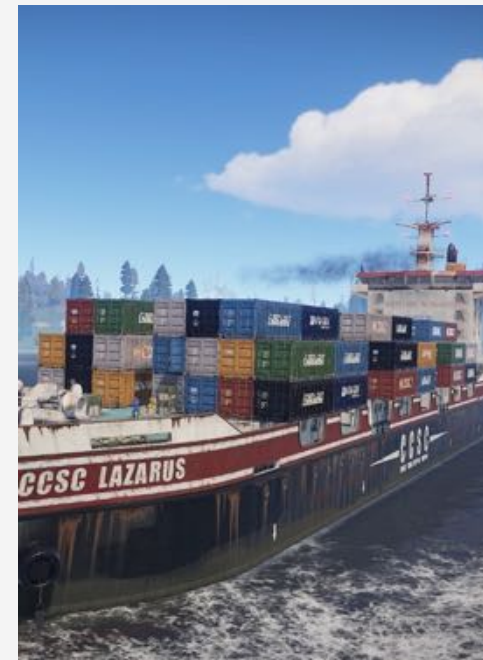
VERIFY YOU CHOICE VIABILITY

Identify reasons of communication loss. Analyze each of the situations.



AT-SCALE, BEYOND THE HORIZON

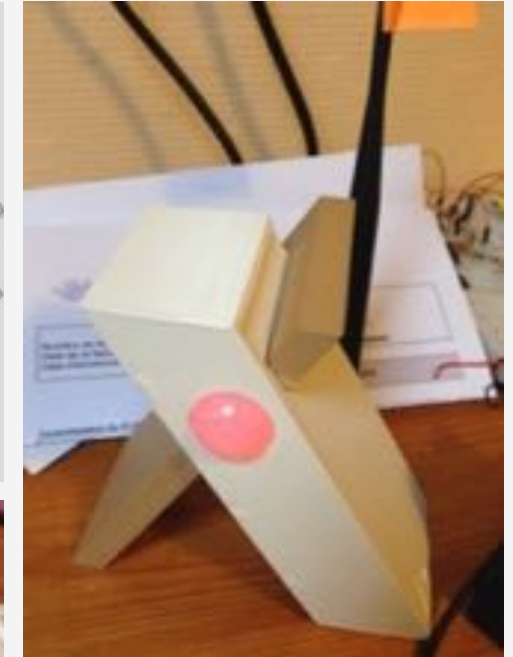
Any captured data is analyzed, imagine what you can get from at-scale data-set. Find the right frequency / energy / precision balance. Look at un-expected use and potential new business transformation of business models...



10-30 weeks

3 POT phase

Design a device with the targeted technologies, supporting the fields constraints, with the expected autonomy, cost compliant ... Automate the main identified Insight generation.



VERIFY TECHNICAL ASUMPTIONS

Small batch of devices, logging information and environmental information but like production expectation. Identify future production constraints and respect of fields constraints. Source different chip providers and start to negotiate price & volumes.



VERIFY YOUR CHOICE VIABILITY

Continue the test field, start negotiate the subscription with the network providers...



CONFIRM VALUE CREATION

With a larger historical set of data and a larger number of device, confirm your value proposal. Start looking at indirect market you could reached, start contacting potential customers.

30-80 weeks

4 INDUS phase

Create the solution: the product with a mass production capability, including test, packaging... Create the application and all what is needed to deploy and maintain the solution.



PRODUCE AT SCALE

Design the product for being made at scale. Electronic, mechanic, assembly, test automation, certifications, patents... This step requires a huge dose of engineering, with potential innovation.



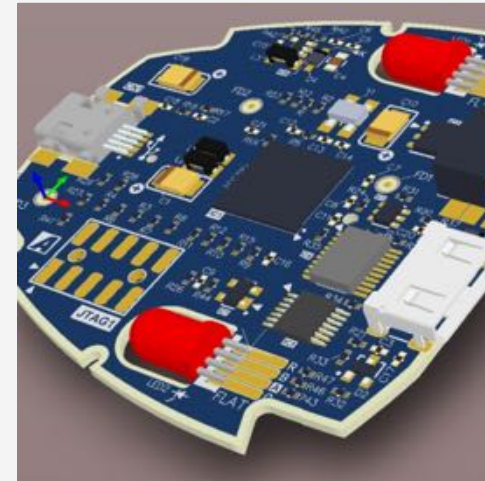
INTEGRATE WITH SERVICE PROVIDER

You need to automate the subscription process, subscription renewal and subscription cancellation



BUILD THE APPLICATIONS

You need to build the entire platform plus the different rendering applications. You can have Insight but also mobile application, websites ... This is mostly classical IT but many things need to be built. Do not forget to include device life-cycle management.

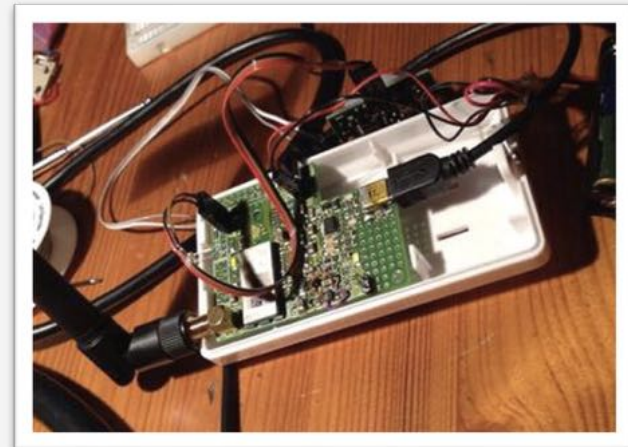


Application

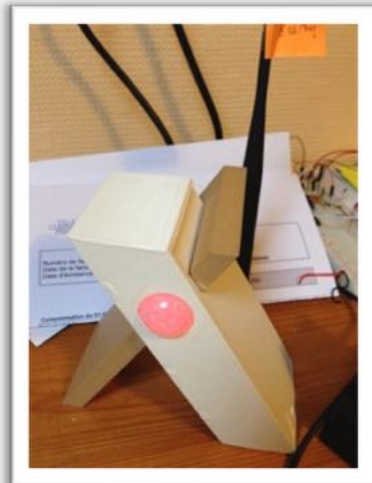
FROM POC TO DEPLOY



POC Raspberry PI with custom made shield for radio transmissions



POT Device with target technology & sensors



POT2 Device with target technology, sensors and target design approach



MYTEEPI

Industrialized product.
Ready for batch production
@ 1000 units

Pivot 1
Behavior is different
From global a platform to a
dedicated device

Pivot 2
Design is different
From a commodity to a
designed device

Evolution of a product from the POC to the DEPLOY

An IoT Project is a complex Project

It can be managed in an Agile approach to get deliverables more frequently, but never consider it as a simple IT project, it's much more complex. Complexity depends on:



DEPLOYMENT SCALE

Making 10 devices will not be the same as 1M



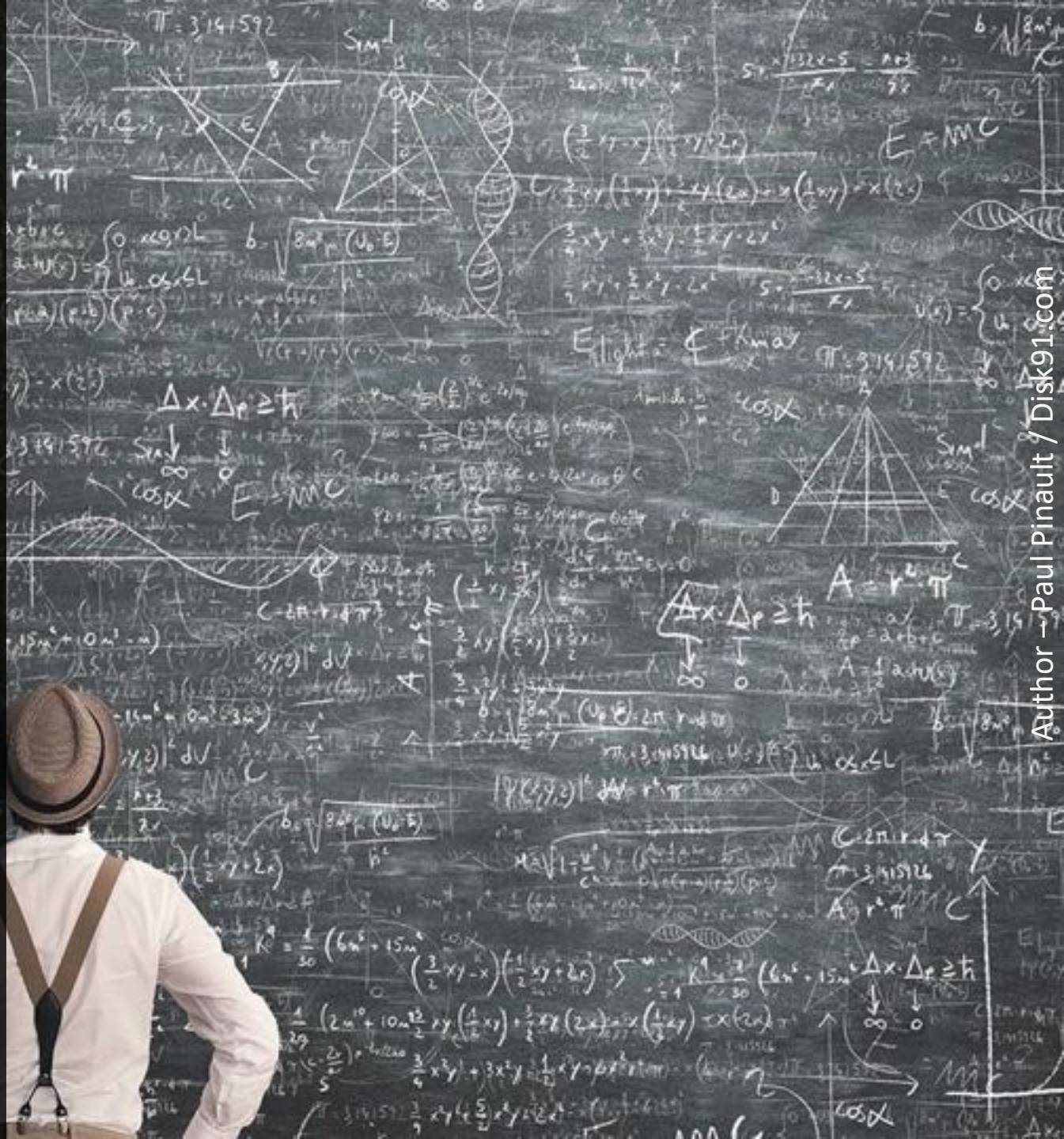
SIZE OF YOUR COMPANY

This is in relation with the risk level you accept to take and the investment you can support



THE GEOGRAPHICAL SCOPE

Hardware deployment requires certification, certifications are made per zones. Technology availability also differ per zone.

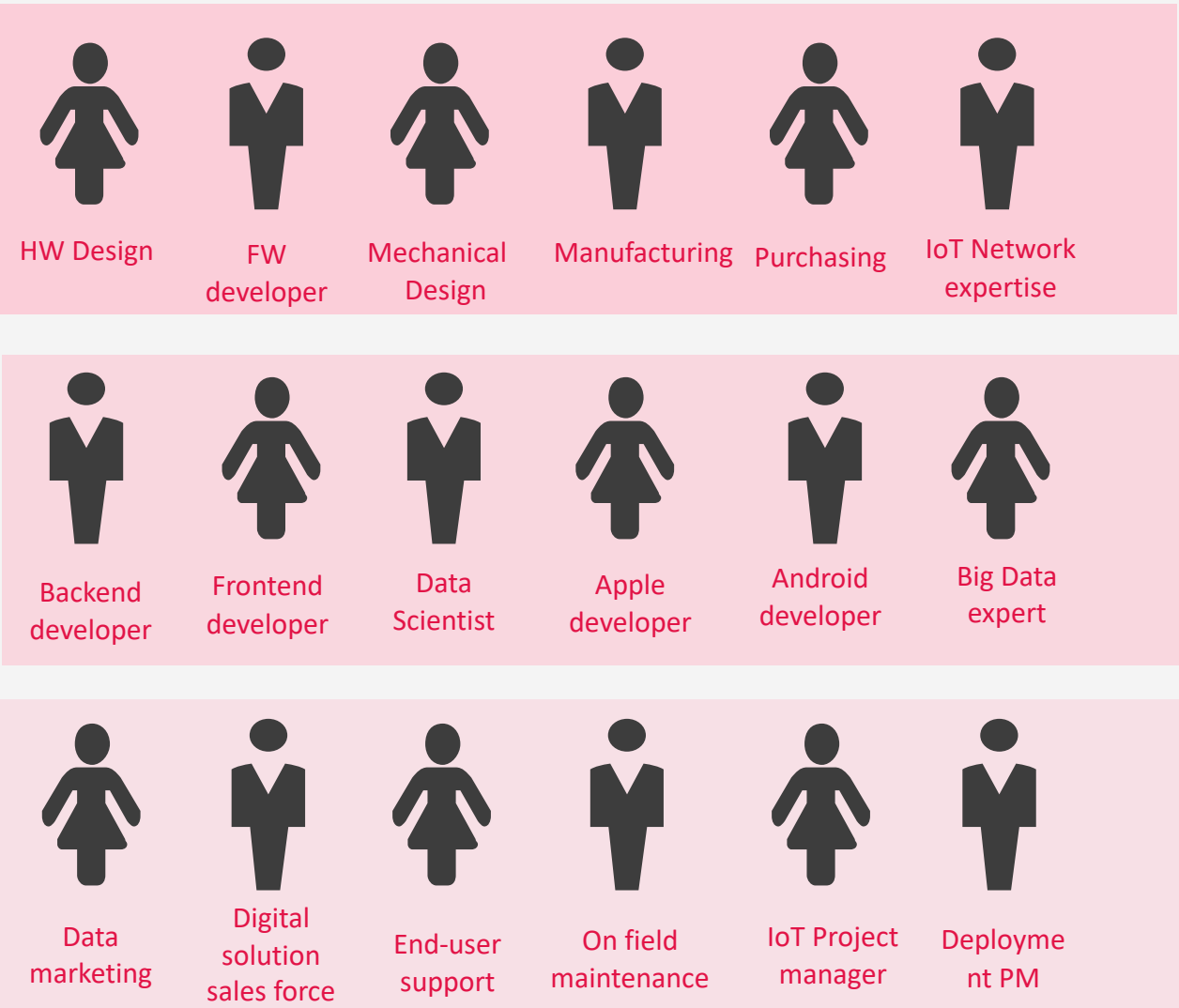


Typical IoT Project team

IoT requires a lot of different expertise You can't expect to find in your existing teams if you're not already an IoT company.

These skill are far away from the one you find in a furniture industry. This is a problem for the IoT transformation.

This problem is bigger than in the digital transformation.



All these expertise are rare and far enough apart that no one has more than 2

IoT is also a question of choice and compromises

Due to the physical world, hardware design and particularly IoT where size, autonomy and price are key elements, you need to make some compromises on your initial expectations otherwise, the experience is, you will never start your project.

All the directions on the right schema are antagonists



Let's make a short break

LEARNING AT THIS STEP



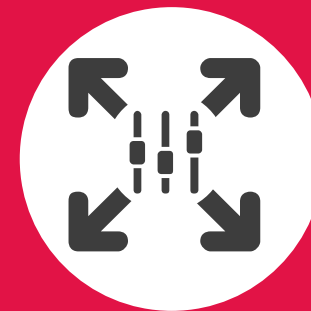
IoT projects are complex

You can make a PoC in a few week but you must not expect the project to be live in a month.



IoT projects needs rare skills

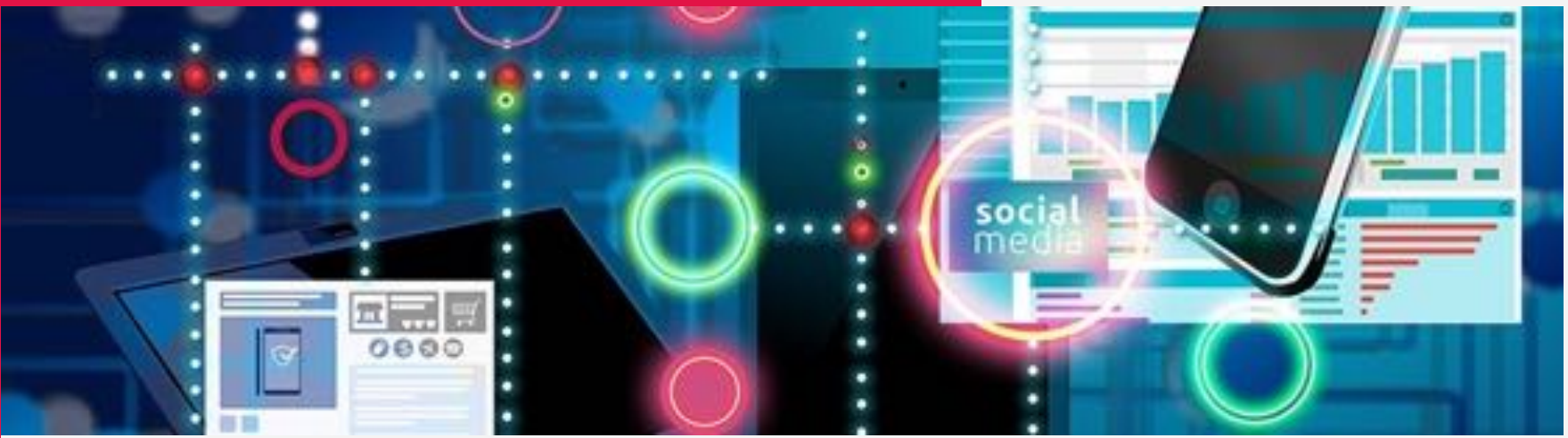
Many different rare skills are needed. This Is a reason why today most of IoT is tech oriented when it should address Things.



Compromises are necessary

There are so much constraints in an IoT project that you need to accept compromises. The key factor of success need to correctly be established at the early stages.

Marketing & communication IoT use-cases



Yes it is Digital content

Vinyl disk with additional content you can access through a Near Field Communication (NFC).

Create a new end-user experience, mix digital and analogical content and sound.

By adding an ID to any physical device and making it accessible with a Smartphone, you can create a new consumer experience.

It also works for restaurants, bar, hotel... make a quick & easy access to additional services in a simple way.

Business model : loyalty and premium services



PASSIV DEVICE

No maintenance,
no end-of-life. No
dara.



BASED ON NFC

NFC is just an ID
authenticating the
product.



BACKEND CONTENT

Extend the experience, protect
against copy. **What is the business
model (no extra revenue)?**

Amazon dash button

Place a re-ordering request just by pressing a single button. It has been stopped by Amazon, here are some of the reasons:

- Cost > 5€
- Complex to setup with a smart phone.
- Alexa could do it.

These issues are fixed by LPWAN and ultra-low-cost: you can imagine the product package automatically detecting its level and reordering by itself.

Amazon is deploying Sidewalk, such devices could be back that way.

Business model: commercial lead.



Low cost device

Cost supported by the brand.
Expose a brand



RELY ON BLUETOOTH

Complex setup with the smartphone



LEAD MANAGEMENT

Each of the click is generating an Amazon automatic order

Rover call to action

Rover sent a marketing campaign to 5000 consumers. The user was pushed to click a button to request a car test drive. The response rate has been 48% compared to the usual 5%.

The ecological impact is large vs the efficiency. You can detect the marketing content opening and interaction to place the right call at the right time and get a better conversion rate.

Business model: commercial lead.



Low cost device

As part of a global marketing costs



RELY ON SIGFOX

No settings, just work.
But subscription model is a problem currently



LEAD MANAGMENT

One shot operation. No long-term cost to support

Louis Vuitton connected luggage

Worldwide airport tracking service for your luggage. Expensive luggage = valuable content. Your customer pain: lost the luggage's content during travel.

Added services for customer. Mainly marketing than business in this case. With a string value you can sell it a high price to cover the long-term costs.

It's also a good way to know your customer habits. Have an app on his/her smartphone.

Business model: strengthening brand



Long Autonomy

Reduced
maintenance,
worldwide



RELY ON SIGFOX

No settings, just work.
But subscription



STRENGTHEN YOUR BRAND

It means you need to invest on your
apps & service. This is costly



Brand protection

A digital product comes with an application. You can make sure of the source of the digital product when in a purely physical product you can get a perfect copy requiring expertise.

As a brand, you can certify your product origin, your customer will be sure of the provenance. You can also force the copied application to be removed from app marketplaces because they are centralized. This is more difficult with manufactured product made in a country where you have no legal level to close the factories.

Business model: protect your brand and future revenues.



Long life duration

Because toys lifecycles are really long



BLUETOOTH

For smartphone integration



LOYALTY AND BRAND PROTECTION

Long life of application with no subscription model. Brand investment more than money making. High quality is required.

Contact tracing

In case of pandemic, IoT allows a massive contact tracing with a high level of privacy compared to cell-phone solutions.

IoT contact tracing can be massively deployed at low cost with no technological requirement compared to smartphone solutions.

The reliability of the radio measures is still the hard part with the associated battery autonomy.

In term of data for statistics and propagation model it is really value added.

Business model: state investment / PIB protection



LONG AUTONOMY

Reduced
maintenance, no
pre-requisites



SIGFOX

Cost, autonomy, no
setup, global



AT SCALE, SECURED...

Here the platform criticality is high in
term of scalability and data sensitivity
for the states

Count strike participant

Number of participants is an important question and the responses from the different sides are usually totally different. Numbers can help to get the truth.

Smartphone density is a good way to count people. The cell tower around and all along the demonstration are capturing the pic of people and the difference with a normal day or a couple of hour before gives a good estimate of the crowd size.

Business model: side use of existing data



**DOES NOT
GET NOTICED**

Meta-data information captured for other purpose



3GPP

Mainly deployed technology



INSIGHT ONLY

This is just insight based on data captured for another service.

Identify, count traffic jam

There are many ways to measure it, on of them is to measure the density of smartphone in a cell-tower area and to measure the time one same smart-phone stays registered to the same cell-tower. Basically its velocity.

This is another example of what we can do with metadata coming from the smartphone networks.

Business model: side use of existing data



**DOES NOT
GET NOTICED**

Meta-data information captured for other purpose



3GPP

Mainly deployed technology



INSIGHT ONLY

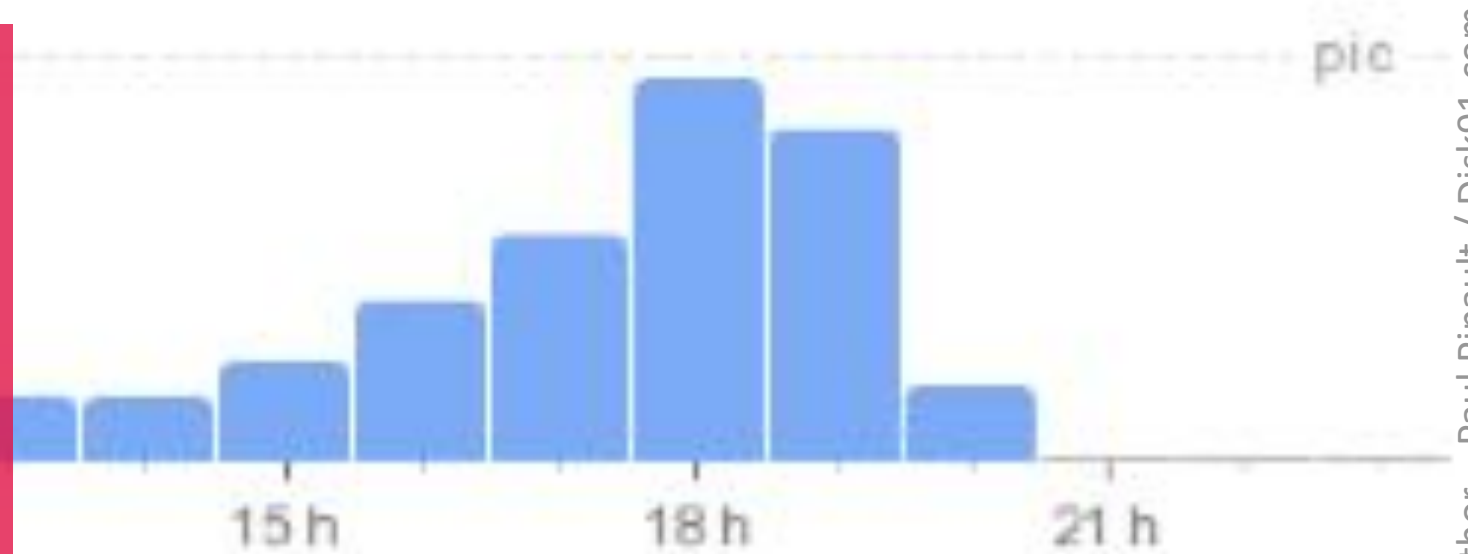
This is just insight based on data captured for another service.

Shop, museum frequentation

This information you can easily obtain, in real time, comes from the smartphone you have in your pocket. Any of you is a bit generating the frequentation reports.

This is a highly valuable information for business size, growth estimation, location value, even fiscal control.

Business model: Insights generation



DOES NOT GET NOTICED

Meta-data information captured for other purpose



3GPP

Mainly deployed technology



INSIGHT ONLY

This is just insight based on data captured for another service. And integrated in multiple services or studies.

Pollutions data

Measure the pollution, accessing to reliable data is a key element to act and control.

There are so many different type of pollution and getting a measure is expensive, so we have not a lot of sensors deployed.

Year after years, we see lower and lower cost sensors. The ability of the crowd to deployed sensors will make transparency higher. It will also improve the data quality and reduce the ability to bypass the rules.

Business model: making a better world



LOW COST

To be able to be crowd sourced or deployed at scale



ANY

Depends of the type of device

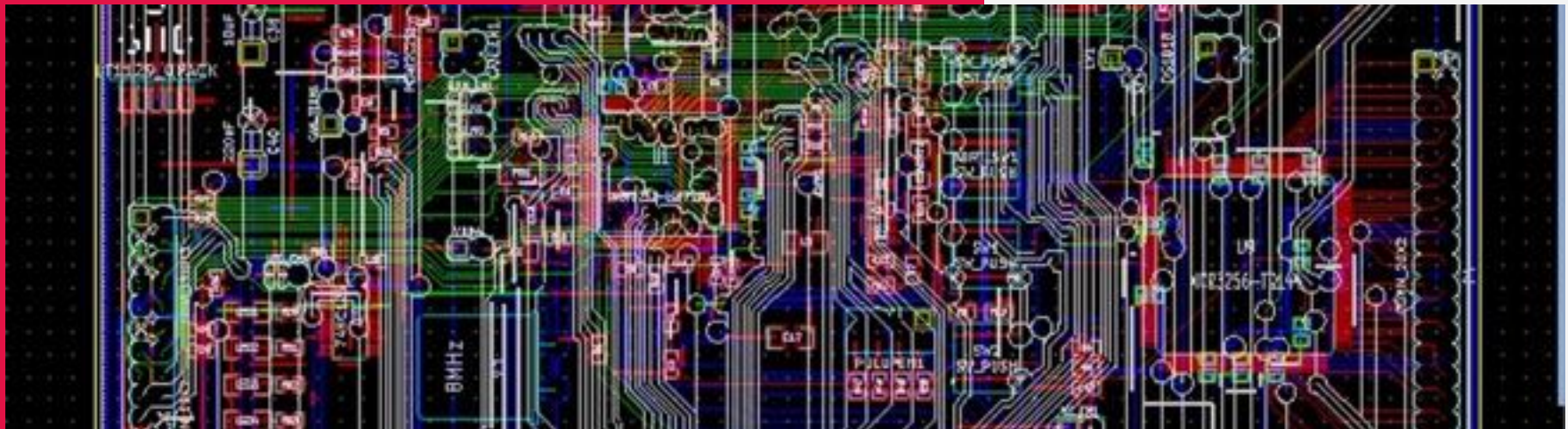


OPEN DATA

Allows anyone to access these data and use them for make change happen.



What are the main technologies in use to make the devices ?





POC Phase – Raspberry PI



Raspberry PI micro-computers are powerful computers:

- 4 core @ 1.5Ghz
- 2GB to 8GB MEMORY
- WiFi, Bluetooth, Ethernet

But low-cost: 50€

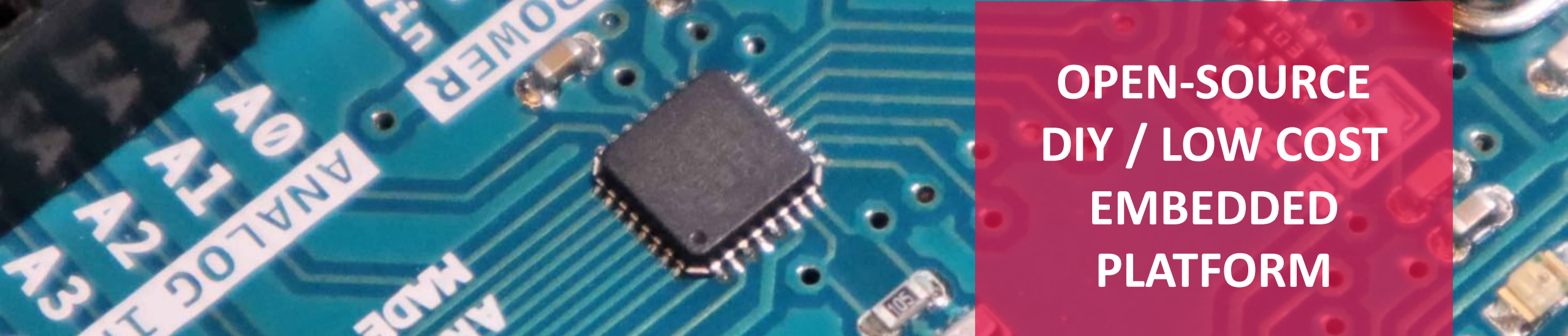
They are offering an environment to execute high level programming languages like C, Java, Ruby, Go, Perl, Python... with the ability to connected sensors.

They are not power efficient, but you can run them on batteries for day to weeks.



Device technologies

POC Phase – Arduino



**OPEN-SOURCE
DIY / LOW COST
EMBEDDED
PLATFORM**

Arduino are accessible low-cost & low-power MCU:

- 1 core @ 16-32Mhz
- 2KB to 20KB MEMORY
- SERIAL PORT

But low-cost: 5€

Thanks to the large ecosystem you can make quick & dirty devices having a long autonomy on batteries (month to years) for a reduced unit price.

Many additional shields and compatible boards are available on the market to avoid electronic design in POC.



Device technologies

POC Phase – Best design = no design

The best hardware choice for POC is when you make no hardware



There are plenty of existing devices on the market, basically around 3000-5000 different solutions you can buy and use out-of-the box.

For a PoC phase by using an existing device you save the design time and avoid the risk of field test bad experience due to your inexperience. Standard developers will be more familiar with device API than hardware developments.

Often, the entire IoT solution can be built on already existing devices ! That's the best choice for investment, time to market and risk taken.



Device technologies

POC/POT Phase – 3d design



3D printing and IoT POC and POT phase really works together. For making sample of the device mechanical design as for adapting a packaging to place the electronic circuits, 3D printer solve many IoT designer problems.

This technology is now accessible for less 500€. The main difficulty is to get your engineers able to design what they need of what the project expect.



Competencies for POC Phases – you can rely on IS/IT teams

A corporate software team can manage a POC phase, even with a reduced hardware experience with the listed technology. They mostly need to get fun with a such project and to have a Hacker mindset.

Having the internal IS team conducting the POC is best. But they need to stop after and let experts (hardware team) conduct the rest of the phases.



Device technologies

POT – INDUS PHASES



**A PLACE OF
EXPERTIZE**

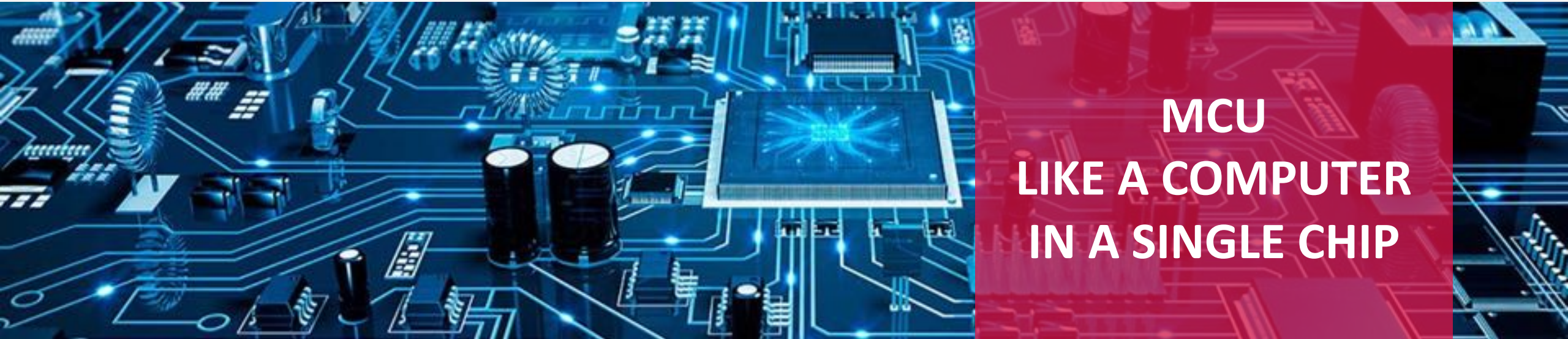
POT and INDUS phase are requiring expertise and a complex work of engineering. If your business is IoT solution, you need to have this team. If IoT is just a solution for improving your regular business, you can rely on an external team. Make sure your have real expert of IoT and not simply a

standard electronic design house. IoT is not M2M, there are power consumption, network expertise and IT integration requiring specific knowledge and experience to be successful.



Device technologies

POT – INDUS PHASES - Technologies



**MCU
LIKE A COMPUTER
IN A SINGLE CHIP**

IoT Brain is usually a Micro-controller: a single chip containing all what a complete computer have: CPU, memory, storage, I/O ports.

The power of the MCU can exactly fit your device needs and cost only what is needed. Price starts from \$0.10 and is

usually around \$2-\$4.

Therefore an electronic design is dedicated to only 1 specific use: each of the components are selected to fit exactly the specific device needs. It reduces the final device cost.



Device technologies

POT – INDUS PHASES - Technologies



COMMUNICATION MODULE/CIRCUIT

Second critical component of an IoT device, the communication circuit. It can be:

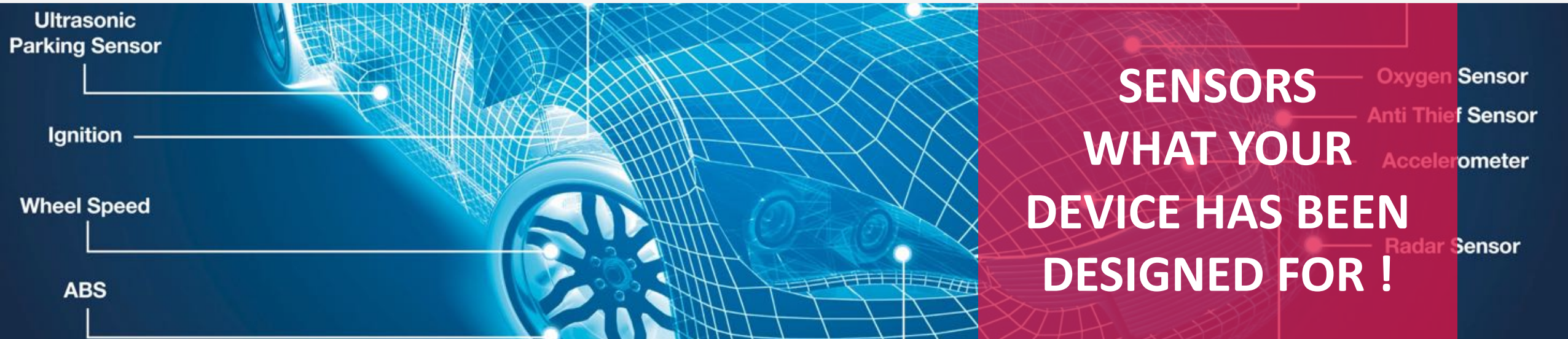
- a module, all in one solution, including communication protocol, easy to use, already certified but more expensive (\$3-\$15)
- A SiP or SoC, they are module made a different ways,

more compact but equivalent.

- A transceiver, this is the low-level radio component, the unit price can be from \$0,1 to \$2 but you need a larger investment for the associated engineering.

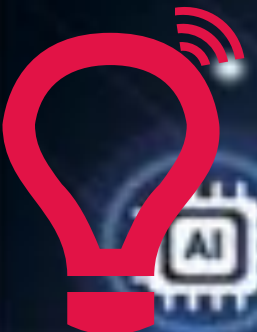
Device technologies

POT – INDUS PHASES – Technologies



There are sensors available to get most of the environmental data. Each sensor capture one data. Sometime 2 or 3 when they are related. Each sensor is a dedicated circuit with different characteristics in terms of precision, power consumption,

price. Sensors can be the main cause of end-device cost, this domain is also moving fast with edge computing and IA inside the sensors.



RISING IoT TECHNOLOGIES

EDGE COMPUTING AND NEURAL NETWORK (available)

More and more sensors includes neural networks. Optimized algorithm for IoT exists.

ULTRA LOW-COST (available)

Ability to make devices for a final price of \$1 - \$2. This is the enabler of IoT at scale with fleets of devices over 1M.

ULTRA LOW-POWER (to be)

Ability to make devices powered by the radiofrequency available locally. Consuming only picowatt, without chemistry.

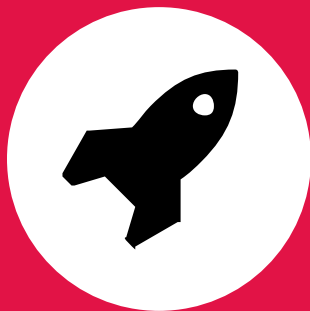
Let's make a short break

LEARNING AT THIS STEP



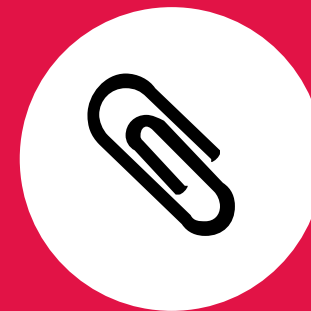
An IS team can manage an IoT POC

Thanks to the use of common technologies and existing products available on the market



POT and INDUS require expertise

Something you can avoid by using product already existing on the market. Otherwise, build your team or find IoT contractors

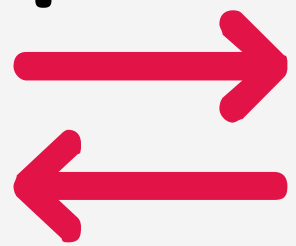


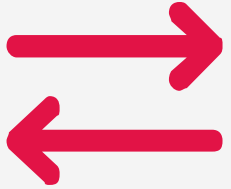
IoT device is an optimized solution

IoT design is a good design when it perfectly fit with the expected behavior. It means it is dedicated to that specific use-case.



What are the main technologies in IoT communications ?





Communication technologies

For human attached IoT



**LOW POWER
SHORT RANGE
COMMUNICATION**

Frequency: **2.4 -GHz**
Tx power: **8dBm / 10mW**
Pic current: **16,5mA**
Coverage: **15m-30m**
Throughput: **1Mb**
Chip price: **1.5€ - 3.5€**
Duty Cycle : **100%**

Rq: v5 can go to 100mW / 300m outdoor

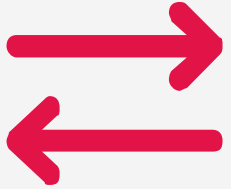
Author – Paul Pinault / Disk91.com

Bluetooth is equipping all modern smartphone and devices can use the Smartphone connections to reach Internet. That way the communication cost seems to be free for the consumers.

Bluetooth can also be used for Smart Home and Smart

Building with long range version of thanks to meshed networks.

You need to know Bluetooth background communications with smartphone is complex to make working and diversity of smartphone is a big issue for Bluetooth IoT designs.



Communication technologies

For home automation



ZigBee®

**LOW POWER
SHORT RANGE
COMMUNICATION**

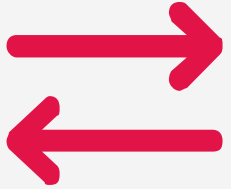
Frequency: **2.4 -GHz**
Tx power: **0dBm / 1mW**
Pic current: **23 mA**
Coverage: **100m / 30m**
Throughput: **250KBps**
Chip price: **5€**
Duty Cycle : **100%**

Rq: 100mW version exists for larger coverage

Author – Paul Pinault / Disk91.com

Zigbee and its competitor Z-Wave has been leader in smart home domain. They are not integrated into smartphone and need to have a Gateway to propagate the data to Internet and the central servers. This extra cost limit the application domains, mostly to smart home. Industrial domains also

makes sense.
Zigbee also supports Meshed networks to extends the coverage.
Zigbee technical name : 802.15.4



Communication technologies

For home & Industry big devices



**HIGH-POWER
SHORT-RANGE
COMMUNICATION**

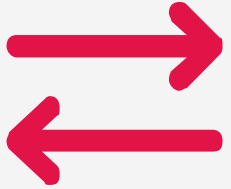
Frequency: **2.4 –GHz** (5GHz)
Tx power: **20dBm / 100mW**
Pic current: **300 mA**
Coverage: **30m**
Throughput: **11Mbps (IoT)**
Chip price: **1,5€**
Duty Cycle : **100%**

Rq: 802.11ah (HaLow) has been designed for IoT and operate sub-giga. But it is not really deployed yet.

WiFi have the advantage to be well deployed at Home and in the Industries & services. It have different negative points limiting its usage for IoT.

- The setup complexity
- The pic consumption over 100mA impacting the battery

- choice.
- The power consumption requiring large battery charge and short autonomy.
- WiFi requires a local gateway (access point), to communicate to Internet where the backend servers are.



Communication technologies

For any low speed IoT context



**LOW-POWER,
WIDE-RANGE
COMMUNICATION**

- Frequency: **868Mhz**
915MHz
2.4GHz
- Tx power: **14dBm / 25mW**
20dBm / 100mW
- Pic current: **30mA / 120mA**
- Coverage: **500m - 10km**
- Throughput: **5,6Kbps**
- Chip price: **2€**
- Duty Cycle: **1%-100%**

LoRa is a point to point radio communication solution allowing wide range coverage. Indoor application, device to device are offering around 500m coverage when outdoor usage will reach 10km to 15km. LoRa needs to be connected to a gateway to access Internet and backend service.

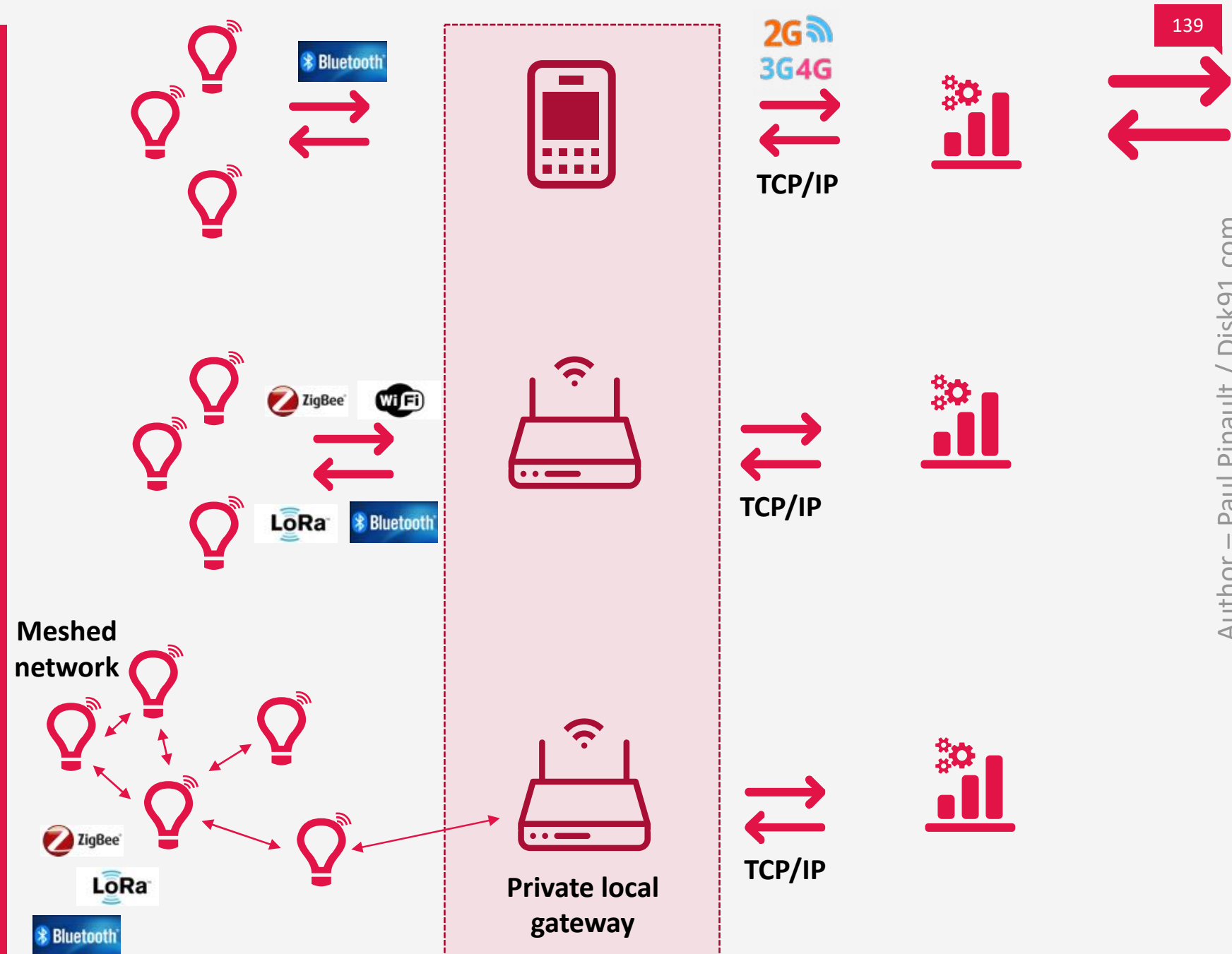
LoRa is used in different smart home solutions, speed, bandwidth, power consumption can be adapted regarding the use-cases.

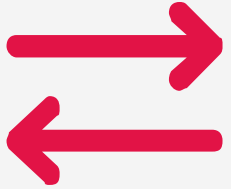
We see some meshed implementation of LoRa rising, allowing to cover cities with crowd sourced network.

Point to point IoT communications architectures

All the previously seen technologies are not TCP/IP based and able to communicate on Internet.

So we have some common architecture related to these technologies where a locally deployed gateway allow to translate the communications to TCP/IP to interact with the solution platform.





Communication technologies

For autonomous short autonomy IoT



GSM UMTS LTE

**HIGH POWER
HIGH SPEED
LONG RANGE
COMMUNICATION**

Frequency: **700MHz – 3.7GHz**

Tx power:
 2G: **33dBm / 2W**
 4G: **43dBm / 20W**
 3G/4G EU: **24dBm / 0.25W**

Pic current: **250mA-2,5A**

Coverage: **5km – 100km**

Throughput: **1Gb**

Chip price: **3€ - 20€**

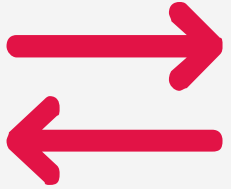
Duty Cycle: **100%**

Technologies from 3GPP consortium are common when you have externally powered device or the ability to recharge the device on regular basis.

This technology allows large amount of data transfer with a global worldwide coverage. There is no usage restriction basically.

The most complex part is to manage the subscription and the SIM or eSIM card with NVNO, Multi-operators, dynamic subscription...

For IoT design, battery cost and module cost will impact the business model with limited value creation.



Communication technologies

For autonomous static IoT with IP



**“LOW” POWER
HIGH SPEED
LONG RANGE
COMMUNICATION**

- Frequency: **700MHz – 2.6GHz**
- Tx power: **23dBm / 0.20W**
- Pic current: **250mA**
- Coverage: **5km**
- Throughput: **4Mb**
- Chip price: **10€**
- Duty Cycle : **100%**

CAT-M0 / CAT-M1 / CAT-M2

LTE-M is a low power solution for LTE technologies. It has been added in the 4G and it will be improved in the coming 5G.

Basically it allows a device to deep-sleep for a long period of time, then resume quickly on the network for short communications. It works well until the device move out

from the network cell.

LTE-M can be deployed where 4G is, not all country currently support it but it the easier to find worldwide.

Fallback to 4G/3G is recommended. Expected energy savings are uncertain.



3GPP rely on SIM card authentication

Sim and subscriptions management create a certain complexity

Sim cards are required to authenticate the device on the network and allow communication.

Sim card belongs to one network operator
1 operator = 1 sim

You need multiple if you want to support local communication instead of roaming. This is possible with eSIM and the ability to upload new SIM from a “technical” operator.

You can also use MVNO (Mobile Virtual Network Operator) managing the roaming negotiation for you and proposing global SIM.

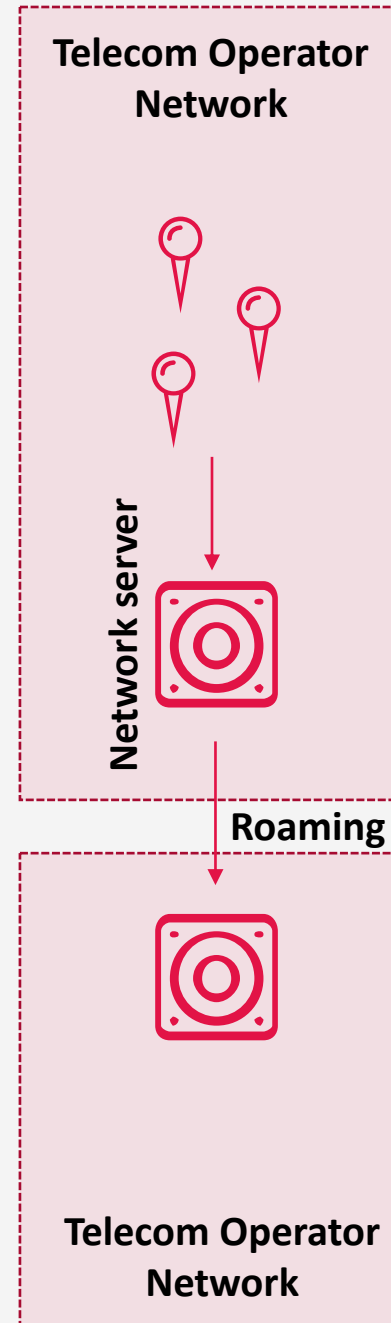
3GPP classical solutions are IP based

The device can directly communicate over TCP/IP. IoT subscription will sometime require a public IP attribution for a direct communication with the device.

These technical solution also simplify device-to-device communication and massive downlink.



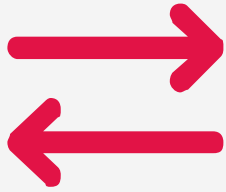
2G
3G4G
TCP/IP

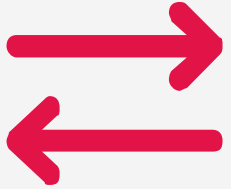


TCP/IP



TCP/IP





Communication technologies

LPWAN - 3GPP Low Power



**LOW POWER
MEDIUM SPEED
LONG RANGE
COMMUNICATION**

Frequency: **800MHz – 1.8GHz**
Tx power: **23dBm / 0.20W**
Pic current: **250mA**
Coverage: **10km**
Throughput: **160Kb**
Chip price: **5€**
Duty Cycle : **100%**

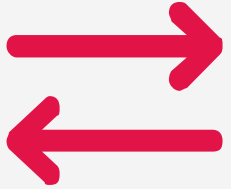
CAT-NB1 / CAT-NB2

NB-IoT is a low power solution for LTE technologies. It has been added in the 4G and it will be improved in the coming 5G.

NB-IoT is different than LTE technologies and simplify it. This allows to have simplified hardware with a lower cost and

lower power consumption. The number of NB-IoT networks, worldwide, is still low but this is really promising. The main issue is the roaming between operators for devices moving out of the operator coverage.

Coverage is directly related to 4G coverage. A sim is needed.



Communication technologies

LPWAN – For deep IoT



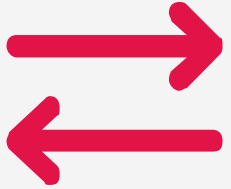
**LOW POWER
LOW SPEED
LONG RANGE
SECURED
COMMUNICATION**

Frequency: **169MHz**
Tx power: **27dBm / 0.5W**
Pic current: **500mA**
Coverage: **50km**
Throughput: **2.4-6.4Kbps**
Chip price: **5€**
Duty Cycle : **10%**

Last technology rising on the LPWAN area, Wize has been pushed by Suez and GRDF to support the water and gaz counters telemetry. For this reason a particular attention has been made on communication encryption. The 169MHz choice made this network really fitting with deep indoor

communication. The coverage is limited to France, Spain, Portugal, Italie, UK, Moroco, Algeria but the real coverage out of main cities is currently unclear.

The technology is new, the ecosystem still limited, this could be promizing for smart city & smart building.



Communication technologies

LPWAN – Private IoT networks



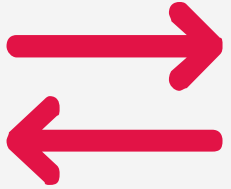
**LOW POWER
LOW SPEED
LONG RANGE
COMMUNICATION**

Frequency: **868Mhz
915MHz
2.4GHz**
Tx power: **14dBm / 25mW
20dBm / 100mW**
Pic current: **30mA / 120mA**
Coverage: **10km**
Throughput: **5,6Kbps**
Chip price: **5€**
Duty Cycle : **1%**

LoRaWAN is a network implementation of LoRa technology. It can be used with public and private networks. Public(nation wide) deployments are really limited over the world and the main use concerns private deployment. The network cost is low (gateways starts at 70€). Some crowdsourced networks like TTN or Helium also complete

the public offering. France have 2 LoRaWan public networks with nationwide coverage. This is an exception.

It is the only LPWAN you can use without a subscription business mode. The complex software stack requires a strong MCU.



Communication technologies

LPWAN – Global worldwide network



**LOW POWER
LOW SPEED
LONG RANGE
COMMUNICATION**

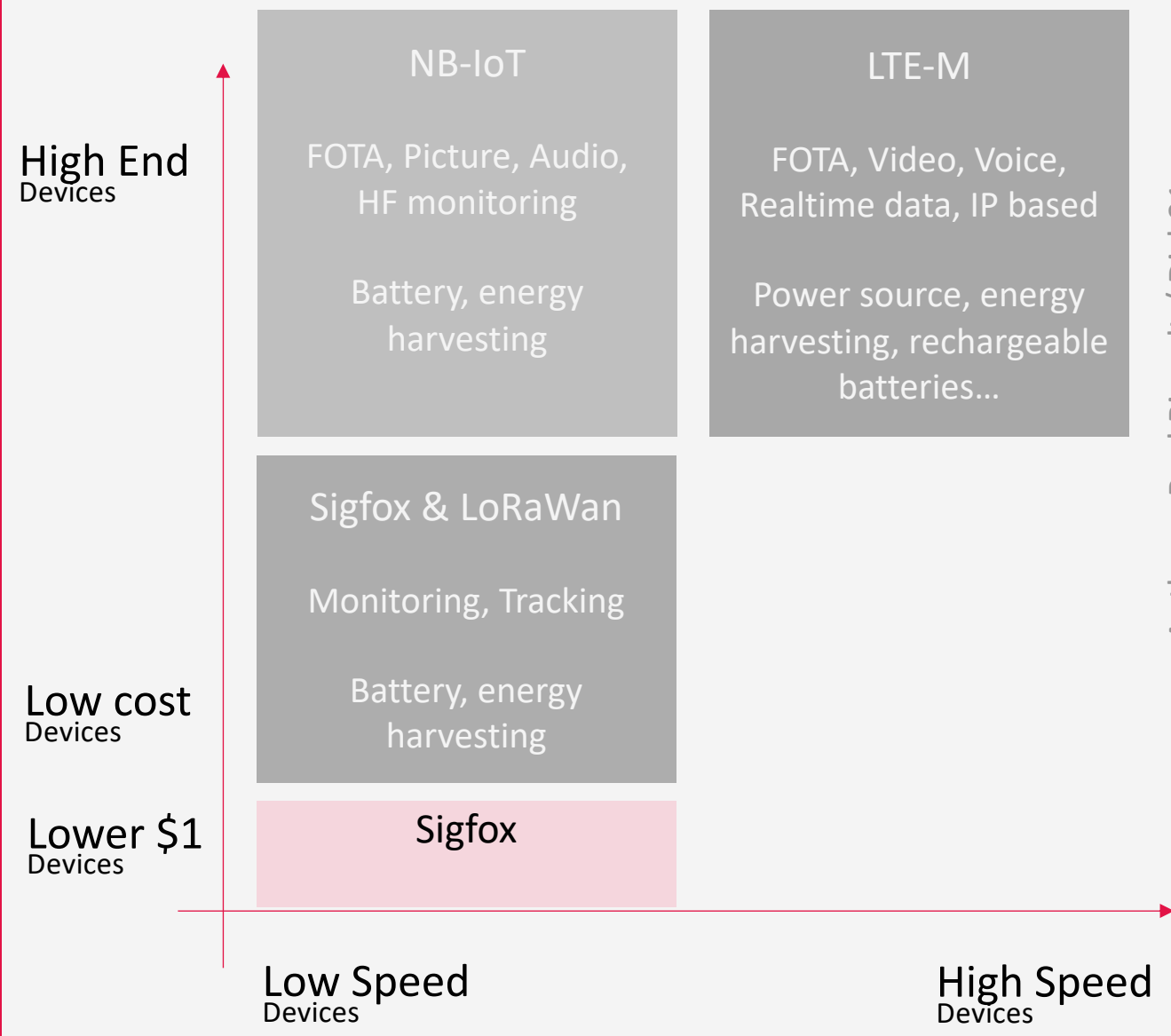
Frequency: **868Mhz
915MHz**
Tx power: **14dBm / 25mW
20dBm / 100mW**
Pic current: **30mA / 120mA**
Coverage: **40km**
Throughput: **100/600bps**
Chip price: **0.2€ - 4€**
Duty Cycle : **1%**

Sigfox is a radio technology (UNB) and a public network operator operating a SDR radio network. The asymmetry of the technology allows and long-range performance for simple transceiver. This is the first technology to enable the Ultra Low Cost IoT

(finished devices under \$1) The key differentiator of Sigfox is being the only one worldwide network operator. Sigfox is a single network with a single network server. Sigfox is a French company.

Technologies Are NOT in competition

They are addressing different use-case, with different total cost approach related to **speed** and **power consumption**.

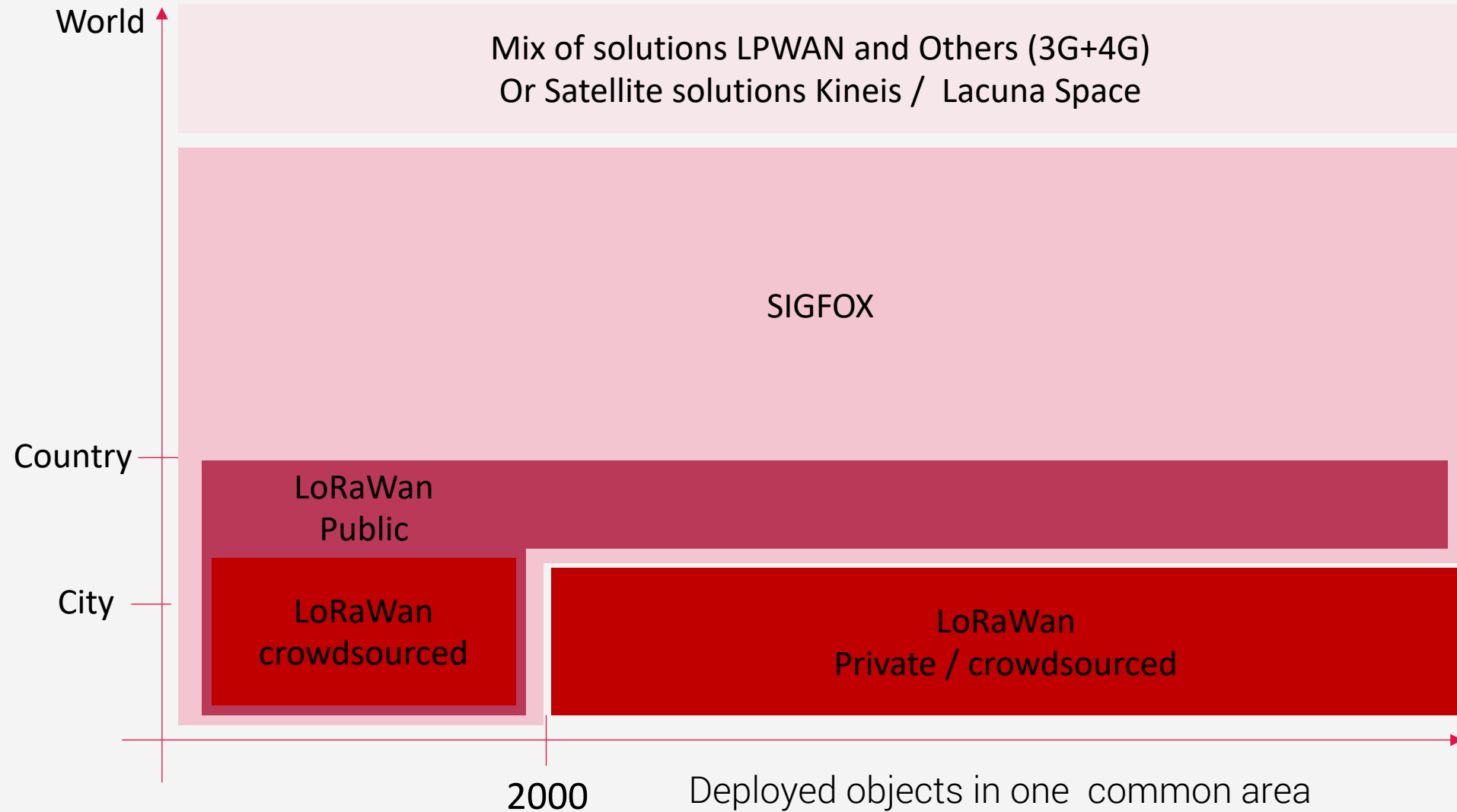


Sigfox

LoRaWan

Low-cost devices

More than the technical difference to serve a specific use-case we can generally tweak, the choice is related to the targeted **deployment scope** and **model**.

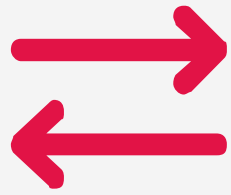


NB-IoT, Wize, LoRaWAN, SIGFOX are the key player of the IoT revolution

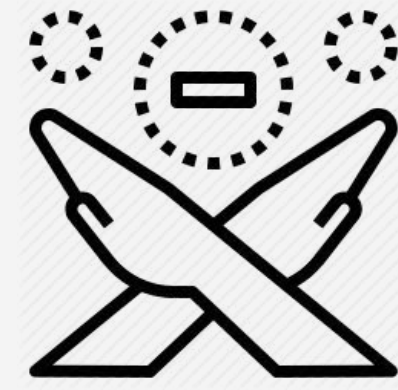
They are the
LPWAN

Low-Power
Wide Area
Networks

LPWAN are the revolution solving this dilemma:



Low-Power
Transmission



Long-Range
(wide area)



Long autonomy
(in years)

Low cost networks
(1 country deployed costs the price of 1 big city with 4G)

Low cost
subscriptions



LPWAN are enabling the “IoT at scale”

IoT at scale is the ability to deploy and manage large fleets of devices, over millions with a viable business model

To connect all kind of existing things, you need to:

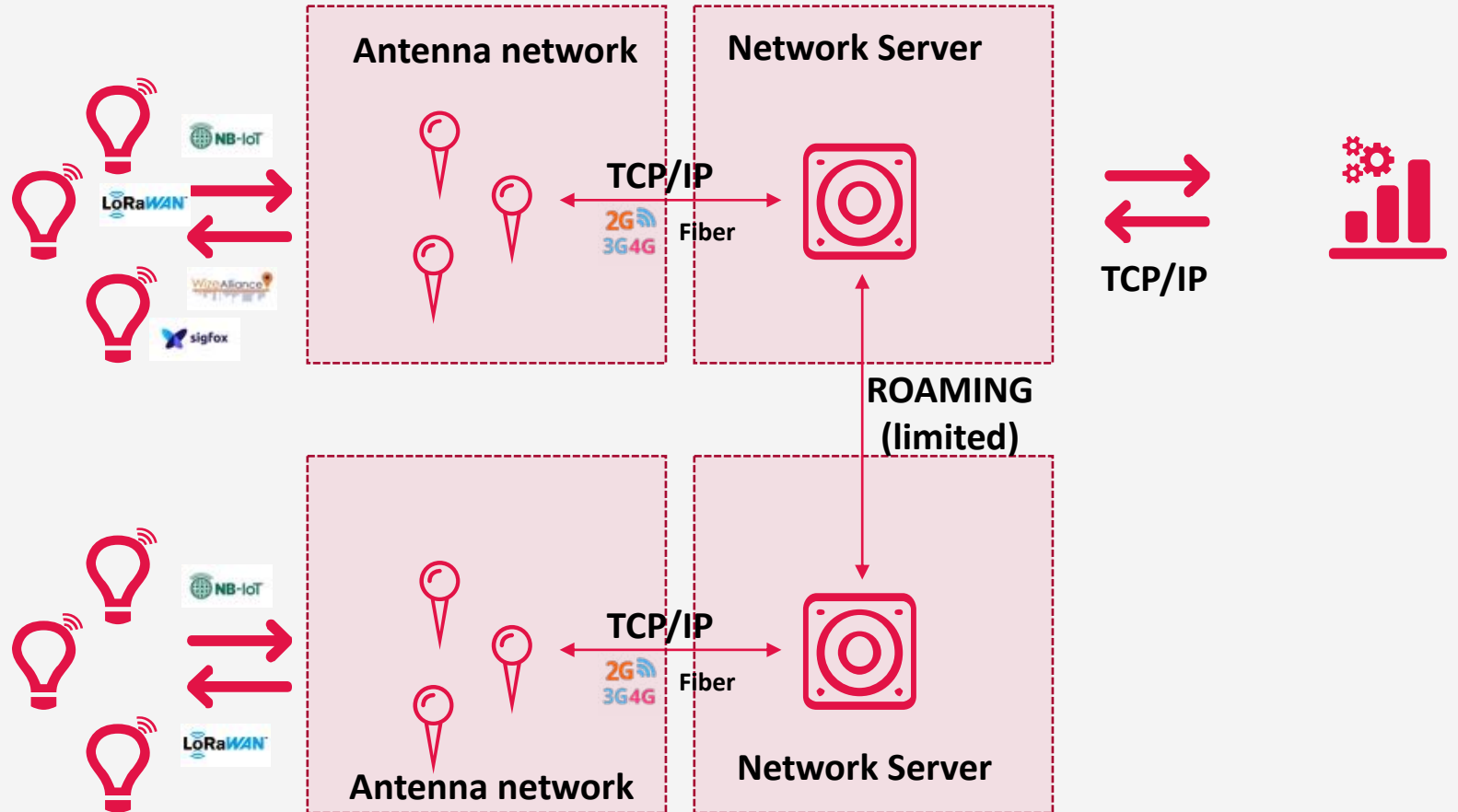
- Break the device cost ✓
- Break the communication costs ✓
- Allow years of autonomy w/o maintenance ✓
- Eliminate user setup ✓
- Reduce the battery size ✓
- Break boundaries ✓
- Cover the world ✓

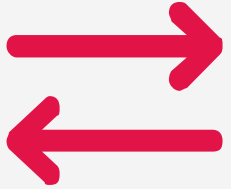
LPWAN have a common architecture

The devices messages are captured by multiple antennas around.

The antennas forward the messages to a network server owned by the network operator (private or public)

Then the network server transfers the payload to the custom backend, eventually, roam it to another network server.

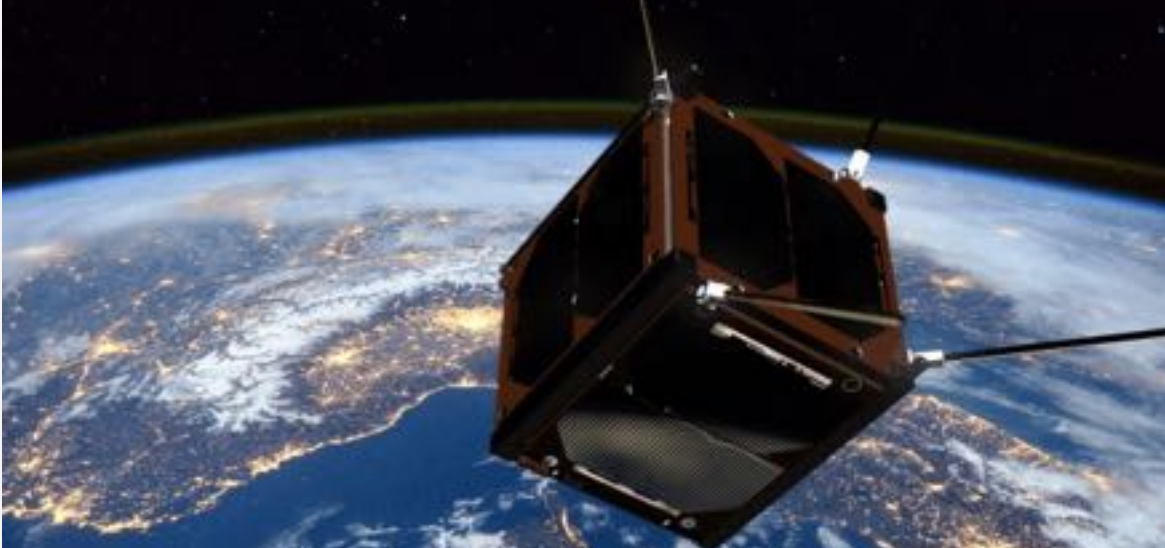




Communication technologies

IoT everywhere with satellites

(Argos)



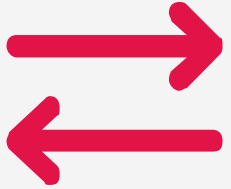
**GLOBAL COVERAGE
LOW POWER
COMMUNICATION**



(LoRaWan)

Multiple IoT operators are looking to the sky to provide a global coverage, particularly on ocean and desartic zones. With a fleet of 15-20 satellites you can cover the world with a communication capability every 10 - 15 minutes for the devices. For Sigfox the objective is to propose device able to communicate with satellite and terrestrial network, all in

one. Lacuna and Kineis are satellite only. The challenge is the synchronization with sats. Compared to Facebook, Google, Musk project requiring advanced transceiver, the IoT solution are really simple and use simple, not motorized, antennas.



Communication technologies

Satellites for global coverage



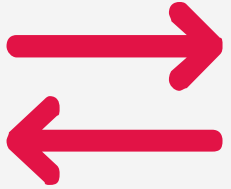
kinéis

**LOW POWER
LOW SPEED
GLOBAL
COMMUNICATION**

Frequency: **399Mhz-401MHz Worldwide**
Tx power: **100mW 20dBm**
2W – 33dBm
Coverage: **Global**
Throughput: **200bps – 4.8kbps**
Chip price: **15-30€**
Duty Cycle : **1.6%**

Kineis is the currently most advanced satellite fleet deployed. It relies on Argos / CNES satellites and his soon launching 25 new satellites to propose a revisit time around 15 minutes. It already propose a global coverage with an average revisit time of 1.5 hour in 2021.

See also - <https://www.disk91.com/2021/technology/internet-of-things-technology/satellites-iot-is-now-ready-for-use-with-kineis/>



Communication technologies

Satellites for global coverage



LOW POWER
LOW SPEED
GLOBAL

Frequency: **1.5Ghz-1.6GHz**
EU, Africa, Asia
Tx power: **25mW 14dBm**
Coverage: **EU, AF, ASIA**
Throughput: **400bps**

Astrocast is getting benefit of the Thuraya constellation and a bidirectional protocol allowing to make sure the frame are transmitted. The sat pass synchronization use a signal received from sats allowing low power mode and communications at the right time. The communications rate will be 15 minutes once the full fleet will be deployed. About 100 LEO satellite by 2025.

See also - <https://www.disk91.com/2022/technology/internet-of-things-technology/astrocast-another-route-to-the-space-iot/>

Let's make a short break

LEARNING AT THIS STEP



There is a large range of technologies

They are not really in competition as they are addressing different type of IoT and different use-cases.



The architecture depends on the technology

The technology determines the architecture and the running costs



LPWAN are the IoT revolution

LPWAN are key enabler for Low Power, Low Cost IoT allowing IoT at scale = IoT in all the things



How to process the IoT Data ? Common architecture, technologies...

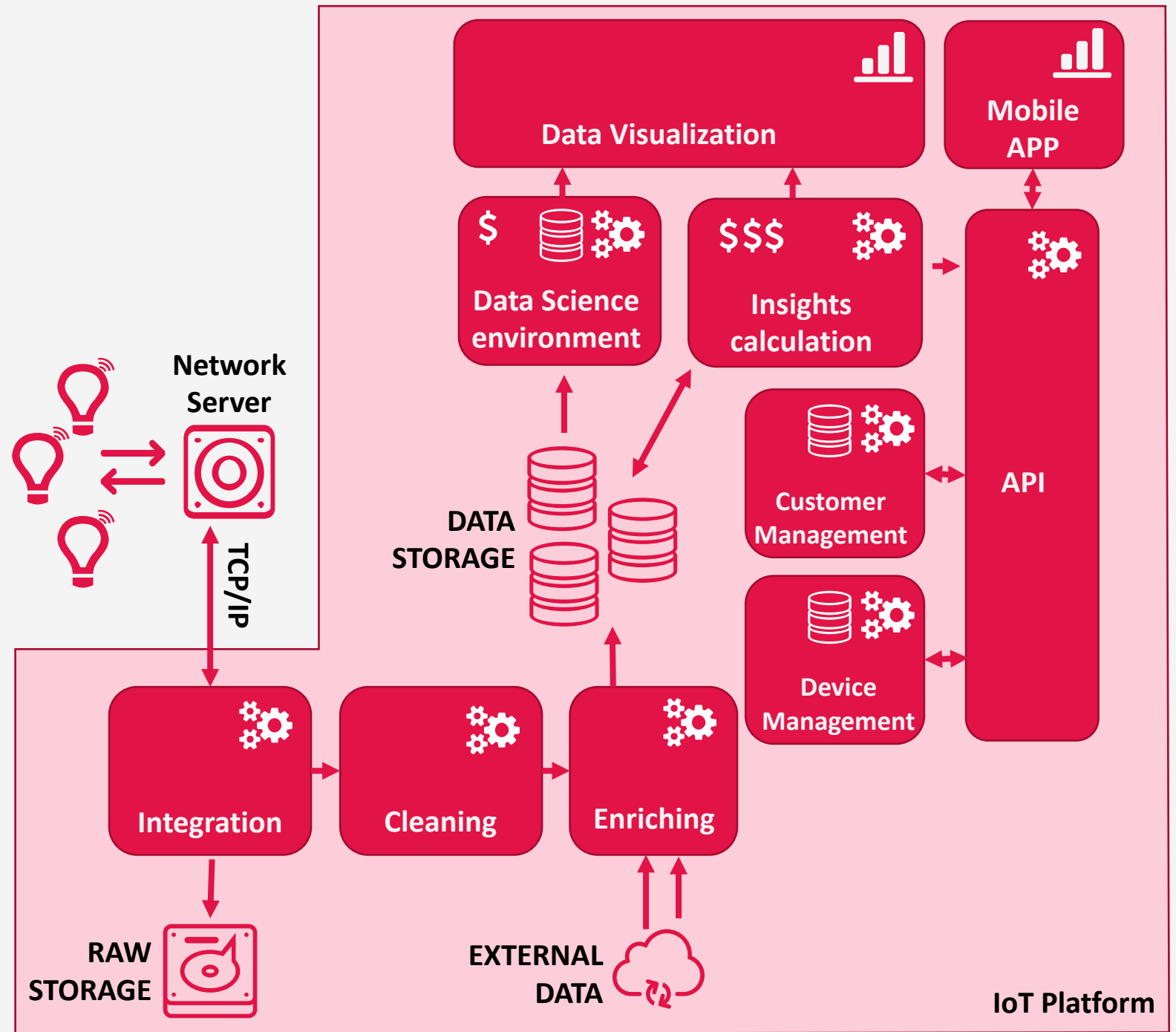




Main components of an IoT platform

An IoT platform is a complex IT architecture where some of the components are highly critical like the “Integration” layer

All the processing layers must be ready for Big Data and scalable.





CLOUD PLATFORMS AS A REQUIREMENT



**CLOUD SOLUTION
ARE SCALABLE
AND HIGHLY
AVAILABLE**

The integration layer can't stop, at any time, because IoT will never pause the transmissions and large Things fleets will always transmit data (by opposition to classical Human activities)

This requires 0 down time capabilities

The power of IoT is to consolidate and process the full history of data making the processing bigger and bigger even with a stable fleet of devices. The Thing's fleet is also subject to scale.

This requires infinite scalability capabilities



ZERO DOWN TIME ARCHITECTURE

CLUSTERING

Ability to dynamically split processing activities between different units.

Loss of 1 or more units will only change the activity balancing to working nodes

BLUE/GREEN DEPLOYMENTS

Ability to upgrade on of the component of the architecture without stopping the systems. Usually comes with clustering, container orchestration.

HIGH AVAILABILITY & DRP

Ability to move or restart any component of the architecture, transparently in case of datacenter / hardware / software failure.

ALL OF THIS REQUIRES A HIGH LEVEL OF ENGINEERING

Therefore, the IoT platforms are usually implemented on top of a Cloud environment, offering them features



INFINITE SCALLING CAPABILITIES

CLUSTERING

Ability to dynamically add new processing node to a computing engine.
Ability to support linear processing time in regard of the number of nodes.

COMPUTING RESOURCE ON DEMAND

Ability to scale the processing engine on demand, to extends the capability in a large order of magnitude progressively or just for a couple of hours.

PRICE LINEARITY

Ability to scale the architecture and process capability with a linear progression of the costs, whatever the scale.

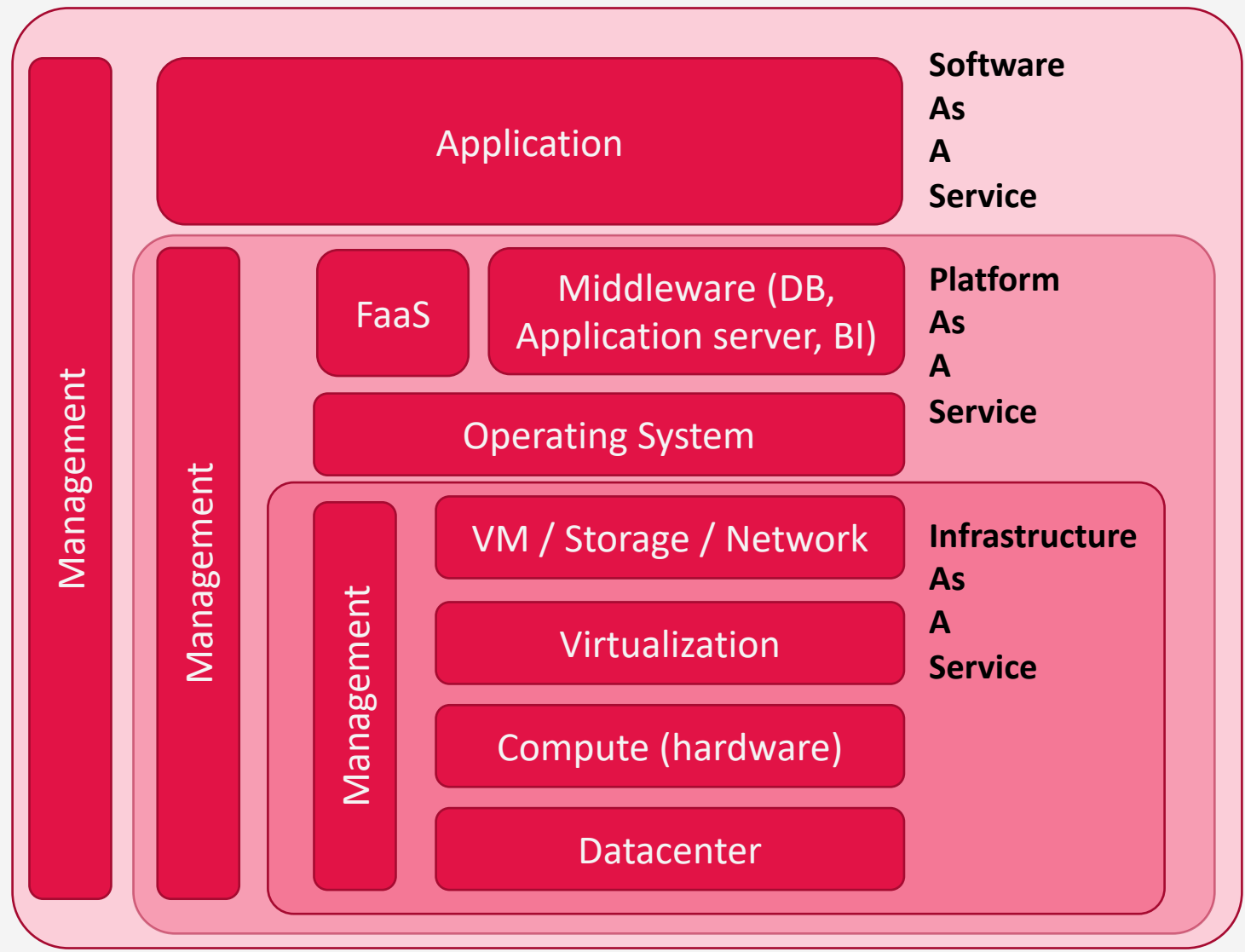
ALL OF THIS REQUIRES A HIGH LEVEL OF ENGINEERING

Therefore, the IoT platforms are usually implemented on top of a Cloud environment, offering them features



Main cloud concepts

Using a cloud environment for you IoT platform will reduce your need of expertise on the critical infra components. Cloud is providing a certain level of management and associated SLA depending on the level you select.



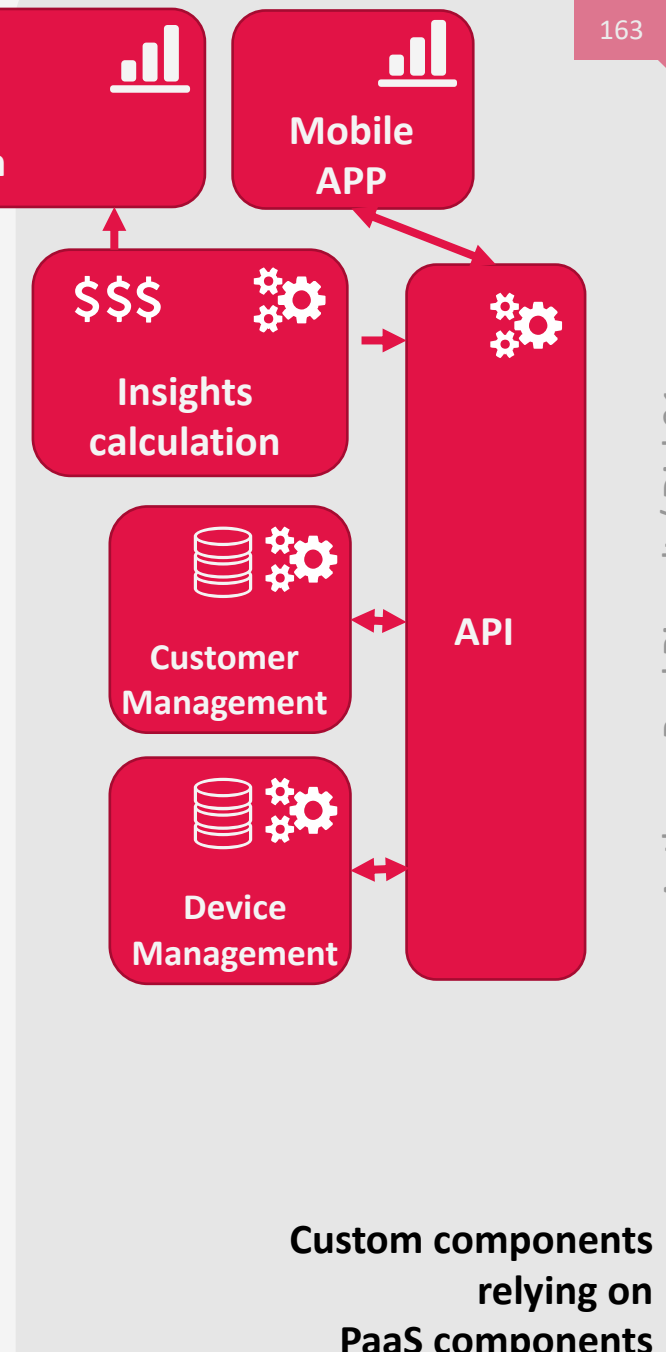
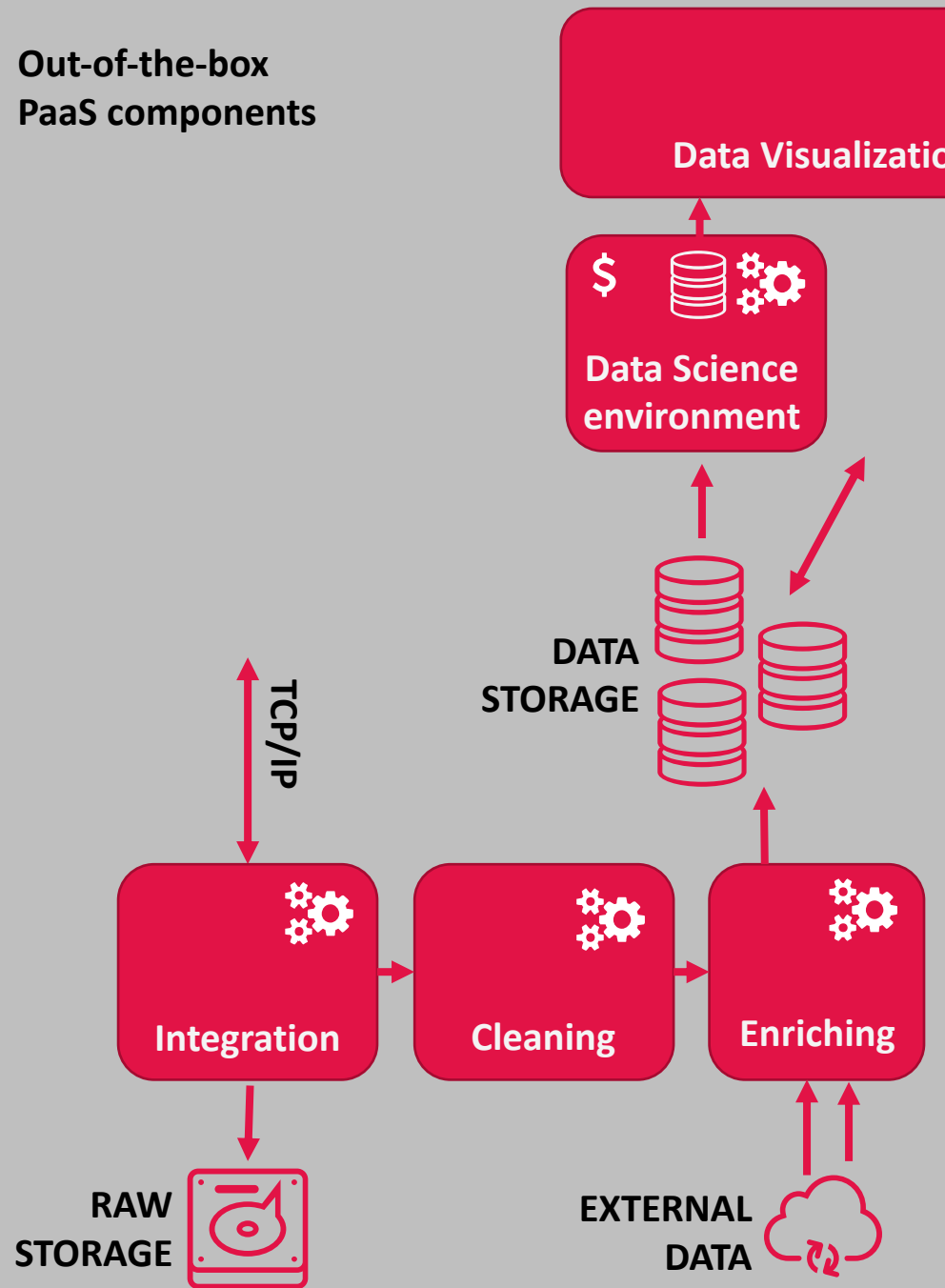


Use of Cloud for IoT platforms

Most of the components will take a benefit of a PaaS approach.

Integration layer to the data visualization are Out-of-the-box existing PaaS pattern ready to be deployed in a single click in most of the Cloud providers.

Out-of-the-box PaaS components





Data is a precious assets which implies responsibility

PERSONAL DATA

B2C IoT requires to register user and these data are personal data. Furthermore, IoT is capturing data, personal data like for a geolocation system. Health data when recording activities, heart rate...

ANONYMIZATION

To be reused in multiple secondary business, the anonymization of the data is a key point. This is also a good way to keep the personal and health data for a long time. Personal data can't be.

ENCRYPTION

To ensure data protection, encryption is a state-of-the-art solution. It is also a protection against data leak: your IoT data are an asset, the value of this assets comes from scarcity - don't be your own competitor.

Let's make a short break

LEARNING AT THIS STEP



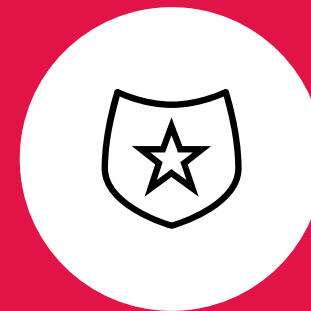
Processing IoT is an infrastructure challenge

Due to the criticality of the data integration



The Cloud providers can be the solution

Complex infrastructure are easier when managed by experts



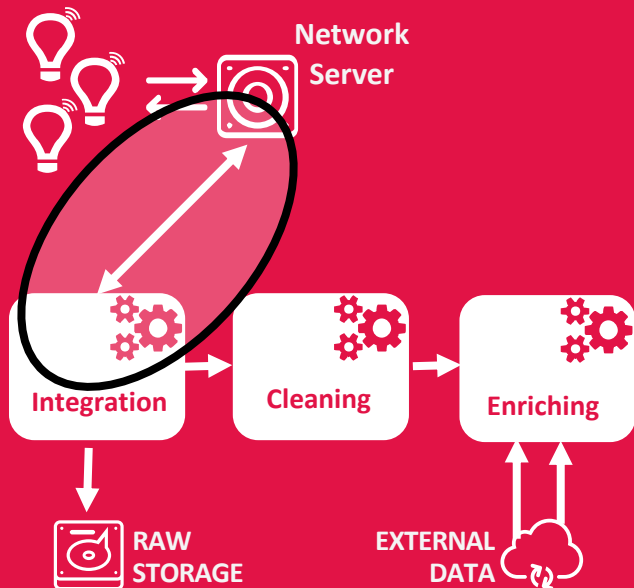
lot Data are sensitives assets you need to protect

So you can focus on your data protection which have a larger value for your business



Data Integration

This component is highly critical and can be implemented in different ways



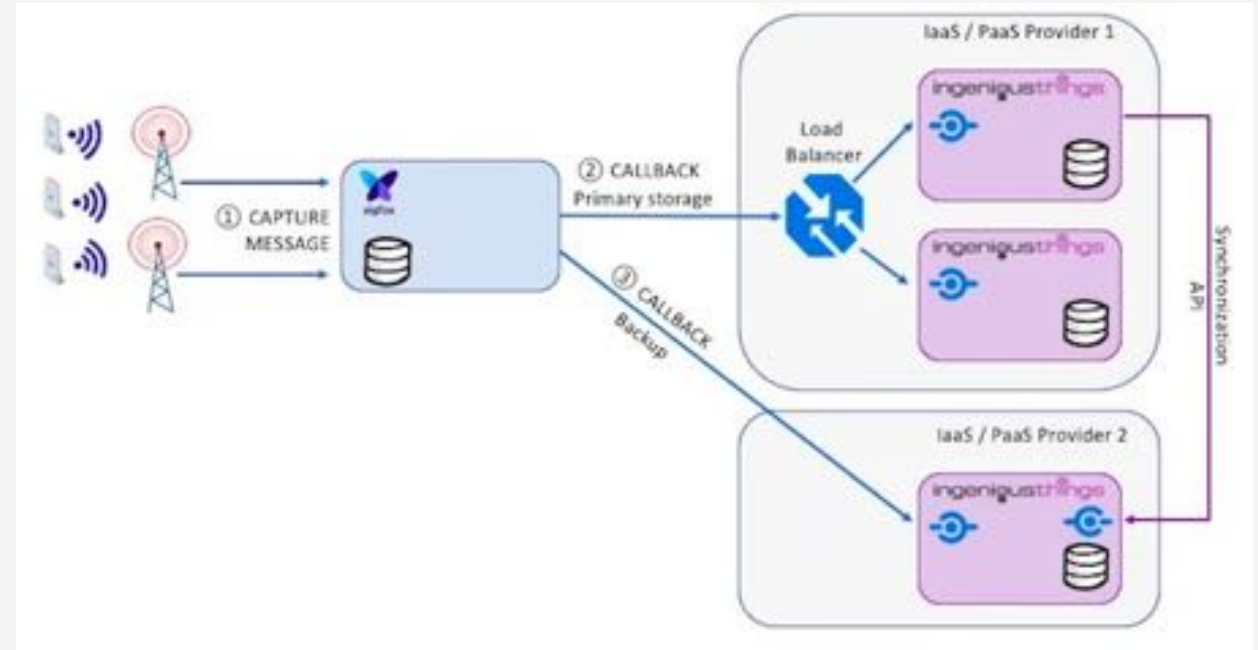
SOLUTION 1

PUSH - HTTP Integration (Callback or Webhooks)

The Network server calls an API on the Integration Layer on every message received / on every seconds when messages have been received.

Common technical solutions:

- API Cluster with backup or multiple sites.
- FaaS (Function as a service)

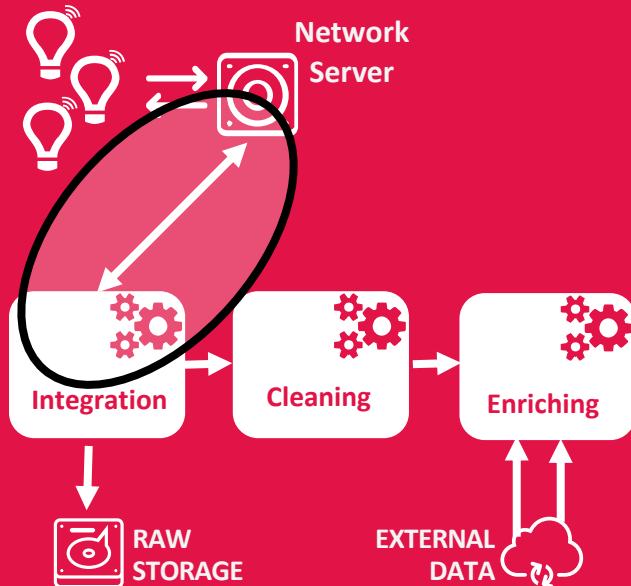


This solution is fully synchronous . As this kind of solution presenting a risk of data loss, there is a backup solution with an asynchronous synchronization mechanism.



Data Integration

This component is highly critical and can be implemented in different ways



SOLUTION 2

PUSH – Message Queue based integration

The Network server push messages over a broker managing message queues. That way, the communication is asynchronous between the Network server and the Data integration layer.

Common technical solutions:

- Use of MQTT (most frequent with IoT)

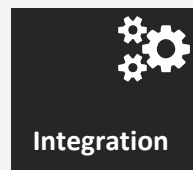
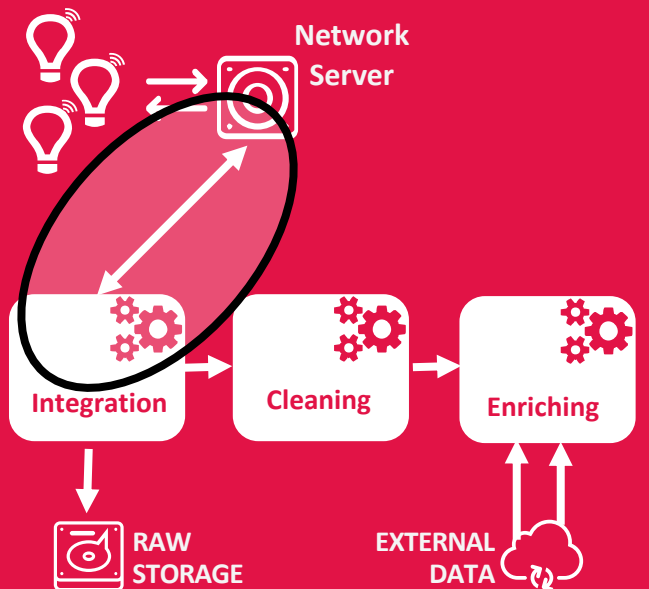
MQTT is a lightweight queuing protocol over TCP managing quality of service. It works well as a cluster.

TCP/IP ready devices can directly implement MQTT communication to report data. This is working well with low quality networks (like cellular networks).



Data Integration

This component is highly critical and can be implemented in different ways



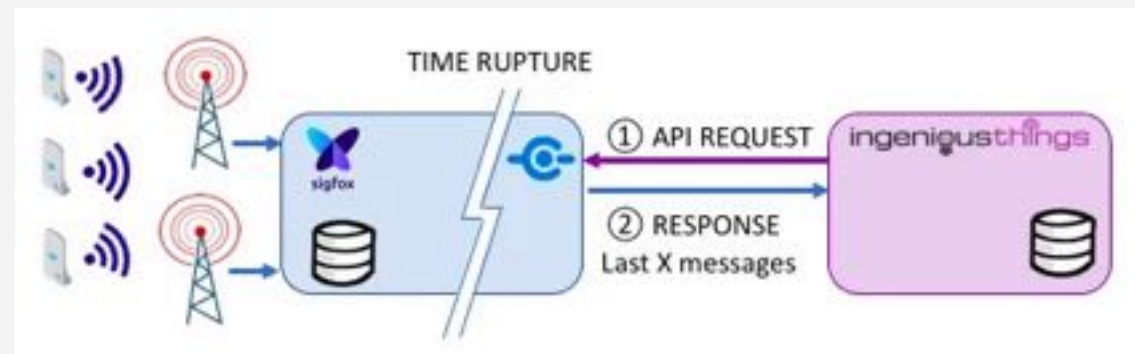
SOLUTION 4

PULL – API CALL ON THE NETWORK SERVER

The application request status of device and extract data from the Network server with API calls. That way the application integration layer is not critical.

This solution is not really recommended until you have large fleets because it creates a time rupture between device's message reception and message processing. So you are not real time anymore.

When your device fleets becomes large and you have message on every seconds, this integration way makes sense to preserve the application resources and reduce the criticality of the integration layer.



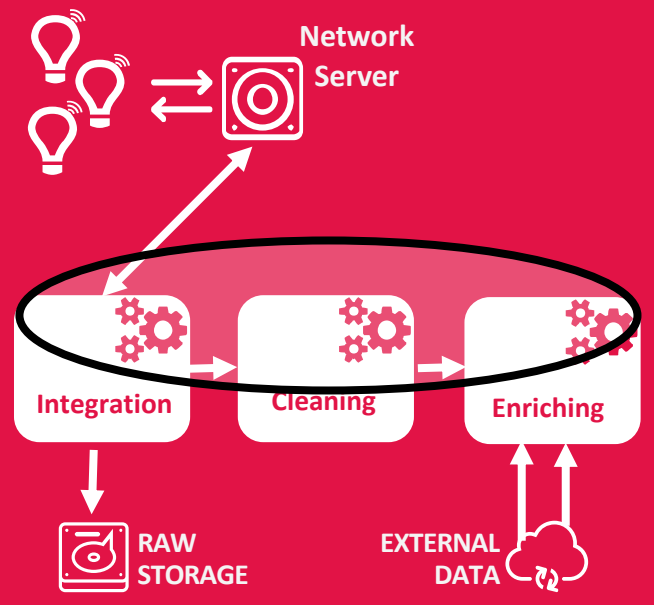
CONCLUSION INTEGRATION LAYER

The way the integration layer is implemented depends on the technical solution offered by the Network Server. It also depends on the fleet size and the frequency of the messages you need to integrated.



REAL-TIME, EVENT PROCESSING

The integrated data is then process, clean, enriched in real time, because users want to see it immediately.

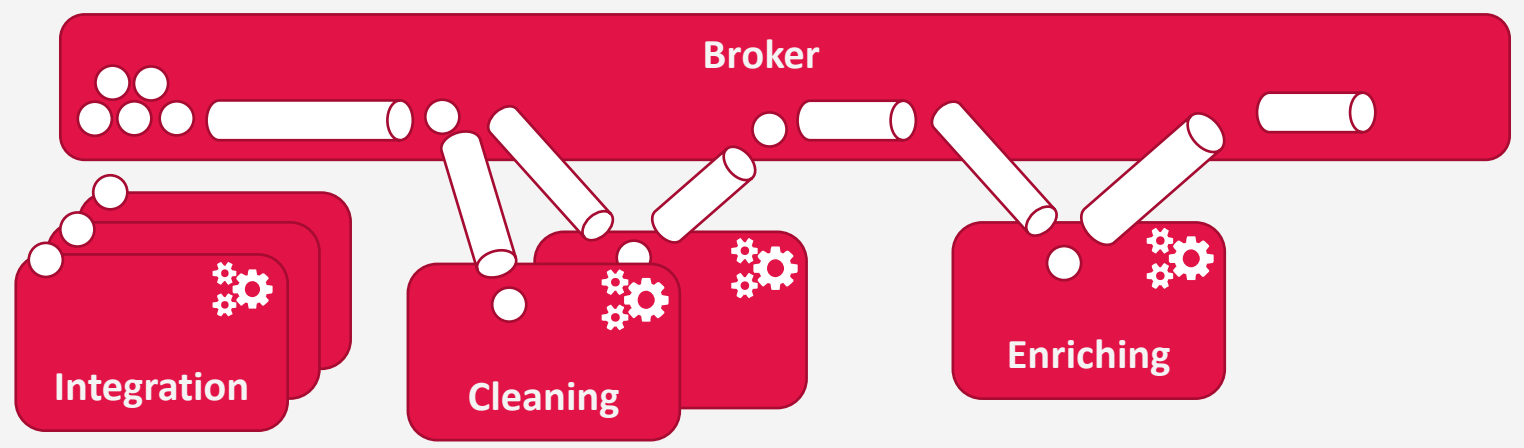


Solution 1 - Message Queuing

One of the problem to solve is the fluctuation of the workload depending on the sensor communications. This workload is composed by a series of messages to process the same way, individually.

One of the pattern is to transform each of the sensor communication in a message send to a Queue. This queue will be consumed and process by the next layer, asynchronously. Scalability is easy to manage as concurrency.

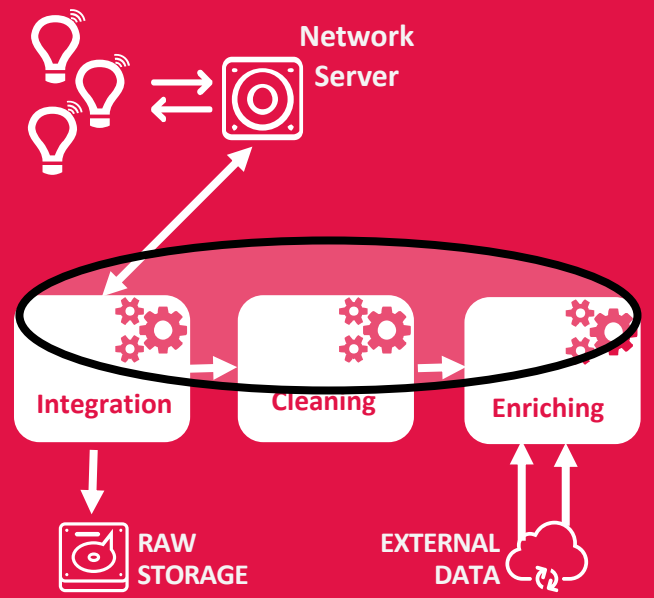
The second problem to solve is the ability to reprocess the whole history because you changed some of the intermediate processing. For the same reasons, this solution is also efficient.





REAL-TIME, EVENT PROCESSING

The integrated data is then process, clean, enriched in real time, because users want to see it immediately.



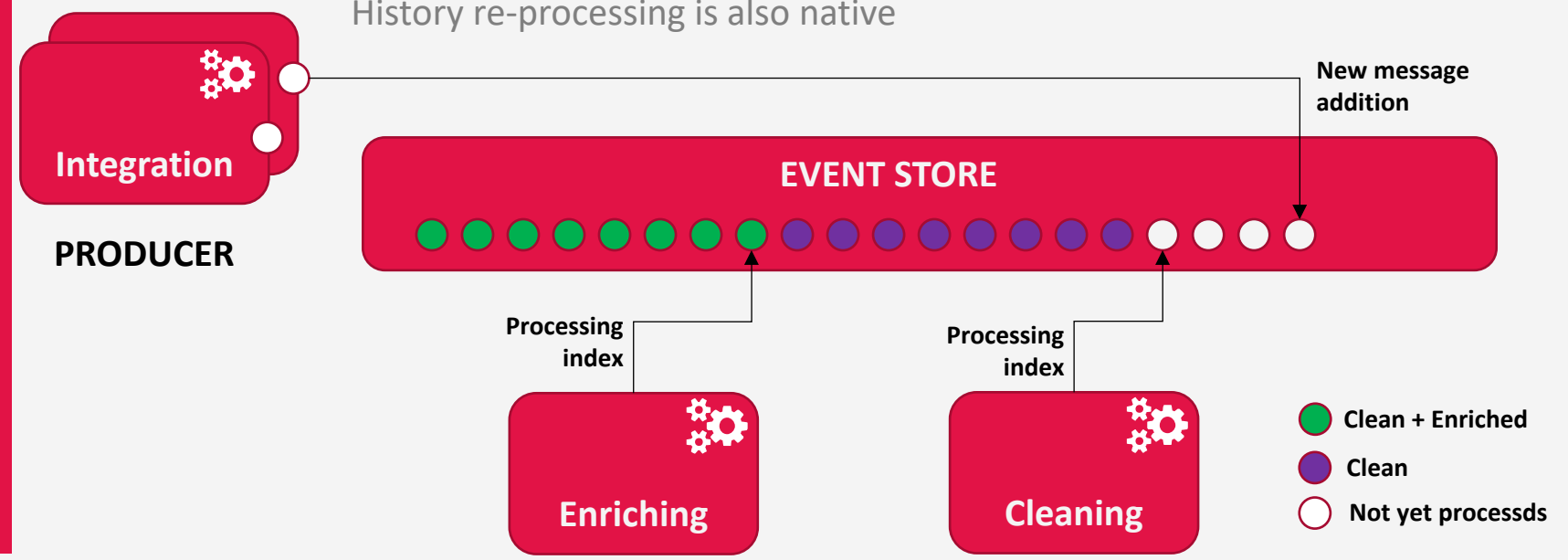
Integration
Cleaning
Enriching

Solution 2 – EVENT SOURCING

Event sourcing is working a similar way with a major difference. In a Message queue architecture, the message is going in and out but not stored. Updating the broker or scaling the broker itself can be a problem. In production the broker can also become saturated if some consumer are dead or undersized to process the messages. Dynamically changing the process tree can also be an issue.

Event sourcing (product like Kafka) is solving this issue with a more scalable architecture. The integrated producer / consumer approach, working directly on the data flow is also very efficient.

History re-processing is also native



STORE RAW DATA FROM SENSORS

Because once refined you lost information and future value.

Integration → Cleaning → Enriching

RAW STORAGE (circled in red)

EXTERNAL DATA

Network Server



STORE THE RAW DATA

DATA is an asset, every time to modify the raw data, you loose a part of the information. Even if at a certain time you think not to do it, later you may discover you were.

Furthermore, it is recommended to keep your processing chain to be able to recompute everything from the first day. It means, the computation data source will be the RAW DATA.

The reason is: more data you have, more insight you create. Most insight will learn from the past and create value even in the past.

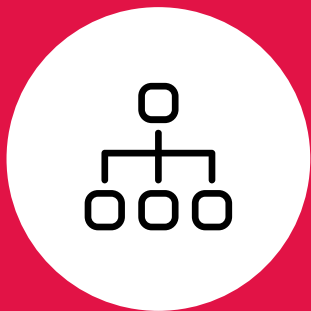
This RAW DATA volume, over the years will take more and more space and some specific technologies could be required. Some technology are use for this.

- Kafka: scalable event store
- Hadoop: scalable file storage
- Mongo DB: scalable NoSQL Databases

The advantages of NoSql database compared to standard SQL database is the native clustering mode but also the ability to mix different sort of message payload in a common repository. Sensors messages will evolve with versions over time, you need to anticipate this.

Let's make a short break

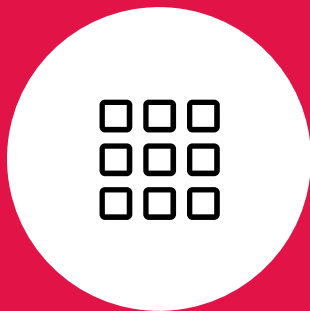
LEARNING AT THIS STEP



• ————— •

Many patterns exist to support the data integration

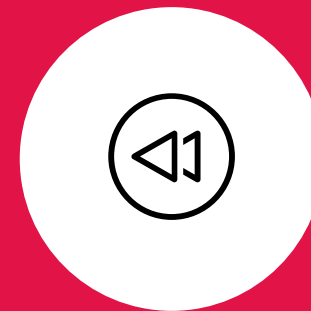
You need to design the solution based on your target volume of data and fleet size



• ————— •

All the technologies are cluster and scalable

That's a key factor of success for a critical component of the solution



• ————— •

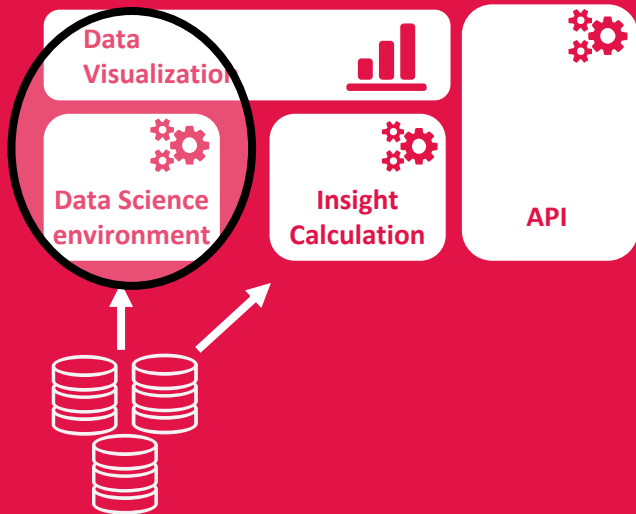
Be prepared to reprocess everything

Your future business will require data processing you can't imagine today.



Extract value from DATA

**Data Science analyze data and propose solution for Insights calculation.
Classical BI allow to display results.**



Laboratory for your data

Data Science experiment the data to create added value insight, performant neuronal networks or statistical studies. The data science work is growing with the size of the dataset and the number of market your solution can address.

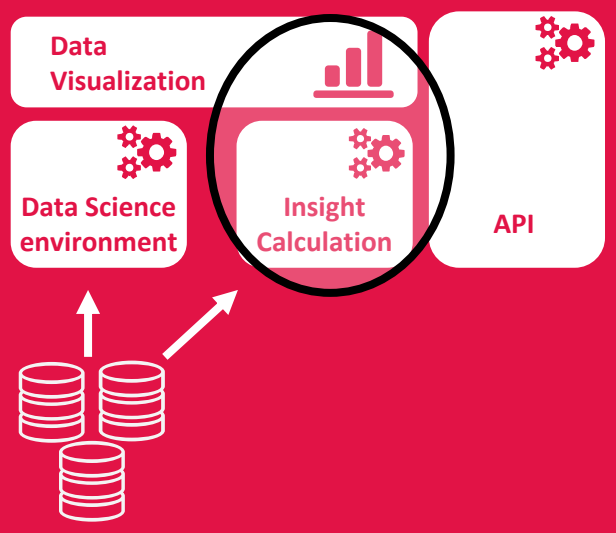
The classical tools for data scientists are:

- R or Python development environment
- Parquet like columnar storage format
- BI reporting environment to create dashboard
- Neural networks execution platform (GPU...)
- Large access to the raw data, enriched data and external data.



Extract value from DATA

Data Science analyze data and propose solution for Insights calculation.
Classical BI allow to display results.



Your product is here

An IoT solution should only distribute Insights and not the Raw data:

- Because its role is to create a proper value
- Because giving raw data makes its value going down to 0.

An Insight is basically the industrialization of the data-scientist work. It must be computed in real time when new data have been received.

Insights are also computed in batch when new Insights are created or upgraded.

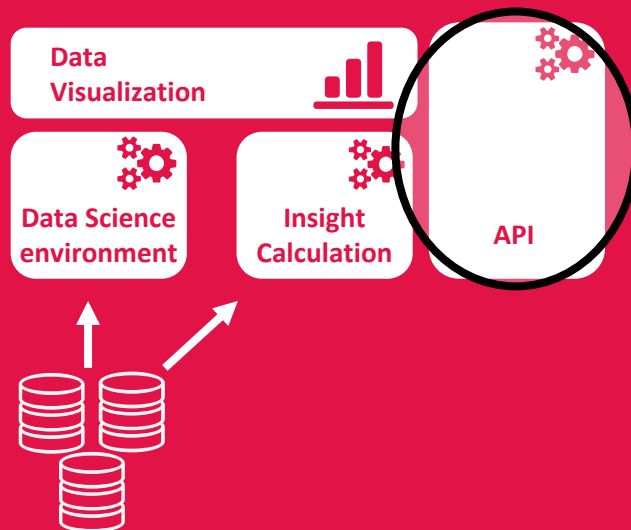
To support a large computation of different Insights on a full history, the Insight computation platform must be highly scalable. Cloud platforms are part of the solution.

- Solutions like FaaS is a good solution for real-time and scalable computation.
- Apache Spark is also a good solution for scalable computation.



Expose your data
for being able to
sell them

An IoT solution have
different ways to
distribute its Insights
but the more scalable
and common are API.



How you sell it is here – think API first

Today the market maturity for API still low but the future of IoT Market is API.

The way to distribute an Insight is an API and your customer will continue to add value on your Insight integrating them is a vertical business or by crossing them with other Insights. This will be automatically processed in real-time thanks to APIs.

So the way you build your web & mobile integration must rely on API: you must be the first consumer of your API product.

This comes with important technical components and platforms:

- **API Management**
 - Ensure the security and control of you API
 - Allow the billing on your API
- **Developer portal & experience**
 - Make your product easy to use
 - Document your product
- **MQTT broker (or other pull solution)**
 - As there are good reasons to prefer a push integration to a pull integration

Even if API is your goal, do not forget market maturity for API is low and you may have to export CSV and other batched flat files ... So you need to think about **ETL, sFTP...** technology also.

Let's make a short break

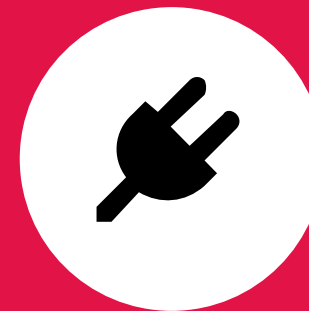
LEARNING AT THIS STEP



Insights are the value proposition



They are created on a data science environment



Then industrialized to be computed and exposed over API



DEVICE MANAGEMENT A KEY CUSTOM COMPONENT



EACH OF THE SENSORS WILL HAVE ITS UNIQUE FIELD EXPERIENCE

One in the field, each of the device will be impacted differently in the environment. This will impact its autonomy. It can make it not working or working partially. The communication conditions will also vary a lot.

The more terrible things for an IoT project is when you need to modify the hardware on field. Being able to configure or update a device remotely is important to reduce the risks. This need to be manage centrally the configuration and being able to push and follow upgrade deployments.

LOG, LOG, LOG! IDENTIFY WEAK SIGNALS

MANAGE CONFIGURATION & UPDATES



DEVICE MANAGEMENT IS CUSTOM

There is no mature software solution to manage a fleet of devices. It is a question of IoT maturity and because this is specific to each of the technology.

This is also impacting the device design.



DEVICE CONFIGURATION

Anything you can configure need to be configurable from the Device Management platform. Configuration history is an important information. Device inventory is the starting point.



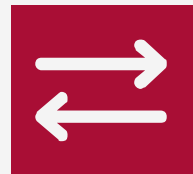
SHADOW CONFIGURATION

A remote device will not immediately apply its new configuration. It can take days for devices not online. It can also be done over multiple communication requiring multiple days. During that time, the configuration need to be consistent and traced.



DEVICE LOGS & ALARMS

To understand the device condition of use and history, you need to measure extra parameters. Environmental temperature is important for many things like batteries. Specific events (like a reboot) are mandatory to trace.



DEVICE UPGRADE

Not all the network technologies allow a remote firmware upgrade. Lower the energy consumption is and lower the capabilities are. Device upgrade is not mandatory, but you need to consider it and established a plan B.



DASHBOARD YOUR DEVICE FLEET MANAGEMENT

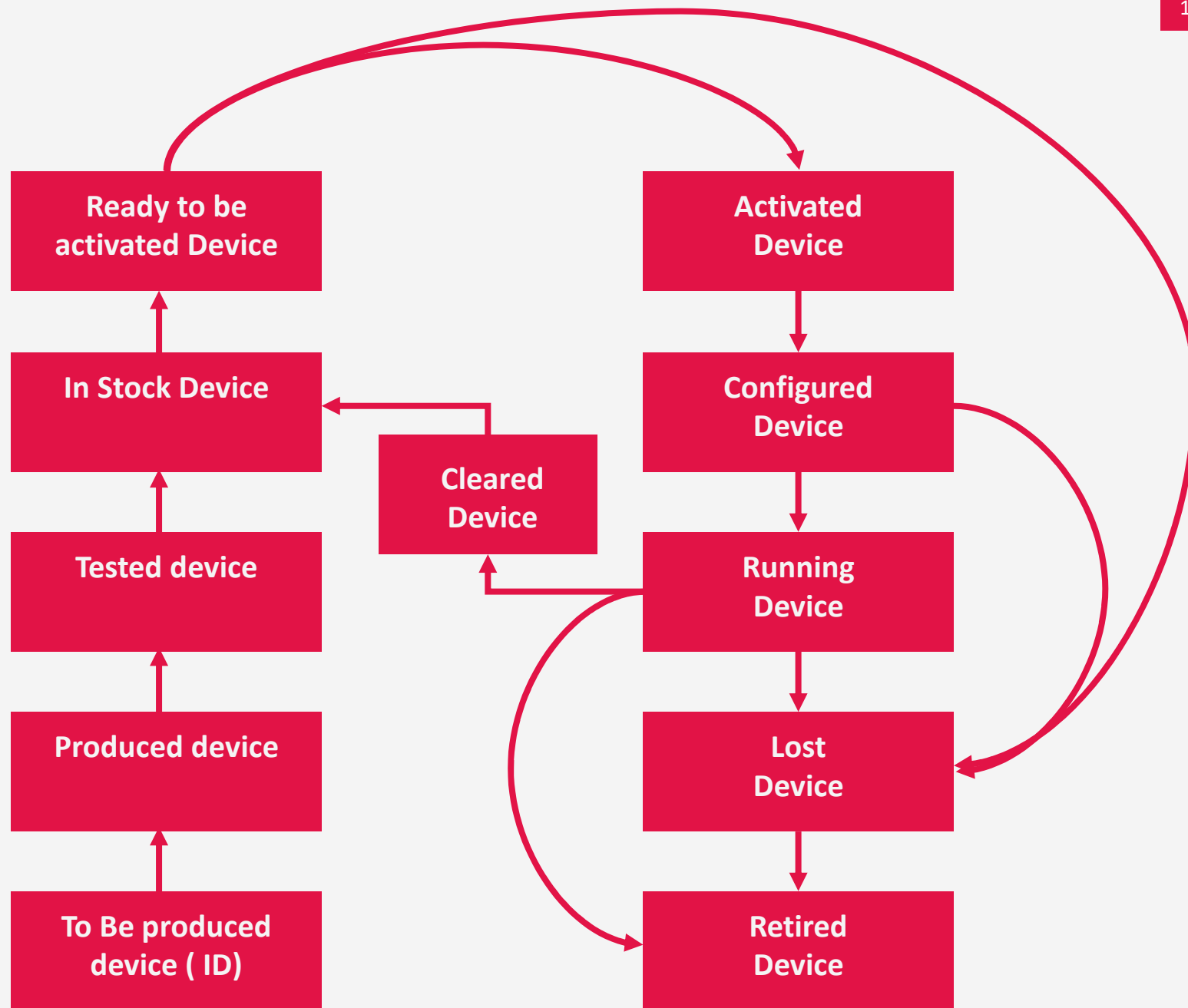
Device fleet management is an expensive but mandatory par of your IoT solution. Without it it is impossible to scale. You need to build an efficient solution for this.



DEVICE LIFE CYCLE

The device management platform also supports the device life cycle.

This is about process: deploy a fleet of IoT devices is a supply chain & logistic question



Let's make a short break

LEARNING AT THIS STEP



A fleet of IoT devices must be managed

It supports the full device cycle management. IoT device is a product you distribute, as any product company



This requires a dedicated tools

It's a kind of ERP, but compared to usual product, that one is communicating, and its interest starts once you move it out of your warehouse.



To reduce the industrial accident's risk once in the field

Because if you need to fix anything in the field it will usually cost more than the cost of deploying a new fleet...

OUT-OF-THE-BOX IoT Platform

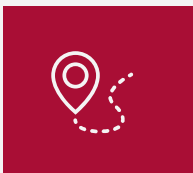
An IoT platform is a complex piece of software. Designing it for a project with uncertainty or a small size could be too expensive or complex.

You can find IoT platform available on the market covering partially the listed features, purchased per devices.



Why not using them ?

They are usually focusing on data visualization with limited Insight computation capability. The key features about device management are usually not implemented or insufficient. Platform is the heart of your service.



So, What are they targeting ?

They are perfect for small fleets of devices (<1000) with limited value addition, like simple tracking platforms. However, you should store your raw data outside in parallel.



Why else, using them ?

Get online quickly for the PoC, PoT phases, make the direct value demonstration easily with limited investments.



Security, how to design a state-of-the-art IoT solution ?





Who wants to attack you IoT ?



Car hijackers ?



Hackers



Security consultant



Script Kiddies



Who wants to attack you IoT ?



Car hijackers ?

Core business activity, but they have other means that better work.



Hackers

They will create the bundle for the script kiddies and make it easier for the car hijackers. Just for fun or fir bunty.

INFOSECTRAIN
CYBER SECURITY CONSULTANT:
A COMPLETE COURSE & CAREER PATH
www.infosectrain.com

Security consultant

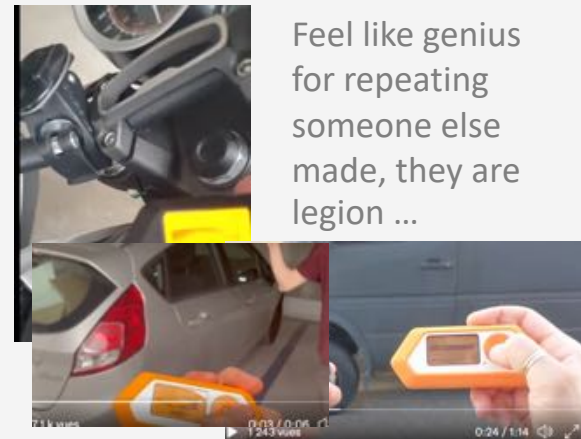
Clearly the villain in the list : he makes money and reputation on something he found, or a hacker has found. Even if no real attack is possible, he will explain all the potential of it's finding out of context.

Fiat Chrysler would not tell FORBES whether or not it would roll out any patches for Miller and Valasek's vulnerabilities. Instead, it brushed off the findings due to the need for direct access to the car via the on-board diagnostics (OBD) port. "Based on the material provided, while we admire their creativity, it appears that the researchers have not identified any new remote way to compromise a 2014 Jeep Cherokee or other FCA US vehicles," the company said in a statement.



Script Kiddies

Feel like genius for repeating someone else made, they are legion ...





Who wants to attack you IoT ?



Car hijackers ?

They are not the main problem, they are taking a risk and lower the risk, the volume of success is limited by the risk.

But some will find an opportunity if the attack to simple enough and lower the risk.



Hackers

You can't fight against hackers and states. Make sure that what they will get will not be easily replicable as scripts for kiddies.

Make sure you can update your solution in case they report things to you.

Have a bounty program to make sure they have an interest in contacting you



Security consultant

You can't fight against the security consultant even if usually the average tech skills are lower. They will hide a part of the truth about how it has been done.

They will make a lot of communication around what can be seen and the press love this. They make great story.

You are basically dead after they hit you.

Manage crisis

Jeep owners urged to update their cars after hackers take remote control

Security bug allows remote attack of Uconnect system, letting hackers apply the brakes, kill the engine and take control of steering over the internet



Script Kiddies

Standards makes scripting generic and applicable to many targets including you.

Adding some specificity on top of standard limits the ability to run script on your solution.

The rest is a question of update and communication. **Usually touch old technologies.**

Author – Paul Pinault / Disk91.com



Hackers

You can't fight against Hackers; they are smarter than you all together and think out of the box.

Some rules:

- don't be stupid
- Make your device less interesting than competitor's one

Rooting

Our weapon of choice:



Dennis Giese and Daniel Wegemer – 34C3



<https://www.youtube.com/watch?v=uhyM-bhzFsl> (31 min)

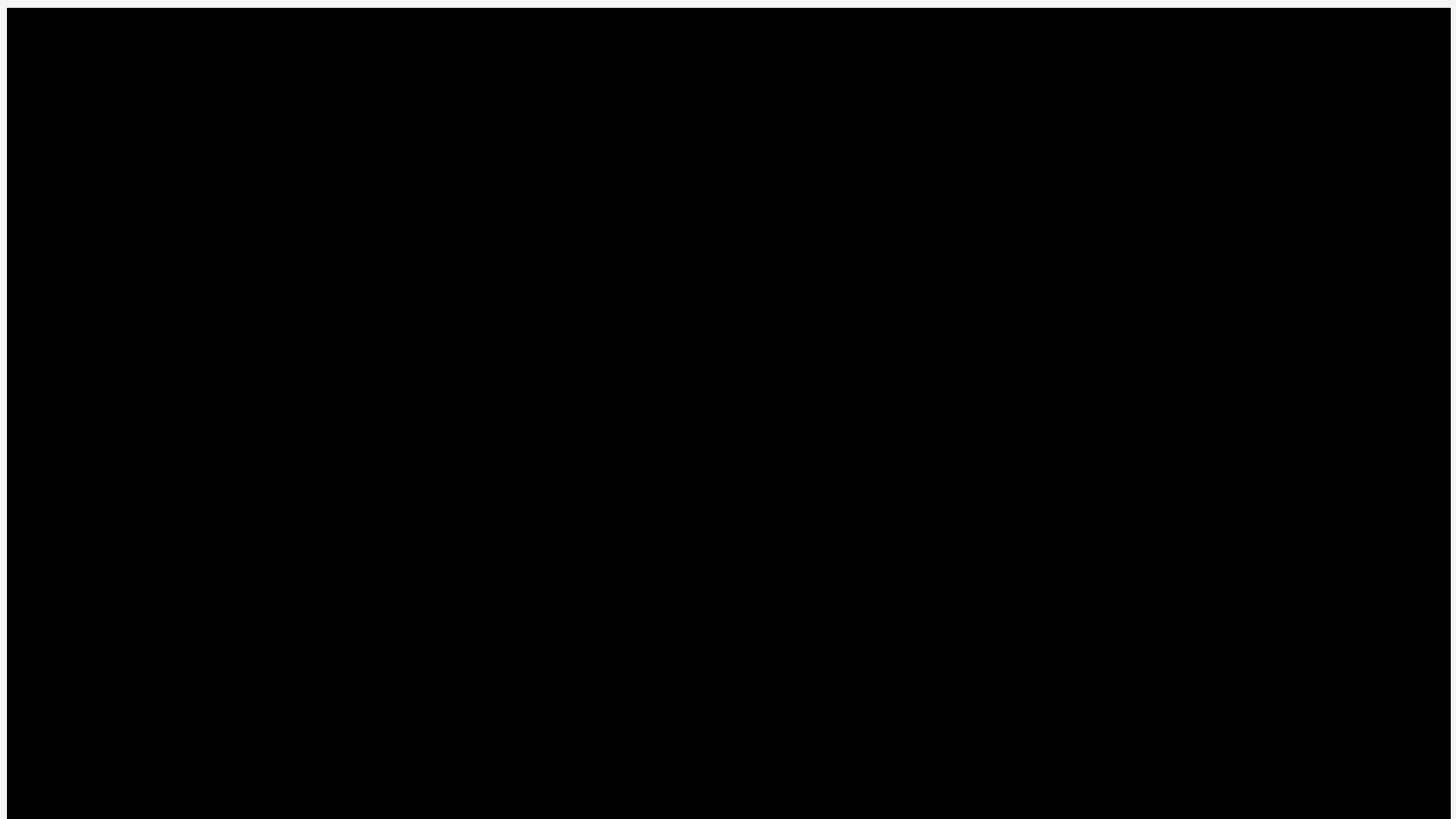


Hackers

Cleaning Robot Hack

- Nice hardware design
- Good architecture
- Stupid decision made at a point

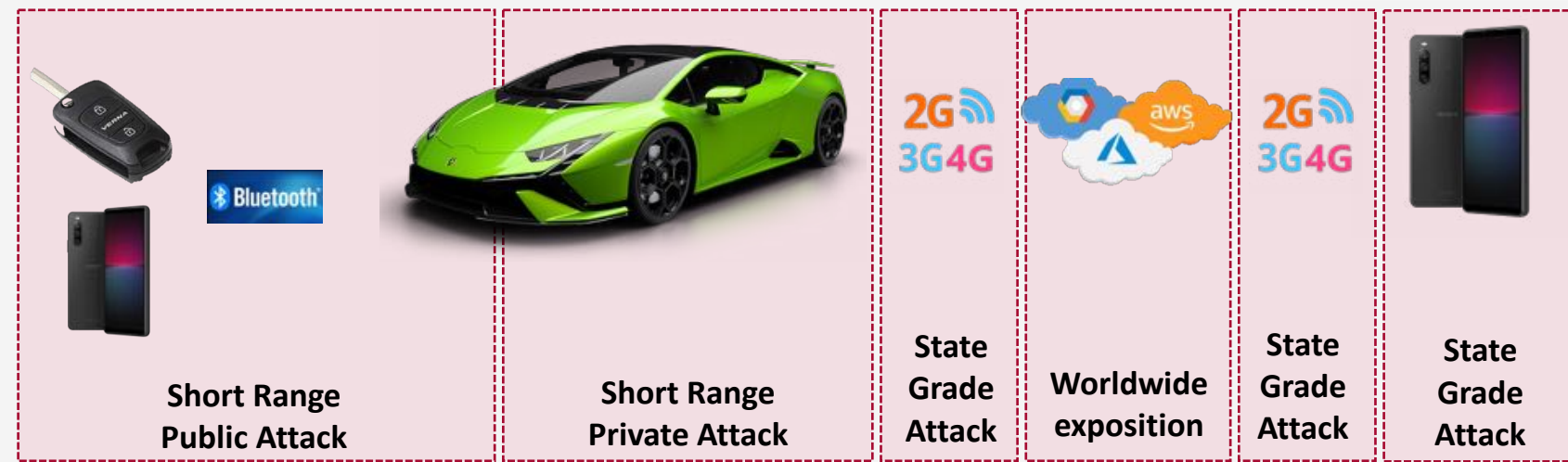
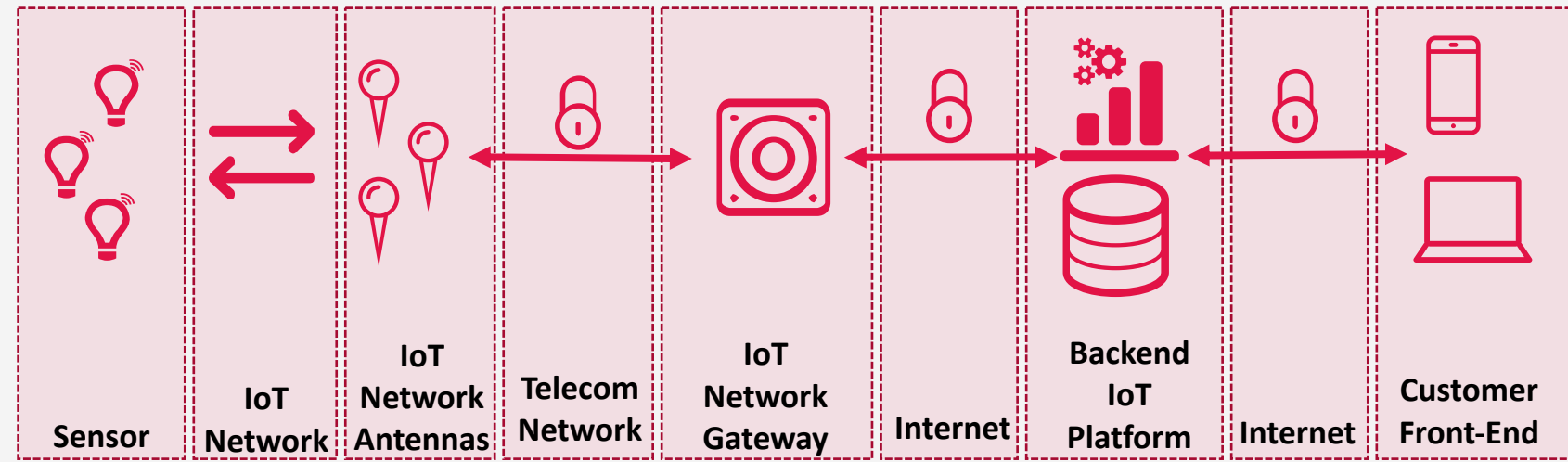
- Never have a shared secret between all the devices !!!





IoT Solution attack surface

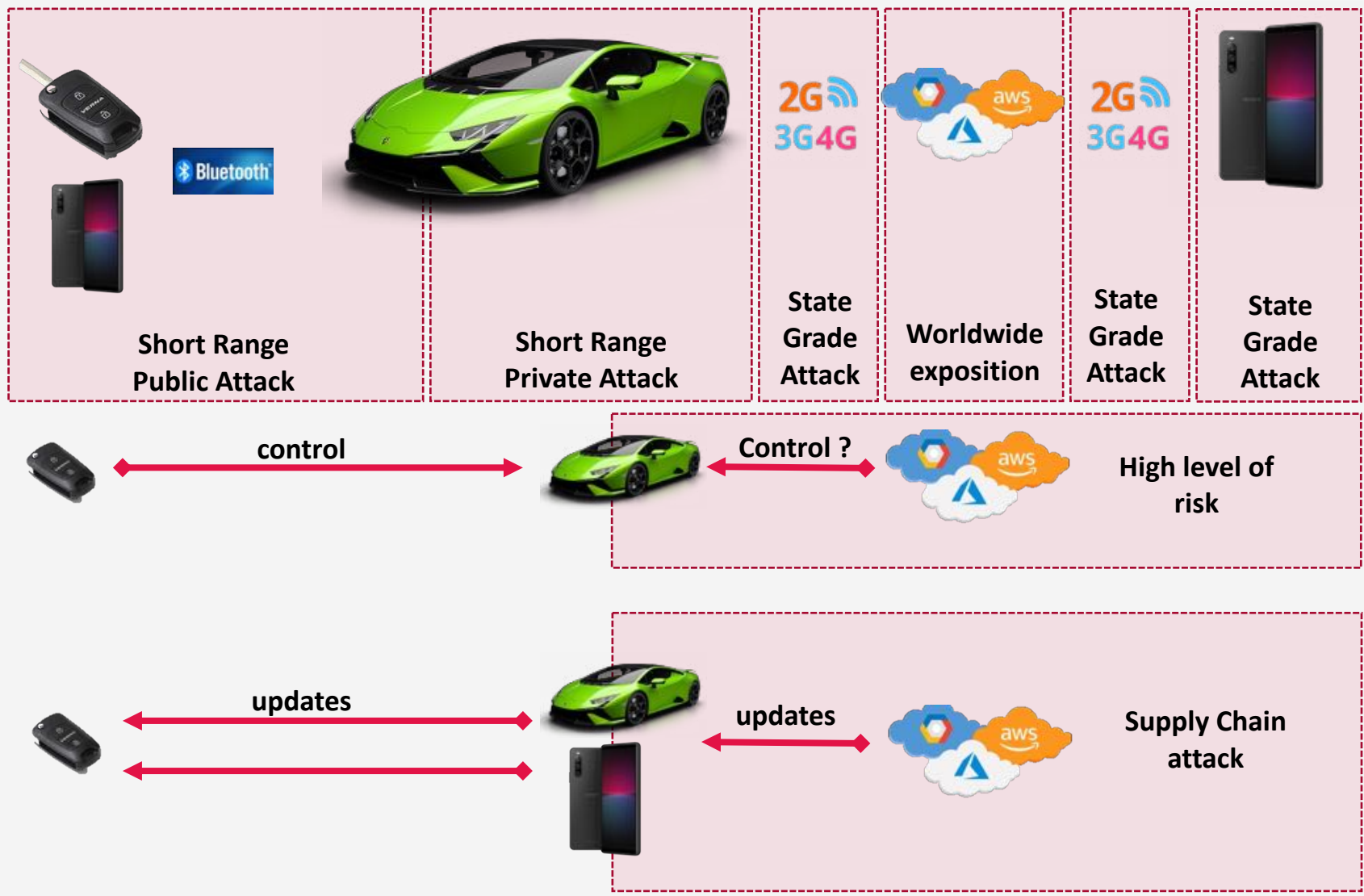
IoT security usually focus on the device security.
An IoT Solution is a wide range of components where security rules apply all along.





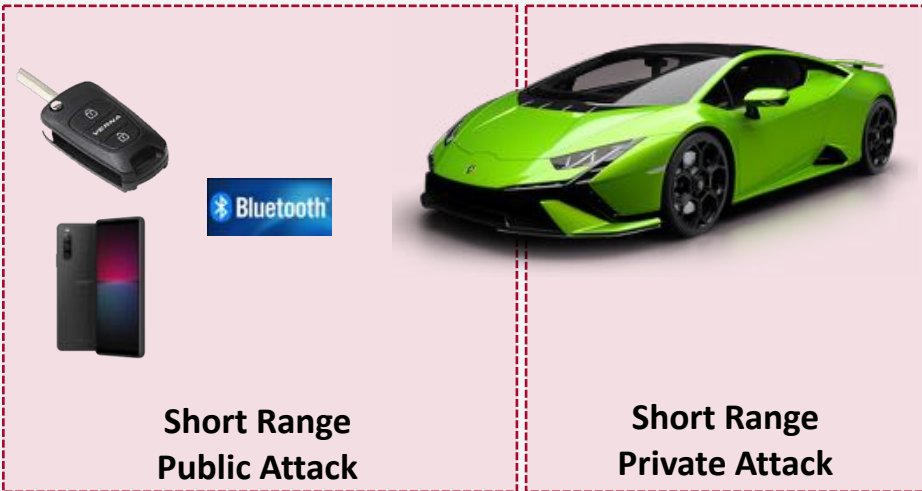
IoT Solution attack surface







IoT security usually focus on the device security.
An IoT Solution is a wide range of components where security rules apply all along.





Focus on the device part, each layer is important



-  **RADIO**
-  **STORAGE**
-  **FIRMWARE**
-  **BOOT DFU**
-  **PCB**
-  **Mechanical**

Protect the radio layer against being listening, repeated, identity usurpation, consider jamming.

Secure the keys, make them unique

Protect the access to the firmware
Make the software as unique as possible

Secure the software update procedure.
Make sure of the Authenticity

Reduce the access to the software

Reduce the access to the hardware & software, force the user to destroy the key to access it.

Security design is a global solution, not layer oriented





OWASP

Framework for best practices...

Mandatory to make sure you have considered it or it's a malpractice...

But it not makes your solution secured

Security Verification Requirements

Design

#	Bluetooth		L1	L2	L3
5.1.1	#	Description			
	4.3.1	Verify that pairing and discovery is blocked in Bluetooth devices except when necessary.	✓	✓	✓
5.1.2	4.3.2	Verify that PIN or PassKey codes are not easily guessable (e.g. don't use 0000 or 1234).	✓	✓	✓
5.1.3	4.3.3	Verify that devices using old versions of Bluetooth with simple modes of authentication enabled require a PIN for pairing.	✓	✓	✓
5.1.4	4.3.4	Verify that for modern versions of Bluetooth, at least 6 digits are required for Secure Simple Pairing (SSP) authentication under all versions except "Just Works".	✓	✓	✓
5.1.5					
5.1.6	4.3.5	Verify that encryption keys are the maximum size the device supports and that this size is sufficient to adequately protect the information transmitted over the Bluetooth connection.	✓	✓	✓
5.1.7	4.3.6	Verify the most secure Bluetooth pairing method available is used. Verify Out Of Band (OOB), Numeric Comparison, or Passkey Entry pairing methods are used depending on the communicating device's capabilities.	✓	✓	✓
5.1.8					
	4.3.7	Verify the strongest Bluetooth Security Mode and Level supported by the device is used. For example, for Bluetooth 4.1 devices, Security Mode 4, Level 4 should be used to provide authenticated pairing and encryption.	✓	✓	✓

<https://github.com/OWASP/IoT-Security-Verification-Standard-ISVS>



Because security requirements change everyday but your technical solution does not !



BLE

Like other technology, there is a difference between the technology life-cycle and the product life-cycle



- 2010 – BLE 4.0
- 2013 – BLE 4.1
- 2014 – BLE 4.2
- 2016 – BLE 5.0
- 2019 – BLE 5.1
- 2020 – BLE 5.2

Technical improvement but also security improvement



No Hardware update over 10 years of car life duration. This could be x4 with electric cars. What about software updates ?

Still, lots of the working vehicles have been designed at a time WEP was a standard...

A good starting point on BLE security <https://forum.digikey.com/t/a-basic-introduction-to-ble-4-x-security/12501>



BLUETOOTH VULNERABILITIES

Bluetooth security as a standard and well-known technology is strongly challenged and press loves to report information about it.

A critical flaw found in Bluetooth Low Energy (BLE) receivers may grant cyber criminals entry to anything from personal devices, such as phones or laptops, to even cars and houses. The [new findings](#) from cybersecurity company NCC Group detail how BLE uses proximity to authenticate that the user is near the device. This has been able to be faked as part of the research, which could affect everyone from the average consumer to organizations seeking to lock the doors to their premises.

This issue is believed to be something that can't be easily patched over or just an error in Bluetooth specification. This exploit could affect millions of people, as BLE-based proximity authentication was not originally designed for use in critical systems such as locking mechanisms in smart locks, according to NCC Group.

Must-read security coverage

- 85% of Android users are concerned about privacy
- Almost 2,000 data breaches reported for the first half of 2022
- In security, there is no average behavior
- How to secure your email

Vulnerabilities found in Bluetooth Low Energy gives hackers access to numerous devices

by **Brian Stone** in **Security** on May 17, 2022, 1:09 PM PDT

NCC Group has found proof of concept that BLE devices can be exploited from anywhere on the planet.



TechnologyAdvice

Buyer's Guide to CRM Software

Download Now >

Home / Innovation / Security

BLURtooth vulnerability lets attackers overwrite Bluetooth authentication keys

All devices using the Bluetooth standard 4.0 through 5.0 are vulnerable. Patches not immediately available.

EXPLOITS AND VULNERABILITIES

BrakTooth Bluetooth vulnerabilities, crash all the devices!

Posted: September 2, 2021 by [Pieter Arntz](#)

Security researchers have [revealed](#) details about a set of 16 vulnerabilities that impact the Bluetooth software stack that ships with System-on-Chip (SoC) boards from several popular vendors. The same group of researchers disclosed the SweynTooth vulnerabilities in February 2020. They decided to dub this set of vulnerabilities BrakTooth.

BrakTooth affects major SoC providers such as Intel, Qualcomm, Texas Instruments, Infineon (Cypress), Silicon Labs and others. Vulnerable chips are used by Microsoft Surface laptops, Dell desktops, and several Qualcomm-based smartphone models.

New Bluetooth vulnerability can hack a phone in 10 seconds

John Biggs [@johnbiggs](#) / 11:22 PM GMT+12 • September 12, 2017 [Comment](#)



Security company Armitis has found a collection of eight exploits, collectively called **BlueBorne**, that can allow an attacker access to your phone without touching it. The attack can allow access to computers and phones, as well as IoT devices.

Major Bluetooth Vulnerability

Bluetooth has a [serious security vulnerability](#):

In some implementations, the elliptic curve parameters are not all validated by the cryptographic algorithm implementation, which may allow a remote attacker within wireless range to inject an invalid public key to determine the session key with high probability. Such an attacker can then passively intercept and decrypt all device messages, and/or forge and inject malicious messages.

[Paper](#), [Website](#), [Three news articles](#).

This is serious. Update your software now, and try not to think about all of the Bluetooth applications that can't be updated.



BLUETOOTH VULNERABILITIES

Bluetooth figures many vulnerabilities over the years:

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-121r2-upd1.pdf> (2017)

	Security Issue or Vulnerability	Remarks	Connections Using Version(s)...
1	Link keys based on unit keys are static and reused for every pairing.	A device that uses unit keys will use the same link key for every device with which it pairs. This is a serious cryptographic key management vulnerability.	1.0 1.1
2	Use of link keys based on unit keys can lead to eavesdropping and spoofing.	Once a device's unit key is divulged (i.e., upon its first pairing), any other device that has the key can spoof that device or any other device with which it has paired. Further, it can eavesdrop on that device's connections whether they are encrypted or not.	1.0 1.1 1.2
3	Security Mode 1 devices never initiate security mechanisms.	Devices that use Security Mode 1 are inherently insecure. For 2.0 and earlier devices, Security Mode 3 (link level security) is highly recommended.	1.0 1.1 1.2 2.0
4	PINs can be too short.	Weak PINs, which are used to protect the generation of link keys during pairing, can be easily guessed. People have a tendency to select short PINs.	1.0 1.1 1.2 2.0
5	PIN management and randomness is lacking.	Establishing use of adequate PINs in an enterprise setting with many users may be difficult. Scalability problems frequently yield security problems. The best alternative is for one of the devices being paired to generate the PIN using its random number generator.	1.0 1.1 1.2 2.0
6	The encryption keystream repeats after 23.3 hours of use.	As shown in Figure 3-7, the encryption keystream is dependent on the link key, EN RAND, Master BD_ADDR, and Clock. Only the Master's clock will change during a particular encrypted connection. If a connection lasts more than 23.3 hours, the clock value will begin to repeat, hence generating an identical keystream to that used earlier in the connection. Repeating a keystream is a serious cryptographic vulnerability that would allow an attacker to determine the original plaintext.	1.0 1.1 1.2 2.0
7	Just Works association model does not provide MITM protection during pairing, which results in an unauthenticated link key.	For highest security, BR/EDR devices should require MITM protection during SSP and refuse to accept unauthenticated link keys generated using Just Works pairing.	2.1 3.0 4.0 4.1 4.2
8	SSP ECDH key pairs may be static or otherwise weakly generated.	Weak ECDH key pairs minimize SSP eavesdropping protection, which may allow attackers to determine secret link keys. All devices should have unique, strongly-generated ECDH key pairs that change regularly.	2.1 3.0 4.0 4.1 4.2
9	Static SSP passkeys facilitate MITM attacks.	Passkeys provide MITM protection during SSP. Devices should use random, unique passkeys for each pairing attempt.	2.1 3.0 4.0 4.1 4.2
10	Security Mode 4 devices (i.e., 2.1 or later) are allowed to fall back to any other security mode when connecting with devices that do not support Security Mode 4 (i.e., 2.0 and earlier).	The worst-case scenario would be a device falling back to Security Mode 1, which provides no security. NIST strongly recommends that a Security Mode 4 device fall back to Security Mode 3 in this scenario.	2.1 3.0 4.0 4.1 4.2
11	Attempts for authentication are repeatable.	A mechanism needs to be included in Bluetooth devices to prevent unlimited authentication requests. The Bluetooth specification requires an exponentially increasing waiting interval between successive authentication attempts. However, it does not require such a waiting interval for authentication challenge requests, so an attacker could collect large numbers of challenge responses (which are encrypted with the secret link key) that could leak information about the secret link key.	All
12	The master key used for broadcast encryption is shared among all piconet devices.	Secret keys shared amongst more than two parties facilitate impersonation attacks.	1.0 1.1 1.2 2.0 2.1 3.0

	Security Issue or Vulnerability	Remarks	Connections Using Version(s)...
13	The E0 stream cipher algorithm used for Bluetooth BR/EDR encryption is relatively weak.	FIPS-approved encryption can be achieved by layering application-level FIPS-approved encryption over the Bluetooth BR/EDR encryption. Note that Bluetooth low energy uses AES-CCM.	1.0 1.1 1.2 2.0 2.1 3.0 4.0
14	BR/EDR privacy may be compromised if the Bluetooth device address (BD_ADDR) is captured and associated with a particular user.	Once the BD_ADDR is associated with a particular user, that user's activities and location could be tracked. For low energy, address privacy can be implemented to reduce this risk.	1.0 1.1 1.2 2.0 2.1 3.0
15	Low energy privacy may be compromised if the Bluetooth address is captured and associated with a particular user.	For low energy, address privacy can be implemented to reduce this risk.	4.0 4.1 4.2
16	Device authentication is simple shared-key challenge/response.	One-way-only challenge/response authentication is subject to MITM attacks. Bluetooth provides for mutual authentication, which should be used to provide verification that devices are legitimate.	1.0 1.1 1.2 2.0 2.1 3.0
17	Low energy legacy pairing provides no passive eavesdropping protection.	If successful, eavesdroppers can capture secret keys (i.e., LTK, CSRK, IRK) distributed during low energy pairing. ¹³	4.0 4.1
18	Low energy Security Mode 1 Level 1 does not require any security mechanisms (i.e., no authentication or encryption).	Similar to BR/EDR Security Mode 1, this is inherently insecure. Low energy Security Mode 1 Level 4 (authenticated pairing and encryption) is highly recommended instead.	4.0 4.1 4.2
19	Link keys can be stored improperly.	Link keys can be read or modified by an attacker if they are not securely stored and protected via access controls.	All
20	Strengths of the pseudo-random number generators (PRNG) are not known.	The Random Number Generator (RNG) may produce static or periodic numbers that may reduce the effectiveness of the security mechanisms. Bluetooth implementations should use strong PRNGs based on NIST standards. See NIST SP 800-90A, SP 800-90B, SP 800-90C.	All
21	Encryption key length is negotiable.	The 3.0 and earlier specifications allow devices to negotiate encryption keys as small as one byte. Bluetooth low energy requires a minimum key size of seven bytes. NIST strongly recommends using Secure Connections Only Mode which requires the full 128-bit key strength (AES-CCM) for both BR/EDR and low energy.	1.0 1.1 1.2 2.0 2.1 3.0
22	No user authentication exists.	Only device authentication is provided by the specification. Application-level security, including user authentication, can be added via overlay by the application developer.	All
23	End-to-end security is not performed.	Only individual links are encrypted and authenticated. Data is decrypted at intermediate points. End-to-end security on top of the Bluetooth stack can be provided by use of additional security controls.	All
24	Security services are limited.	Audit, non-repudiation, and other services are not part of the standard. If needed, these services can be incorporated in an overlay fashion by the application developer.	All
25	Discoverable and/or connectable devices are prone to attack.	Any BR/EDR/HS device that must go into discoverable or connectable mode to pair or connect should only do so for a minimal amount of time. A device should not be in discoverable or connectable mode all the time.	All
26	The Just Works pairing method provides no MITM protection.	MITM attackers can capture and manipulate data transmitted between trusted devices. Low energy devices should be paired in a secure environment to minimize the risk of eavesdropping and MITM attacks. Just Works pairing should not be used for low energy.	4.0 4.1 4.2
27	With two already paired BR/EDR/HS devices, mutual authentication may not always happen with Security Mode 3 and 4	With two devices already paired, if device A is the authentication initiator to B, encryption setup will begin after that initial authentication. If the encryption setup being successful is good enough to satisfy B, then B may never bother to attempt to authenticate A.	1.0 1.1 1.2 2.0 2.1 3.0



UNCERTAINTY

Question is never

“will it be unsecured ?”

but

“How to manage the soon coming security break”

The screenshot shows a news article from 'Journal du Geek'. The header includes the site name and a menu icon. The article is categorized under 'ORDINATEURS'. The title is 'L'un des meilleurs algorithmes de chiffrement du monde vient de tomber'. The text below the title reads: 'Les algorithmes de chiffrement les plus puissants du monde ont parfois des failles toutes simples, il suffit de savoir les exploiter.' The author is identified as 'Tristan' and the date is 'le 5 août 2022'. At the bottom of the screenshot is a photograph of a laptop keyboard with a blue combination padlock resting on it.

Interesting story : NIST (main expert about encryption) had a worldwide contest for the next encryption algorithm generation, quantum resistant !

After a long work of multiple years of selection and review of the different proposal, they finally select 4 and one of them is SICK (well named !)

It has been 1 hour of computation on a single core computer to break the code !



MANAGE UNCERTAINTY

You do not master the
future security

1

BELIEVE ON SECURITY STANDARD

You have not choice about this, in case of any trouble you will be faulty if not respecting the standard, owasp ... even if the customer experience is lower.

2

DO NOT (ONLY) BELIEVE ON SECURITY STANDARD

Adding your secret sauce will preserve you from being under attack the same way as the majority when the breach will appear

3

MAKE SURE YOU CAN DEPLOY UPDATES QUICKLY

In 2022 remote controlled update is a mandatory solution to have. You need to make sure it works; you need to make sure it is secured, and you need to make sure it will continue to work in 20 years

4

PEN TEST YOUR SOLUTION ON REGULAR BASIS

It's always better to be the first informed by a security breach. Security is too much dynamic with a large creation of toolkits and new approach to consider you can master this. Open your solution to pen-test and bug bounty on regular basis is the best way to get the feedback.

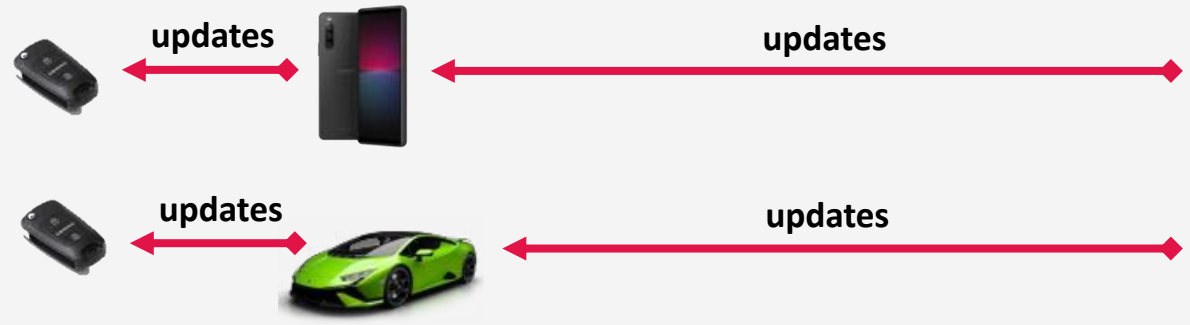
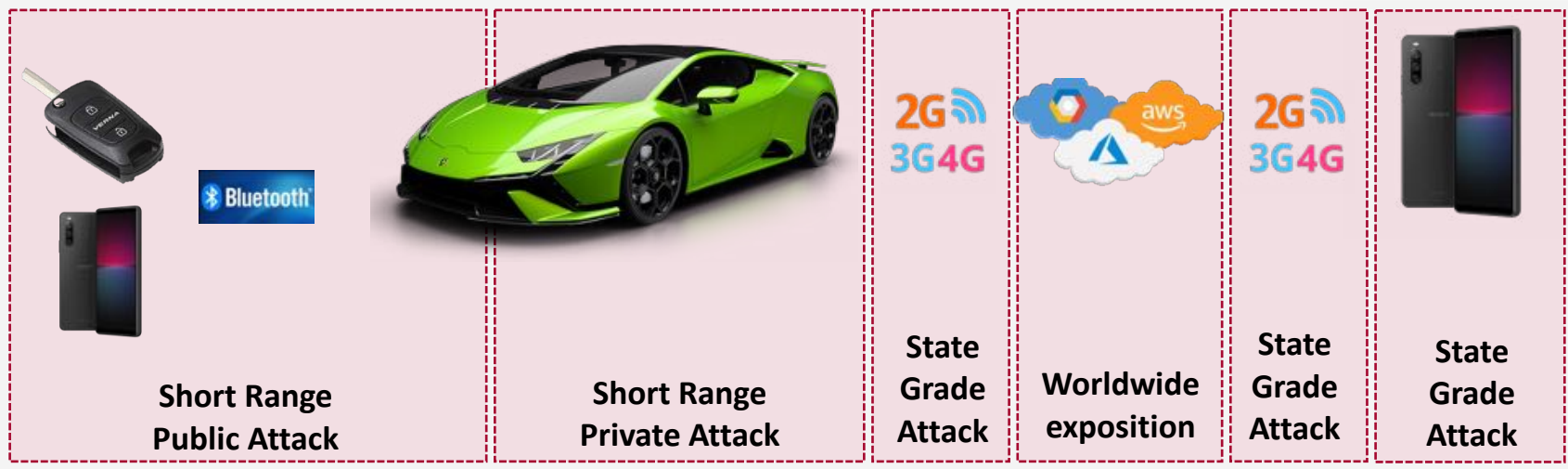
Because security is a day-to-day activity it requires support revenues and not only design fees

Slides about trust chain



IoT UPDATE CONSIDERATION

That's important to consider the options in regard of the device life duration ...



What's best option ?

Are you certain smartphones will work the same way in 20 years ?
Are you sure you will maintain mobile application for the next 20 years ?



IoT UPDATE CONSIDERATION

Over a technical solution, Update is a question of process and run.

Update needs to be designed before the hardware released.

1

PERFORM REGULAR UPDATES

If you only update device fleet during crisis, the update itself will start being source of new crisis.

2

DEFINE ROLL OUT UPDATE RULES

Do not deploy the entire park at once... process group by group ... you are quite sure that it will crash on 1% of target every time ... are you sure you can manage this ? 1% of 1.000.000 Rollback solution is mandatory

3

SIGN THE UPDATES

Each device should have a different update, sign specifically for itself. That way your control supply chain attack better than "robotrock"

4

ROLLBACK & BATTERY IS ALWAYS A MESS

Upgrade process is costly in terms of energy ... battery control is a key point; this is one of the reason why the upgrade process will fail. At any step of the upgrade process, the device has to switch back into the previous version. At the design step, the required flash, watchdog must be in place to cover this.

Hackers in Action



Starlink Analysis

Step 1 - get the firmware

Do not let them access the circuits easily !

Identifying eMMC test points

Reading eMMC in-circuit

Reading eMMC in-circuit

SD card reader

TXS0202EVM Level shifter

Low Voltage eMMC Adapter by exploit.ee.rs

Power-cut

```

center_power_cut.t.trip 99.0
cpu0_power_cut.t.trip 128.0
cpu1_power_cut.t.trip 118.0
dof_power_cut.t.trip 118.0

center_power_cut.persistence_limit 2000 # 40 seconds
cpu0_power_cut.persistence_limit 2000 # 40 seconds
cpu1_power_cut.persistence_limit 2000 # 40 seconds
dof_power_cut.persistence_limit 2000 # 40 seconds

power_cut_reboot_delay 30000 # 10 minutes

Forced-idle

```

```

"channel_id": 13,
"direction": "uplink",
"end": 14.1875,
"start": 14.125
},
{
"channel_id": 14,
"direction": "uplink",
"end": 14.25,
"start": 14.1875
},
"laser_channel_definitions": [
{
"color": "LASER_COLOR_RED",
"frequency_ghz": 192700,
"itu_channel_id": 27
},
{
"color": "LASER_COLOR_BLUE",
"frequency_ghz": 193500,
"itu_channel_id": 35
}
]

```



Starlink Analysis

Get access on the machine.

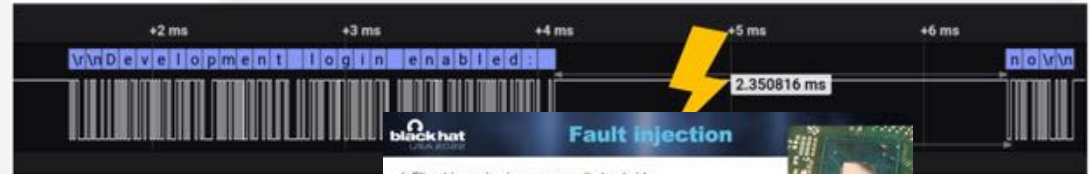
Remove all unnecessary traces, they are a great help for hackers.

black hat USA 2022 Obtaining root

```

Development login enabled: no
SpaceX User Terminal.
user1 login: echo -n "Development login enabled: "
if [ $(is_production_hardware) -eq 0 ]; then
  echo "yes"
  sed -i -e 's/^\(root:[^:]*\)\/root:tSXNnW65X1Er.\/' /etc/shadow 2>/dev/null || true
else
  echo "no"
  if [[ $(whatVehicleAmI) = "uterm" ]]; then
    # Discard console output for production user terminals.
    consoletype=ttynull
  fi
fi

```



black hat USA 2022 Fault Injection

- ✓ Flip-chip packaging exposes die backside
 - Laser Fault Injection, Body Bias Injection, Electromagnetic Fault Injection
- x PCB is too big for our automatic XYZ positioning equipment
 - Likely cumbersome to do on a roof...
- x No development kits
 - Differential clock input
 - (But PLL?)
 - Reset line
 - Voltage Fault Injection

black hat USA 2022 Exam

```

Development login enabled: [ 7.387682] 002: Unable to handle kernel NULL pointer dereference at virtual address 0000000000000000
[ 7.387702] 002: Mem abort info:
sh: 0: unknown operand
[ 7.387704] 002:  ESR = 0x36000006
yes
[ 7.387707] 002:  EC = 0x25: DABT (current EL), IL = 32 bits
[ 7.387711] 002:  SET = 0, FnV = 0
[ 7.387714] 002:  EA = 0, s1PTW = 0
[ 7.387716] 002: Data abort info:
[ 7.387718] 002:  ISV = 0, ISS = 0x00000006
[ 7.387721] 002:  CM = 0, WNR = 0
[ 7.387723] 002: user pgtable: 4k pages, 39-bit VAs, pgdp=00000000a51fd000
[ 7.387730] 002: [0000000000000520] pgd=00000000a50d1003, pud=00000000a50d1003, pmd=0000000000000000
[ 7.387739] 002: Internal error: Oops: 96000006 [#1] PREEMPT_RT SMP
[ 7.387748] 002: Modules linked in:
[ 7.387753] 002: CPU: 2 PID: 275 Comm: syslogd Not tainted 5.4.34-rt21-gfd24730 #1
[ 7.387760] 002: Hardware name: spacex satellite user terminal (DT)
[ 7.387766] 002: pstate: 00000005 (mzcv daif -PAN -UAO)
[ 7.387770] 002: pc : do undefinstr+0x2c/0x1d8
[ 7.387787] 002: lr : el0_undef+0xc/0x10
[ 7.387793] 002: sp : ffffffff0145b3e70
[ 7.387797] 002: x29: ffffffff0145b3e70 x28: ffffffff802580a00
[ 7.387803] 002: x27: 0000000000000000 x26: 0000000000000000
[ 7.387808] 002: x25: 0000000020000000 x24: 0000000000000000
[ 7.387814] 002: x23: 0000000000000000 x22: 000000000000403fb0
[ 7.387818] 002: x21: 00000000ffffffff x20: 0000000000000000
[ 7.387823] 002: x19: 0000000000000018 x18: 0000000000000000
[ 7.387828] 002: x17: 0000000000000000 x16: 0000000000000000
[ 7.387832] 002: x15: 0000000000000000 x14: 0000000000000000

```

```

388 Development login enabled: yes
389
390 SpaceX User Terminal.
391 user1 login: root
392 Password:
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412 The Flight Software does not log to the console. If you wish to view
413 the output of the binaries, you can use:
414 tail -f /var/log/messages
415
416 Or view the viceroy telemetry stream.
417
418
419 ~#id: 7-0x10: [r-0x10: [999;999H-0x10: [6n[root@user1 ~]# id
420 uid=0(root) gid=0(root) groups=0(root),10(wheel),1000(signers)

```



Starlink Analysis

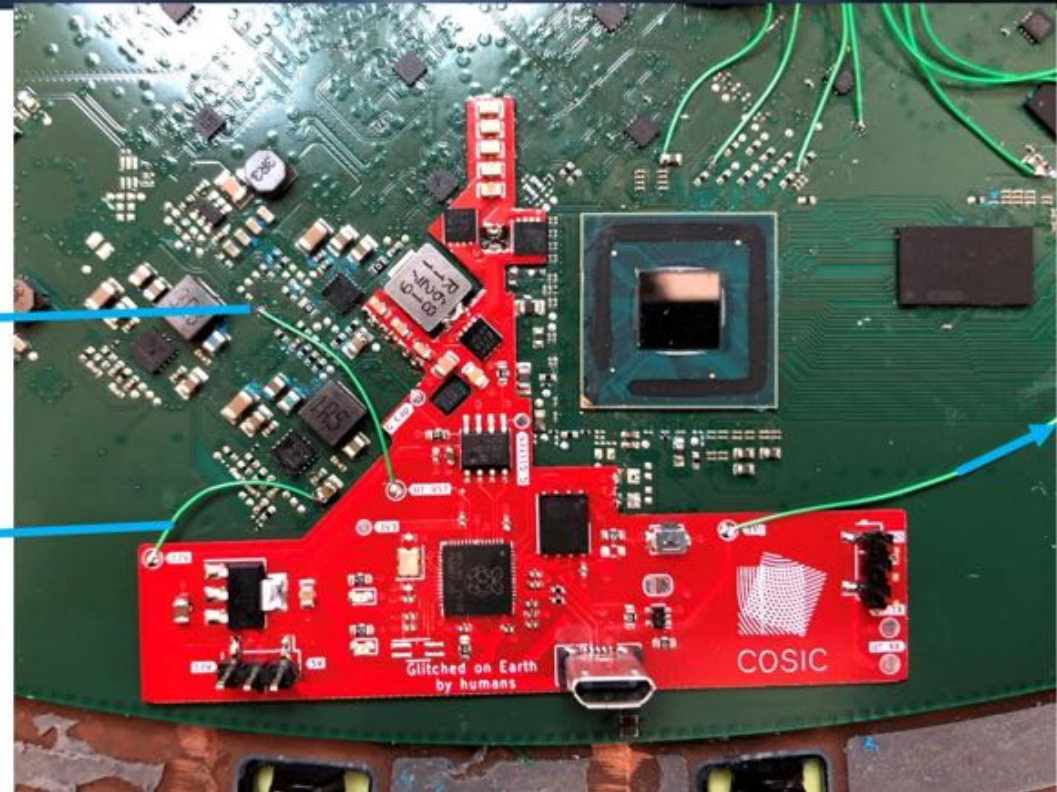
Make it simple for the others...

I said : Never let them play with the PCB !

Core voltage regulator enable pin (for power cycling)

12V for MOSFET drivers and standalone power

1V8 for level shifter





Starlink Analysis

React ...

Hacker always win !

black hat USA 2022 **SpaceX strikes back**

- I did a firmware update...
- Previously unused eFuse is now blown and disables UART output
- Modchip was designed to trigger on UART

```

if (L'\xffffffff' < BSEC_UART_EN) {
  DAT_30204160_UART_EN = L'\xde486bc3';
}
if (DAT_30204160_UART_EN == L'\xde486bc3') {
  _GLLCFF_SYSCFG_PIO_A_BASE = _GLLCFF_SYSCFG_PIO_A_BASE & 0xf;
  DataSynchronizationBarrier(3,3);
  _GLLCFF_SYSCFG_PIO_A_BASE_A0 = _GLLCFF_SYSCFG_PIO_A_BASE_A0;
  DataSynchronizationBarrier(3,3);
  uVar1 = 10000000;
  if ((_BOOTMODE_REGISTER_09130048 & 1) != 0) {
    uVar1 = 200000000;
  }
  set_uart_baud(&UART_BAUDRATE, uVar1, 115200);
  printf(s_INFO: _AUTOSTARTUP_MODE = _d_3000b08e, (ulong)(_BOOTMODE_REGISTER_09130048 & 1));
}

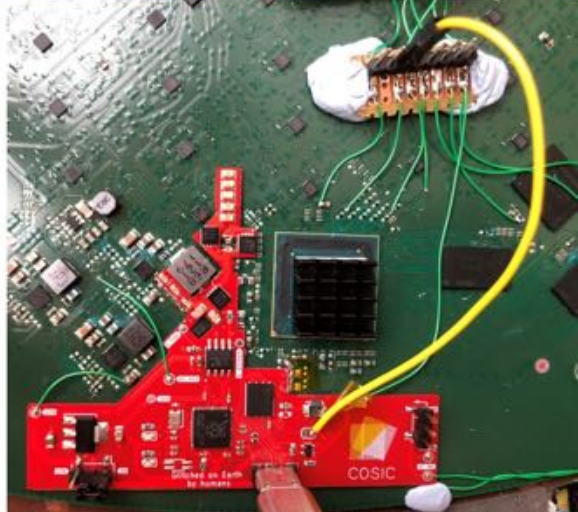
```



#BHUSA @BlackHatEvent

black hat USA 2022 **Overcome**

- Trigger on eMMC D0 instead of UART
- Modchip could be easily adapted
 - Disconnect UT UART TX
 - Connect to eMMC D0
 - Update glitch parameters from Python
- Alternative: new PCB revision





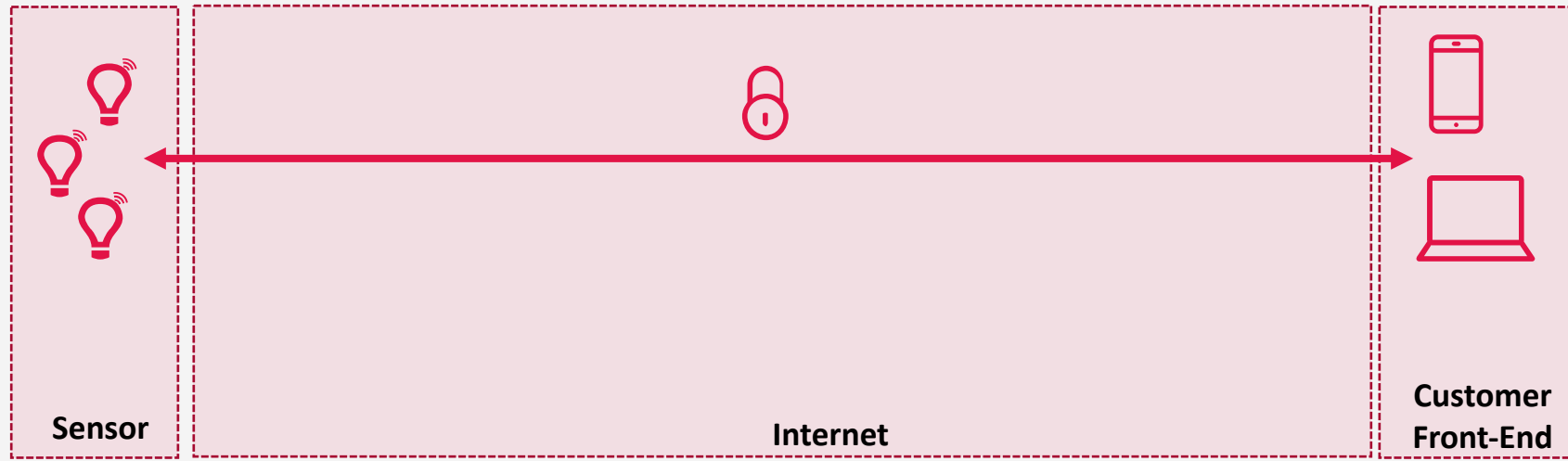
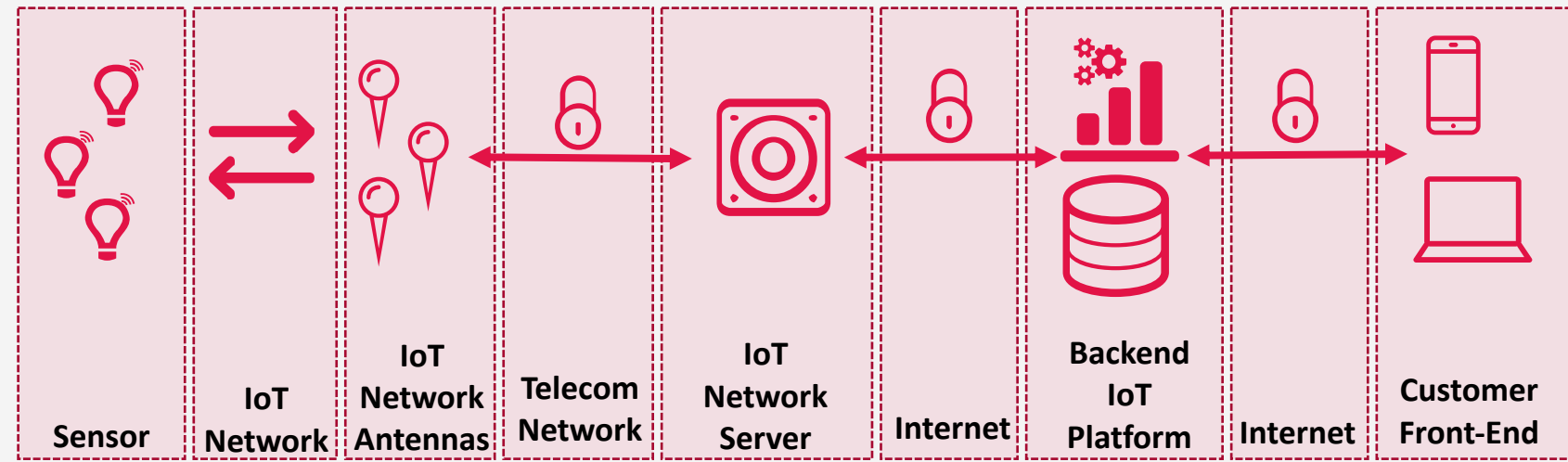
IoT is finger pointed for lack of security, What is the truth, what to do ?





IoT Solution attack surface

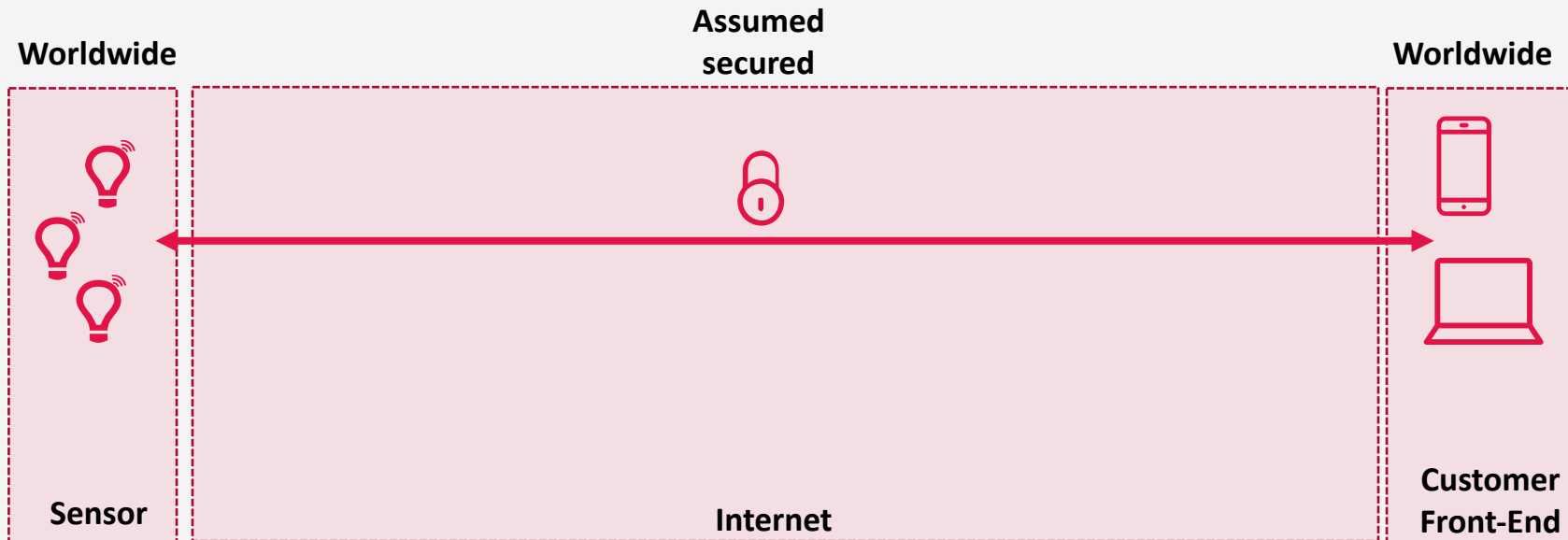
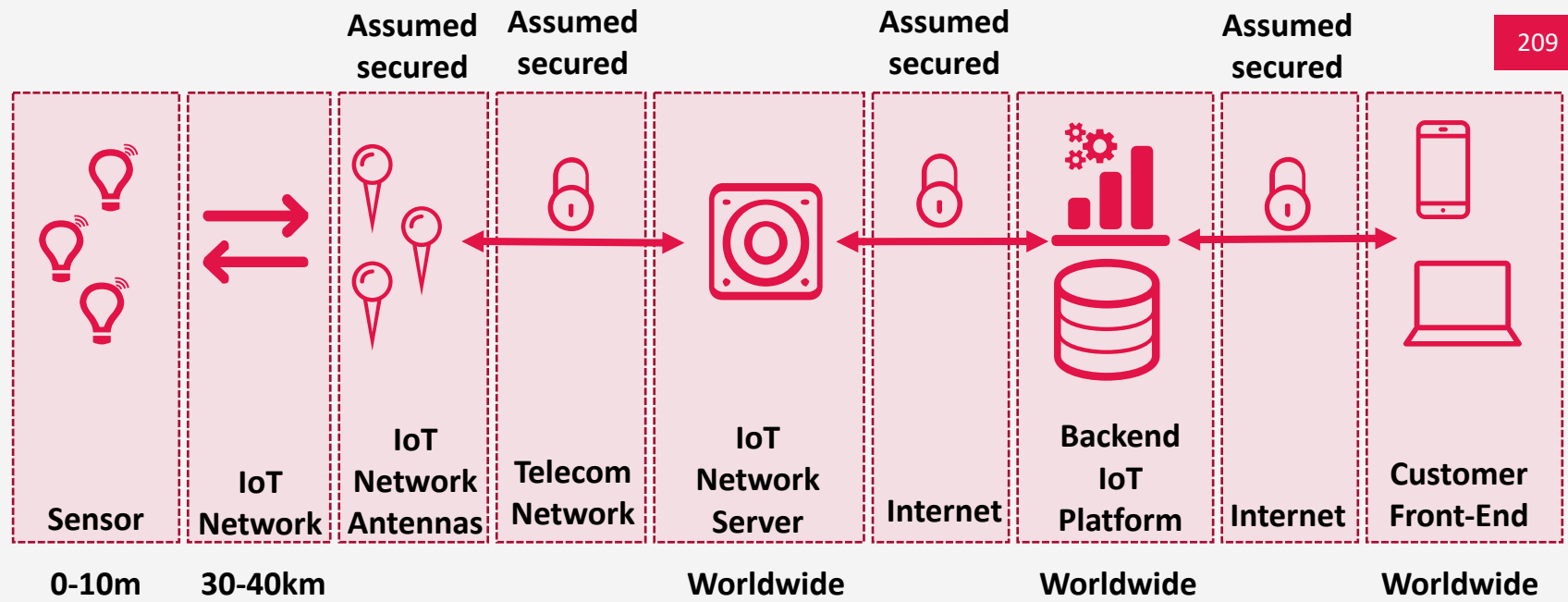
IoT security usually focus on the device security.
An IoT Solution is a wide range of components where security rules apply all along.





Attack distance weighting

Distance between the targeted element and the attacker determines the risk level and its impact. Each of the component have different level of risk that way.



This is not an IoT: this is computer with a camera. You need to secure it like a server



DIRECTLY ACCESSIBLE FROM INTERNET, WORLDWIDE

USUALLY RUNNING AN OUTDATED OPERATING SYSTEM

WITH A POOR SOFTWARE QUALITY NEVER MAINTAINED

Why ? Because it is not an IoT Solution, You've just bought hardware!

Device layer attack

You need a physical access to the device or a near proximity. Bluetooth, Serial port ... are common vectors.



HOW ?

Device Update mechanism, physical manipulation, hardware modification and addition are the classical way to attack an IoT device.



WHY ?

Ransomware, destruction, competition, data thief ...
Because it's possible or because it's cool to talk about IoT security





A connected thermostat hacked to maintain temperature over 37°C until you pay a ransom.



Everything in the thermostat runs with **root** privileges. “**We got command injection by the SD card**, so it was a local attack,” Tierney explained. “With root, you can set off alarm (and set the frequency very high) and can heat and cool at the same time.” While this was a local attack, it also isn’t impossible to pull this off without gaining physical access to the device. The thermostat owner can use the SD card to load custom settings or wallpaper

A connected thermostat hacked to maintain temperature over 37°C until you pay a ransom.



DEVICE SECURITY IS PART OF DESIGN

As a device maker, you need to define the security expectations.

Security engineering cost is high and can only be handle on project start.

Define the right level, not the highest level

Practice pen-test !

1

CONTRACT FOR MAINTENANCE

Make sure your device firmware will be maintained by an internal team or an external team. Protect budget for this.

2

EXPECT ENCRYPTION FOR ALL KEYS

Any key use inside the device need to be secured. Local storage is usually sure enough, Secure elements are more for paranoid or IP protection.

3

EXPECT ENCRYPTION FOR ALL COMMUNICATIONS

Any communication shall be encrypted by default. The engineering cost at start is low. Each of the devices must use different credential. Potentially integrate different encryption solution as your device may be live for 10 years (think about WEP)

4

MANAGE YOUR IDs

Every device must have different IDs, ensure they are not sequential, not visible from outside the packaging... Make sur a successful physical attack on one device will not allow remote access on all other devices.

5

PROTECT FIRMWARE AND REMOVE DEBUG BACK DOOR

It is common to have an unprotected device with firmware possible download or developer backdoor for debugging phase. Ensure you close them all.

IoT Network Attack

This kind of attack is possible short range and allow a certain level of security for the attacker. Depending o, device feature you can steal data or gain control of the devices.



HOW ?

By listening the device communication as radio wave are accessible for all.
By faking the device or network to communicate with device or IoT platform



WHY ?

Get access to industrial secrets, track people or assets. Destroy industrial machine, rob a house...
Also to attack you brand is a competitive market





Only trust your code !

Listening radio wave is nothing you can prevent.

LoRaWan is easy to listen but the traffic is encrypted... until it's broken

Sigfox is complex to listen (existing solution only work around 2 meters)... until it is becoming easy.

1

APPLY THE NETWORK ENCRYPTION CAPABILITIES

All the modern radio solution have an encryption layer. You need to enable it or request developers to consider it.

2

NEVER CONSIDER NETWORK ENCRYPTION SECURED

Even if these solutions are secured today, nothing make you sure it won't change in the device lifetime duration (10 years). Just think about WEP ...

3

IMPLEMENT YOU OWN END-TO-END ENCRYPTION

Add an applicative END-TO-END encryption. This will add a protection if the network standard is broken. This will also protect your data against a Network Server data leak. (more probable than a device being listen, with larger impact)

4

MANAGE ERRORS AND WEAK SIGNALS

There are multiple ways to attack a system from the network. You should track weak signals like communication loss, reboot, sequence rupture, frame with invalid key received...

Let's make a short break

LEARNING AT THIS STEP



● ——— ●

SECURITY IS PART OF THE DESIGN & COSTS

Ensure you manage the security at the beginning of the project



● ——— ●

SELECT THE RIGHT LEVEL OF SECURITY

Identify the risk exposure, find a good compromise and trace your decisions



● ——— ●

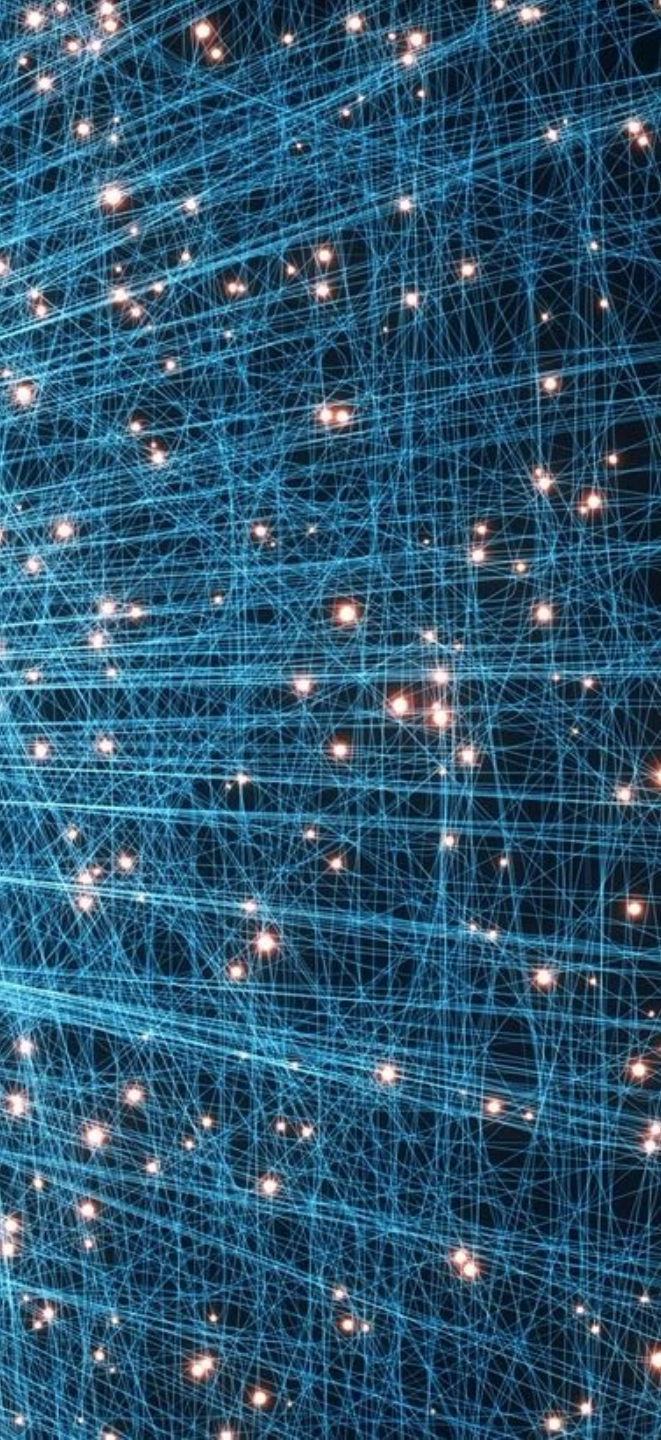
ENCRYPT EVERYTHING SENSITIVE

There is no reason to not encrypt local keys, communications... so just do it



Trust in IoT ?





Type of trust in

IoT trust chain

●
Device Identity

Make sur the physical device is the one you think it is.

●
Data Signature

Make the data has been signed by the right device

●
Data protection

Protect clear data in case of steal, loss, made public, accessible to competitors, foreign intelligence...

●
Data integrity

Make sure the IoT Data has not been deleted, corrupted, inserted after all



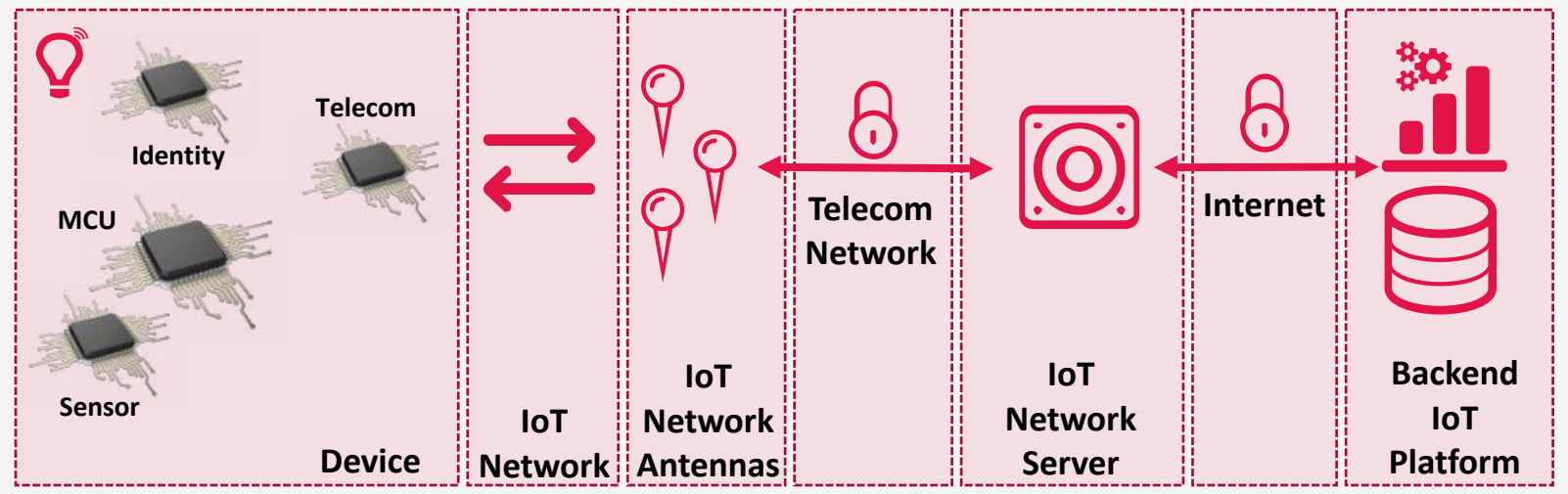
IoT data trust is not a mature area

Most of the focus is given on the transmission and the telecom mechanism are employed to trust the whole chain. But this is not working.

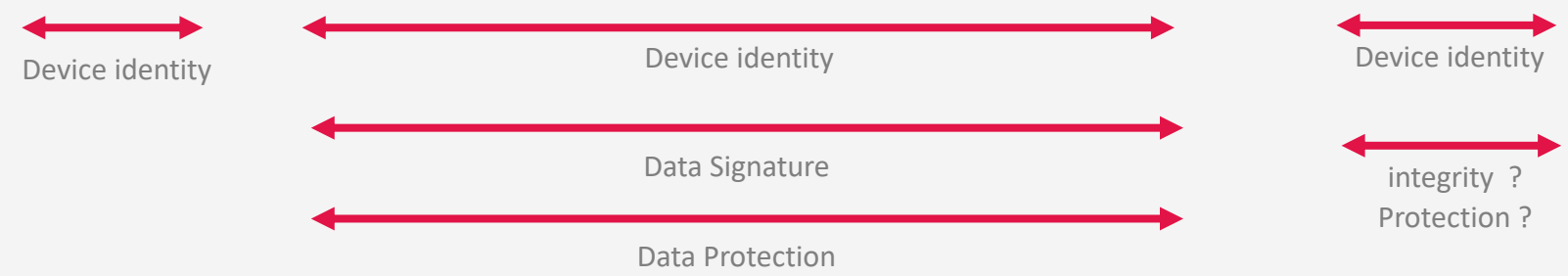
Main reason are: why trusting a temperature data ? IoT market is not yet solution oriented.

Where the concepts apply

From where to where the previous concept should apply



Where the concepts are currently deployed





DEVICE IDENTITY & DATA SIGNATURE

These two concepts basically works altogether:

- The device identity is also the way to sign the data.
- We need to make sure the identity can't be transferred.
- Identity is public
- Signature is based on a secret

1

IDENTITY

Identity can be provided by:

- QR-CODE / BAR-CODE
- RFID
- NFC
- MCU / SENSORS BURNED ID
- SECURE ELEMENT

Static / Easy to use / Easy for usurpation
 Static – Dynamic / Possible usurpation
 Static – Dynamic / Hardened
 Static – Dynamic / Complex to reproduce
 Static – Dynamic / Made to not being reproduced



DO NOT PRINT IT ON THE DEVICE !!



DEVICE IDENTITY & DATA SIGNATURE

These two concepts basically works altogether:

- The device identity is also the way to sign the data.
- We need to make sure the identity can't be transferred.
- Identity is public
- Signature is based on a secret

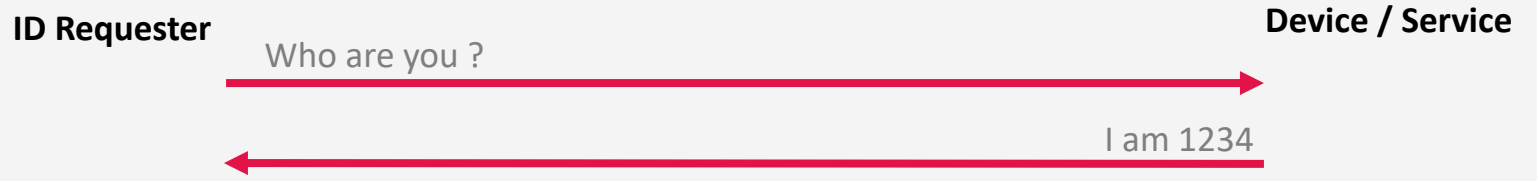
1

IDENTITY

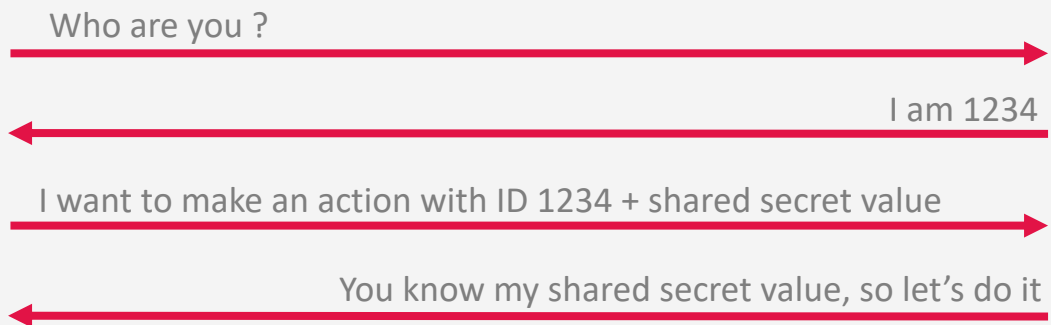
Identity can be provided by:

- QR-CODE / BAR-CODE Static / Easy to use / Easy for usurpation
- RFID Static – Dynamic / Possible usurpation
- NFC Static – Dynamic / Hardened
- MCU / SENSORS BURNED ID Static – Dynamic / Complex to reproduce
- SECURE ELEMENT Static – Dynamic / Made to not be reproduced

Stage 1 – public IDS / no protection



Stage 2 – public IDs + shared secret





DEVICE IDENTITY & DATA SIGNATURE

These two concepts basically works altogether:

- The device identity is also the way to sign the data.
- We need to make sure the identity can't be transferred.
- Identity is public
- Signature is based on a secret

1

IDENTITY

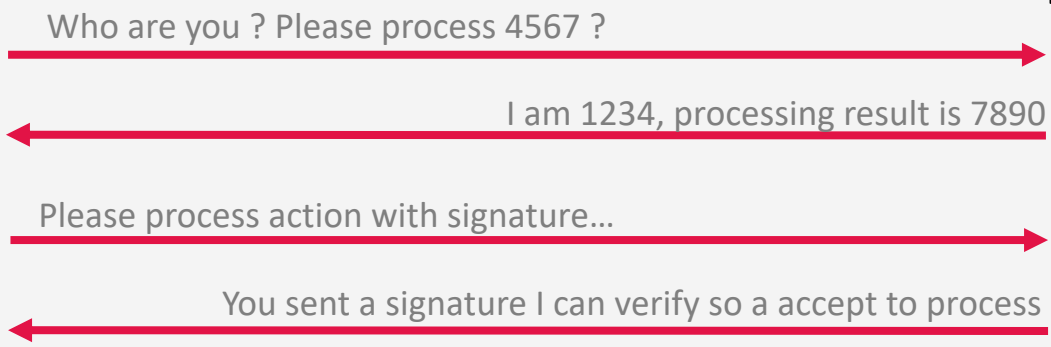
Identity can be provided by:

- QR-CODE / BAR-CODE Static / Easy to use / Easy for usurpation
- RFID Static – Dynamic / Possible usurpation
- NFC Static – Dynamic / Hardened
- MCU / SENSORS BURNED ID Static – Dynamic / Complex to reproduce
- SECURE ELEMENT Static – Dynamic / Made to not be reproduced

Stage 3 – Identification based on processing

ID Requester

Device / Service





DEVICE IDENTITY & DATA SIGNATURE

**These two concepts
basically works
altogether:**

- **The device identity is also the way to sign the data.**
- **We need to make sure the identity can't be transferred.**
- **Identity is public**
- **Signature is based on a secret**

2

SIGNATURE

Signature Key source

- Commissioned during production process
- Commissioned on setup
- Commissioned during the first communications
- MCU / SENSORS BURNED ID Static – Dynamic / Complex to reproduce
- SECURE ELEMENT Static – Dynamic / Made to not being reproduced

KEY CONCEPTS

- Signature is only known by the Service Provider
- Signature is securely stored on the Service Provider side
- Signature is securely stored on the device side according to data sensitivity.

- Signature signs the data
- Signature is per object and can serve different purpose like identity.
- Signature is unique

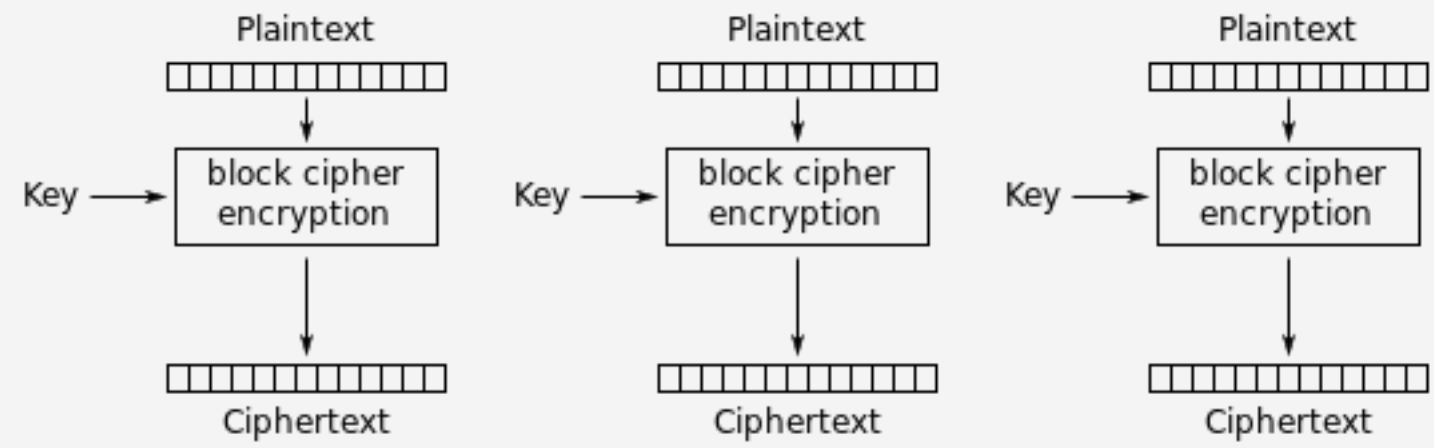
- Signature process supports small frames and reduced processing capabilities (no certificates...)

- Signature has no expiration; renewal process is possible but complex.



POSSIBLE SIGNATURE DESIGN

SIGFOX, uses AES-CBC-MAC to sign and prove the source identity of the messages, but it's better to compare to AES-ECB at the frame level



Electronic Codebook (ECB) mode encryption

- The key is shared between the emitter and the receiver
- The message to sign contains some variable element whatever the content is, like a sequence number.
- The source message size have a predefined size linked to the encryption key size, some dummy data needs to be added.
- As a result, we get the encrypted version of the message. Now you can get the last 2 or more bytes to be your message signature.
- Signature over messages must not be linked if your network is losing packets.



DATA PROTECTION

This concept ensure a third party will not be able to capture, still, copy the data.

3

DATA PROTECTION

Encryption mechanisms

- Device to Platform encryption is needed to protect the data.
- Raw data should be kept encrypted as much as possible even in the IoT platform.
- Encryption keys are secrets not accessible from any means, according to the device access potential risk
- Different encryption protocol can be integrated inside the device to ensure protection over device lifetime.
- Key generation is random
- Key renewal is a plus

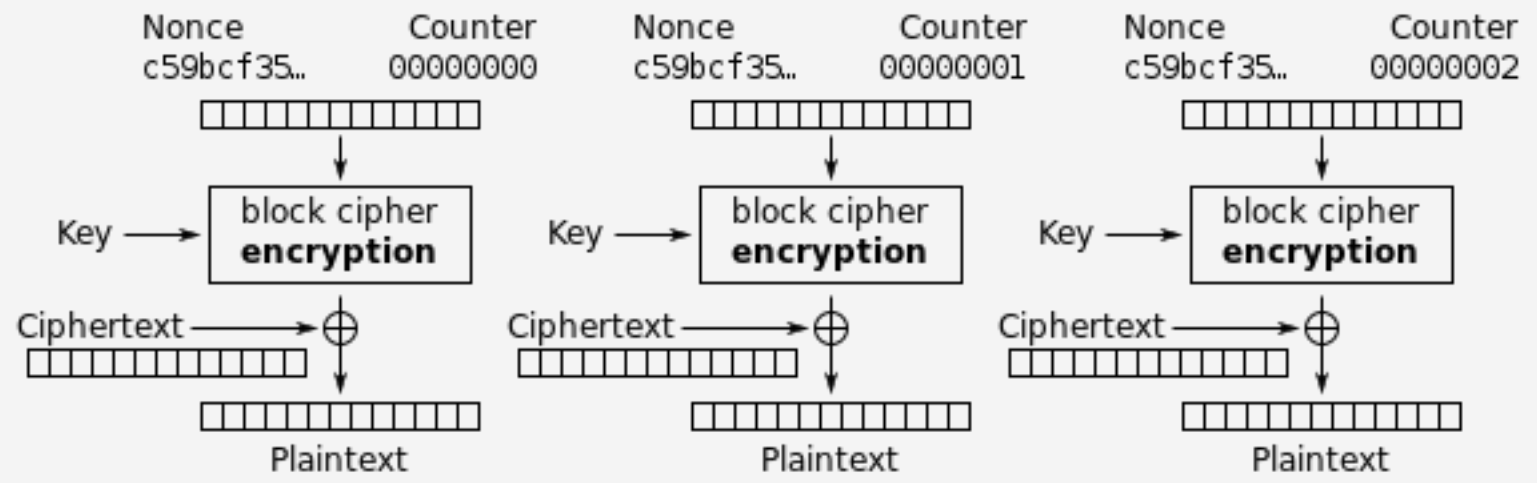
KEY CONCEPTS

- Encryption is END-TO-END.
- Do not trust the communication encryption layer
- Use unique encryption keys per devices
- Only Service provider knows the encryption keys
- Encryption keys can't be retrieved from the device
- Encryption keys size and processing is compatible with short frame and short processing capacity
- Encryption supports frame loss



POSSIBLE ENCRYPTION DESIGN

LoRaWAN, SIGFOX, uses EAS-CTR to encrypt the messages



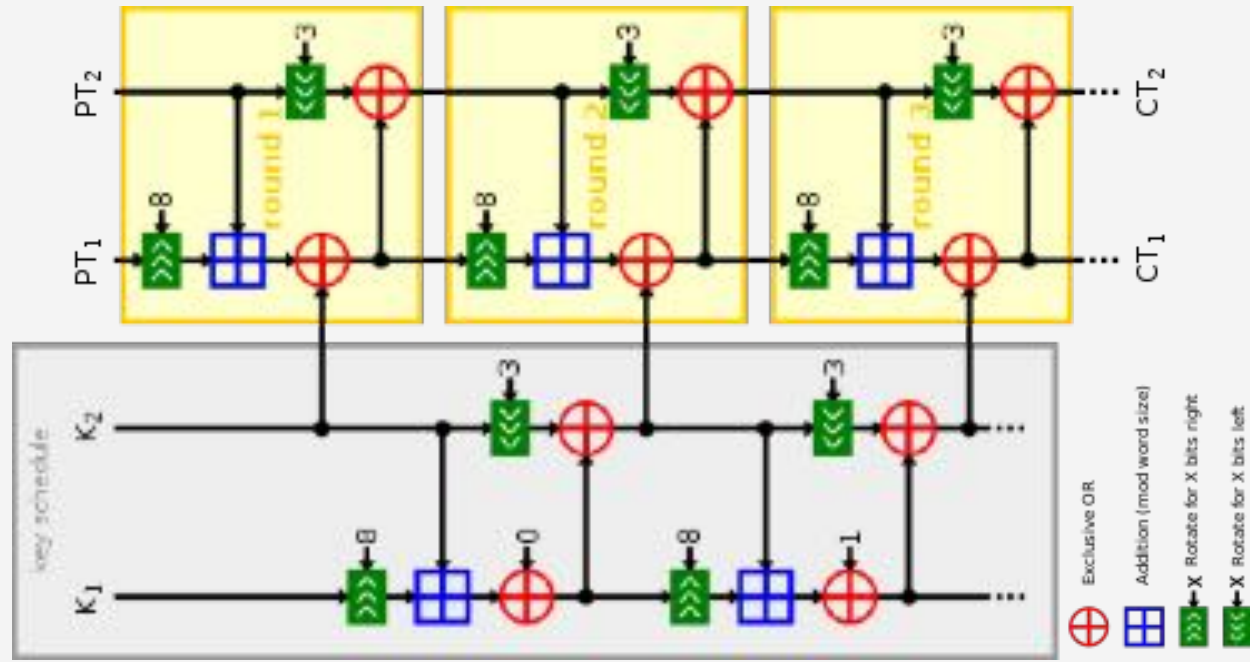
Counter (CTR) mode decryption

- The Nonce is shared between emitter and receiver, the Key also. It can be a session key or a static key.
- The counter can be retrieved directly from the received frame, it is not a secret.
- Even if only a single bit change (the counter), the overall output of the process is totally different (that is AES basics)
- And XOR is performed between the result of the encryption and the message, so the size of the message can be variable and lower to the size of the encryption key.
- This method is a "RANDOM" XOR, xor operation is bit flipping, it could have a consequence if a part of the original message is known.



POSSIBLE ENCRYPTION DESIGN

**SPECK-32 mix the bits on
a 32bits block**



- SPECK-32 is not liked by security expert as NSA is supposed to have the ability to decode ... but they kept it secret so ...
- It mixes and transform bits inside a 32b value depends on the key.
- It is fast to implement and run
- It adapts to variable payload 4,8,12,16... bytes
- It can be used with AES-CTR as well



DATA INTEGRITY

This concept ensures the data will later be able to be proven as legit: no addition, no removal, no modifications

4

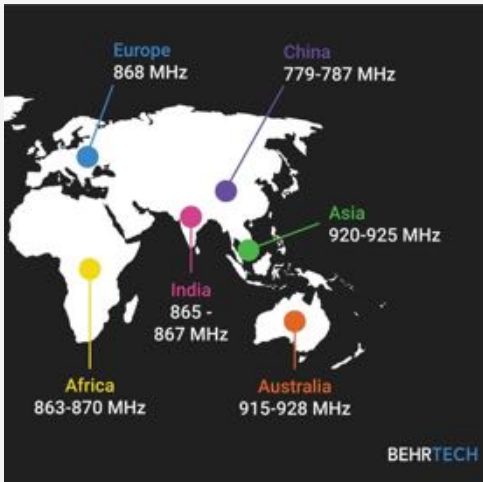
DATA INTEGRITY

Blockchain mechanisms

- Blockchain solutions allows to record data and ensure no modification of the data after being registered into it.
- IOTA blockchain is an example of solution providing a such use case.

KEY CONCEPTS

- Prove the sequence of the communications
- Make sure they can't be modified at any time later
- There is no need to store the data itself in the chain or store it in clear text
- Frame sequence reduce insertion / deletion risk at reception time (but the networks are subject to loss and this is not a proof at the end)



ISM 868MHz Band

European regulation

Freedom comes with responsibilities





Shared radio band

SIGFOX & LoRaWan are using ISM bands, they are free for use in condition you respect rules defined by the regulation. This regulation differ in the different zones. The purpose is the same, share the radio band in a balanced way between the user. In Europe, the rule is to limit communication to 1% of the time per device. In North America it's to not transmit on the same channel for more than a given time.



9



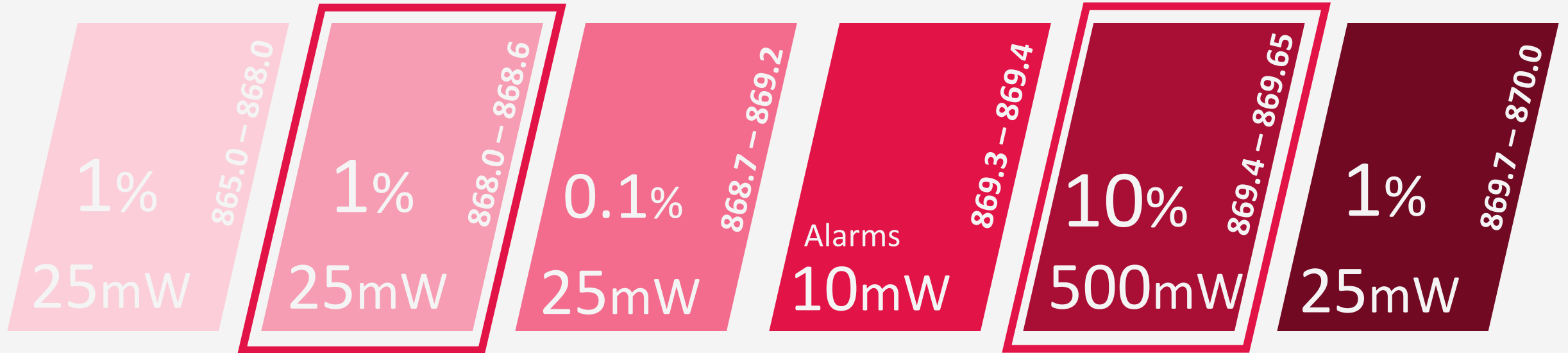
European regulation on 868MHz ISM band

865Mhz-870 Hz



Uplink Channels

Downlink Channels



European regulation is defined by different laws like ERC-REC-70-03E for EUROPE and the application in FRANCE is based on ARCEP 2012-0612 and 2014-1263 published on JORF 30/01/2015.

It limits the transmission time for any equipment to a certain percentage of the time during a sliding hour. This proportion of time depends on the frequency band. This is what we named DUTY-CYCLE. This is the percentage value in the above description. It also limit the transmission power.

ISM band are free of use and shared between many different type of devices. The regulation ensure a fair-use of these bands.

Regulation uses different concepts for applying the fair-use principles.

- Duty Cycle
- Maximum effective radiated power

DC

DUTY CYCLE

Is the percentage of time a device can transmit over a certain radio-frequency band during a rolling hour.

1% Duty Cycle means a maximum transmission of 36s during the running hour.

ERP

EFFECTIVE RADIATED POWER

ERP measures the combination of the power emitted by the transmitter and the ability of the antenna to direct that power in a given direction. It is basically the maximum power an IoT device can deliver. The unit is in mW or dB.

EIRP

EFFECTIVE ISOTROPIC RADIATED POWER

EIRP is an equivalent of ERP but considering an isotropic antenna when ERP is half wave dipole antenna. Basically, we have the following formula:

$$EIRP = 1.64 * ERP \text{ in Watt} / EIRP = ERP + 2.15 \text{ in dBm}$$

dBm

DECIBEL MILLIWATT

Power unit uses in radio wave communications.

$$P(\text{dBm}) = 10 * \log_{10}(P(\text{mW}) / 1 \text{ mW})$$

1mW	10mW	25mW	100mW	500mW	1W
0dBm	10dBm	14dBm	20dBm	27dBm	30dBm

ISM band are free of use and shared between many different type of devices. The regulation ensure a fair-use of these bands.

Main bands in Europe:

- 169 MHz
- 433 MHz
- 868 MHz
- 2.4 GHz

Usable bands for LoRaWan

- 433 MHz
- 868 MHz
- 2.4 GHz

Standard band for LoRaWan is 868 MHz in Europe

433 MHz

433 MHz is limited to 10mW

This is limiting the coverage. 433MHz also requiring larger antennas. This band allow 10% duty cycle, but this is impacting the network scalability. 433MHz gateways are not the norms. European public networks are on 868 MHz.

The better indoor penetration gain is lost by the reduced transmission power. It can make sense in short range deep indoor IoT where you want to save energy with a better penetration and lower transmission power.

868 MHz

EUROPEAN STANDARD

This is the main frequency used in Europe for LoRaWan networks. This frequency is common to European countries and a part of Africa and Middle East. North/South America, Asia are using different frequencies.

2.4 GHz

INTERNATIONAL STANDARD

LoRaWan now support 2.4GHz for international applications. This band can be use in most of the countries with common regulation rules. This band has a lower indoor penetration and reduced coverage. For these reason it is not the preferred choice currently to deploy networks.

ISM band are free of use and shared between many different type of devices. The regulation ensure a fair-use of these bands.

Main bands in Europe:

- 169 MHz
- 433 MHz
- 868 MHz
- 2.4 GHz

Usable bands for LoRaWan

- 433 MHz (China)
- 868 MHz (EU + Africa)
- 2.4 GHz (WW)
- 915 MHz (America/Asia)

Standard band for LoRaWan is 868 MHz in Europe

433 MHz

433 MHz is limited to 10mW

This is limiting the coverage. 433MHz also requiring larger antennas. This band allow 10% duty cycle, but this is impacting the network scalability. 433MHz gateways are not the norms. European public networks are on 868 MHz.

The better indoor penetration gain is lost by the reduced transmission power. It can make sense in short range deep indoor IoT where you want to save energy with a better penetration and lower transmission power.

868 MHz

EUROPEAN STANDARD

This is the main frequency used in Europe for LoRaWan networks. This frequency is common to European countries and a part of Africa and Middle East.

915 MHz

AMERICAN STANDARD

902-920MHz is the FCC (USA + CANADA) standard frequency, South America and Asia are also using frequencies around 900MHz but they are not complying FCC.

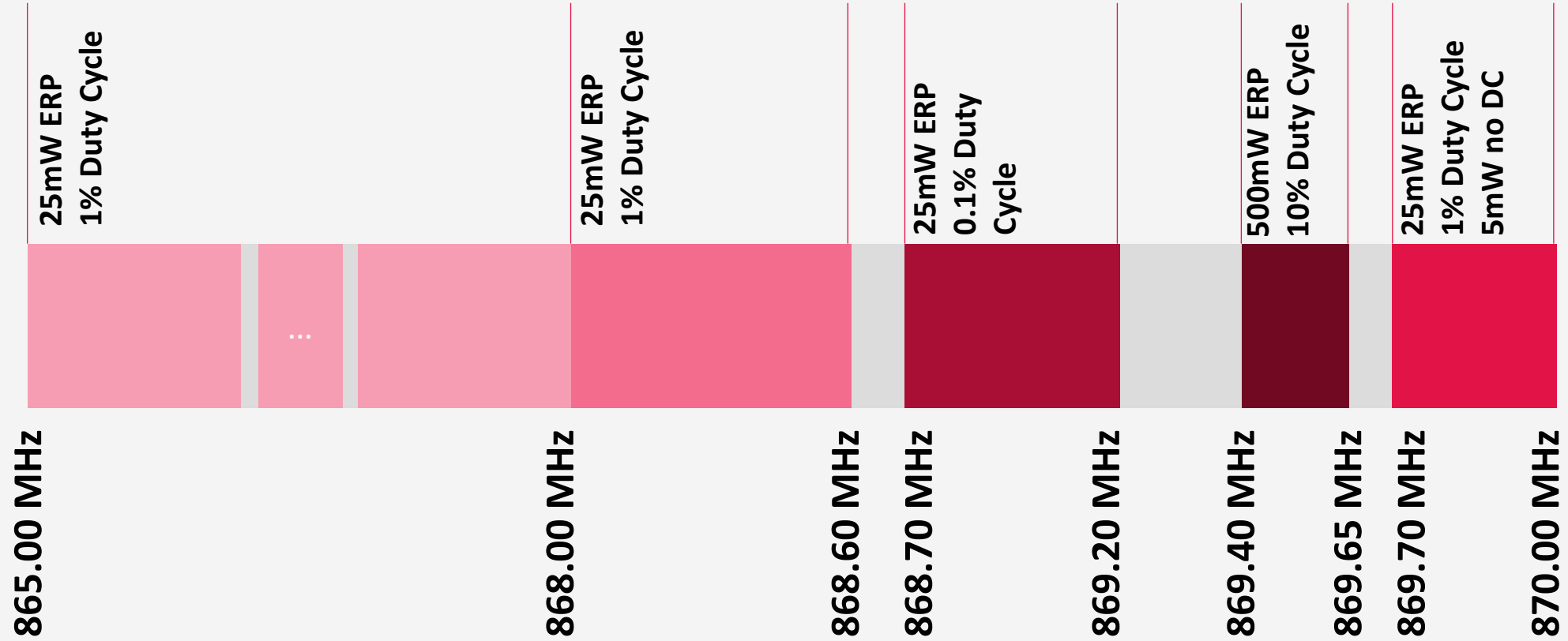
2.4 GHz

INTERNATIONAL STANDARD

LoRaWan now support 2.4GHz for international applications. This band can be use in most of the countries with common regulation rules. This band has a lower indoor penetration and reduced coverage. For these reason it is not the preferred choice currently to deploy networks.



CEPT / ERC-REC-7003E



IoT networks & devices must comply to regulation in term of transmission power and fair-use.

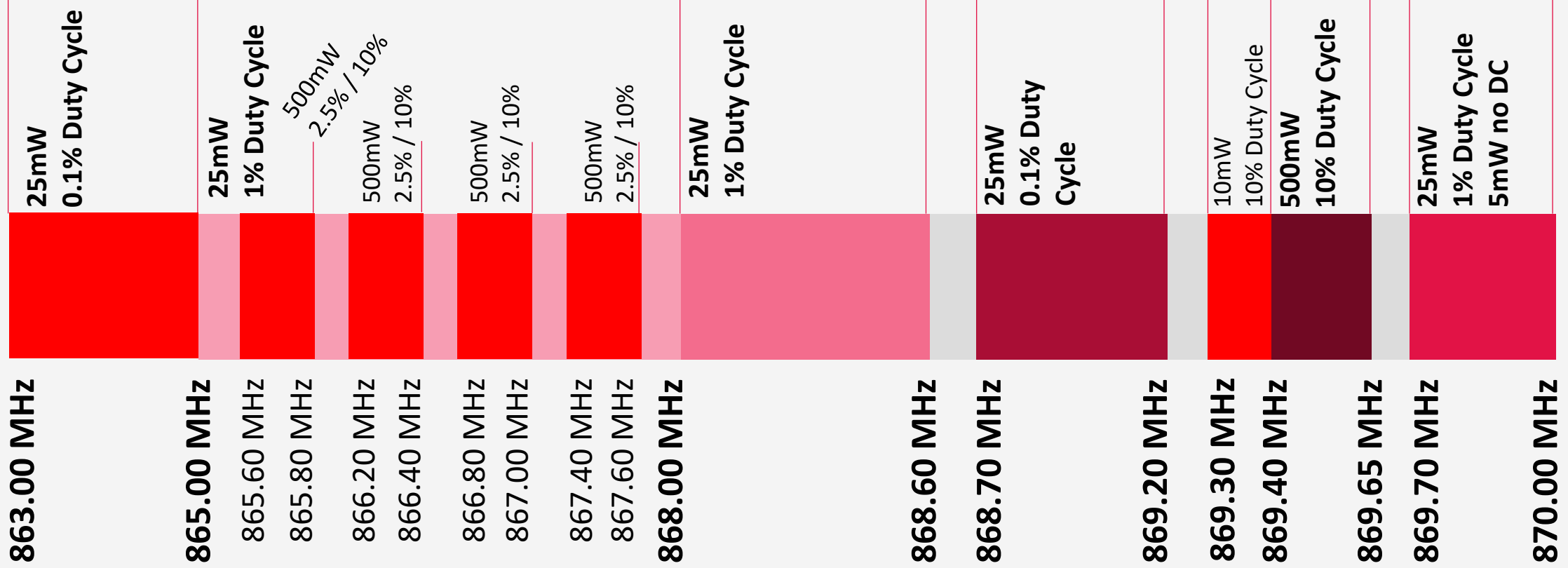
<https://docdb.cept.org/download/25c41779-cd6e/Rec7003e.pdf>



SCAN ME



OFCOM / IR2030



OFCOM follows CEPT recommendation with some interesting particularities for IoT networks

https://www.ofcom.org.uk/data/assets/pdf_file/0028/84970/ir-2030.pdf



FCC Fair-Use Rules

ISM band are free of use and shared between many different type of devices. The regulation ensure a fair-use of these bands.

Regulation uses different concepts for applying the fair-use principles.

- Channel Hoping
- Maximum time over the air
- Minimum time before reusing a channel
- Transmission power

CH

CHANNEL HOPPING

This is the number of different channel a device MUST use over the different communications. FCC requires to use more than 50 different channels. LoRaWan uses 64 channels.

**MT
OTA**

MAXIMUM TIME OVER THE AIR

The regulation have a maximum communication time over a single channel at 400ms. Consequently, SF12/SF11 can't be used in US915. The maximum payload size in SF10 is 10 bytes.

**MTB
RC**

MINIMUM TIME BEFORE REUSING CHANNEL

This is the time to wait before being able to reuse a channel. 20 seconds. With 64 channels, and 400ms on each, you can continuously transmit (no duty cycle). With 8 channels, you need to apply a duty-cycle about 16%.

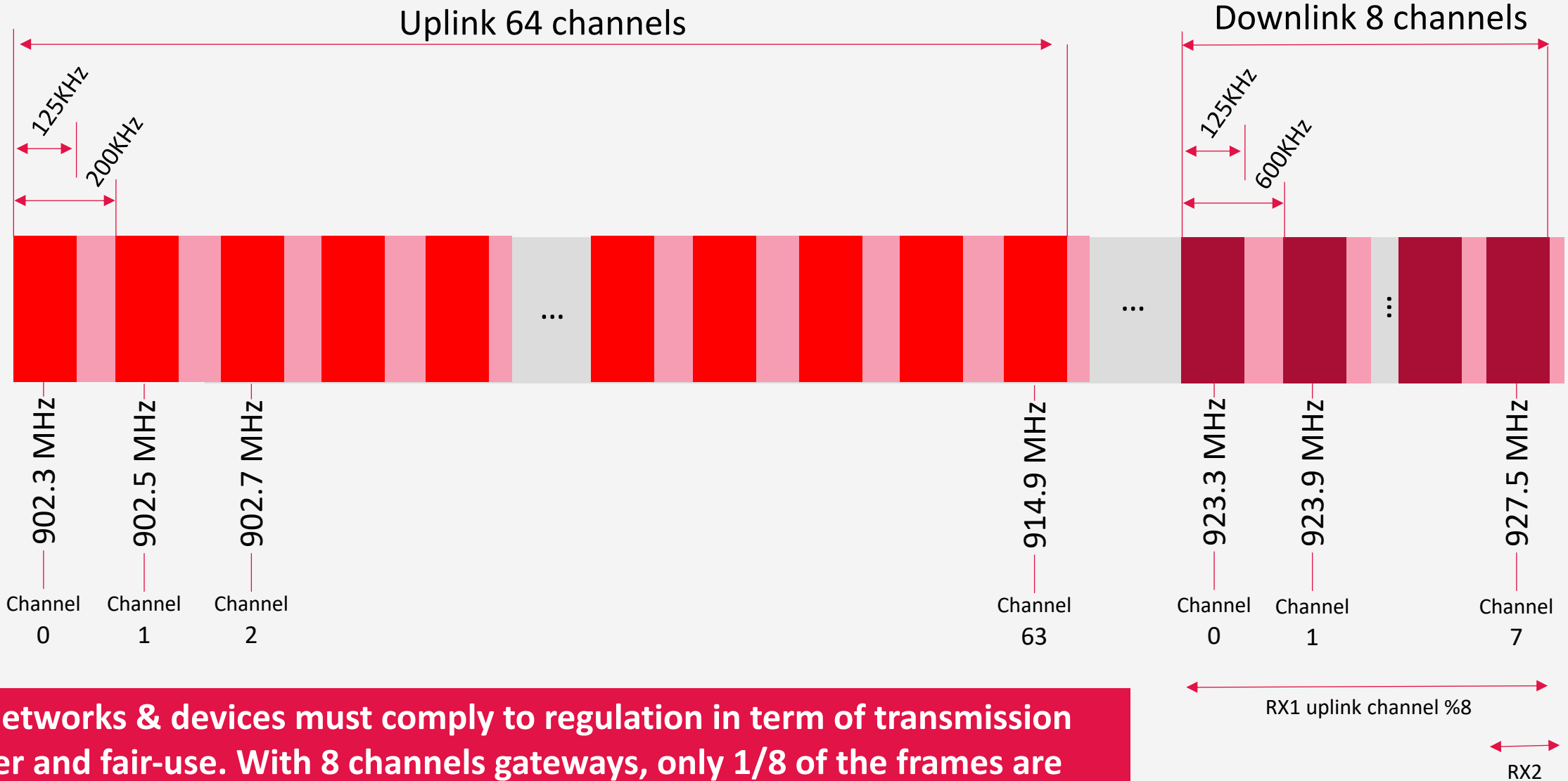
TP

TRANSMISSION POWER

Transmission power for uplink and downlink is limited to 27dBm but usually 20dBm is implemented as the regulation authorize to have less than 64 channels when the transmission power is lower than 21dBm.



FCC / 902MHz – 928MHz



IoT networks & devices must comply to regulation in term of transmission power and fair-use. With 8 channels gateways, only 1/8 of the frames are received. Multiple transmissions are required.

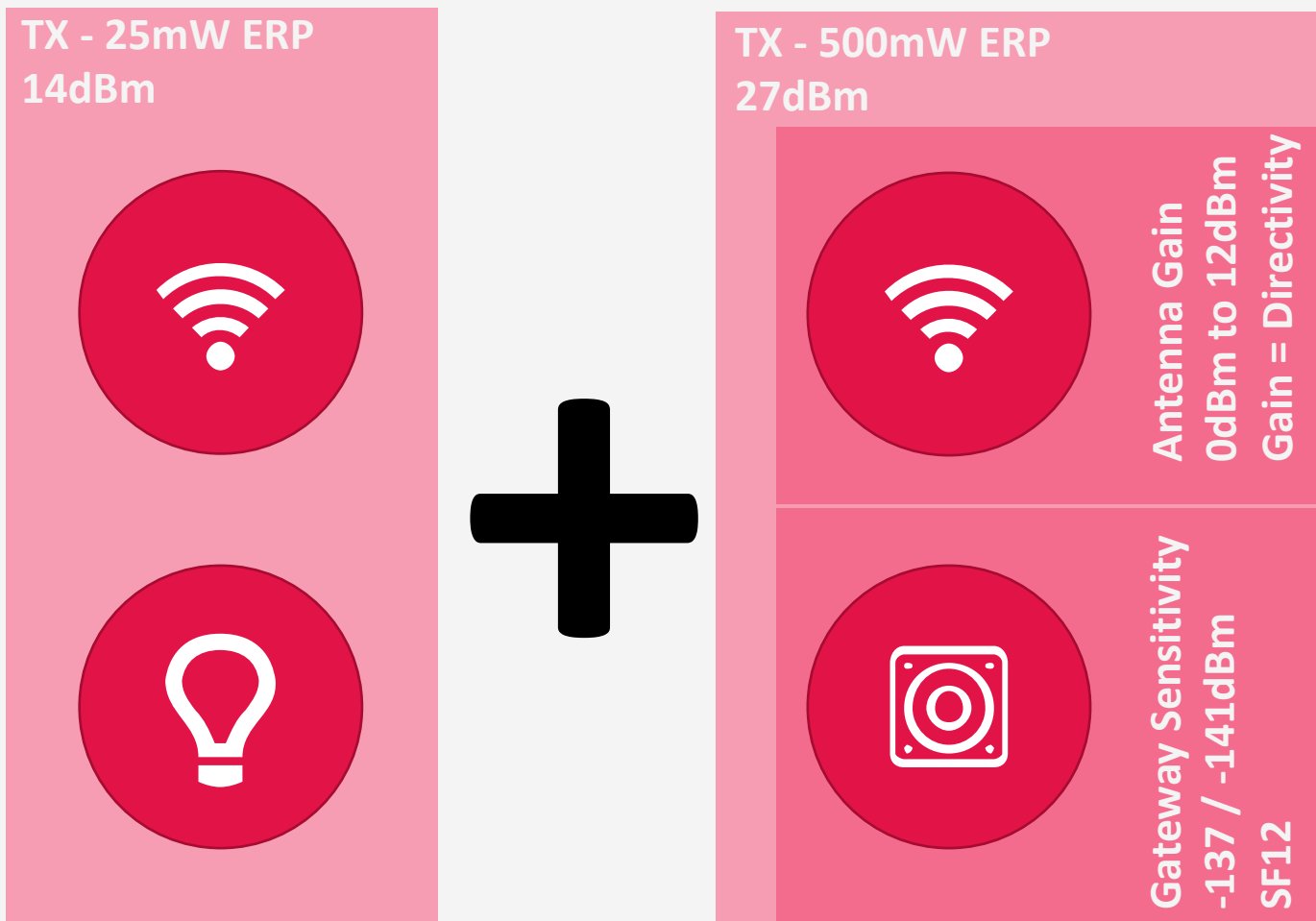
Transmission budget link impacts the coverage but also the device power consumption and therefore the long-term maintenance.

Device using an antenna with gain can reduce its transmission power.

Device with a negative antenna gain will increase power.

Gateway antenna gain will offer a larger TX budget link and extends the reception coverage.

But the transmission will have to be reduced to stay in the maximum of 500mW ERP.



TRANSMISSION BUDGET LINK



LPWAN Sigfox & LoRaWan Technologies in detail.



2 French technologies



3



- Created in TOULOUSE (FRANCE) in 2009
- FRANCE fully covered since 2013
- Found rising
 - 15M€ in 2014
 - 100M€ in 2015
 - 150M€ in 2016
- Bankrupt in 2020
- Acquired by Unabiz (Taiwan)
- Hardware device solution from most of the silicon vendors
- 72 countries deployed and seen as a single global network (as of Nov. 2020)



- Created in GENOBLE (FRANCE) in 2009
- Acquired by SEMTECH in 2012 for a price range between 5M\$ and 25M\$
- SEMTECH is a Silicon vendor with an exclusivity. 1 licence acquired by St Microelectronics.
- LoRaWan 1.0 released in 2015
- Deployed by about only 5 telecom company nation wide.
- Thousands of private networks
 - TTN – crowdsourced global network
 - HELIUM – crowdsourced global network as a blockchain (900K gw)

French technologies now American



- Created in GENOBLE (FRANCE) in 2009
- Acquired by SEMTECH in 2012 for a price range between 5M\$ and 25M\$
- SEMTECH is a Silicon vendor with an exclusivity.
- 1 license acquired by St Microelectronics.



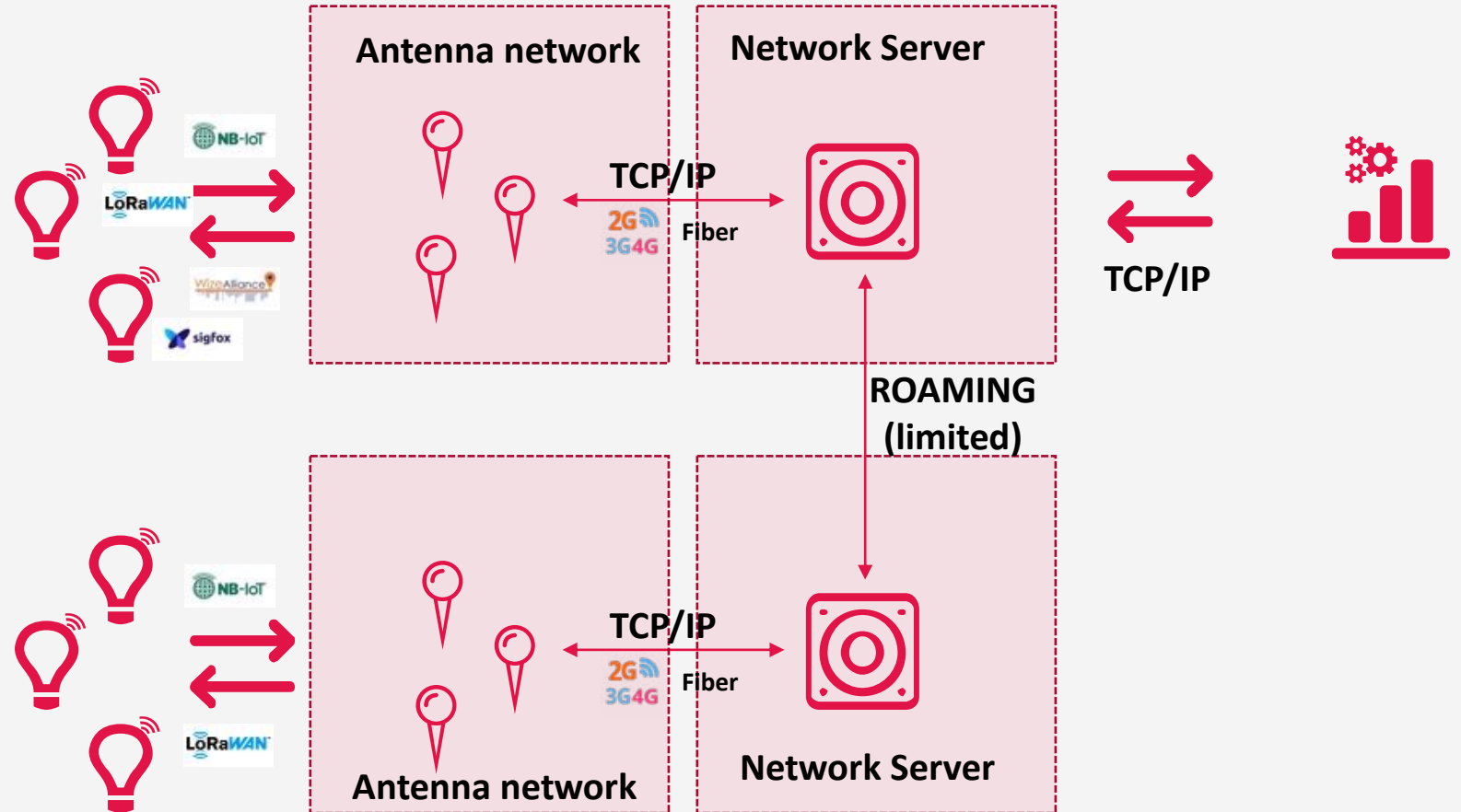
- A norm to build a network with LoRa technology
- LoRaWan 1.0 released in 2015
- Deployed by about only 5 telecom company nation wide.
- Thousands of private networks
- Public crowdsourced networks
 - TTN – crowdsourced global network, free of use, 20K gateways
 - HELIUM – crowdsourced global network as a blockchain, low cost, 900K hotspots

LPWAN have a common architecture

The devices messages are captured by multiple antennas around.

The antennas forward the messages to a network server owned by the network operator (private or public)

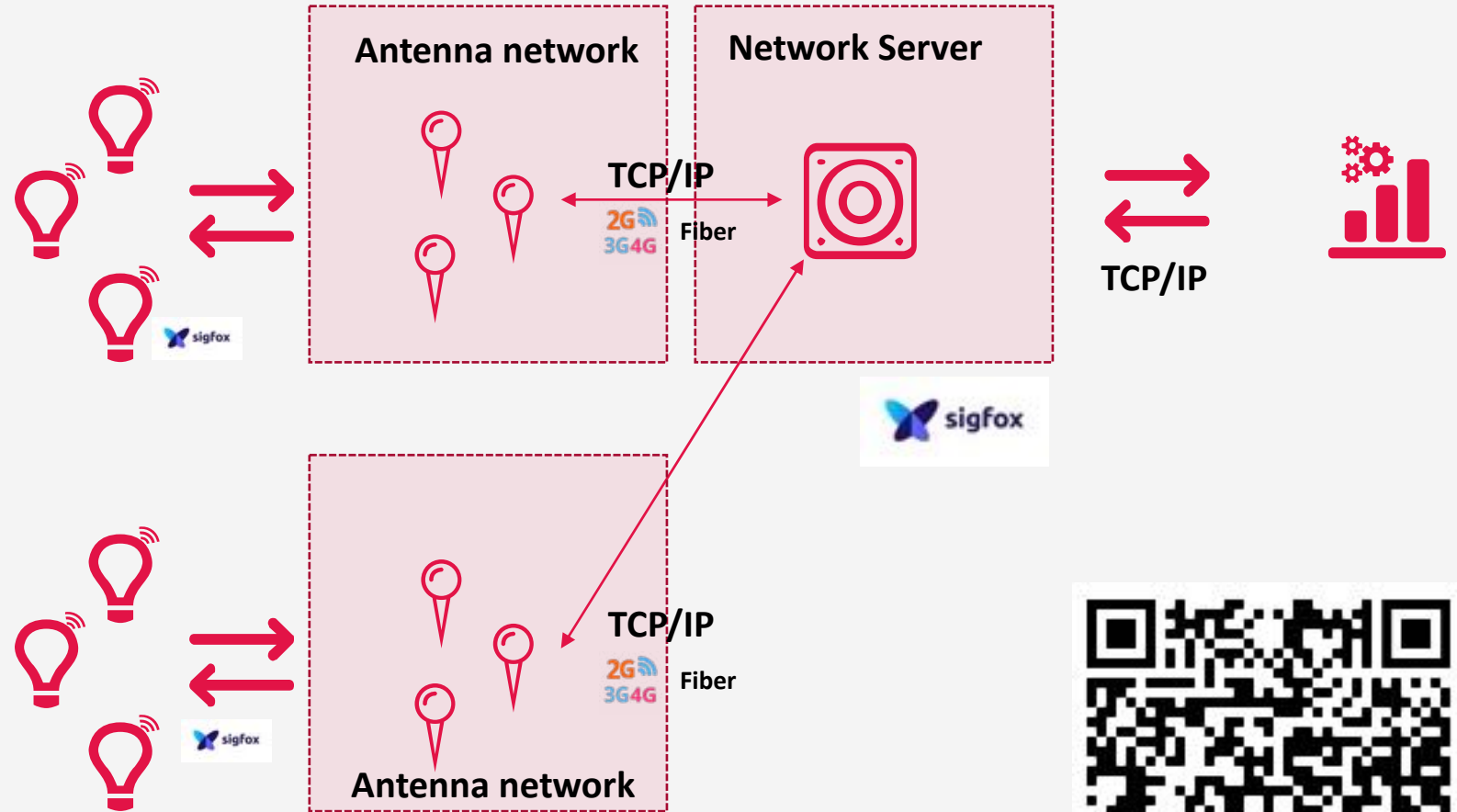
Then the network server transfers the payload to the custom backend, eventually, roam it to another network server.



LPWAN have a common architecture

Sigfox is a particular case with a World-Wide network and a single Network Server

70 countries
1.1B people



4





Compared to classical communication network, LPWAN are using non connector mode. It means a device can deep sleep for month, wake up, fire a message and back to sleep.

This means a lot of power saving and a strong resilience against jamming.

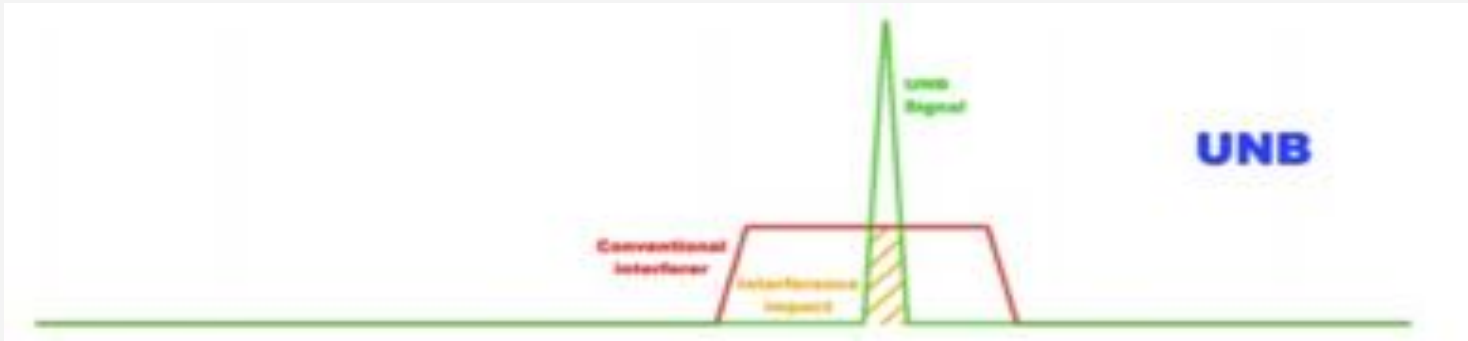
Network do not have edge access control, but centralized control managed by network server.

**Save power:
don't be
connected**



Make a radio signal viable over long distance with a reduced power

2 different ways to reach a single target



SigFox – Ultra Narrow Band

Have a signal on the smallest possible bandwidth to pass over the noise



LoRa – Spread spectrum

Use a large radio band to pass through the noise without losing the signal



Is an asymmetric technology

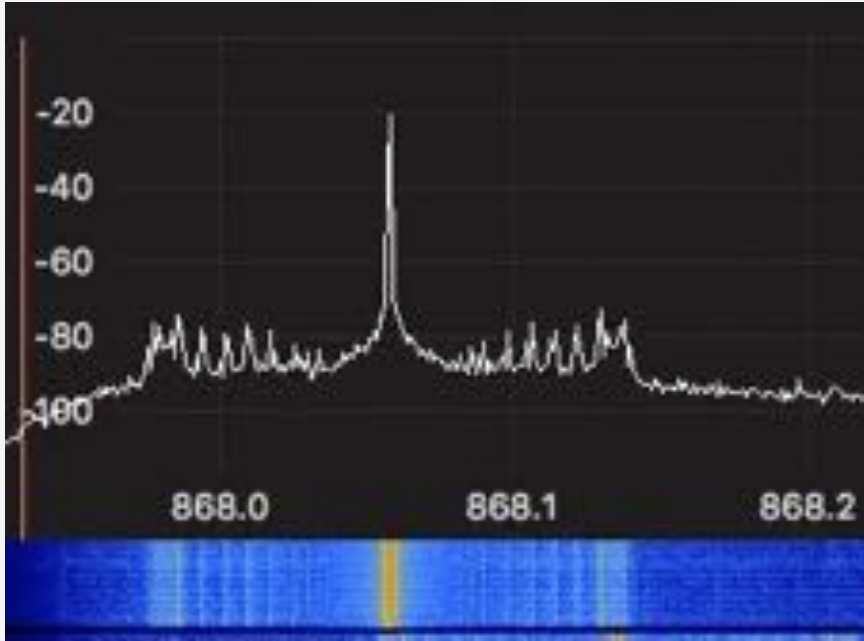
The technology use for transmitting data is simple when the technology required to receives Sigfox messages is highly complex and based on Software Defined Radio.



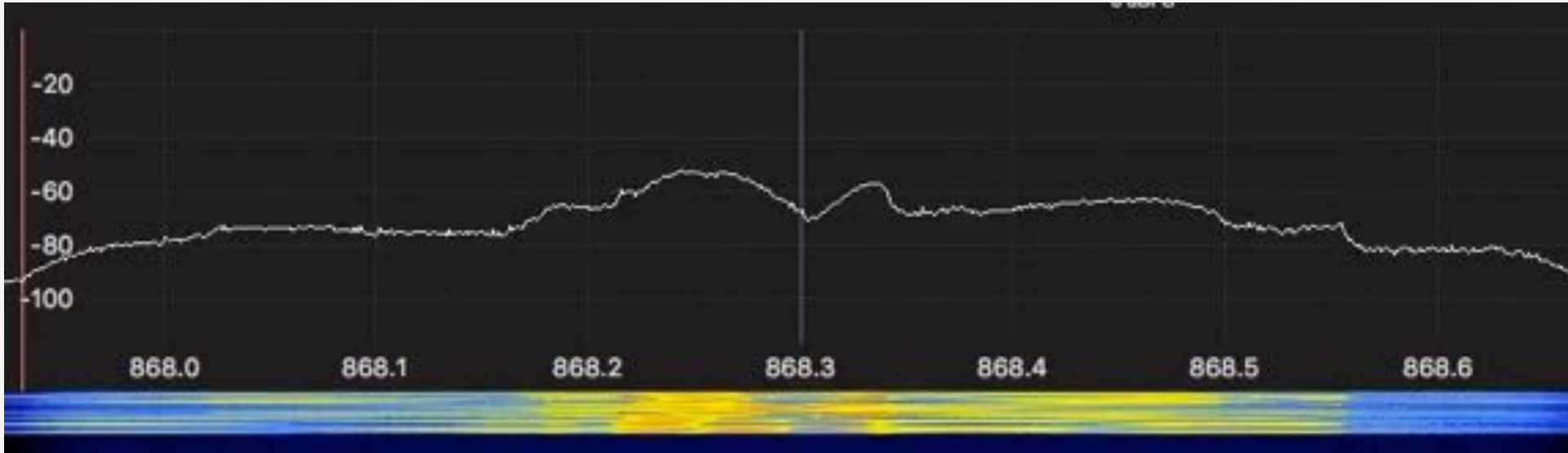
Is a symmetric technology

Transmission and reception are based on the same technology and complexity level.





The radio technology is totally different for reaching the same goal



7

Let's make a short break

LEARNING AT THIS STEP

1

LPWAN SIGFOX & LoRa ARE 11 YEARS OLD NOW

Both has been created in FRANCE and now deployed all over the World

2

THEY RELY ON ISM BAND TO BE DEPLOYED AT LOW COST

This means respecting regulation rules in place to share the ISM band between all the different technologies using it.

3

THE TECHNOLOGIES BEHIND ARE DIFFERENT

But they are reaching the same goal: allowing to communicate over long distance with a minimum of energy



Sigfox, one IoT network to cover the entire World





sigfox

An asymmetric network

The technology use for transmitting data is simple when the technology required to receives Sigfox messages is highly complex.



6



252

A Software Defined Radio Network

Simplicity and efficiency



ISM BAND (free of access)

Use of 868MHz band in Europe, Africa. 902MHz -920 MHz in North, South America and Asia. In each of them the exact frequencies differ.



LOW POWER / WIDE AREA

With only 14dBm in Europe, the coverage is 60km. Distance record was 1023km from Spain to Eire in 2016. Only 1000 antennas allows to cover most of a country like FRANCE. Compared to 4000 for LoRaWan and 50.000 for 4G



LOW THROUGHPUT

Transmission is limited to 100 **bits** / seconds in Europe and up to 600 **bits** / seconds in North America. This is related to the different regulations.



FIXED PACKET LENGTH

User payload limited to 12 byte per frame. Only available options are 0, 4, 8, 12 bytes.



BI-DIRECTIONAL

Devices can receive message from the network (DOWNLINK) up to 4 times a day, right after an uplink communication. A device can request more than 4 downlink per day. Other are best-effort only.



REGULATION APPLICATION

The application of the regulation is under the device maker responsibility. You can transfer up to 6 consecutive frames in Europe if you want.



Sigfox over the technology



Sigfox is at first a global, world-wide telecom operator. Here is a big part of the innovation.

A single device can communicate all over the world without roaming consideration.



Sigfox is deployed in many countries and growing fast

- 73 countries in February 2021
- 5,8M KM2 covered
- 1.3B people covered
- 17.2M devices connected in 2021
- 63M messages / day in 2020

X2 on every 18 Months 2013-2019



Reduced “Time to get the first fired frame”

As everything is already defined in the protocol, in a developer perspective, the time to getting started with the Sigfox technology is short. Device design is also simplified, and regulation difference have a limited impact in most of the use-cases.



Security and reliability



MESSAGE SIGNATURE

All the messages are signed with an EAS processed and indexed. It proves the emitter identity and allow to reject usurped or replayed messages in a 4096 messages cycle.



ENCRYPTION

Clear payload is the default setting. AES-CTR can be activated when the devices has been designed for. It is part of the standard Sigfox lib. Sigfox is complex to receive for real: open-source receivers are only working under 2 meters.



JAMMING PROTECTION

As Sigfox doesn't require any reception for firing a message it's really complicated to JAM it. This is one of the reason it has been chosen in Securitas solutions. To jam Sigfox you basically need to jam the different base-station around... forget it.

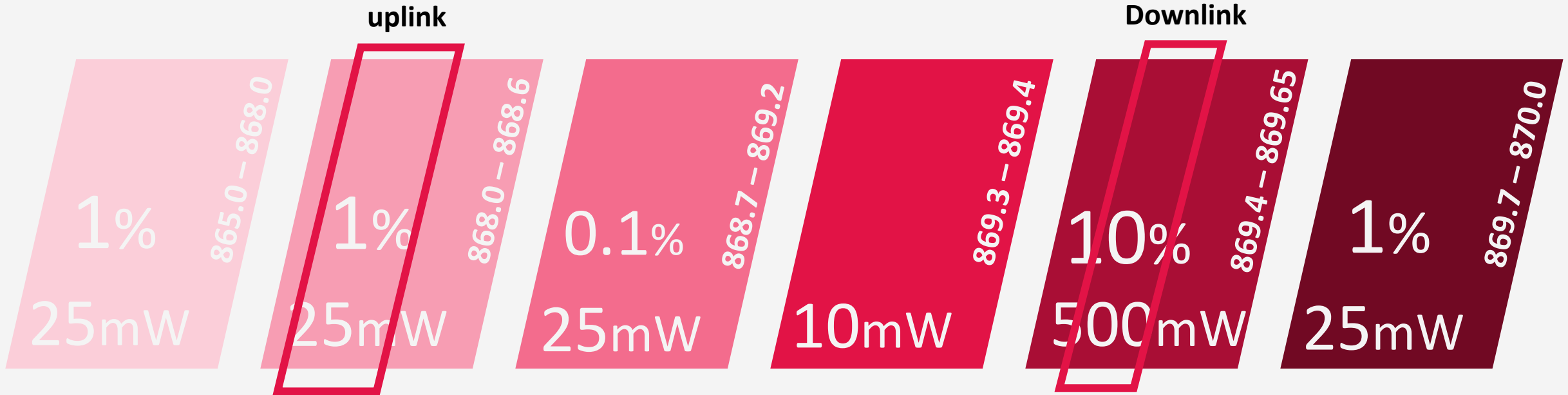


COMMUNICATION RELIABILITY

Every frame is replicated to get 3 transmissions of the same message on different frequencies. It allows a 99.99xx deliverabilty is the covered zones.



USE OF 865Mhz-870 Hz



Sigfox only 200KHZ. In Europe it is centered on 868.130MHz. In these 200KHz there are 2000 channel, each of them have a size on only 100Hz

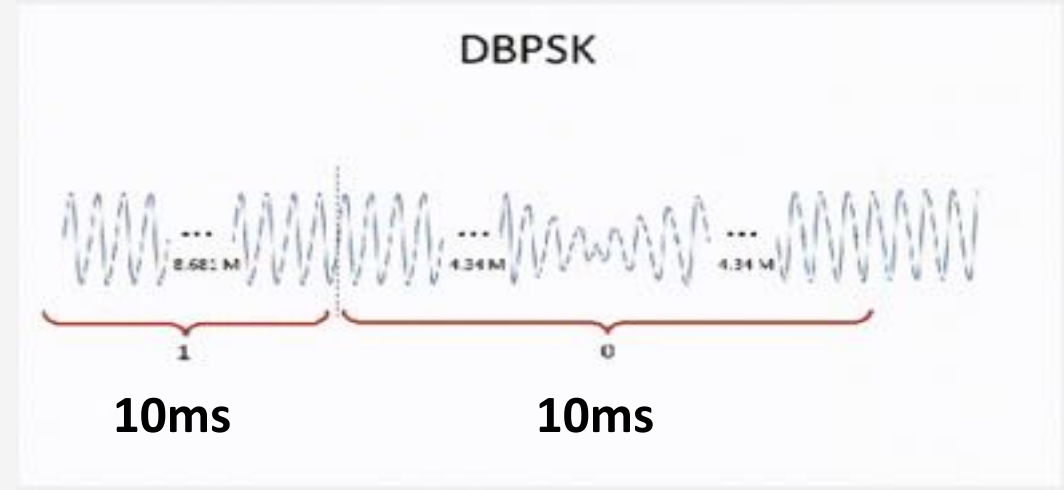
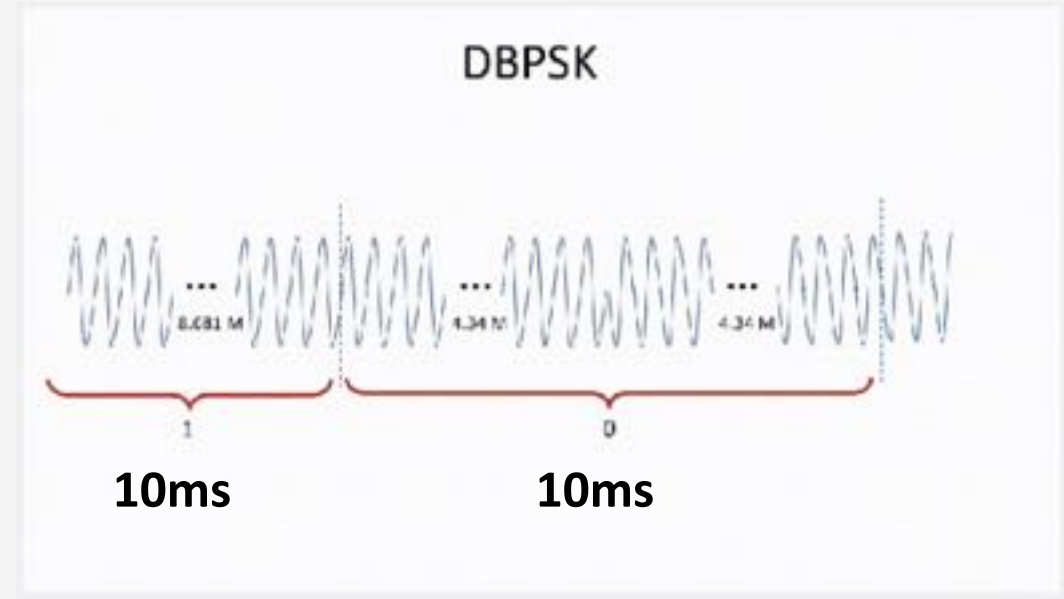
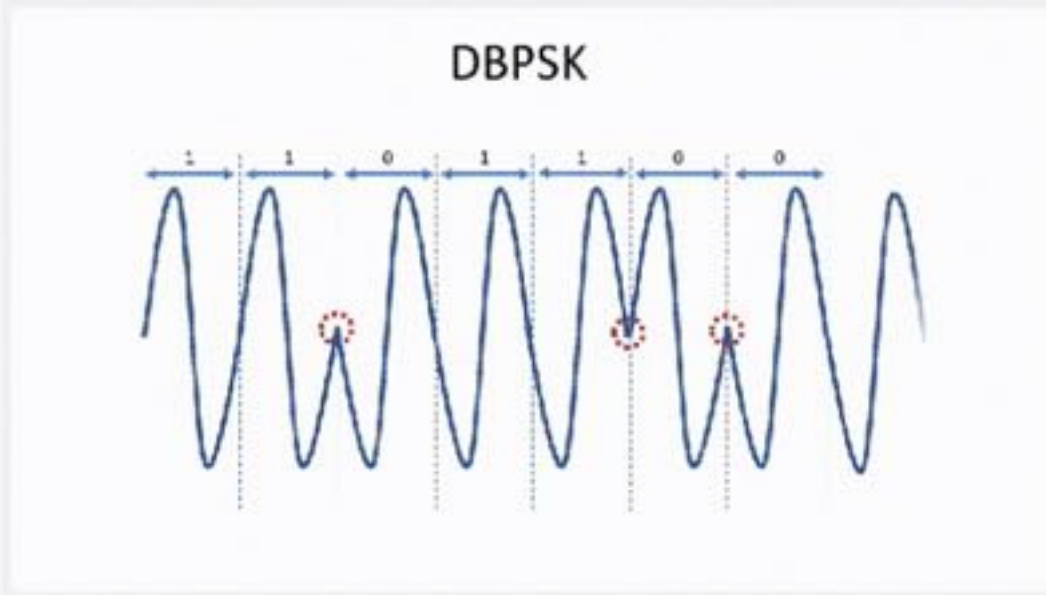
DOWNLINK are using a 10% duty cycle band for two reasons:

- A base-station responds to many different devices
- The radio situation for a base-station is better than for a device. You need more power to be received by a device.



SigFox – Transmission radio sur DBPSK

Differential Binary Phase Shift Keying



Temps d'une trame:

- 12B : 2,08s
- 8B : 1,76s
- 4B : 1,44s
- 1B : 1,2s

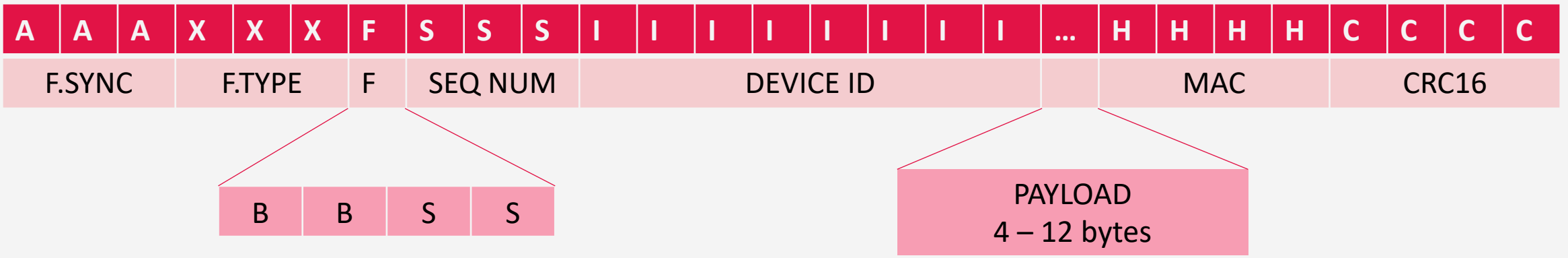


8



Sigfox – Uplink data frame format

1 single type of frame skeleton for all the communications



F.SYNC : Preamble – 20 bits 01010101010101010101 – clock sync and Sigfox message identification

F.TYPE : Frame type (related to payload size and repeat)

F : Flags : Flags (bit value, downlink, byte added in payload)

Seq NUM : Sequence number, incremented on every communications

Device ID : device address, uniq

Payload : User data

MAC : CBC-MAC Signature based on NAK (Network Authentication Key)

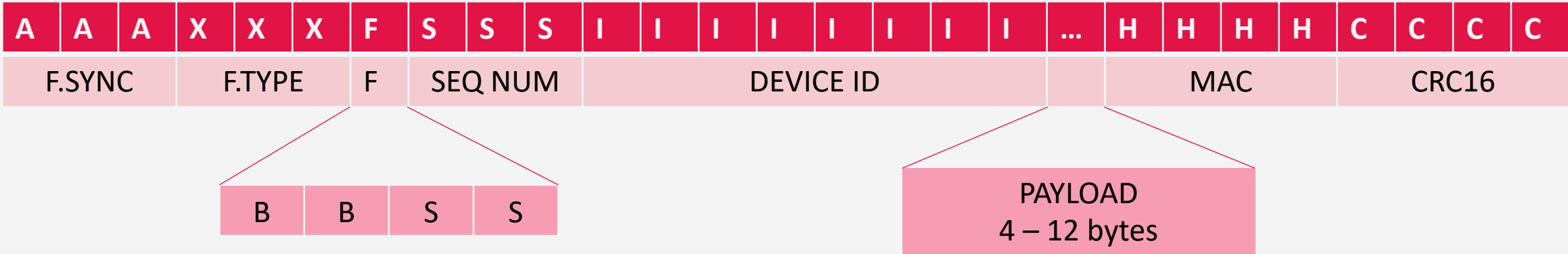
CRC16 : Frame bit validation





Sigfox – Uplink data frame format

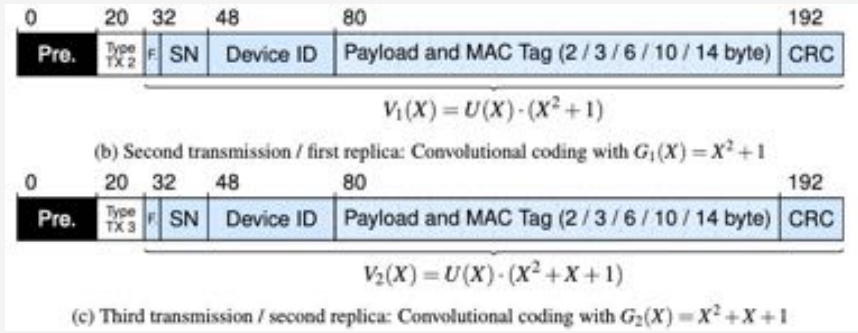
1 single type of frame skeleton for all the communications



The medium PAYLOAD is identified by the F.TYPE Field / each of the repeat have a different encoding

- 0 bit/byte - 06B 6E0 034
- 1 bit - 06B 6E0 034
- 1 byte - 08D 0D2 302
- 4 bytes - 35F 598 5A3
- 8 bytes - 611 6BF 72C
- 12 bytes - 94C 971 997

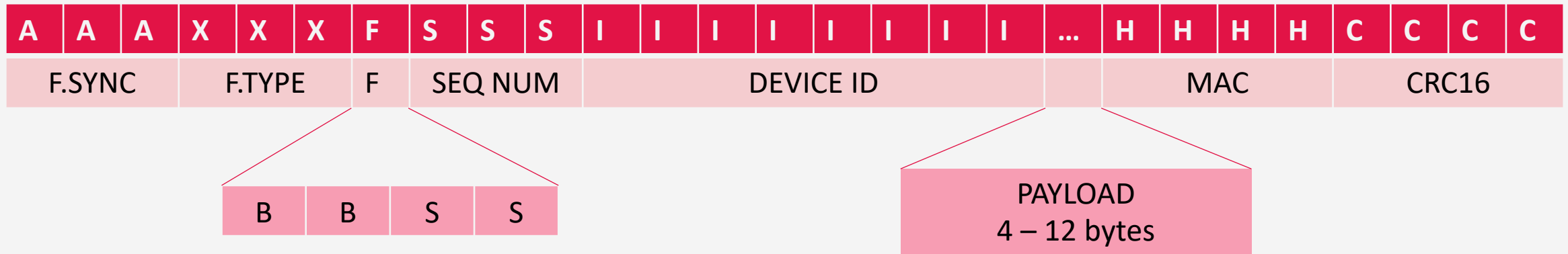
1st frame is sent with no specific encoding
 2nd and 3rd frames use Convolutional Codes





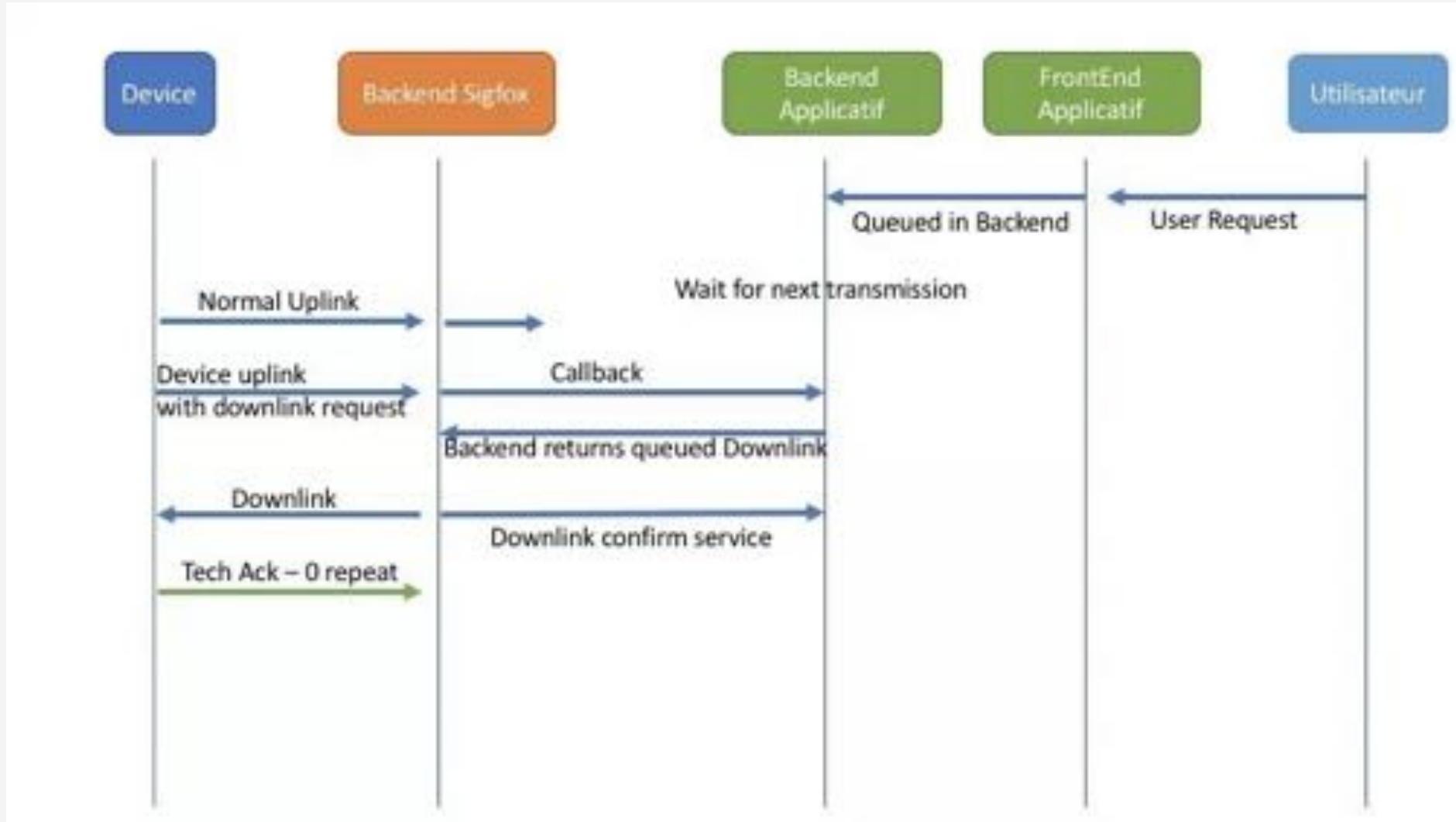
Sigfox – Uplink data frame format

1 single type of frame skeleton for all the communications



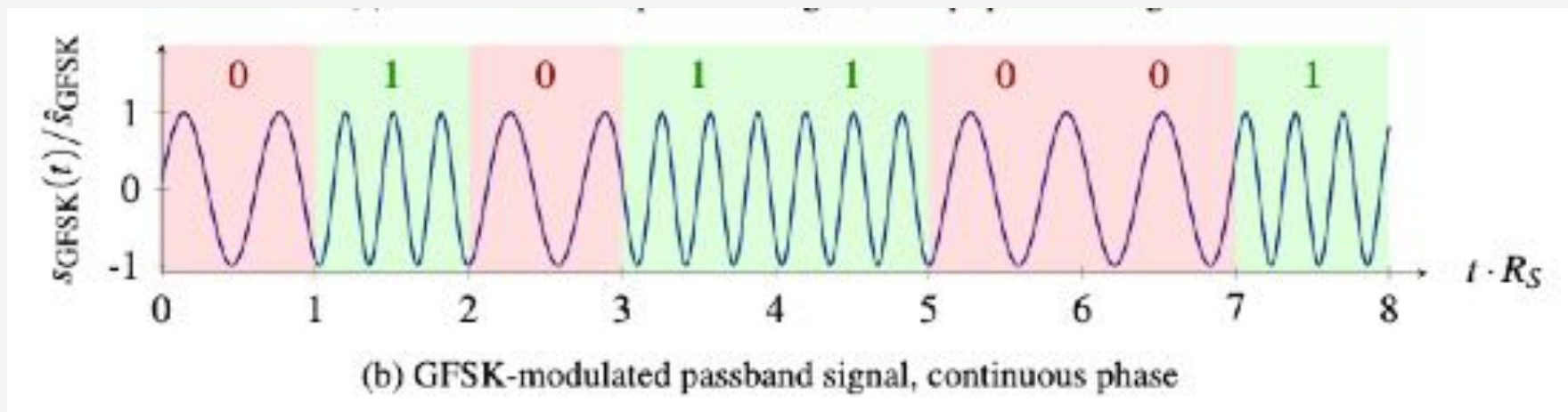
- MAC computation use a secret KEY (NAK) shared between device and Sigfox backend.
- MAC includes F, SEQNUM, DEVICE ID, USED PAYLOAD
- MAC computed with EAS-128-CBC, only a part of the result is kept to create the MAC (from 2 to 5 bytes)

Sigfox – Downlink communications



SigFox – Downlink transmission is GFSK

Gaussian Frequency-Shift keying (because a device can't receive DBPSK)



Symbol rate

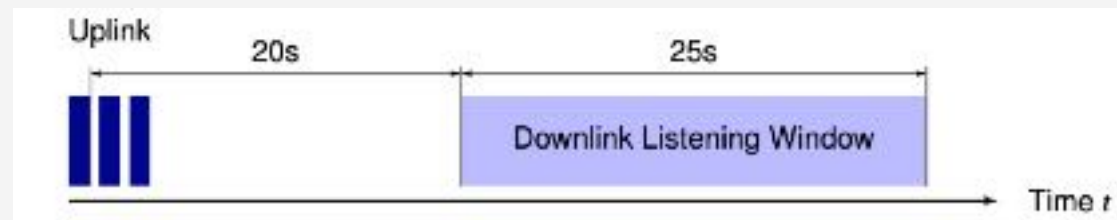
- 600 Bit/s

Frequency

- Determined from the uplink message frequency

It works long-range because

- Frequency is 869.4MHz to 869.65MHz
- So the transmission power is 500mW





Sigfox – Downlink Frame

Sent by the network on downlink request



PREAMBULE – 0x2AAAAAAAAAAAAAAAAAAAAAAB227

EEC – Error correction, redundancy information

Payload – Downlink Data

MAC – Authentication for the destination, EEC + PAYLOAD

C – CRC-8

Destination is not identified in the DOWNLINK frame:

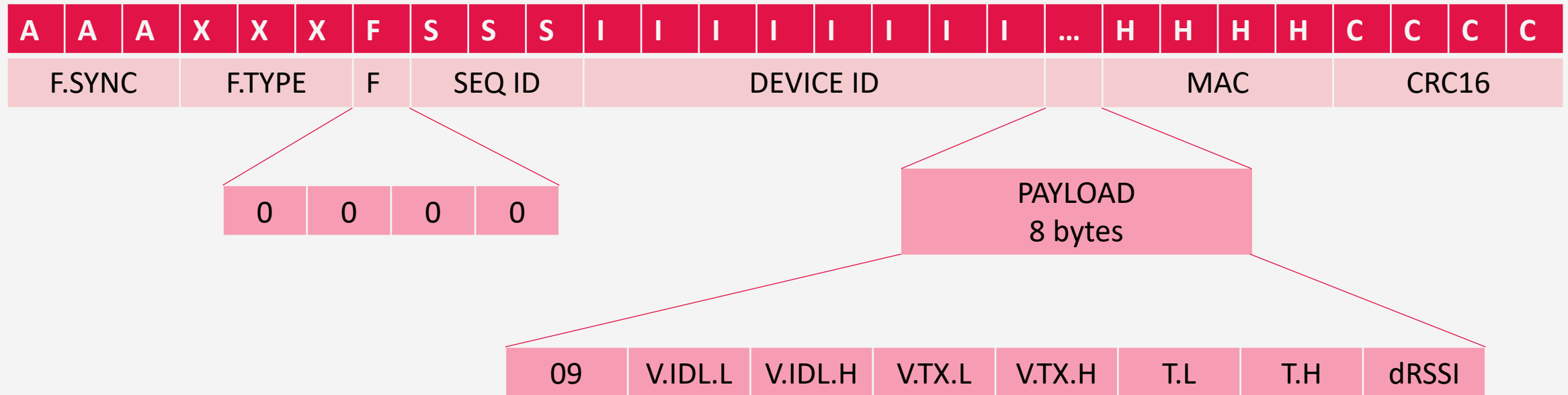
Any device can read the downlink frame, only the one knowing the NAK used to compute MAC will resolve the MAC challenge correctly. MAC also include Uplink SeqId in its computation. That way, only one device will consider the frame as valid.

That way, 4bytes of transmission are saved, collision risk is reduced.



Sigfox – Frame RX OOB (downlink confirmation)

Sent by the device on downlink reception as a confirmation (no repeat)



V.IDL : Idle voltage

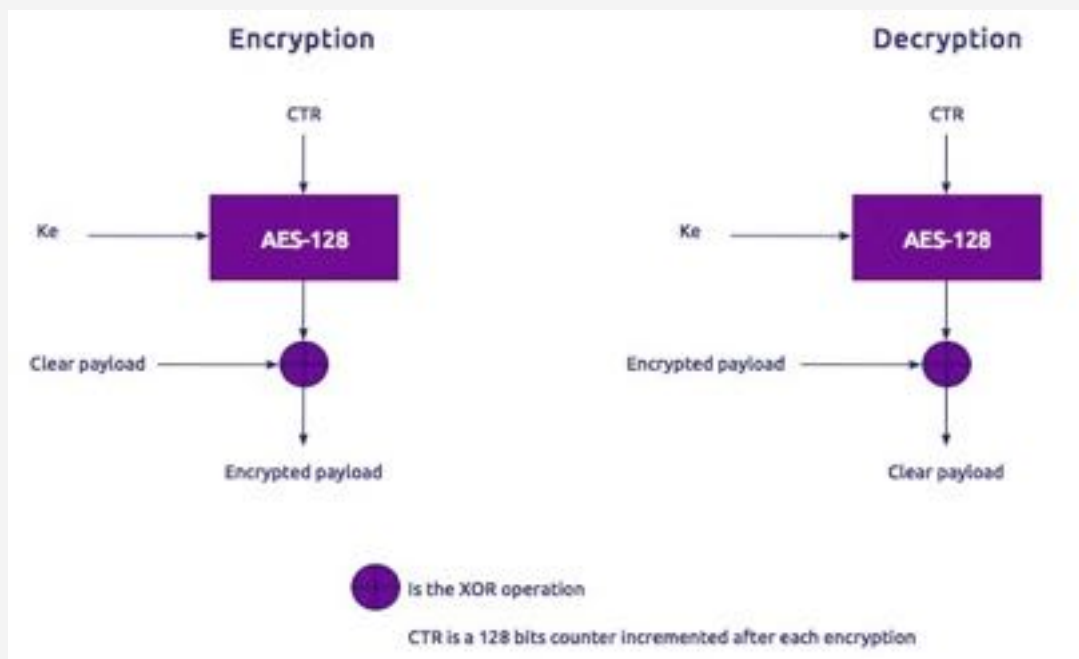
V.TX : Voltage during the last Sigfox transmission

T : Temperature

dRSSI : Downlink reception signal level

Sigfox – Frame encryption (uplink & downlink)

Activable per device, request to be made at Sigfox



The solution is equivalent to LoRaWAN encryption.

- The Ke is not negotiated but derives from the Device ID and NAK.
- CTR is composed by a derivate vector from DeviceID and NAK + the addition of a 16bits Sequence ID
- The AES(KE,CTR) gives a different key for each communication (modulo 65536). This key is a source for an XOR operation with the frame bits.

Encryption protects against data listening over-the-air. It also protects against replay attack.





10



267

11



Sigfox get benefit of a large ecosystem with hundreds of available devices and tons of device-kit.

Standard radio chip + MCU price starts about \$1.5 / Ultra low-cost solution starts at 0,20€ for radio + MCU solution.

[https:// partners.sigfox.com](https://partners.sigfox.com)

[https:// makers.sigfox.com](https://makers.sigfox.com)

Devkit includes 1 year of communication

Sigfox has been used to closely work with the startup eco-system even if in the last year they are most focusing on big company & at scale projects

SIGFOX NETWORK SERVER

Also call Sigfox backend. It receives messages and help IoT solution administrator to manage the subscription and device fleet.

Network server is where you link your device with your final application.



13



268

A screenshot of the Sigfox portal dashboard. The top navigation bar includes the Sigfox logo and menu items: DEVICE, DEVICE TYPE, USER, GROUP, BILLING. A user profile icon is visible in the top right. A left sidebar contains menu items: NEWS, SERVICE MAPS, and KNOWN ISSUES. The main content area features a 'Welcome to sigfox portal' message with a decorative graphic. Below this is a 'Release 9.8' section with a description of system improvements and a list of changes: 'Devices and contract', 'Simultaneous operations on a device [correction]', 'Downlink display [correction]', and 'Azure callbacks statistics [correction]'. A date stamp '21 SEPTEMBER 2020' is displayed on the right side of the main content area. The footer contains copyright information and a link to terms and conditions.

TRACKING USE-CASES

The main Sigfox use-cases in volume are in two domains:

- Security
- Assets tracking

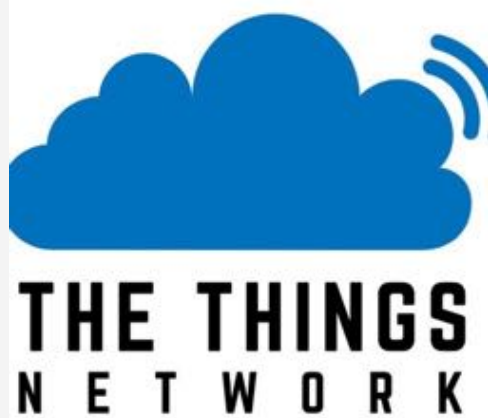
In the domain, Sigfox propose a solution to get a device localization from a single frame based on received radio signal or WiFi signals around. This avoid using a GNSS chip for getting a location.

Precision and compliance vary:

- 1km to 20km for received radio signal
- 30m for WiFi signals when exists

This option is ATLAS.





LoRaWan, many IoT networks deployed on your own





A POINT-TO-POINT RADIO COMMUNICATION TECHNOLOGY



A NETWORK RUNNING OVER LoRa.



Numbers (as of March 2023)

240.000.000

**LoRa compatible
transceivers already
distributed by Semtech**

3.200.000

**LoRa based
gateway chips sold**

**This could cover 4x the total earth surface and
10x the surface where human live. But the real
coverage is ... 5-10% ?**



POINT-TO-POINT RADIO TECHNOLOGY



ISM BAND (free of access)

Use of 868MHz band in Europe, Africa. 902MHz -920 MHz in North, South America and Asia. In each of them the exact frequencies differ. Each channel is 125KHz large.



VARIABLE PAYLOAD LENGTH

User payload can be 59 to 250 bytes depending on Spread Factor and regulation. FCC have a maximum authorized time in the air.



LOW POWER / WIDE AREA

With only 14dBm in Europe, the coverage is 15km. Distance record was 832km from a balloon (cheating). Only 4000 antennas allows to cover most of a country like FRANCE.



BI-DIRECTIONAL

Devices can receive message from the network (DOWNLINK) right after an uplink communication. Downlink messages are used to ack transmission and to transfer data to the device. Firmware update capability, in certain conditions, has been proven.



LOW THROUGHPUT

Transmission is limited to 250 **bits** to 5400 **bits** / s depending on Spread Factor choice, for 125kHz bandwidth. Can be 11kbps for 250KHz.

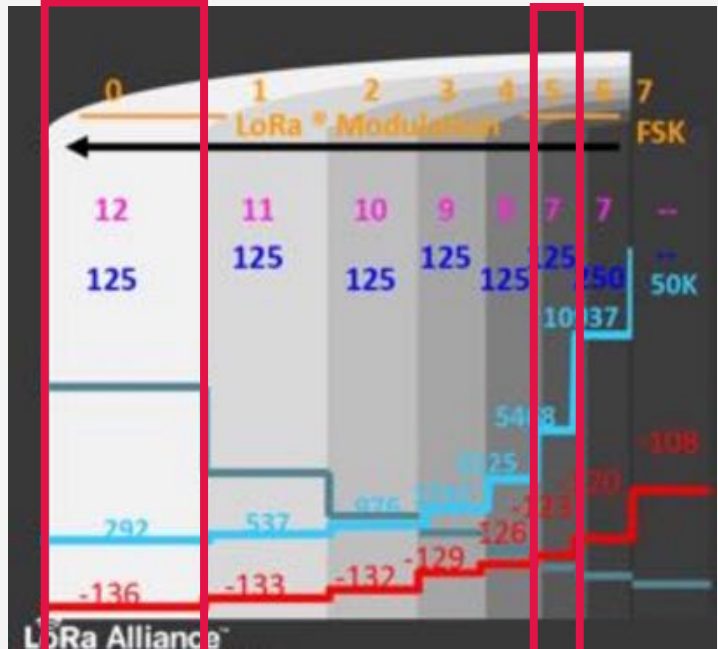


REGULATION APPLICATION

Usually, the regulation rules are managed in the LoRa and LoRaWan stacks. Therefore, what you can do depends on the implementation and the zone you are.

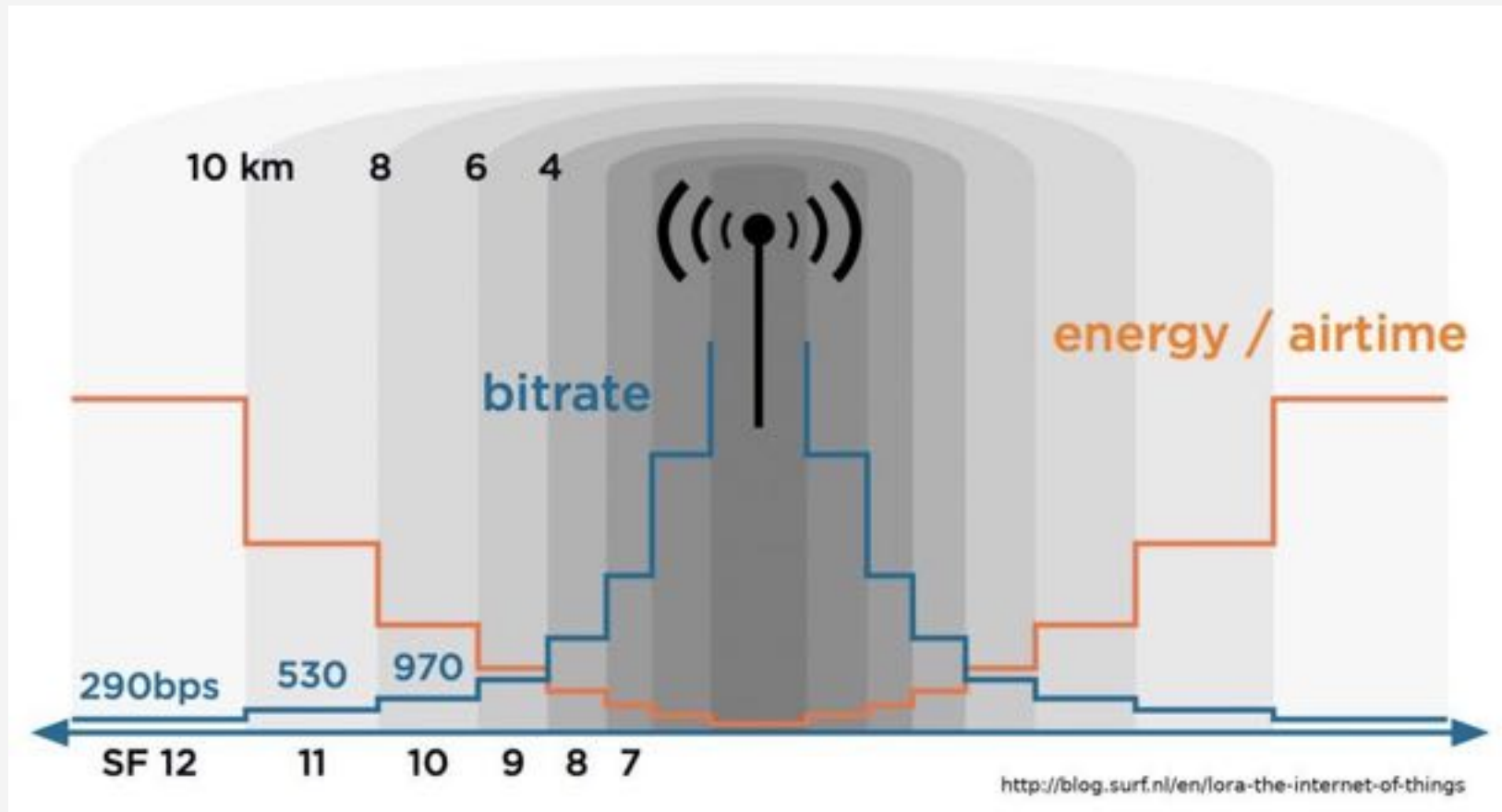


LoRa SPREAD FACTOR – SPEED AND COVERAGE



SF12
250bps
-136dBm
sensitivity

SF7
5400bps
-123dBm
sensitivity



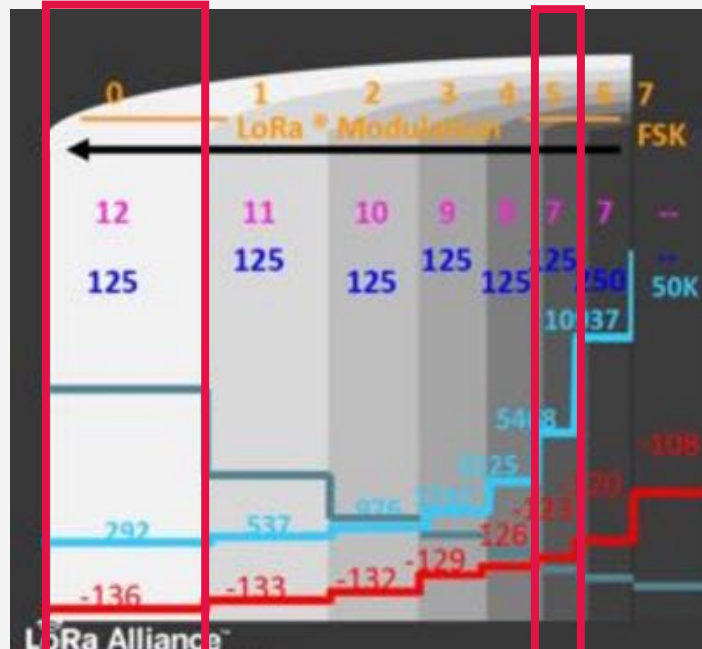
<http://blog.surf.nl/en/lora-the-internet-of-things>

Getting larger coverage vs saving energy can be achieved different ways:

- SF12 vs SF7 is 12,5dBm sensitivity equivalent. This is 16x less power needed to reach the same distance.
- SF12 vs SF7 is 20 times slower. This costs 20x more energy.

To optimize energy, it is better to reduce SF (higher data rate).

To optimize coverage, it is better to use High Gain gateway antenna then to use higher SF (lower data rate).

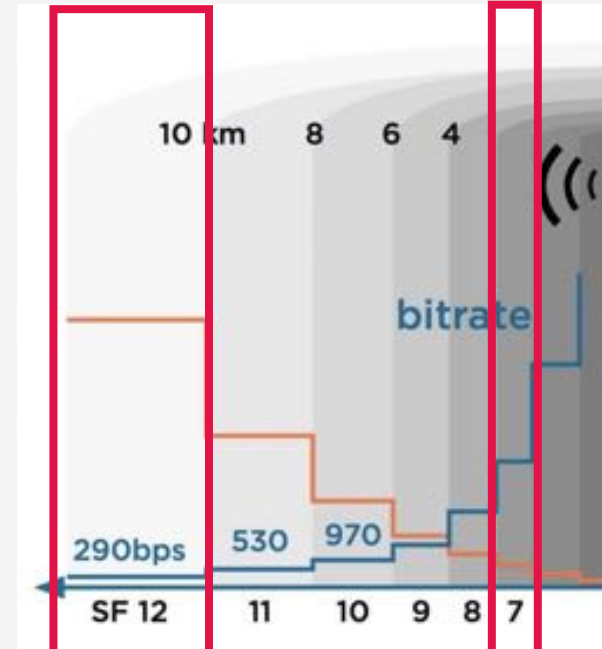


SF12
250bps
-136dBm
Sensitivity

SNR
-20dBm

SF7
5400bps
-123dBm
sensitivity

SNR
-7,5dBm



SF12
250bps
Reaches
10Km

SF7
5400bps
Reaches
2-4Km

Radio Link Quality

LoRaWAN includes different mechanism to check the link quality.

These solution are based on bi-directional communications and the risk of loss in both direction is high.

You need to consider the response content and positivity but not directly act on a nonresponse situation.

Taking a decision of changing parameters, rejoin is a project specific decision. Rejoin is high risk of not being able to reconnect. The session keys are maintained by the LNS server. There is not expiration defined in norms.

1

LINK CHECK

A device can send a LINK CHECK and receives as a response two information: Number of GW and dBm margin. This is basically a link quality indicator. The device can use this information to reduce its transmission power.

2

ACKNOWLEDGMENT

Device can request to ack a communication. The communication is acknowledged by the LNS. You need to have in mind false negative are frequent. They are due to radio collision, device radio environment, Semtech UDP protocol loss, gateway Duty-Cycle constraints or LNS/network processing time higher than 1-2s.

3

RETRY MECHANISM

Based on Acknowledgment mechanism, the RETRY system is going to resent the message up to the desired number of time the same message until the acknowledgment is received. The third repeat will be DR-1, the 5th DR-2, the 6th DR-3 automatically to improve chance to get received. This can impact your transmission capability due to Duty-cycle.

4

ADR - ADRACKReq

After 64 consecutive unconfirmed uplink, the ADRACKReq flag is added to request a network confirmation. After 32 nonresponse, the device is going lower DATA-RATE. Impacts duty-cycle.



HIGHER SPEED – HIGHER DATA FREQUENCY



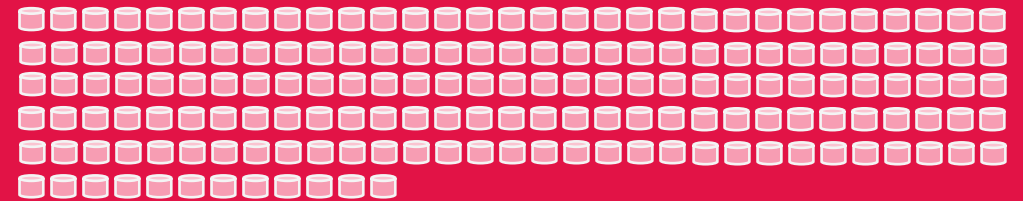
Time to transmit 10-bytes of data



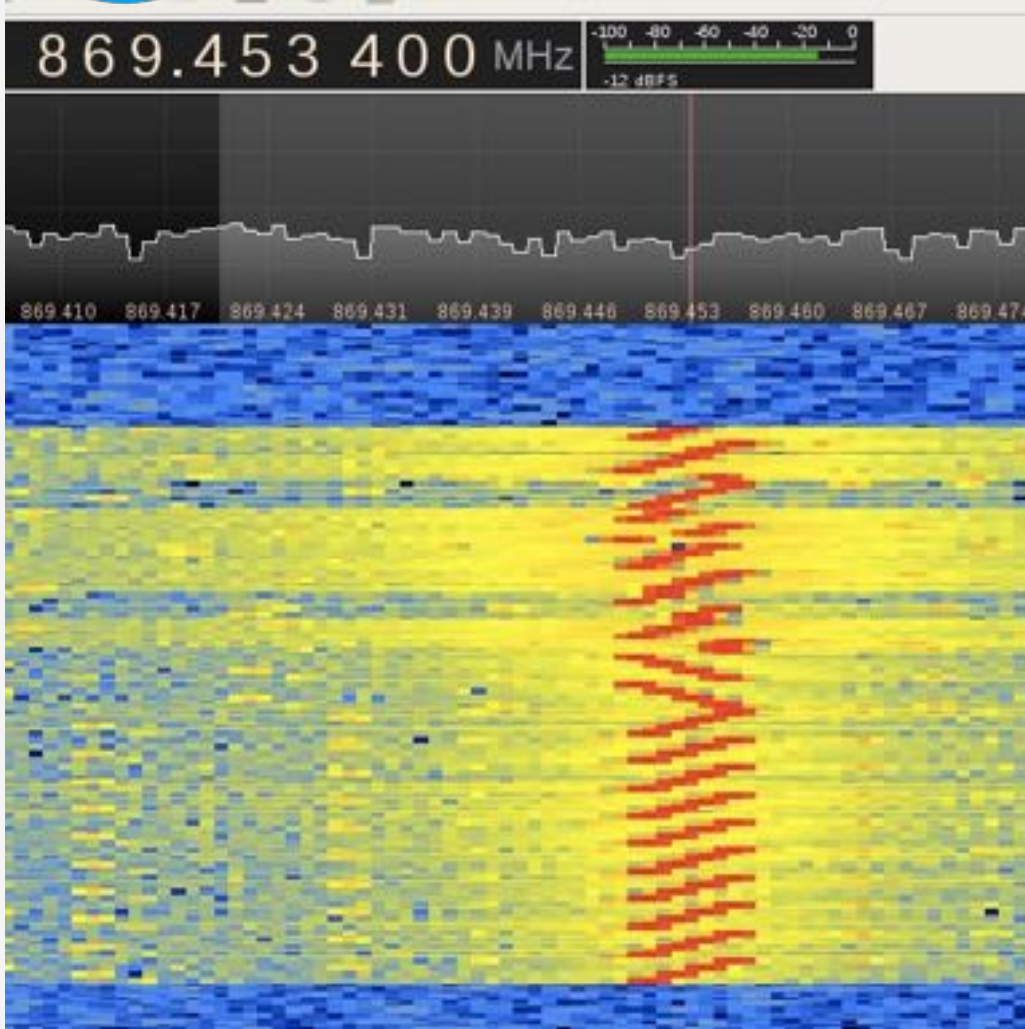
Transmission period for a 10-bytes message (in EU)



In 15 minutes @ 250bps
6 messages transmitted, once every 2'18''

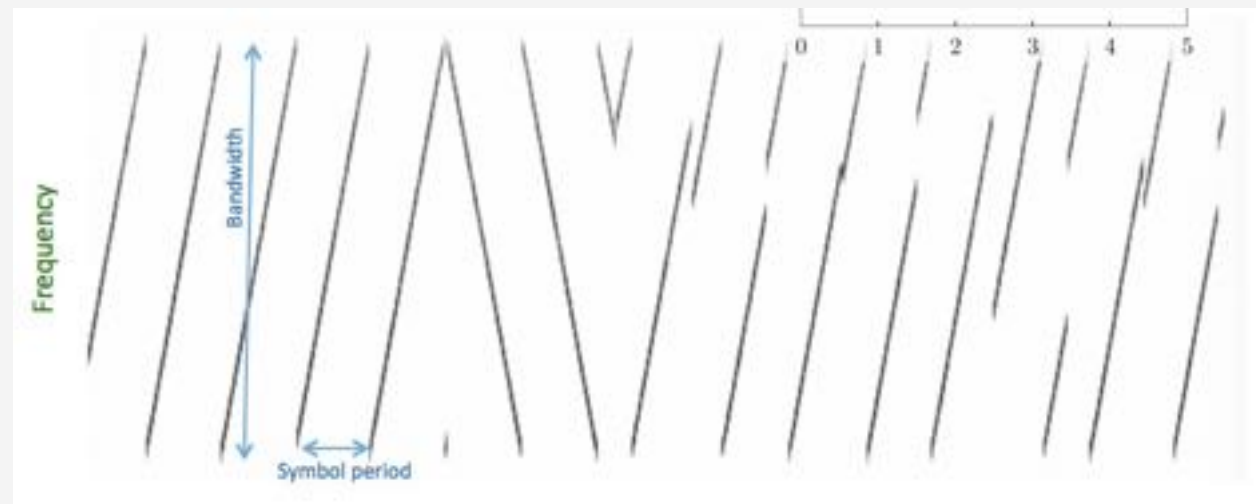
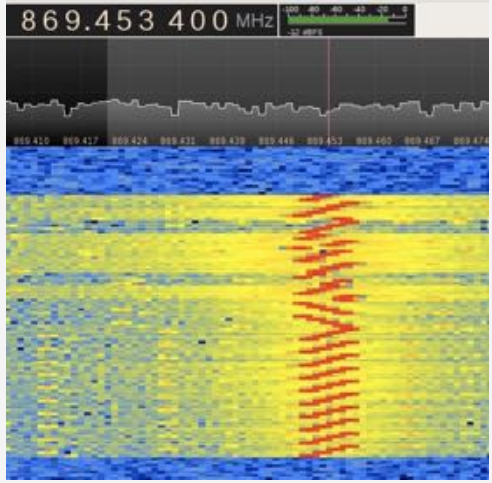


In 15 minutes @ 5400bps
162 messages transmitted, once every 0'5''54

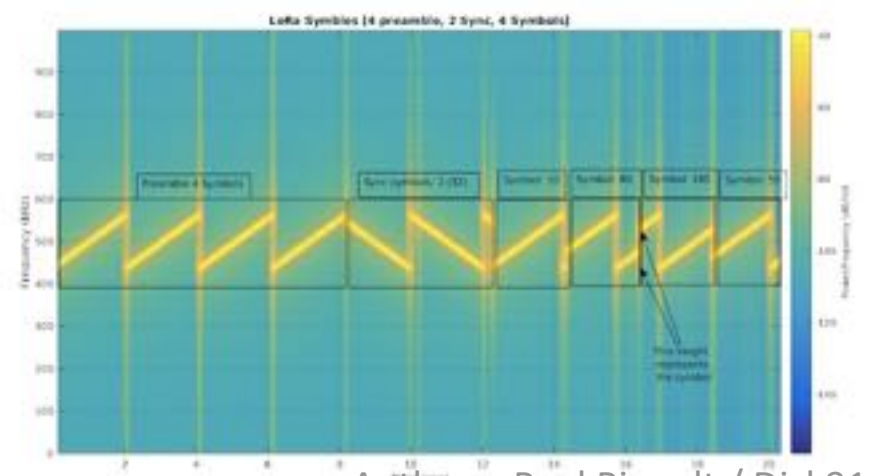
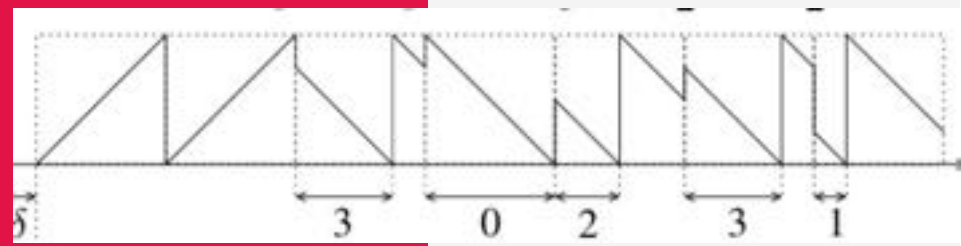
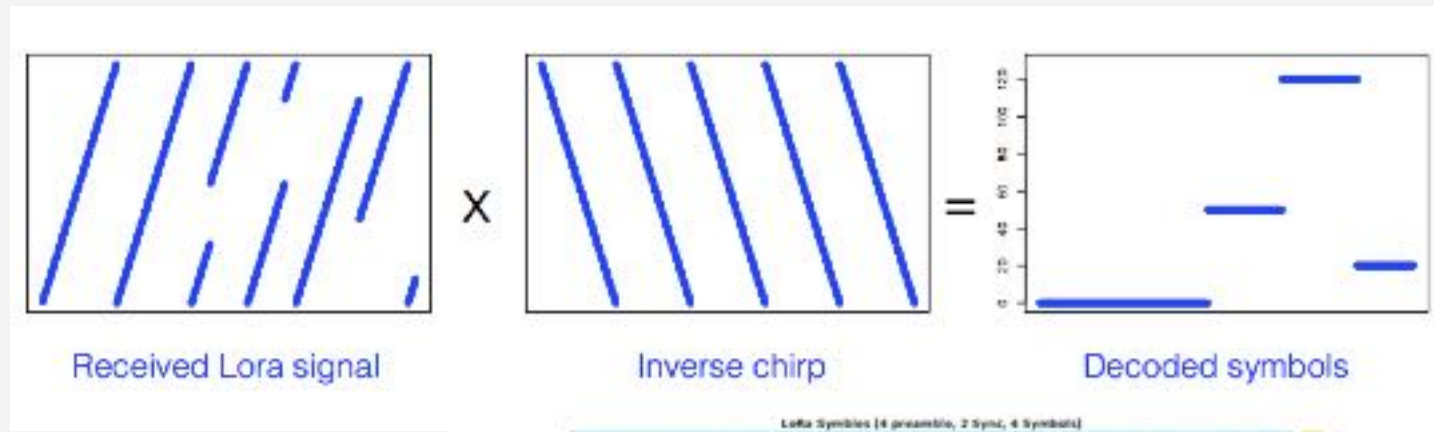


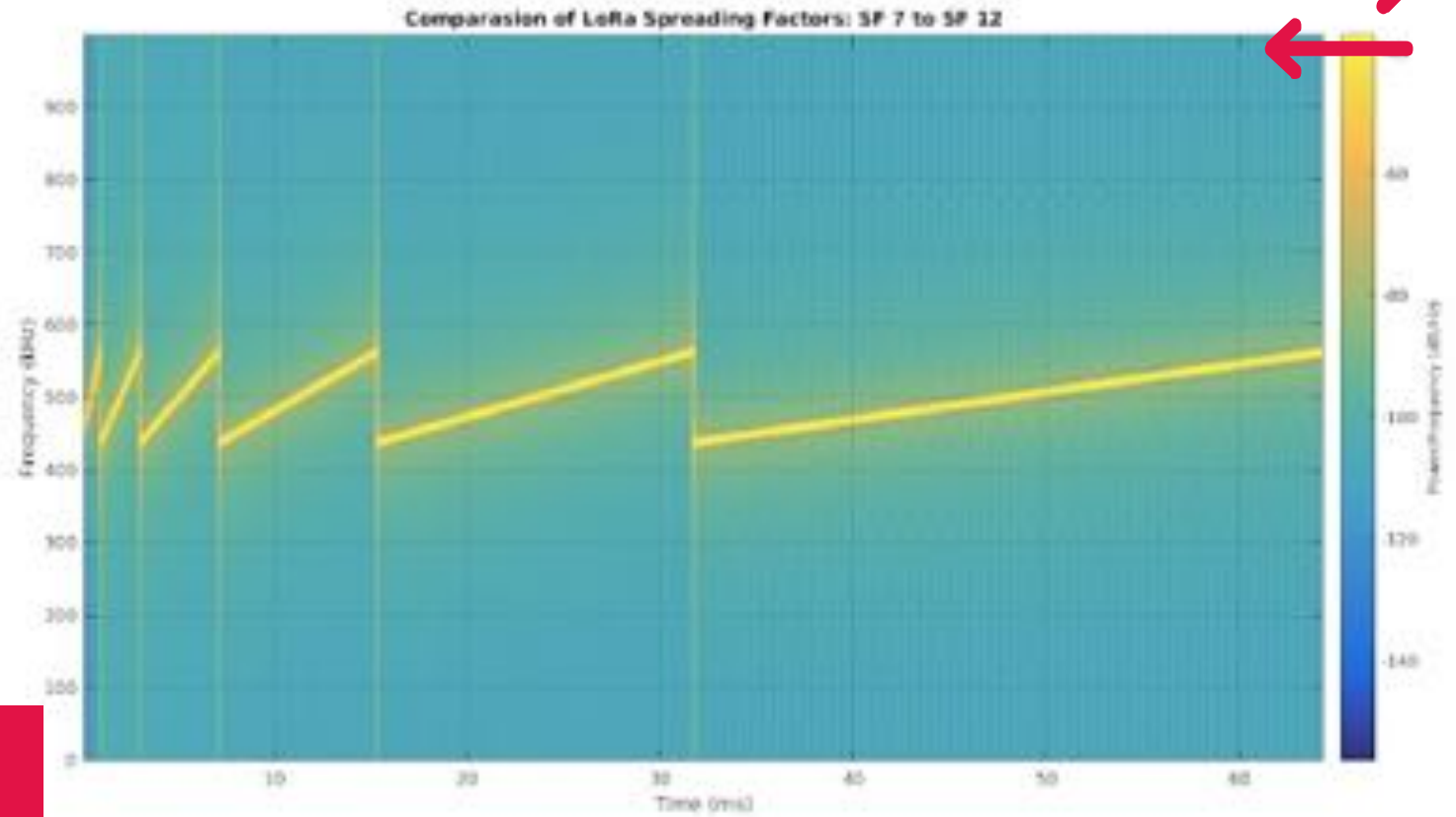
Data are transmitted by shifting the radio signal frequency. This movement creates a pattern encoding the data.

Any other noisy signal in the middle of this movement will be ignored.



LoRa Symbol decoding principle





LoRa Spread Factor principle

Getting more time to execute the frequency movement pattern allows a better decoding over noise. Better distance achieve, less loss, but lower throughput

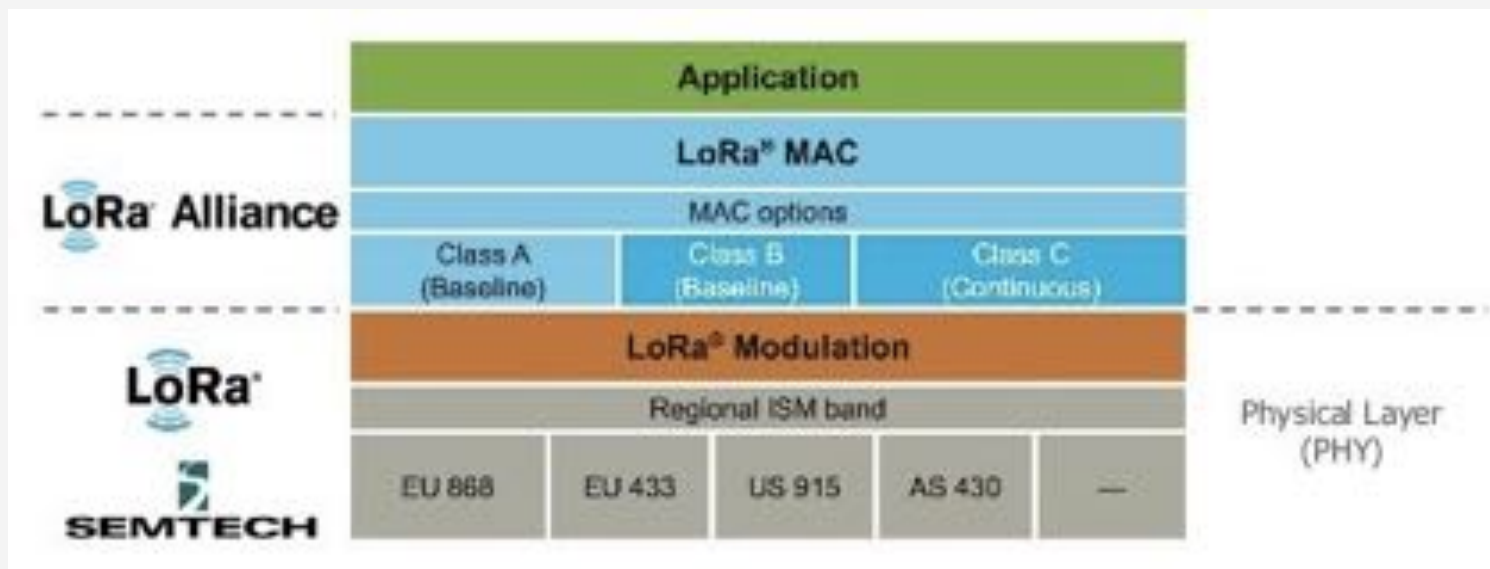


LoRaWan is one of the existing network implementation for LoRa.

Amazon SideWalk is another implementation of LoRa to build a network.

LoRa is also widely used in point-to-point application.





LoRa Wan

Use LoRa layer 2 communication and add a protocol on it to support a network integration with different devices and gateways. This can be compared with a TCP/IP layer with many differences.

LoRa

Point to point communication, we can compare LoRa with WiFi in terms of network layer.



LoRaWAN is a specification defined by LoRa-Alliance (telecom operators and industrial companies, 500+ actors) since 2015.

It defines one of the way to create a network over LoRa with the ability to support multiple public operator in each area



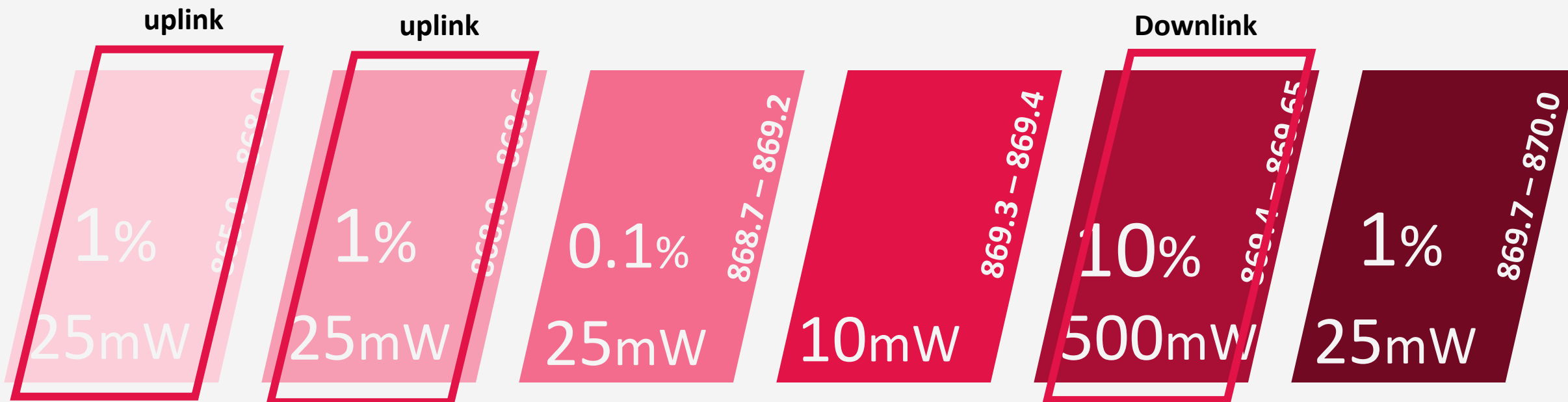
Defines the frequencies to be used (part of them), the frame format, encryption, ADR commands and the way to join a network

2 join procedures has been defined: OTAA (regular one, with session keys negotiation) and ABP (where the sessions keys are static). Over The Air Activation vs Activation By Personalization.



Defines the encryption procedures

Encryption is mandatory in a system where multiple networks co-exist. The encryption protects each operators against the competition as it protects the customer payload to be captured. The algorithm and the key generation are defined by the LoRaWAN specifications.



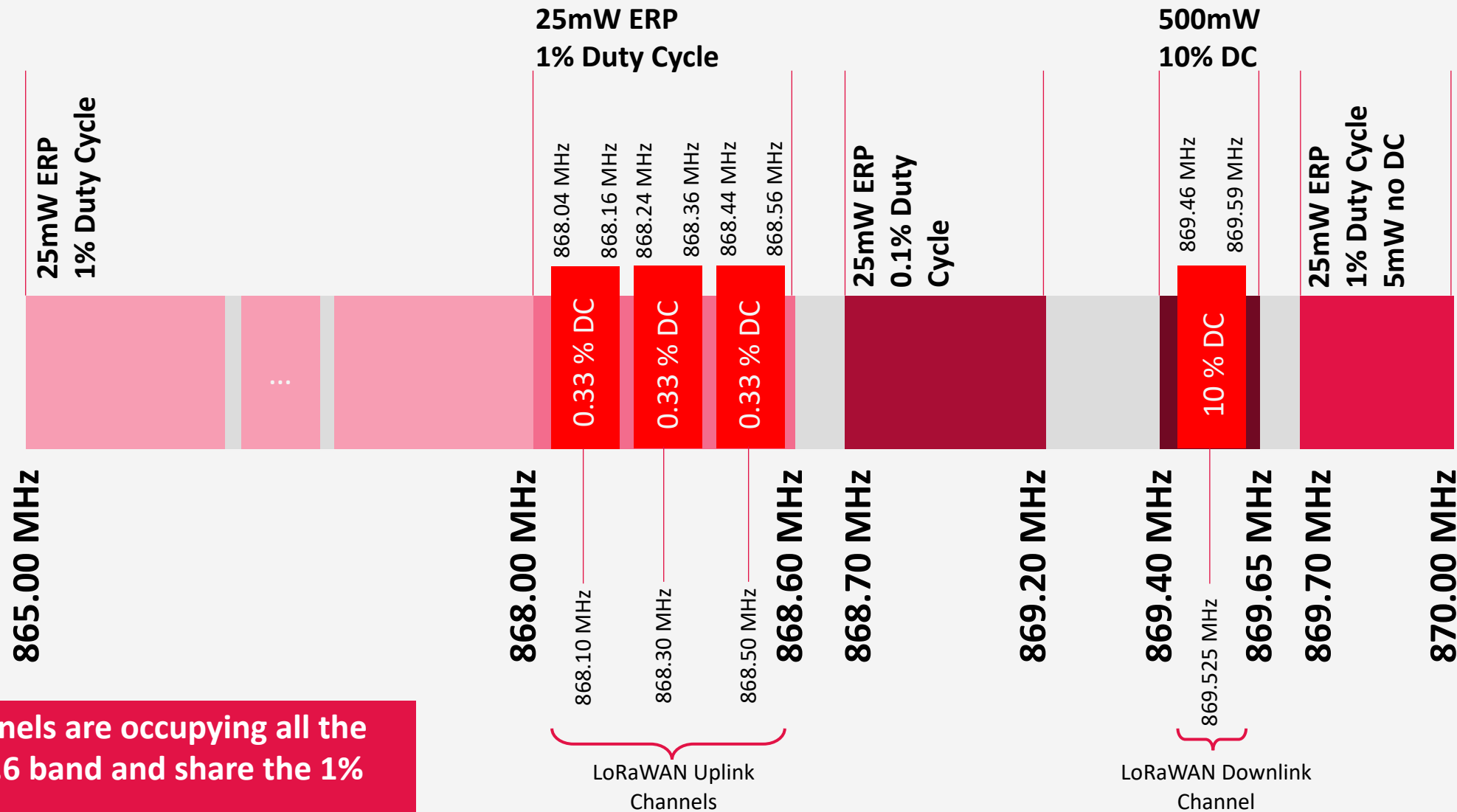
LoRaWAN defines, for Europe, 3 standard channels any device will use for the JOIN process. Each of them are 125kHz (375KHz are used). Center frequency are 868.1 868.3 and 868.5 in Europe. They are occupying all the 868.0 -> 868.6 band. LoRaWAN networks in Europe supports 8 channels, other 5 channels are defined by the network operator, usually, in the other 1% bands.

In FCC zone, the constraint is to use a minimum of 64 different channel with channel hopping. This requires 64 LoRaWan gateways (rare and expensive) most of the implementations currently implement only 8 channels gateways. The devices will have to communicate over 64 channels to respect the regulation. Consequently, 75% of communications are lost.



The LoRaWAN norms defines 3 uplink channels + 1 downlink any network must implement

LoRaWan mandatory channels



Uplink channels are occupying all the 868.0 – 868.6 band and share the 1% Duty Cycle.
 Downlink channel is fully occupying all the 869.4-869.65 band.

https://lora-alliance.org/sites/default/files/2018-07/lorawan_regional_parameters_v1.0.3rev_a_0.pdf

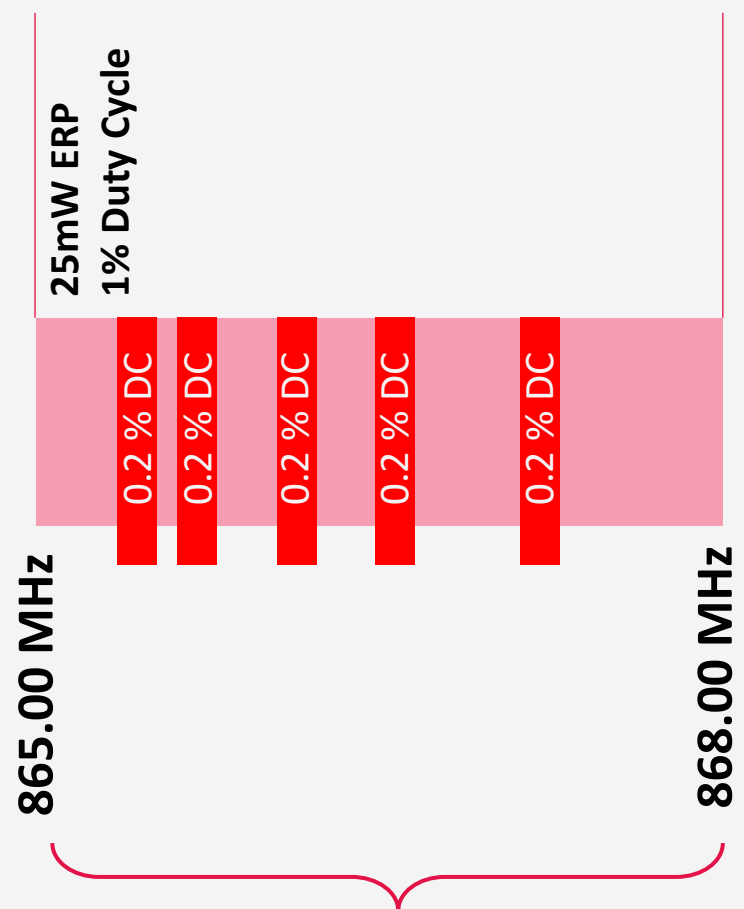


Each of the LoRaWAN networks can configure 5 custom 125KHz channels.

Configuration can be dynamically sent by network as part of the Join Accept message. Not all the network server respond with it.

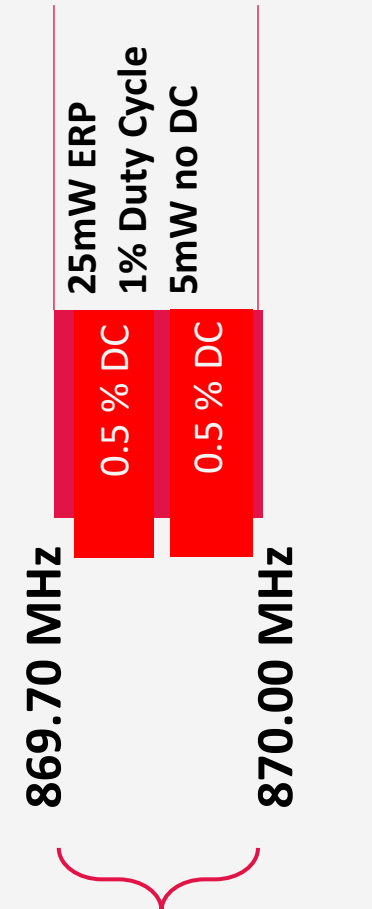
LoRaWAN device code usually hardcode the bands and associated regulation rules (power and Duty-Cycle)

Even if in UK 865-868MHz band could be use for larger DC or higher power, you need to modify LoRaWAN stack for it.



LoRaWAN Uplink channels

15 different channels
Can be defined
They are sharing the Duty-cycle



LoRaWAN Uplink channels

2 different channels
Can be defined
They are sharing the Duty-cycle

<https://lora-alliance.org/sites/default/files/2018-07/lorawan1.0.3.pdf>



A device can achieve 3% duty-cycle

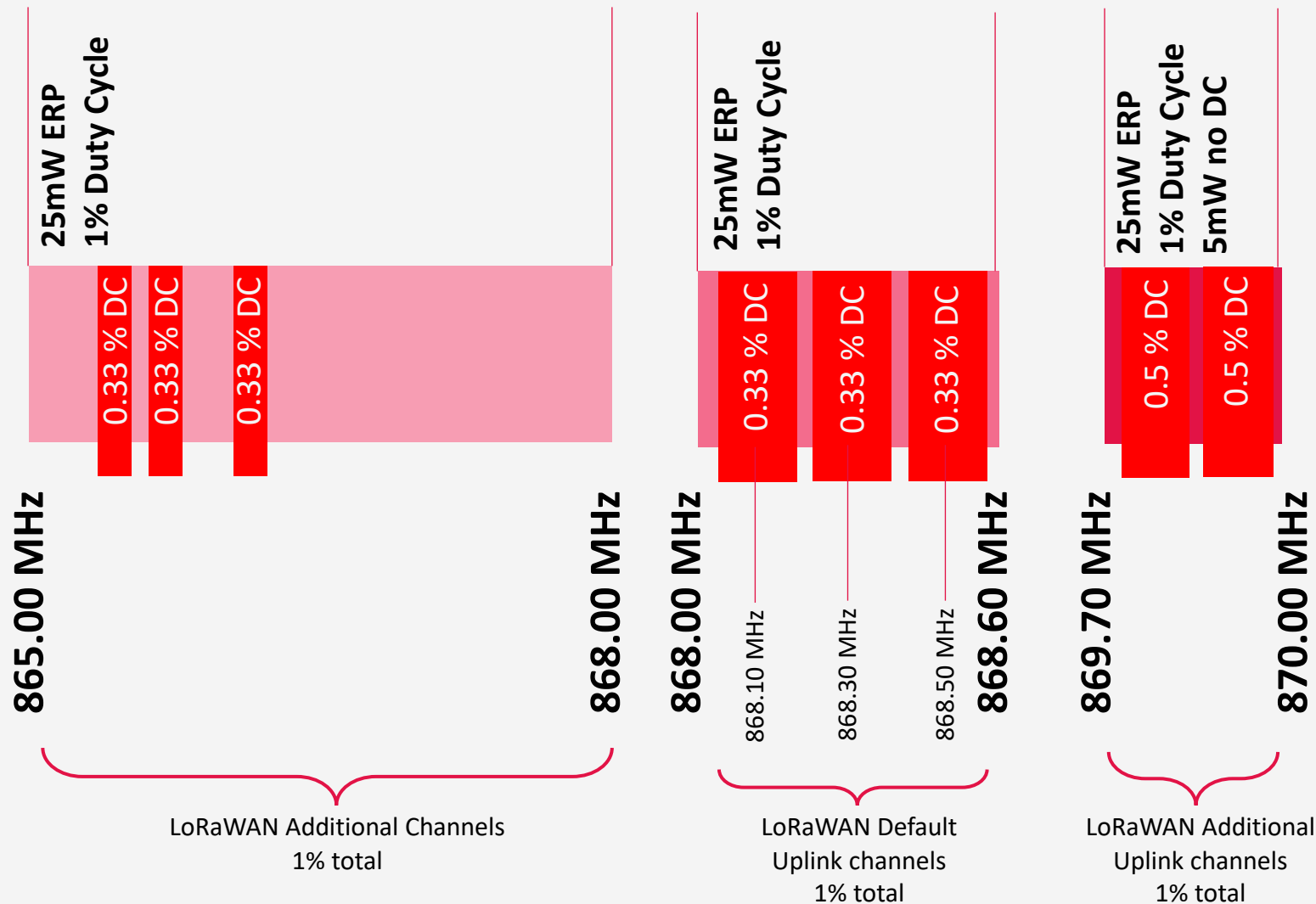
Different settings are possible and will define the overall device DUTY-CYCLE.

DUTY-CYCLE application is per band and cumulative in the different bands.

DUTY-CYCLE is shared between channels inside a given band.

This allows up-to 3% duty cycle by selecting the right bands.

LoRaWAN applies DC on every channel undependably right after transmission instead on rolling hour.



LoRaWAN® 3 communication classes



A Class – uplink and downlinks right after an uplink

One of the available, non busy, channel is selected for the transmission. Once the communication has been made, the selected channel is busy according to the regulation. This communication can be followed by a downlink response when the device request for it. This downlink can have a payload or simply be an acknowledgement from the network. Gateway downlink capability is limited.



B Class – scheduled downlink

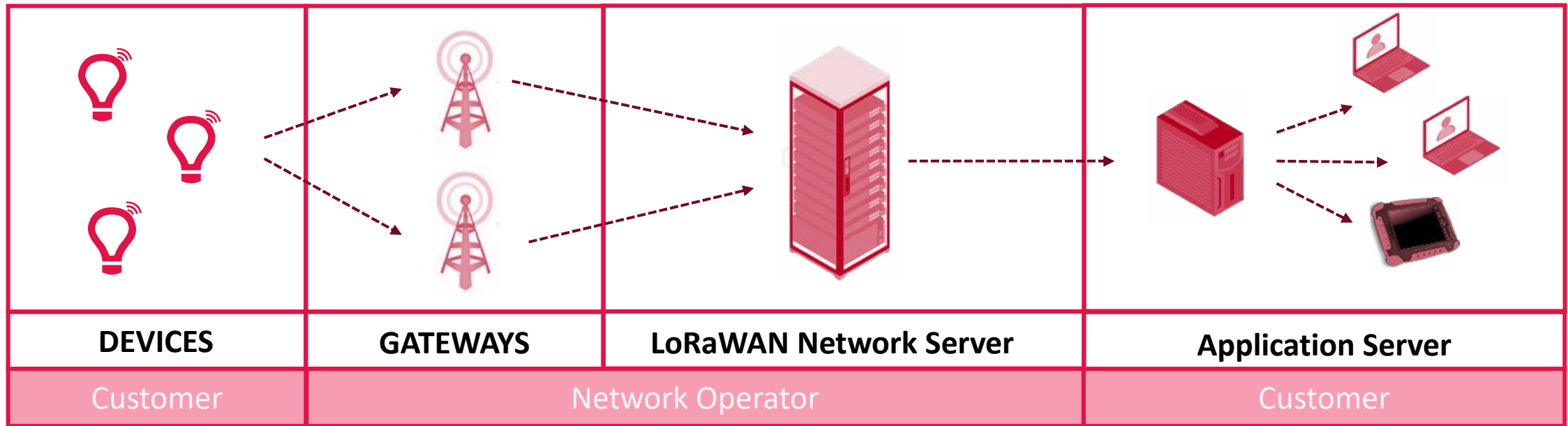
Instead of having to transmit a data to be able to receive a message, this mode allow to have a rendez-vous. It means clock synchronization and it is rarely implemented but allows multicast like for firmware distribution.



C Class – continuous reception

This is basically a Gateway mode. It is applicable for powered components as reception is power consuming (even if less than transmission)

LoRaWAN Network architecture



LoRaWAN Network Server (LNS)

All the DEVICES are communicating to GATEWAYS, a gateway receives all the LoRaWAN messages, this includes messages already received by another gateway of the network. It also includes GATEWAY from other networks. All the packets are transferred to the NETWORK SERVER (LNS)

The NETWORK SERVER is decrypting the communications (only the NETWORK SERVER you belongs to, has the keys for it), it also manage the JOIN procedure and ADR (Adaptative Data Rate) parameters with the DEVICES. It also forward the PAYLOAD to the CUSTOMER IT (Application Server) usually using HTTP POST or MQTT integration protocol.



LoRaWAN architecture

All the DEVICES are communicating to GATEWAYS, a gateway receives all the LoRaWAN messages, this includes messages already received by another gateway of the network. It also includes GATEWAY from other networks. All the packets are transferred to the NETWORK SERVER (LoRaWAN cloud here)

The NETWORK SERVER is decrypting the communication (only the NETWORK SERVER you belongs to have the keys for it), it also manage the JOIN procedure and ADR (Adaptative Data Rate) parameters with the DEVICES. It also forward the PAYLOAD to the CUSTOMER IT usually using HTTP POST or MQTT integration protocol.



OTAA INPUTS

DevEUI

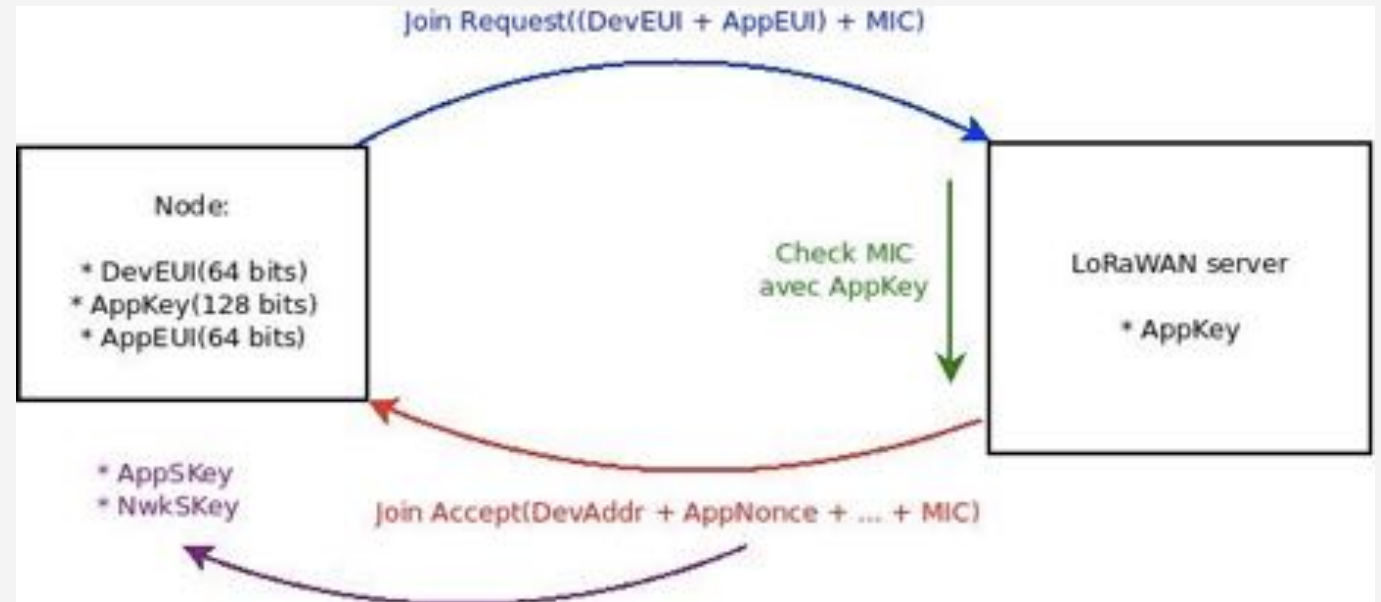
Device Uniq ID – IEEE unique (64b)

AppEUI

Application Uniq ID – IEEE unique (64b)

AppKey

Secret KEY only known by the device and the Network Server. Used for generating signature and encryption keys. (128b)



OTAA OUTPUT

AppSKey

Session key used to encrypt the communications

NwkSKey

Session key used to sign the communications

DevAddr

Device ID to be used during the current session. This is a 32b ID, shorter than the DEV EUI.

JOIN / REJOIN PRACTICE

To limit the risk of jamming due to device not able to connect, the LoRaWAN stack limits the JOIN process to a lower Duty-Cycle.

Remark: in my experience, a large part of the traffic received by my gateways is caused by devices out of subscription trying to connect but being rejected by LNS.

Frequent rejoin is basically not a good practice. A network disconnection does not kill the session keys.

1

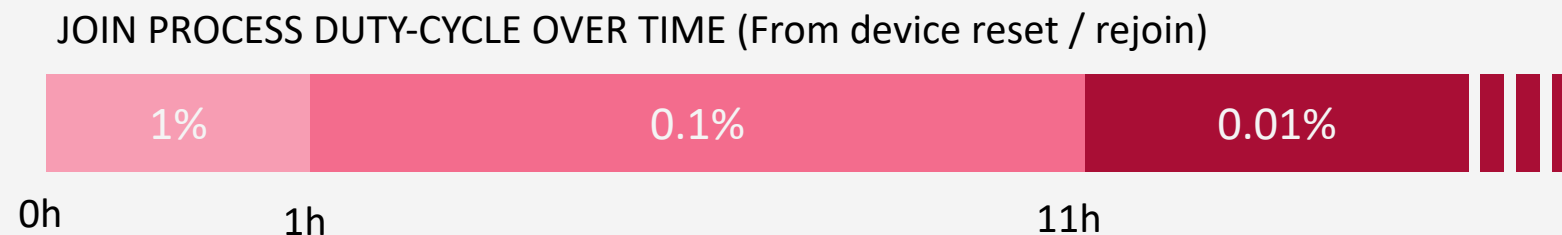
WHY REJOINING

The only good reason for rejoining is session key rotation. The LNS is not supposed to lost the session key and the norms does not defined expiration. That said, In case of LNS problem causing a Session loss, REJOIN can be used after many failed communications. Recommendation is to have them as rare as possible.

2

JOIN PROCESS BACK-OFF

In case a Rejoining process has been implemented after X lost messages ; because in most of the case these loss are related to a gateway issues, all the devices will try to rejoin in the same area causing a high risk of jamming and collision. To reduce this risk of collision, such devices need to implement a random timer between JOIN Request sequence and randomly select one of the 3 join channels. On top of this a specific duty cycle is applied



LoRaWAN Network Server (LNS) maintains the session information : DevID, Network S key (authentication), Application S key (encryption)

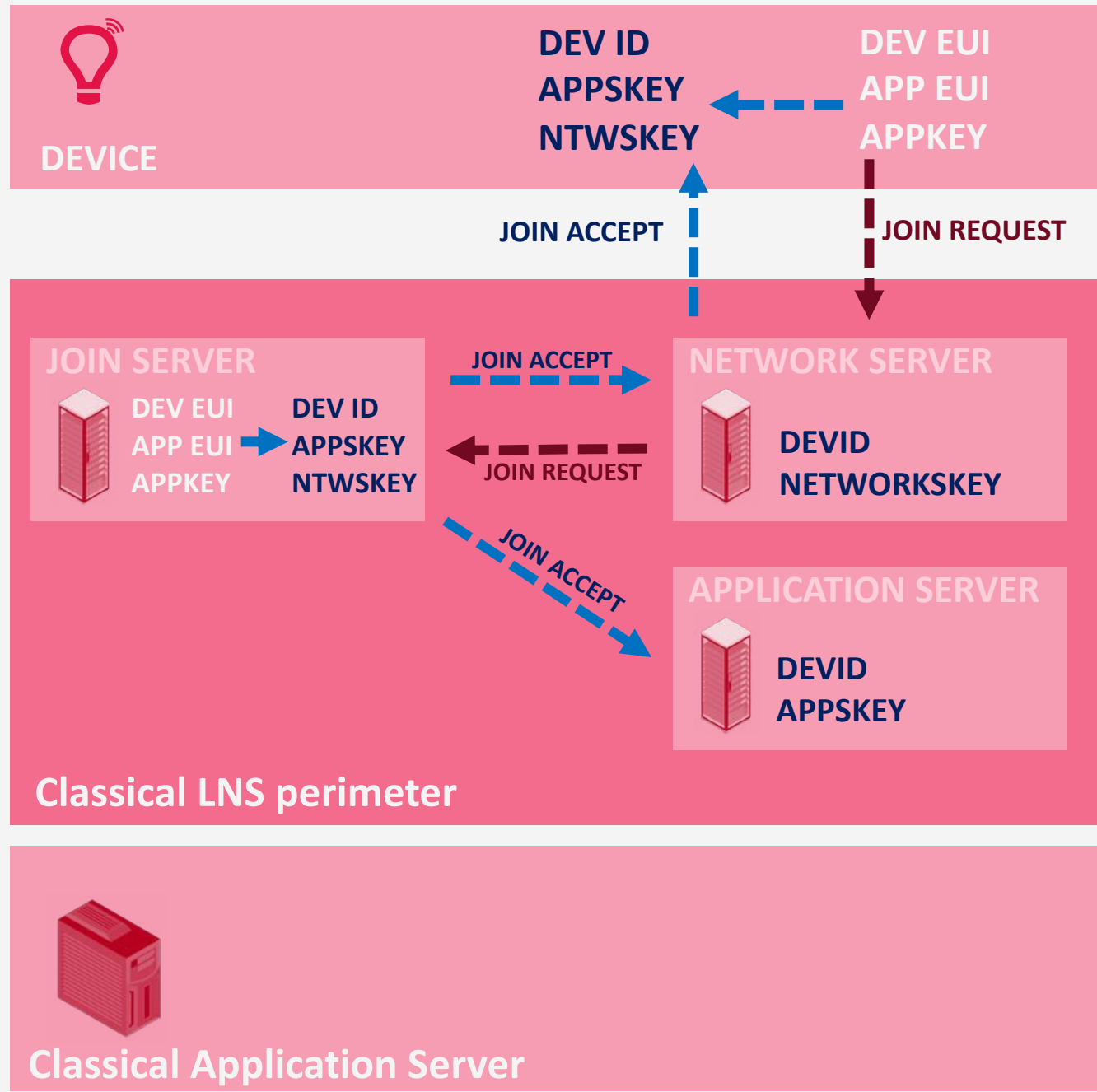
DevEUI, AppEUI, AppKEY are shared between device and JOIN SERVER.

The JOIN SERVER and DEVICE use derivate JOINEUI, DevNonce and DEVEUI to locally generate NwksKey and APPSkey.

JOIN SERVER propagates these session key to LNS components

The join process is just this session key negotiation.

Session never expire.





MAC Command

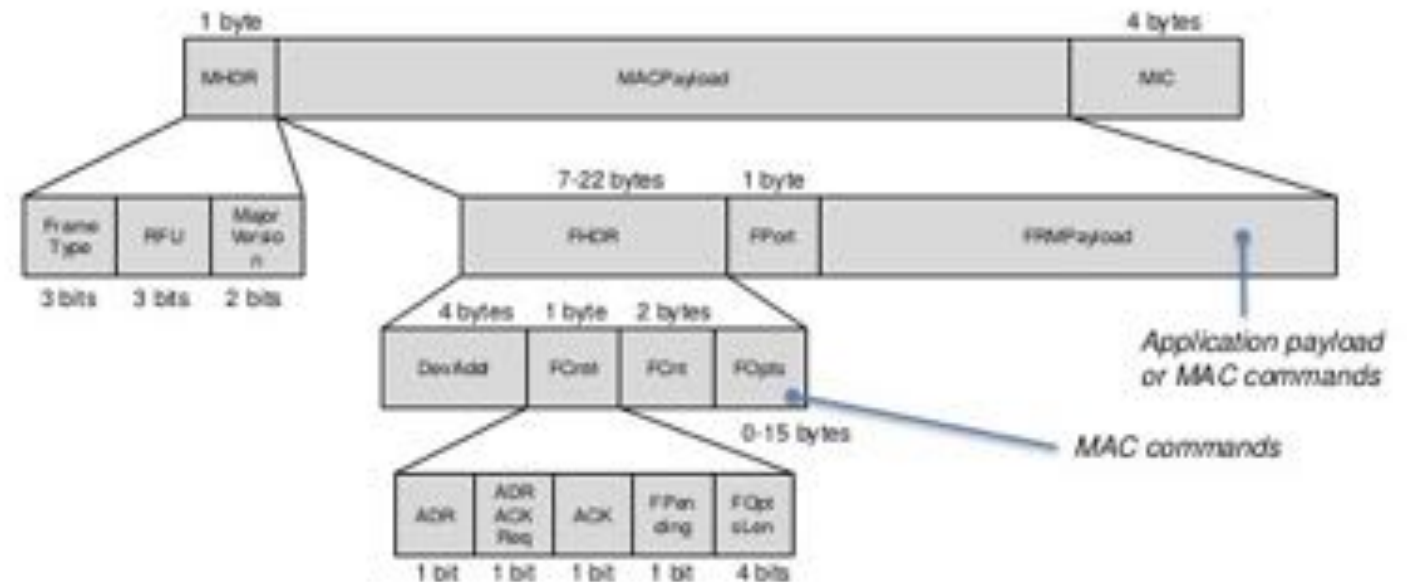
Allows the network server to place some specific request to the device like force a Spread Factor, channel list, transmission power ...As a designed you must manage configuration change you did not expect.

MIC

Frame authentication

Protocol complexity is higher than Sigfox, therefore, the memory and flash footprint for LoRaWAN is higher than Sigfox. For this reason ultra-low-cost is not a reachable target for it.

Frame Format



LPWAN@IETF98



ADR (Adaptative Data Rate) allows the network to setup the device:

- **Data Rate**
- **TX Power**

The ADR implementation really depends on the networks.

Considering ADR for a fleet of static devices (metering, smart home...) really makes sense to preserve the power consumption of device around the gateways.

It will reduce maintenance cost over time.

ADR is managed by the LoRaWan Network Server

1

ADR IS OPTIONAL

ADR is an option the network operator can activate in the network server. This option allows to control the device configuration. This impact the development as you do not master time-on-the-air and power consumption anymore. Consider worst case during design.

2

ADR FOR THE BEST

For a fleet of static devices, ADR allows to dynamically optimize the device power consumption and network scalability.

3

ADR FOR THE WORST

Not applicable for mobile devices: the previous ADR calculation will be wrong when the device will receive it. ADR is mostly implemented in networks to protect scalability by limiting your ability to switch to low DR.

4

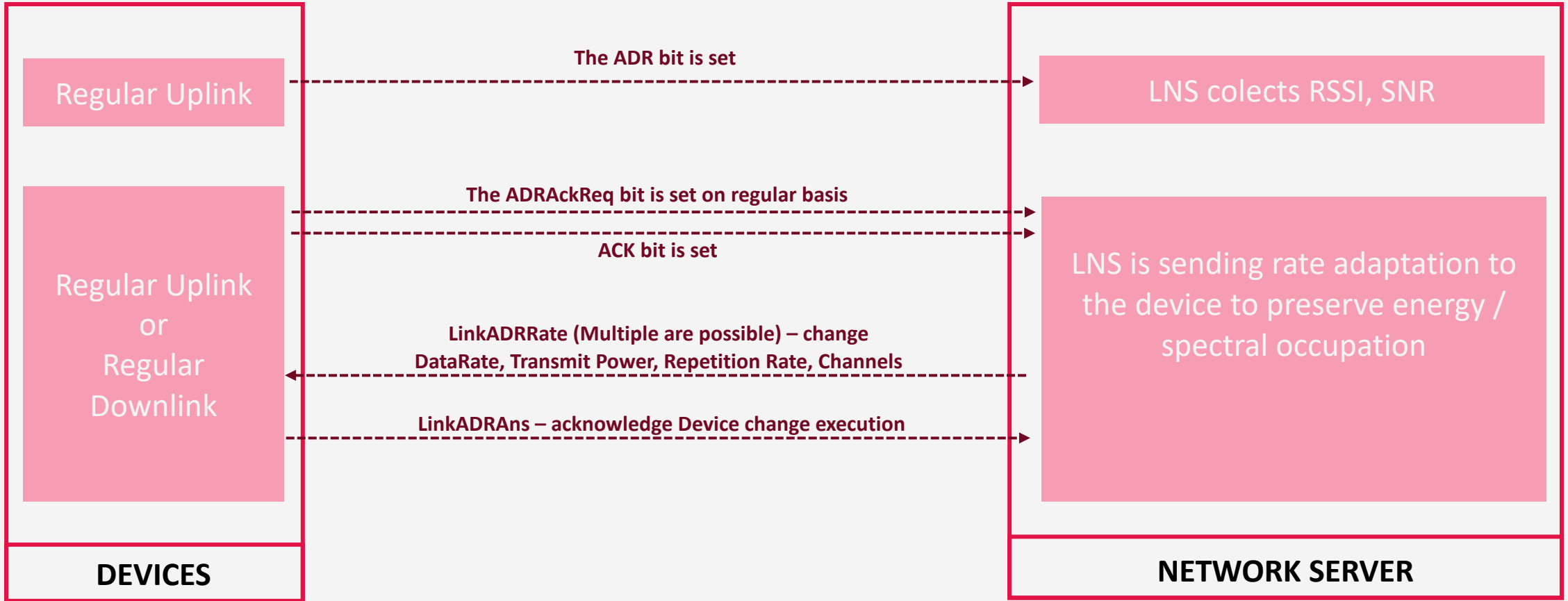
ADR ON ACK

To receive an ADR command, the device needs to communicate, including an Acknowledgment request. Once ADR is activated the flag will be set on regular basis by the LoRaWan MAC layer.



ADR is an optional feature the LNS can implement or not. It can be mandatory on some networks

ADR can be set on device when RF conditions are stable



LNS usually takes 20 Uplink communications to determine the right DataRate / Tx Power and propose the device a new configuration
Usually, device request for parameter update (ADRAckReq) every 64 communications in EU868.

LoRaWAN[®] DOWNLINKS



DOWNLINK are immediately following an UPLINK communication

The first one is on the same frequency as the UPLINK 1 second after it

Speed can be different. The channel rules are applied (power, duty-cycle...)
This time is short for a Gateway – Network Server communication.

The second one is on 869.525Mhz allowing a 27dBm transmission

It happen 2 seconds after Uplink. Gateway gets more time to receive the Payload from the Network server



A downlink is acked by the device, multiple downlinks can be chained.

The downlink payload have to be queued in the network server: there is not enough time to loop the request with the customer IT.

LoRaWan scalability

Congestion model show large degradation with 1000 devices communicating 1% duty-cycle within a single gateway range. All LoRaWAN networks around are cumulative. Network operators are protecting scaling by different ways.



DUTY-CYCLE REDUCTION

Limit the total amount of messages / day in the subscription. Use 2 bands to be in the 2% instead of 3. Use of lower density 865-868 band.



DATA-RATE CONSTRAINT

Force devices to use higher speed data-rate to reduce the individual time on the air per message.



TX POWER REDUCTION

Reduce short range devices power to reduce the collision rate perimeter.





LoRaWAN scalability

Different factors are limiting the scalability

- No congestion management
- 3 channels are common for all the networks
- About 1000 device in a same area (even in different networks) will saturate the 8 available channels. (it depends on SF and duty cycle...)



Strength

- Ability to offer TDOA location computing (Time Difference Over the Air) for non-GPS tracking (hundreds of meter precision)
- Ability to deploy private networks at low cost.
- Ability to support mobility with a reasonable loss rate.
- Throughput enabling multiple use-cases.



Weakness

- Complex channel management in roaming and complex roaming. Channel map for a network operator have to be global.
- A really limited number of public offer and complex roaming capability makes it limited to private usage or country usage when covered.
- Software complexity making it a bit more expensive than competitors on the device side. Even if the price is decreasing. Today it is starting at 5€ / device.



Public Application

The map displayed here has been made with a single LoRaWAN antenna network deployed in a high position. All the city around is covered. The investment is about 500€ in 2020 for a such result.



Smart city application

Sensors deployed all around the city



Local mobility

Collect information about public transport or parking availability ...



Public network

Offering an IoT network access to all the citizens for private purpose.

Private deployments



What we get with a simple indoor gateway

An investment around 300€ allows to get a coverage in an industrial site, even Indoor and without interacting with existing network



Indoor vs Outdoor coverage



10 km coverage is what you can get with a good outdoor spot.

Indoor antenna performance are usually around 300m around.

On the left: an example of two gateways coverage (outdoor has a larger coverage than what your see here, outdoor did not).

Scale is the same



The Things Network



Is a crowdsourced network, deployed World-wide and free for use. Deployed by passionate people it proposes a good quality network In the main big cities.

Open-source mindset. This network is use in many business application: the network server is use for simplifying private deployment.

A professional version is available with Network Server SLA. TheThingsIndustry is the most innovative organization in the LoRaWan area since 2015. They are also pushing the market by making low-cost hardware and opensource solution.

Basically it is Uber for Telecom industry



Created in 2015

30.000 Gateways running in **150** countries

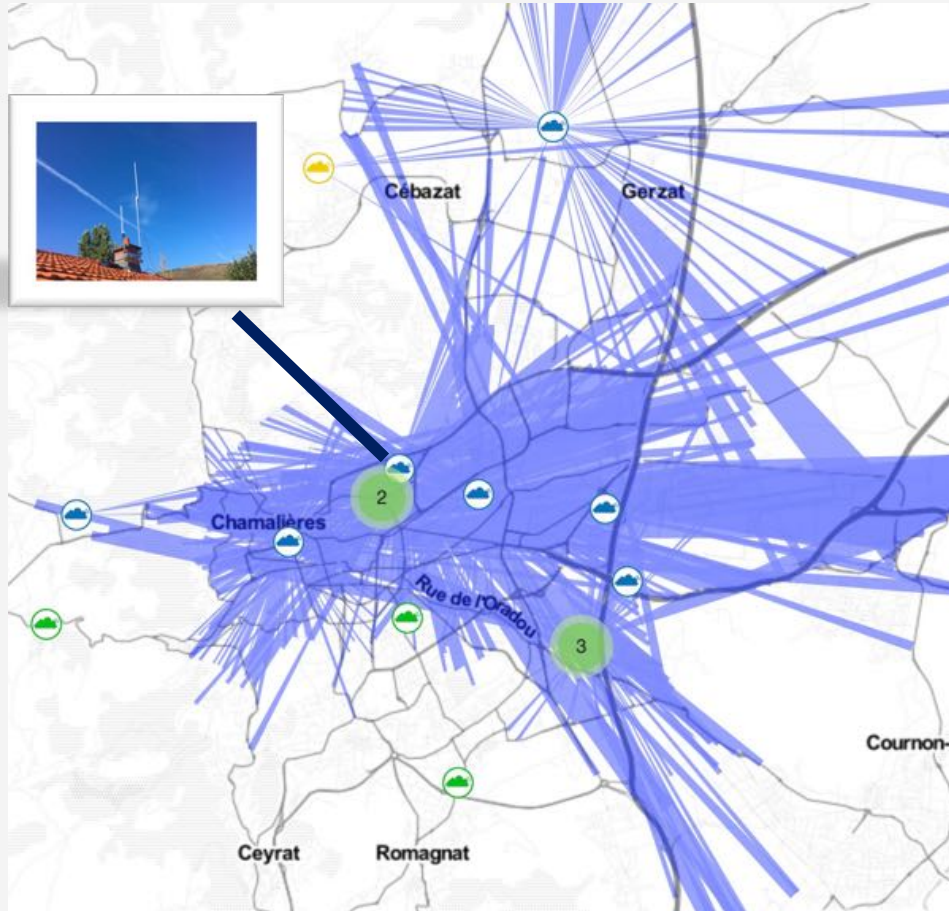
500.000 devices using it

9M messages / day 2020

65% market share on covered zones.

Most of the gateways have been deployed in Europe.





Coverage example made by a short number of people in a medium size city.

**Helium is a blockchain for LoRaWan Distributed
Global crowdsourced IoT Network**

Helium is a blockchain for LoRaWan Distributed Global crowdsourced IoT Network

Coverage is provided by a community of people instead of a company. Like TheThingsNetwork

Helium is a blockchain for LoRaWan Distributed Global crowdsourced IoT Network

Investment on hardware is rewarded by a crypto token. Blockchain's rules pilot the deployment and supports the main telecom industry processes.

Helium is a blockchain for LoRaWan Distributed Global crowdsourced IoT Network

The network is global, it has started in North America, now covering Europe quickly and start in Asia.

Helium is a blockchain for LoRaWan **Distributed** Global crowdsourced IoT Network

The network supports multiple LoRa Network Servers (Routers) as private networks on top of the Gateways (Hotspot) public infrastructure.



People-Powered Networks.

Start a Wireless Revolution

Powered by the Helium Blockchain, The People's Network represents a paradigm shift for decentralized wireless infrastructure.



helium

An IoT network based on LoRaWan technology.

Deployed by people, at home, worldwide.

Powered by a blockchain to create an incentive and manage telecom operator's processes

Helium uses cookies on this site to enhance your user experience, understand site usage, and assist in our marketing efforts.

I Agree



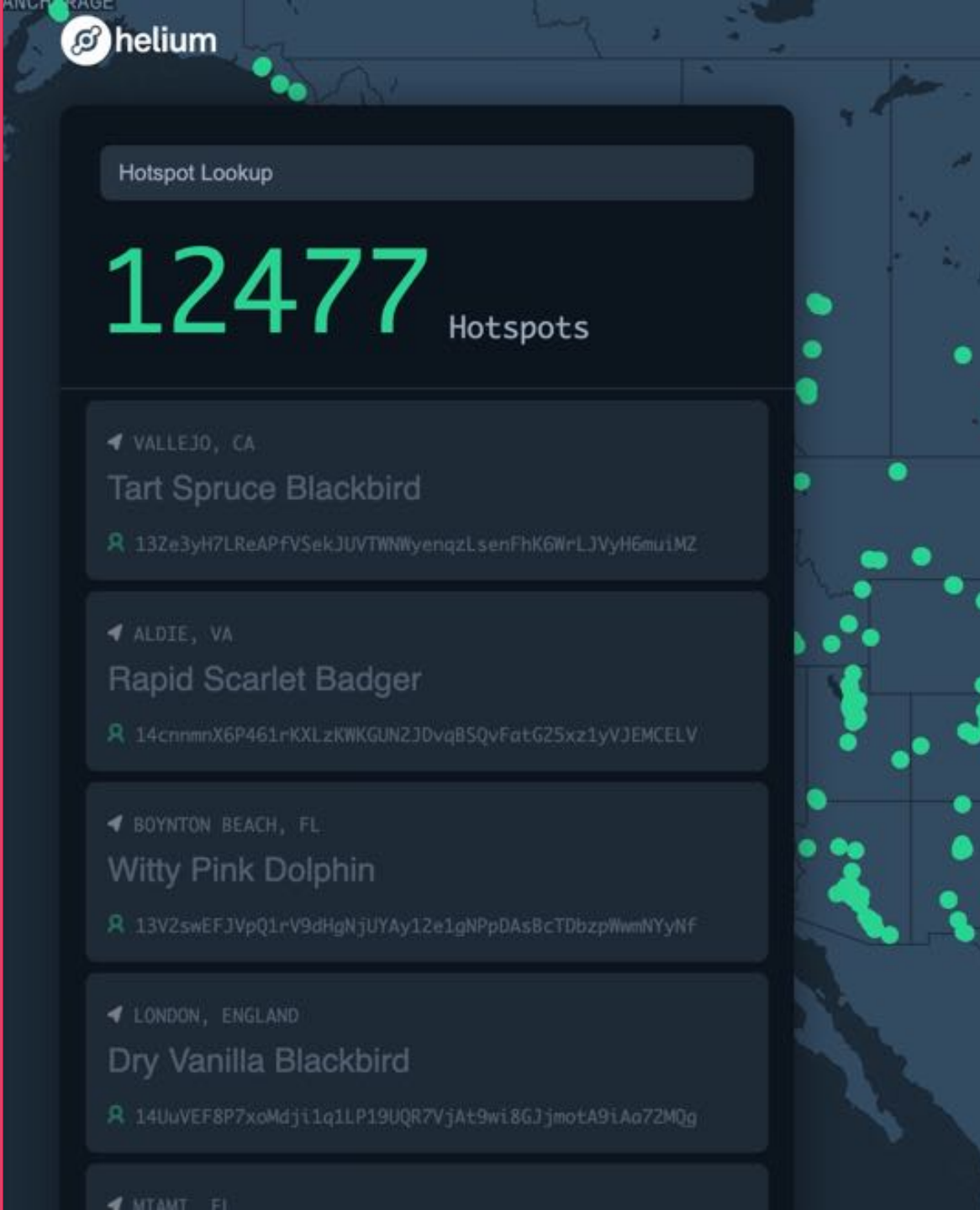
**12500 Hotspot deployed in 6 months. Mostly in the USA.
77000 deployed in a years.**

Growing fast as today your cash back is about 1-2 weeks.

Limited coverage due to indoor installation in most of the case.



Crowdsourced



HELIUM

Hotspot Map → Block Explorer

Is also crowdsourced IoT network, but it targets a different category of people to deploy the network. Instead of tech passionate, it target crypto investors.

Helium is an IoT network managed with a blockchain. Helium contributor are mining HNT tokens against coverage. Communication are billable with a flat and low price.

Basically, it is UBER + BITCOIN for Telecom industry

May	2020	3.025 HS
Nov	2020	12.477 HS
Feb	2021	18.700 HS
July	2021	77.100 HS
August	2021	100.000 HS
October	2021	220.000 HS
Nov.	2021	320.000 HS
Sept.	2022	954.940 HS
Feb.	2023	986.820 HS

July 2023 Status

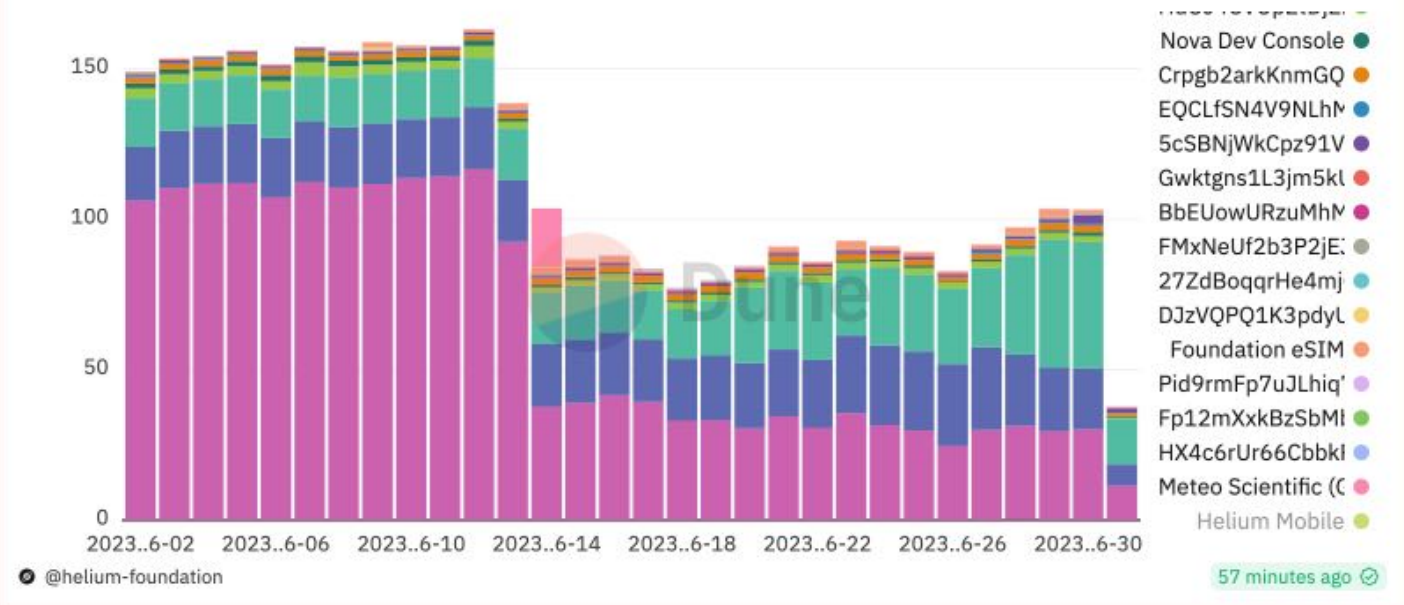
> 420K active hotspot in month, globally stable on the last 6 months.

> Some mee-too blockchains try to take a part of it with Y connectors

> Some big players leaves the game like bobcat

> Hotspot have been made simpler, less need for maintenance, good stability.

Helium DC Burned for Network Usage by Organization

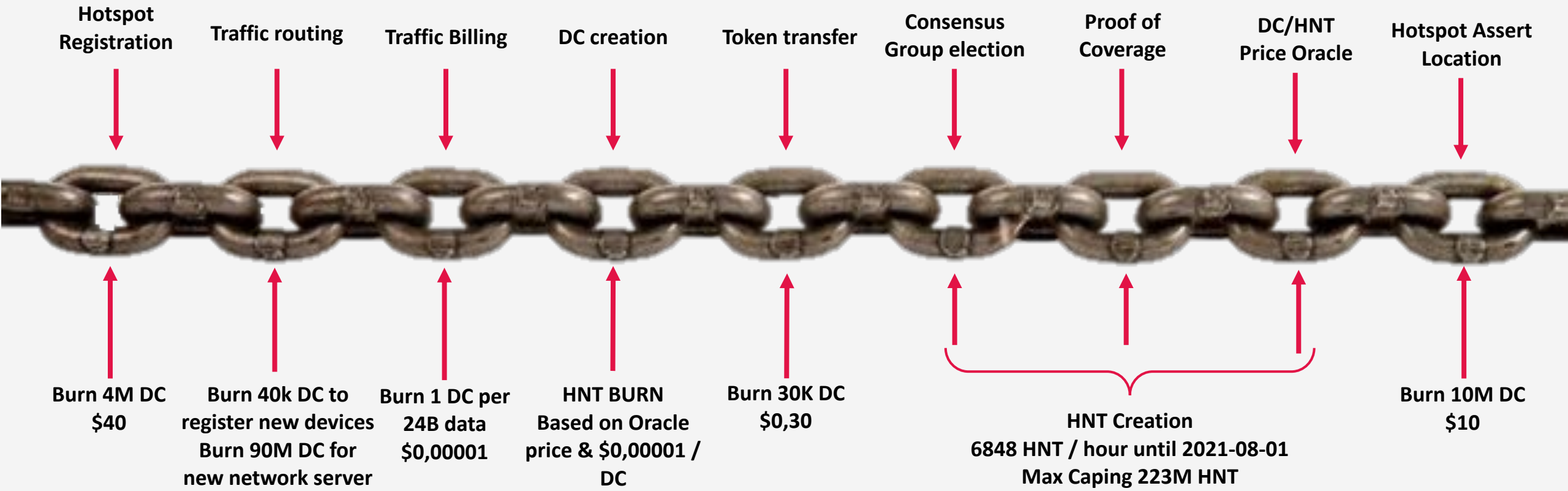


Helium BUSINESS Usage per day in \$ (\$1 = 100k messages eq or 24Bytes)

Main console filtered due to gaming past month (add \$50)
(drop due to normal packet purchasing (duplicates evolution))

About 10M packets processes per day for business applications
As part of it 60% is roaming packets for Telcos

What is a Telecom blockchain



A Blockchain Based Network

Mining is done using Proof of Coverage (PoC). Unlike Proof of Work, it relies on radio communication and has a light power consumption.



FOR NETWORK INFRASTRUCTURE OWNERS

A crypto token (HNT) is mined during PoC and data transfer. Uses are:

- Burn into DC at market rate
- Sell on crypto exchanges



FOR NETWORK USERS

Acquire a specific token (DC) with a fixed price for data transfer



DATA IS ROUTED ON NETWORK SERVERS

Payload is routed to the right network server. Today Helium propose one.

Helium network growth



Objenious network size
For 95% France coverage

4000

TTN network size 5 years
after being launched

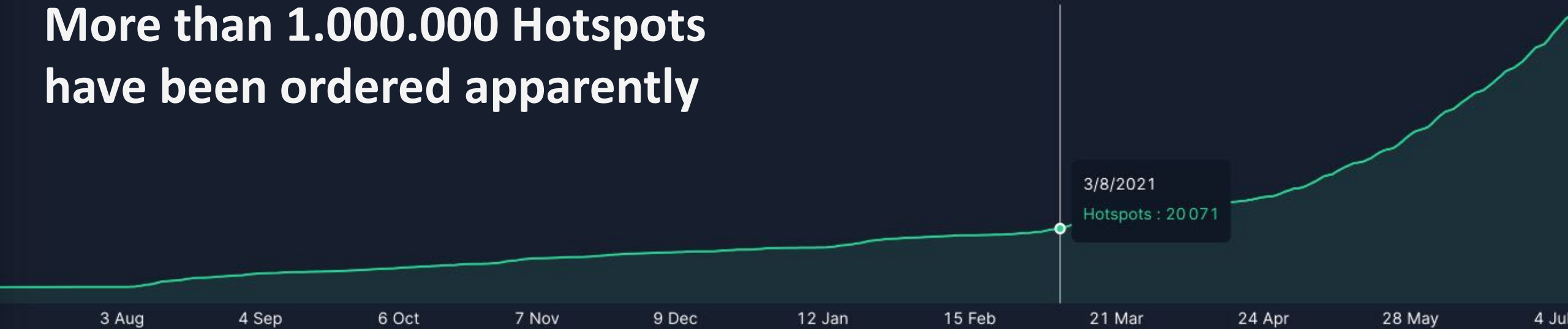
20000

77000

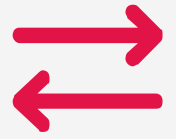


Hotspot Network Growth

More than 1.000.000 Hotspots
have been ordered apparently



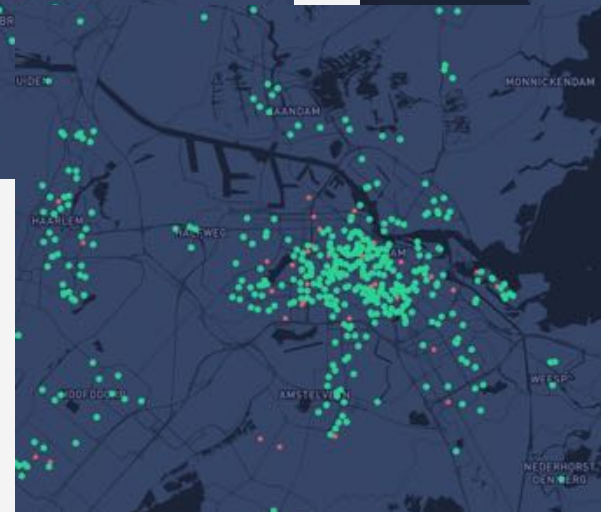
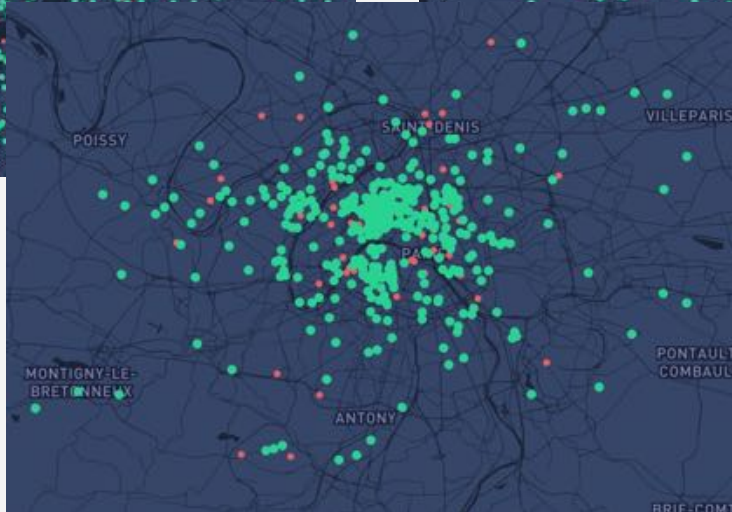
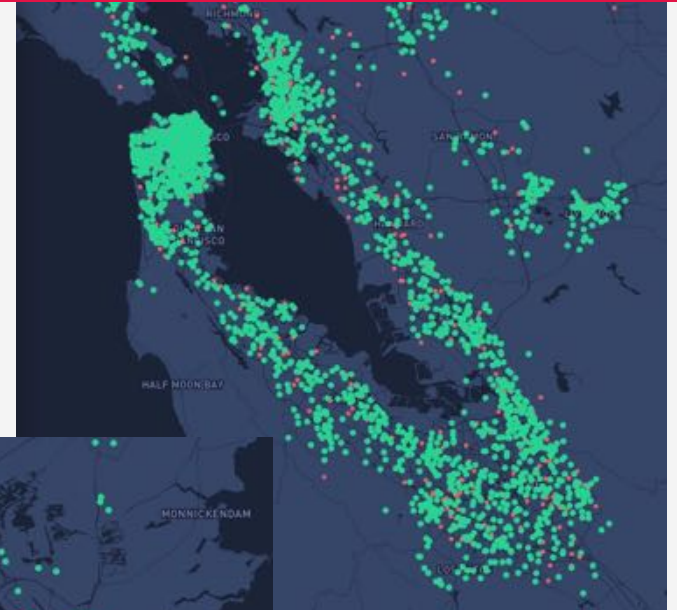
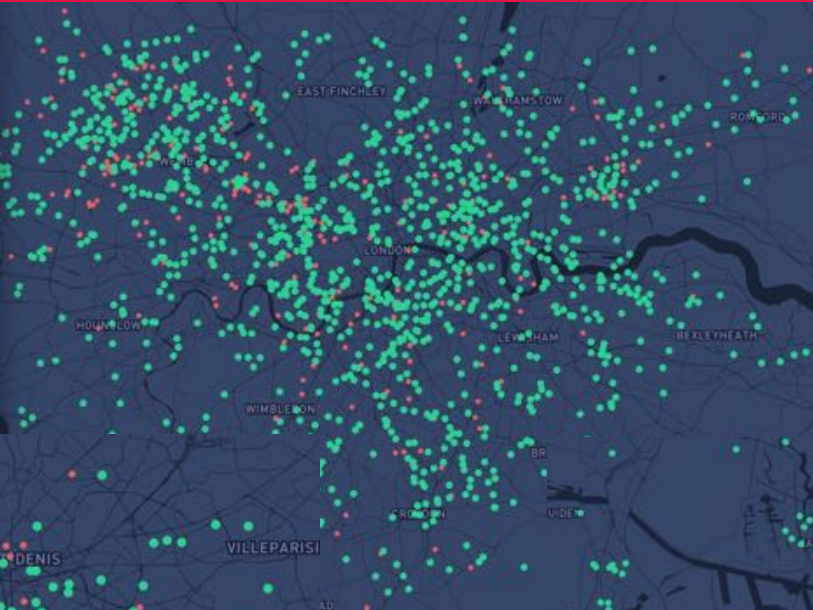
Helium is high density LoRaWan



New York

London

San Francisco



Paris

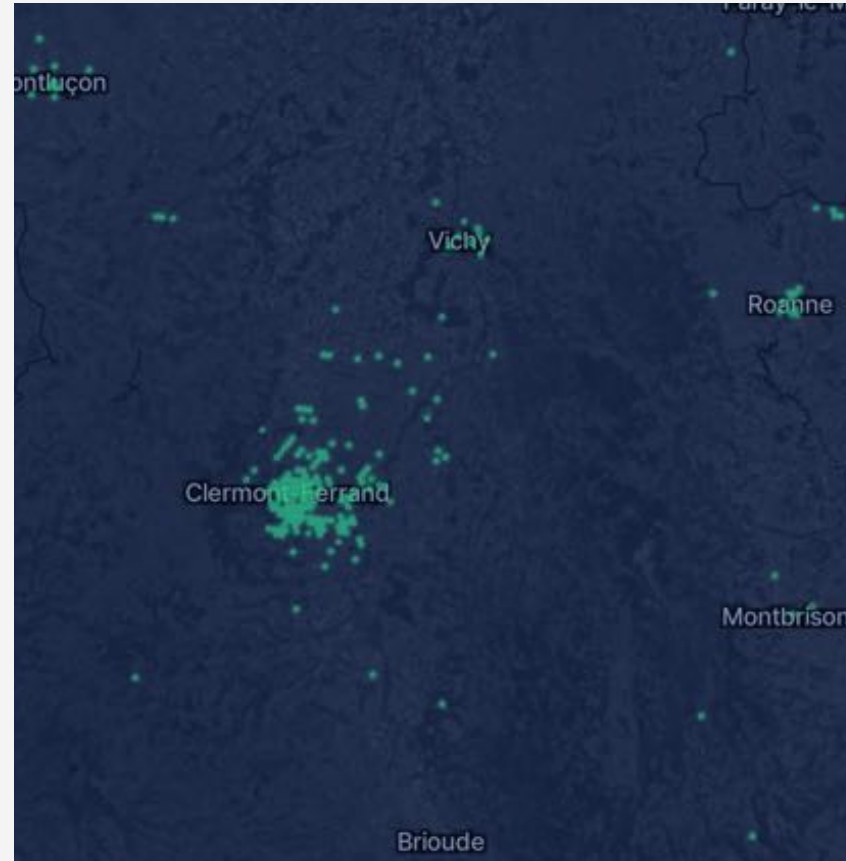
Amsterdam

Helium at Clermont-Ferrand

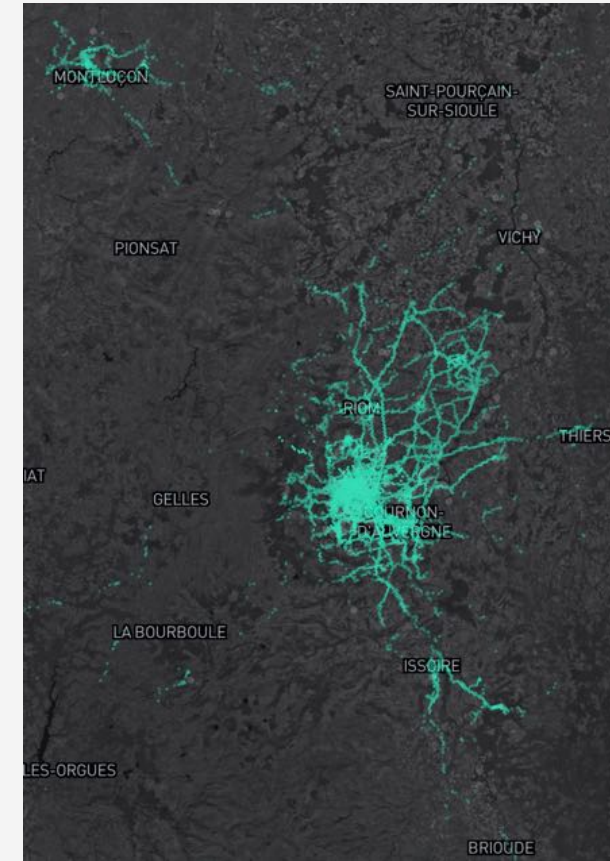
EUROPE CONTEXT



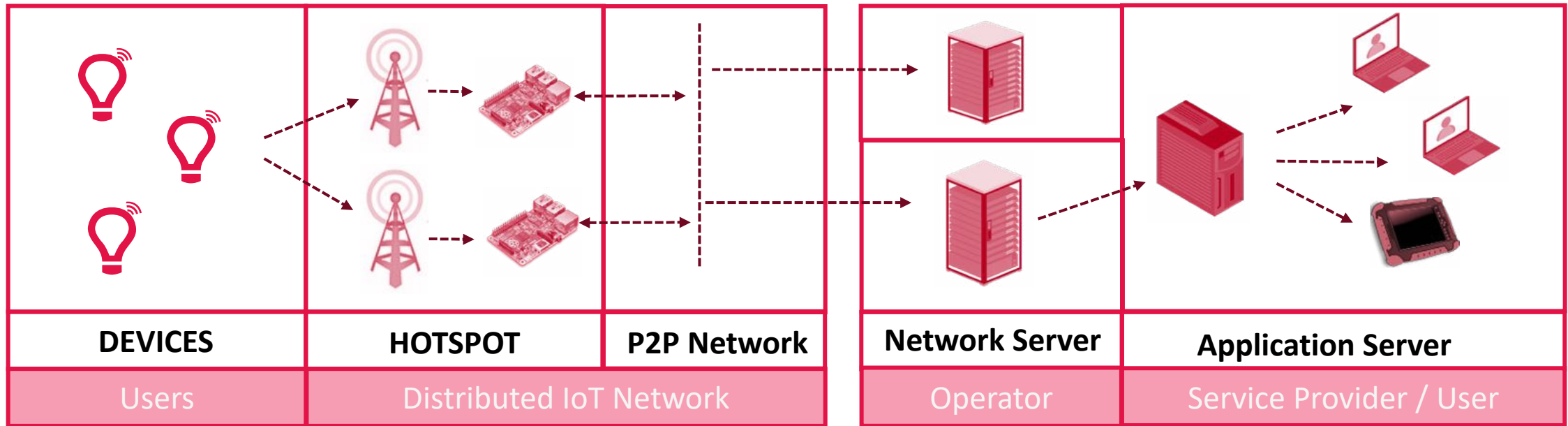
CLERMONT-FD



COVERAGE MAP



helium Network Architecture (before HIP 71)



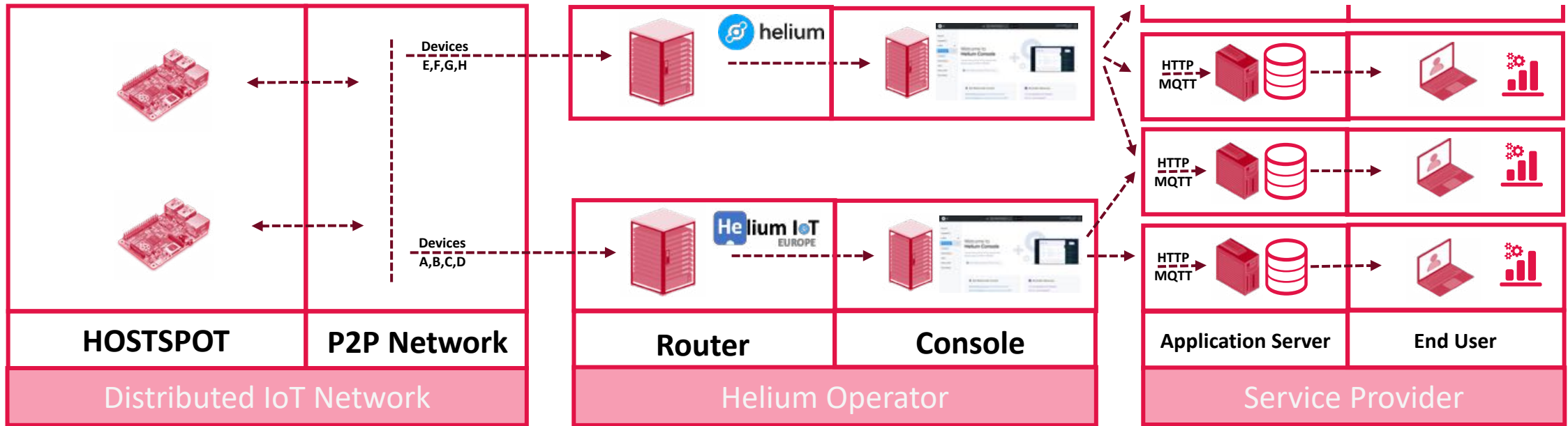
Helium distributed architecture

The HELIUM network is composed by hotspots. A Hotspot is a LoRaWan gateway associated to a Miner. A miner is lightweight and can run on a raspberry Pi. It is running in a docker container.

The miners are connected altogether over a P2P network. They are maintaining / running the blockchain.

Device communication passes through these different layers and are routed up to their specific Network Server. The distributed network supports multiple Network Servers. (Network Servers are centralized components in this architecture). Application servers works on helium as on any other Network Server. Nothing specific. The data itself is not inside the blockchain.

helium Network Server Architecture (before HIP 71)



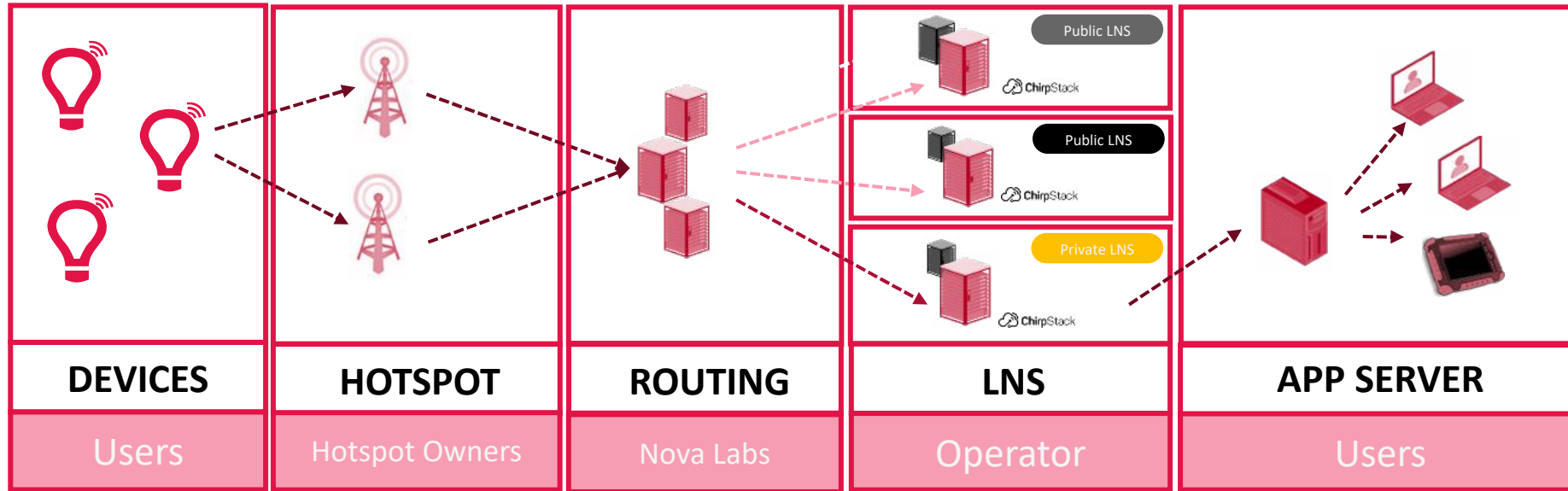
Helium Network Server Architecture

Devices are declared by Service Provider in a console. This one is belonging to a Helium Operator. There is no restriction to become a Helium Network Operator, so you can build your “private” network on top of Helium. The router is registering these devices on the blockchain to create a direct route from the Hotspots to the router the devices are belonging to. Router receives only data

concerning its registered devices. Router is accepting or rejecting the data. Once accepted, the router pays for the communication. So basically, its not the device burning DC but the Router, devices are belonging to. The Helium integrator then pass the data to the service provider. This on stores the data. No data are stored in the previously described stages.



helium Network Server Architecture (current)



Helium Network Server Architecture

Helium have a geo-replicated routing infrastructure where all the hotspots push the received packets. This infrastructure is verifying the packet, purchase it to the hotspot and route it to the right LNS.

LNS are running Chirpstack, open-source agnostic LoRaWan Server.

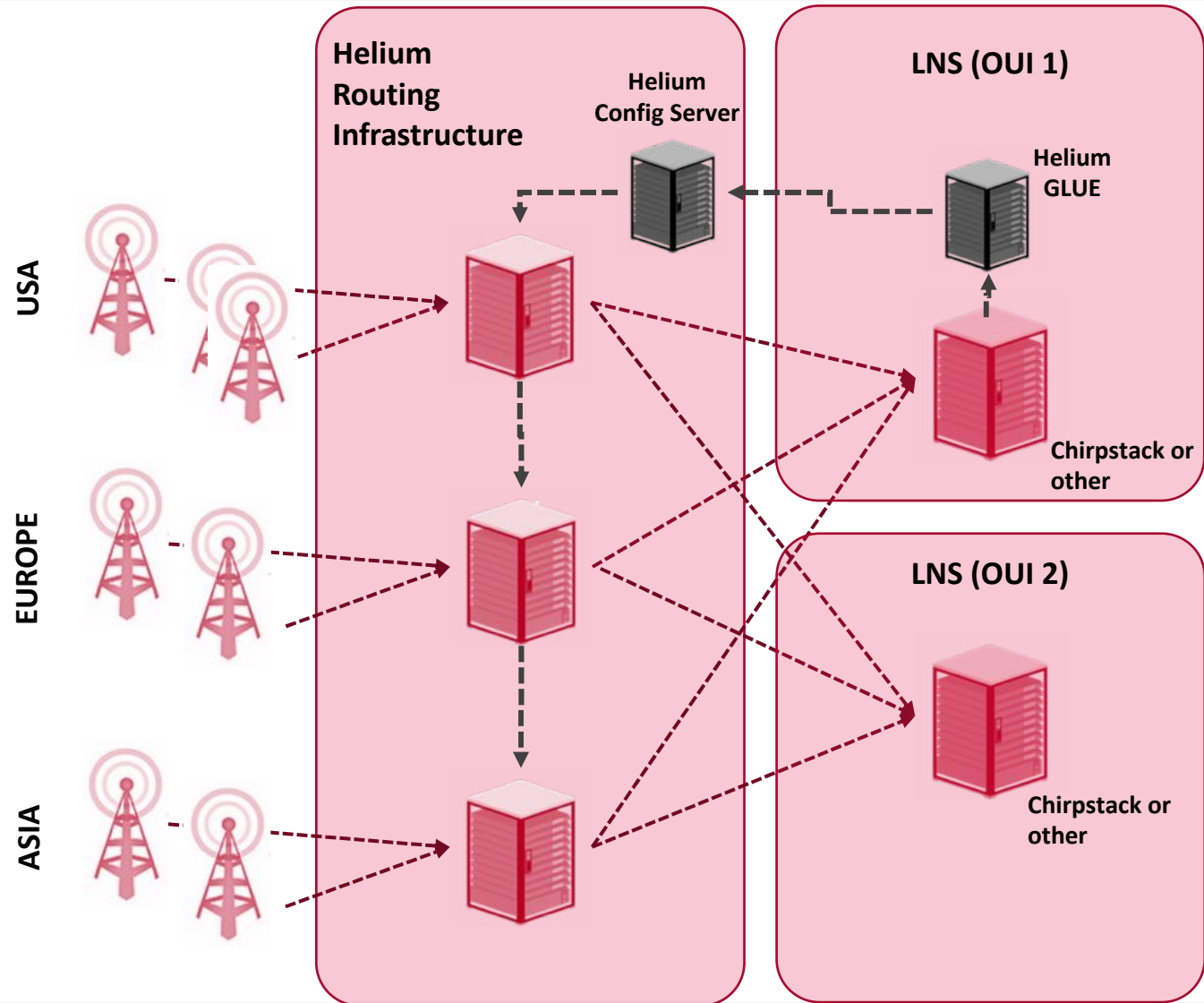
Devices and sessions needs to be declared in the Helium Routing service by the LNS. This requires API call to Helium Routing service (Config Service) on: Device Addition, Device Deletion, Device Session creation... Specific open-source project has been created to support this (see my github)

Routing Architecture

> Hotspot transfers the packets to the nearest Helium router with geo-dns.

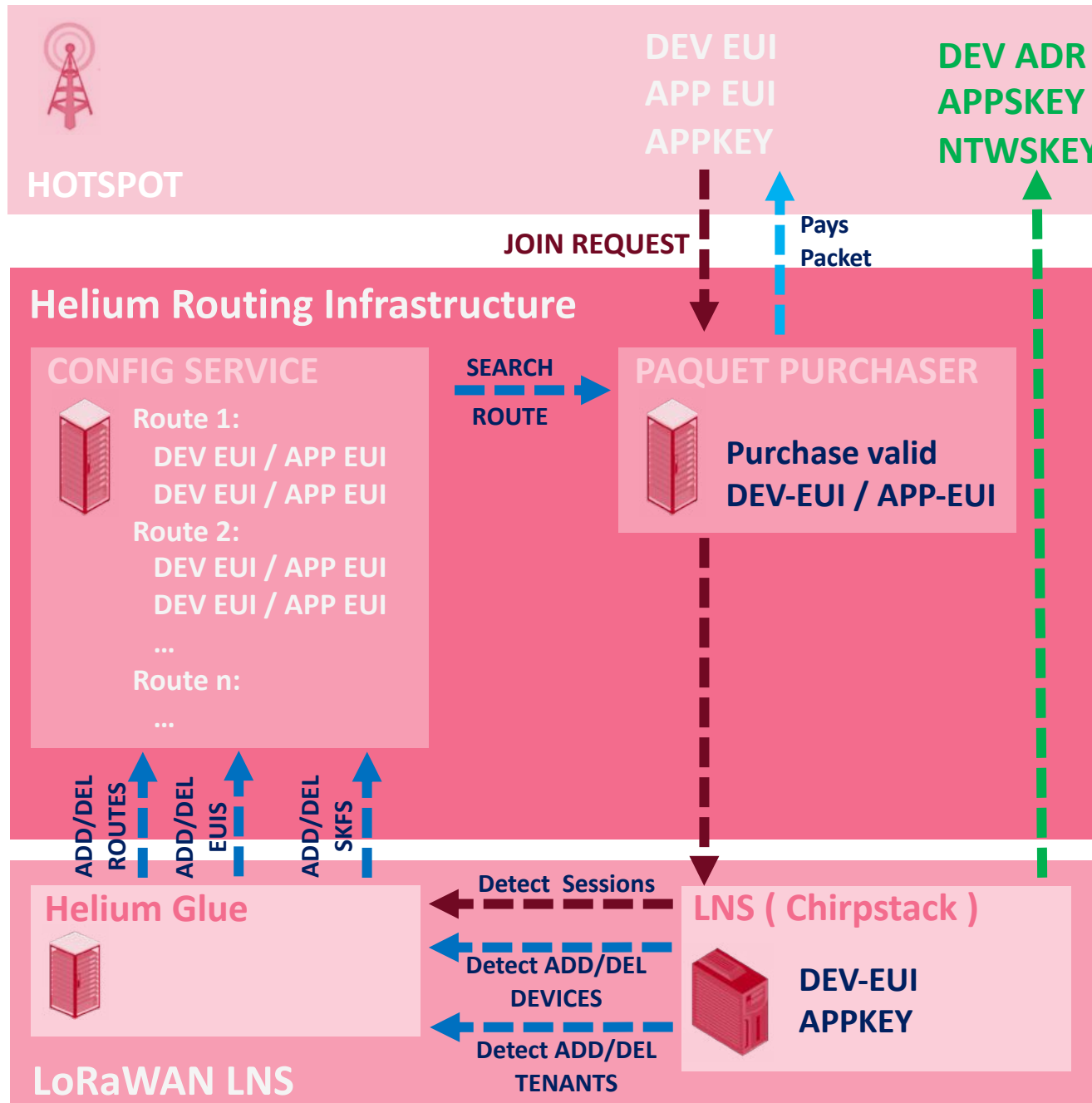
> Router verify then transfer the packet to the LNS owning the packet

> Helium Glue configure Helium routing infrastructure to correctly verify and route the packets.



JOIN PROCESS

- Helium router is searching for a route with a corresponding DEV-EUI / APP-EUI to accept the JOIN Request.
- Helium Glue detects device addition & deletion to maintain the Config Service database with valid DEV-EUI/APP-EUI.
- Helium Glue detects session creation to maintain the list of SKF (Session Key Filters) to the config Service. Basically the NTWSKEY list per DEVADR
- Routes are managed by Helium Glue, can be global or per tenant. Route allows multiple LNS per OUI



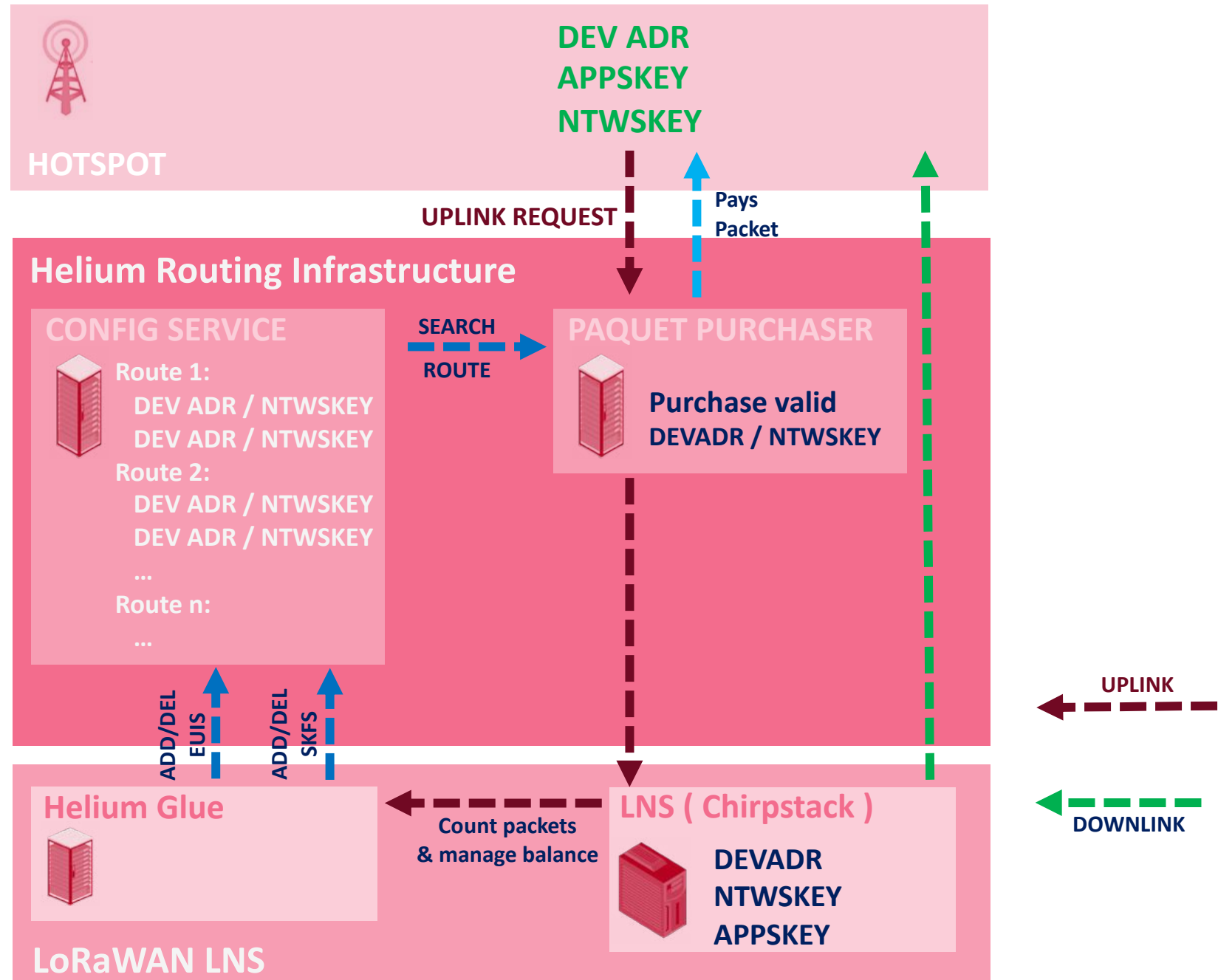
UPLINK PROCESS

> Helium router is searching for a route with a corresponding DEV-ADR / NTWSKEY by verifying all signatures for the DEVADR.

> Valid packets are sent to LNS and paid to hotspots. Depends on max_copy route param, one or multiple packets are paid.

> Helium Glue, in public usage, manage per device / account, packet balance. When a balance is reaching 0, the Glue will deactivate routes in config service.

> Downlink are free of charge.



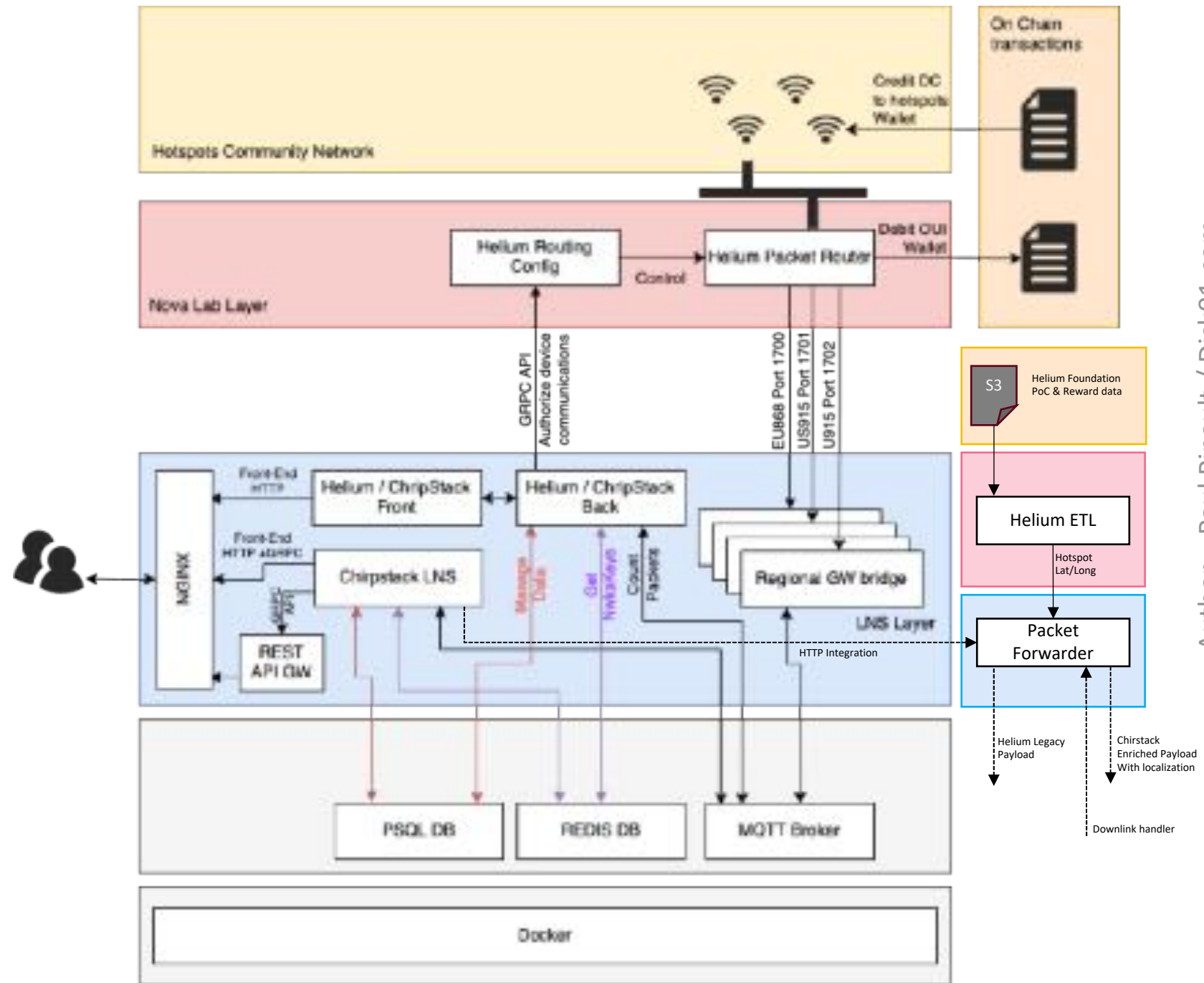
Helium GLUE

> Chirpstack tenant & device creation / deletion can be found in the PSQL Database.

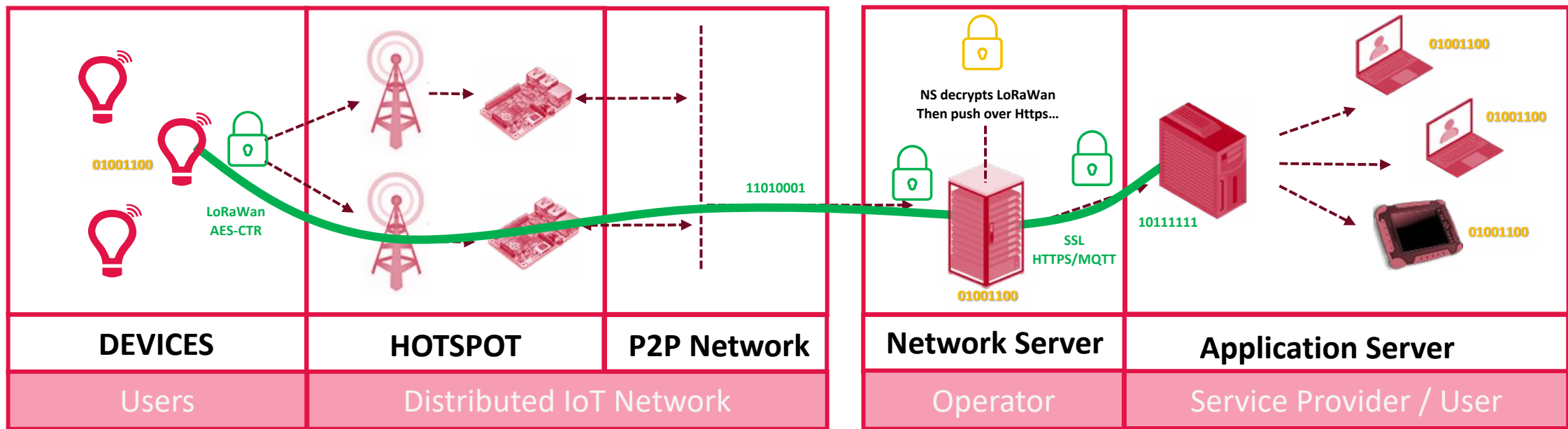
> Session Key are maintained in REDIS Database

> Packet count & JOIN request can be detected with MQTT.

> Chirpstack is per Region, not a global LNS. But we can dynamically update the region.



helium End to End Encryption principle

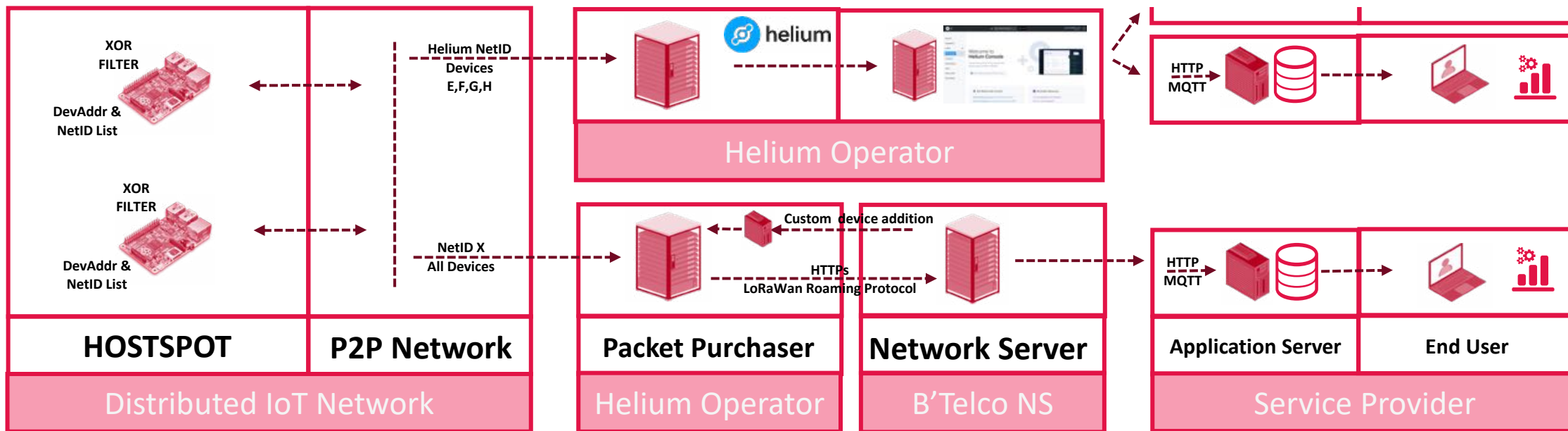


Helium data protection

The HELIUM network rely on LoRaWan technology. The communications are encrypted with a session key negotiated with the Network Server. Only the device and the network server can decrypt the payload. In an architecture you can have a private Network Server on a public infrastructure, it means you can protect the device

data from End-to-End with no tiers manipulating the raw data. This is unusual in the classical LoRaWan public architecture. Usually, you need to add an applicative encryption layer to ensure an End-t—End security. Something not a lot of devices support.

helium Roaming Architecture



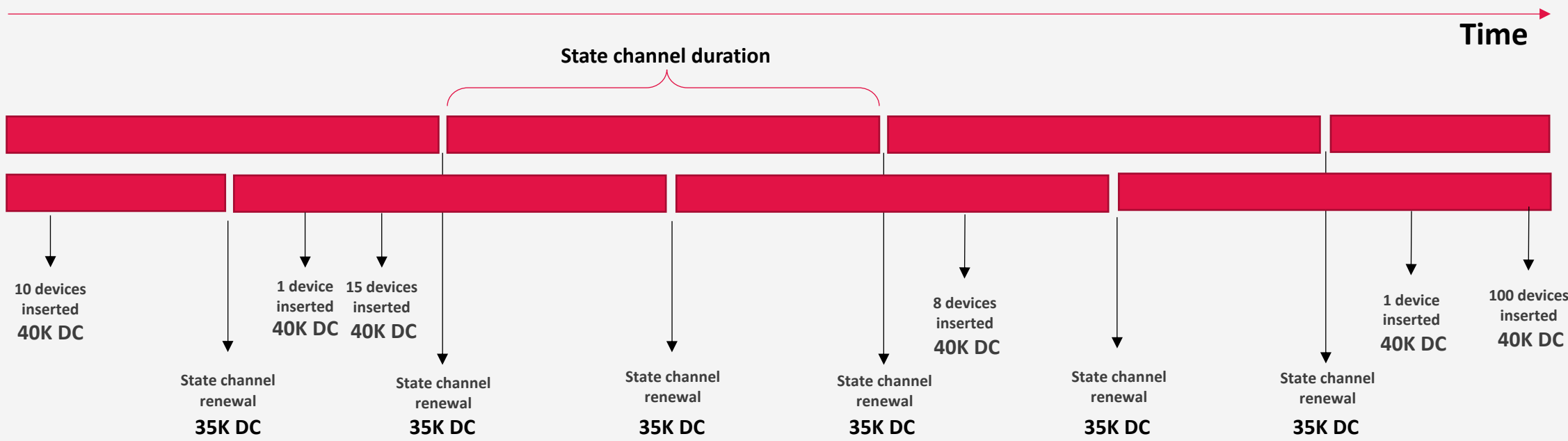
Helium Roaming Architecture

A specific instance of the Helium router is registered to receive the traffic coming from a specific NetID, it also need to have a XOR filter initialized with the list of devEUI / AppEUI to allow the device JOIN.

Router transfers the packets according to the LoRaWan

Roaming specification to the other network network server. The Roaming is unidirectional.

The device list synchronization requires a custom link from the roamed network and a custom program to declare new devices in the XOR filters.



Author – Paul Pinault / Disk91.com

Helium Router transaction

Helium has a message-based transaction cost but also running cost at the Router level. A State channel is an autonomous blockchain with a predefined life duration (from an hour to a week) to store the packet exchange history and manage the contract between the hotspots and the router. At the end of the state channel life, the payments to hotspots are reported on the main blockchain and converted in HNT creation.

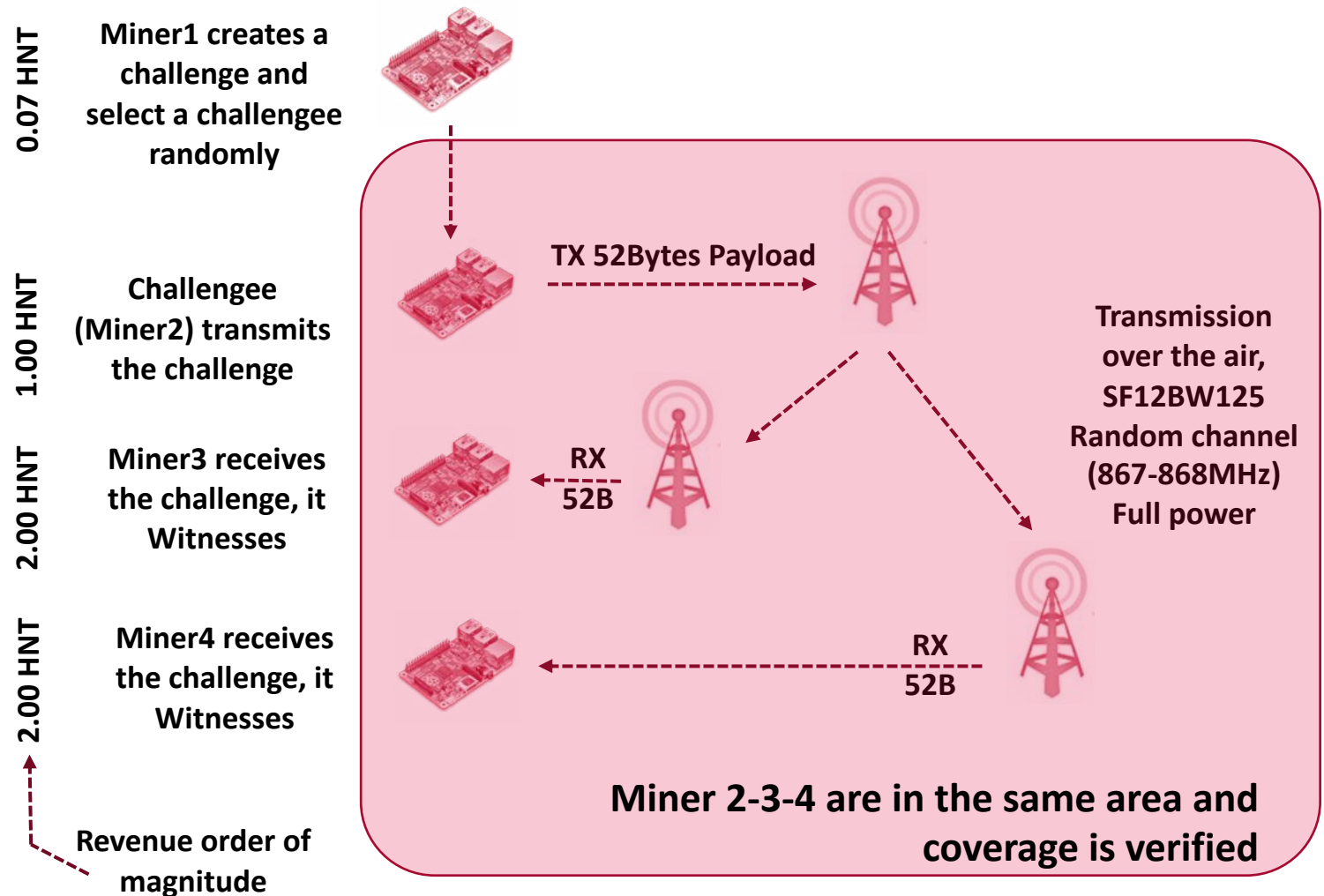
The state channel creation is a transaction burning 35K DC. Router creation also needs an investment of a minimum of 9M DC to create an OUI (1M DC) and buy some DevAddr (8 minimum) for 1M DC each. The devices also needs to be registered to route them to the router. It cost 40k DC on every transaction, each of it can have multiple devices.

PoC Principles

> Hotspot create Challenge on every 240 blocks (about 4 hours). Challenge goes to a random target : Challengee

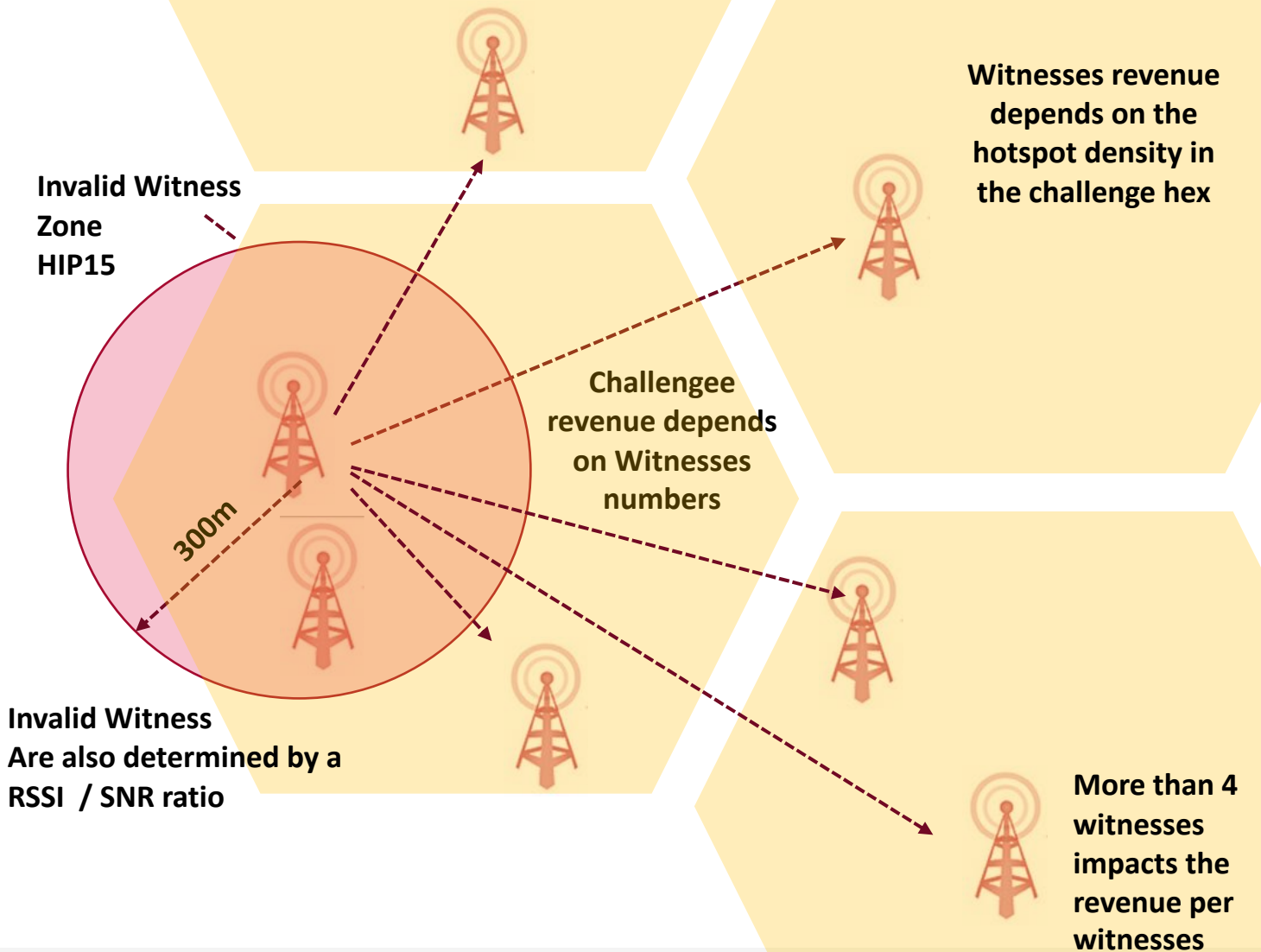
> Challengee transmits a 52bytes message over the air. It is the PoC packet.

> Hotspots around receives the message and report reception to the chain. This is a Witness.



Witness Validity And Revenue Adaptation

- > The purpose is to facilitate the network extension instead of concentration
- > Encourages outdoor antennas and larger coverage
- > Encourages to deploy on locations that extend the coverage step by step

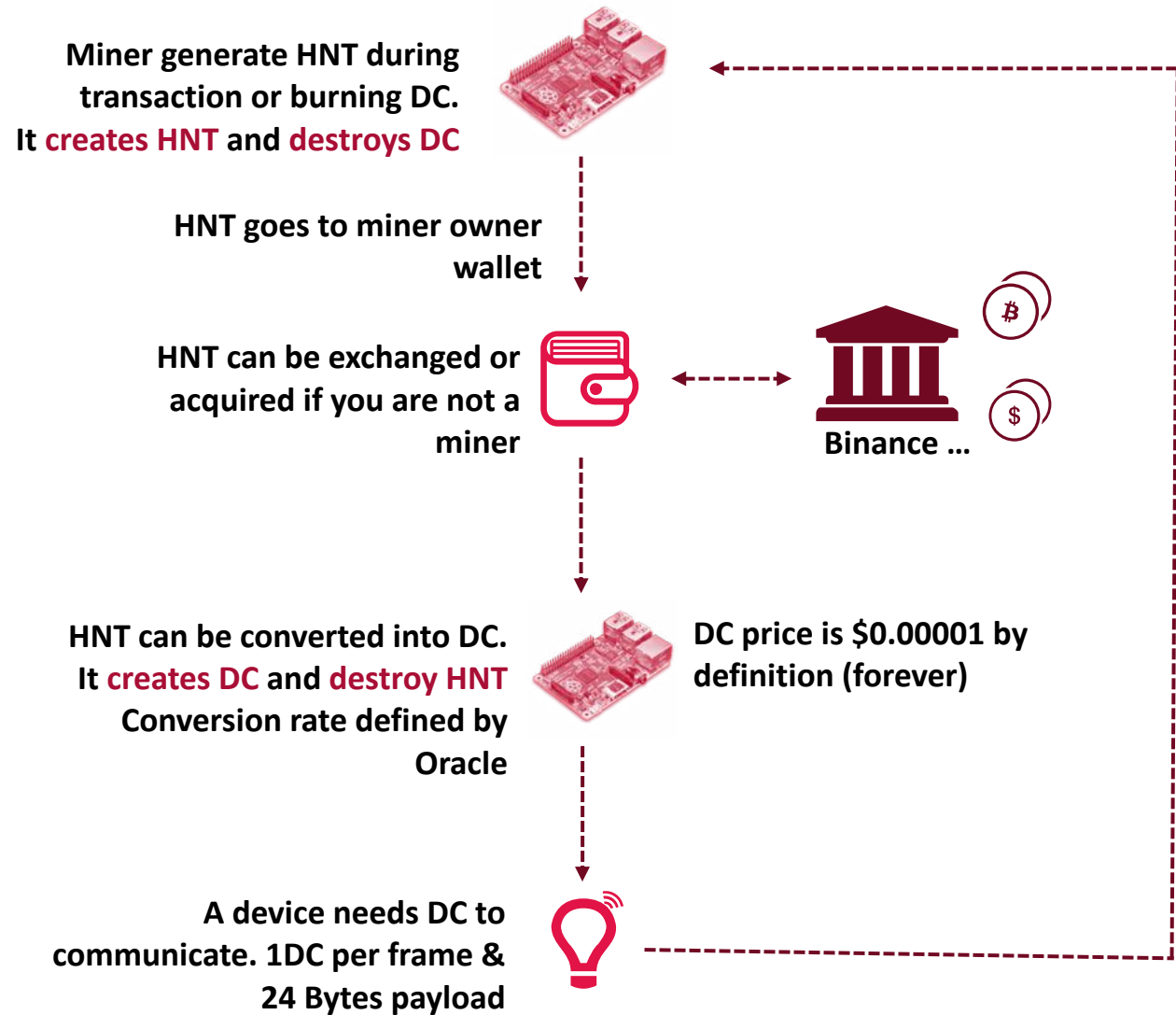


DC Principles

- > Blockchain transaction creates HNT
- > HNT can convert to DC for communications.
- > Every 24 bytes communication burn 1 DC.

With a fixed DC price and the HNT <-> DC burn principle, the HNT value is directly related to the data traffic processed by the network.

	HNT	DC
Value	Market rate	\$0.00001
How to acquire?	Mined	Burn HNT
Transferable	Yes	No





Helium token valuation depends on offer and demand and subject to speculation. Compared to classical stock option, token is not a shared of a company, but something consumed as part of the service offered. Currently, most of the token are consumed by the Hotspot creation.

In a first scenario, let's consider that the miners directly sold what is produced. Assuming Helium Inc has no interest in

selling the HNT collected. In a such scenario, the Token valuation will be \$0.14 per HNT assuming 10.000 hotspot registered per month: the needed rhythm to achieve the 150K hotspot at end of the year.

This scenario is wrong as most of the miner have interest in stacking / holding.

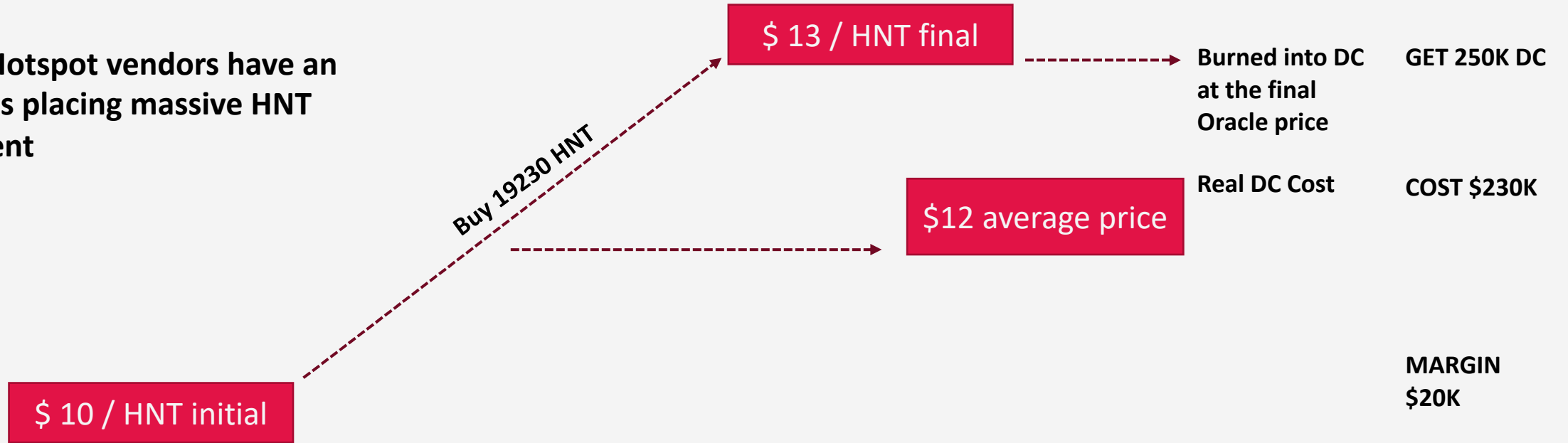


As of May 2nd, binance global HNT wallet is 14 399 357 HNT for 85 200 000 circulating supply floating is 17%, exchange about 1.2M HNT/day 8% rotation
<https://explorer.helium.com/accounts/14YeKFGXE23yAdACj6hu5NWEcYzzKxptYbm5jHgz9A1P1UQfMv>

In this second scenario, with 10% of floating HNT, the valuation on the market growth to \$1. You also see that whatever is the HNT valuation, there is no impact on the DC market and the hotspot manufacturer have no specific interest in HNT value for making their business. They can buy a high HNT price to burn into DC without impacting their business model.
 Today on market, the exchanged volumes are around 2.5M

to 5M HNT per days eq 150M / month.
 HNT burn impact is low on this volume of exchange but it depends on the real floating market size. (on the 150M HNT exchanged, how many different HNT ?)
 Difference between Market value and valuation is speculation.

Helium Hotspot vendors have an interest in placing massive HNT investment



There is an interest in placing large orders in a short time for hotspot vendors. The price of acquisition is not a problem as higher it becomes, higher is the DC rate change. With \$250k to \$500K they can be 2% to 8% of the market size for a single day. (on May 2nd, average HNT volume is 1M HNT / 18M USDT)
 This can make regular token boost on the market.

Today is not what is driving the value on middle long-term range, but it can have some interesting effects on short term value.



3GPP - Traditional telecom technologies applied on IoT





Multiple technologies

LTE-M is a power saving version of LTE (aka 4G)

NB-IoT is the LPWAN solution from 3GPP

Both have been added in best effort mode to 4G

Both will natively be provided and improved with 5G equipment's.



Telecom operator technologies



- LTE-M => LTE-MTC - Machine Type Communication
- eMTC => enhanced Machine Type Communication
- LTE CAT-M1/2
- IP Based – directly accessible



- LTE CAT-NB1/2 => Narrow Band
- Accessible through an operator network kernel

Both are using licensed spectrum with no duty-cycle restrictions
Both are deployed by telecom operator and subject to subscription

3GPP Roadmaps



LPWA Standards (release 13):

- eMTC (Cat-M1)
- NB-IoT (Cat-NB1)
- EC-GSM-IoT

Enhancements (release 14):

eMTC (Cat-M2)

- Positioning (OTDOA)
- Single-cell multicast
- Inter-frequency measurements
- Higher data rate
- VoLTE

NB-IoT (Cat-NB2)

- Positioning (OTDOA)
- Single-cell multicast
- Power reduction
- Latency reduction
- PRB
- Mobility and service
- Higher data rate
- New power class

Further Enhancements (release 15):

eMTC

- Extended coverage mode
- Faster system acquisition, Early data transmission
- Wake-up radio
- Higher density

NB-IoT

- Faster system acquisition, Early data transmission
- Wake-up radio
- Higher density
- Cell size extension
- TDD support

5G Migration (release 16):

eMTC/NB-IoT

- In band eMTC/NB-IoT
- 5G NR deployment options (SA/NSA)
- Mesh networking
- Non-orthogonal multiple access (NOMA)
- Grant-free uplink

LTE-M is

- Cat-M1/Cat-M2
- eMTC

Nb-IoT is

- Cat-NB1/Cat-NB2

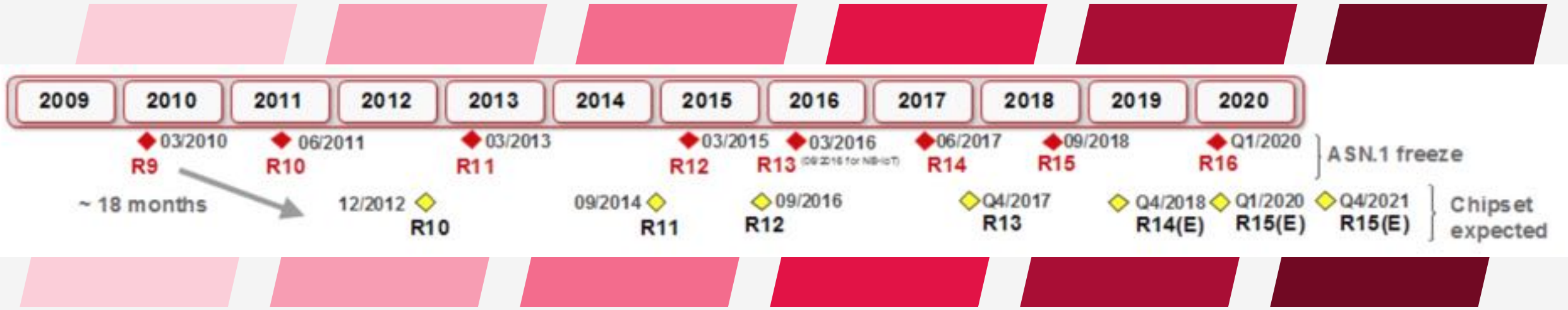
Release 13 has been deployed in France in 2019 for LTE-M (Orange)

Release 13 has been announced in France in 2019 for Nb-IoT (SFR)

Author – Paul Pinault / Disk91.com

Deployment time-line is impacted by chip time-to-market

Radio chips are available 18 month after spec



The chip industry need a reasonable time to implement the new 3GPP specification in silicon. It's about 18 months process before getting a released version. Then the design of object hardware can start for a second 18 months process. Therefore we have a 3 years shift between technology announcement and market availability.

On the operator side update can be software when the within the same generation. Hardware deployment (with large investment) is needed to change from a generation to the next one.

3GPP Solutions

LTE-Cat M / LTE-Cat NB are solutions based on 4G (LTE)



V.T.E [7][8]	LTE Cat 1	LTE-M				NB-IoT		EC-GSM-IoT
		LC-LTE/MTCe	eMTC			LTE Cat NB1	LTE Cat NB2	
		LTE Cat 0	LTE Cat M1	LTE Cat M2	non-BL			
3GPP Release	Release 8	Release 12	Release 13	Release 14	Release 14	Release 13	Release 14	Release 13
Downlink Peak Rate	10 Mbit/s	1 Mbit/s	1 Mbit/s	4 Mbit/s		27 kbit/s	80 kbit/s	474 kbit/s (EDGE) 2 Mbit/s (EGPRS2B)
Uplink Peak Rate	5 Mbit/s	1 Mbit/s	1 Mbit/s	7 Mbit/s		62 kbit/s (multi-tone) 20 kbit/s (single-tone)	105 kbit/s	474 kbit/s (EDGE) 2 Mbit/s (EGPRS2B)
Latency	50–100ms	not deployed	10ms–15ms			1.6s–10s		700ms–2s
Number of Antennas	2	1	1			1		1–2
Duplex Mode	Full Duplex	Full or Half Duplex	Full or Half Duplex			Half Duplex		Half Duplex
Device Receive Bandwidth	1.4 – 20 MHz	1.4 – 20 MHz	1.4 MHz	4x1.4 MHz		180 kHz	180 kHz	200 kHz
Receiver Chains	2 (MIMO)	1 (SISO)	1 (SISO)			1 (SISO)		1–2
Device Transmit Power	23 dBm	23 dBm	20 / 23 dBm			20 / 23 dBm		23 / 33 dBm

At least a software update is needed on all operator equipments over 4G.

3GPP Solutions in the 5G

	Next Generation
	5G
Range (Outdoor)	< 15 km
MCL	164 dB
Spectrum	Licensed (7-900 MHz)
Bandwidth	shared
Data Rate	<1 Mbps
Battery Life	>10 years
Availability	2025

5G release 15 is still not really documented on Internet about LTE-M & NB-IoT improvement.

Operators need to change all the telecom equipment to support 5G.



LTE-M outdoor coverage



Orange network coverage in France. Dark orange is indoor coverage. Light orange = outdoor only.

Basically 4G network coverage