Edge Intelligence & Trust

Fabrizio Cardinali, CEO Knowhedge, f.cardinali@knowhedge.com

knowhedge
your edge to know how

Helping our customers towards **O**pen **K**ey **E**xponential **I**nnovation & Human-Machine Collaboration

knowhedge

your edge to know how

Hi, I am Fabrizio Cardinali…

…Digital Startupper since the 90s…

… «Open Innovator» & «Business Angel» Today.

Consorzio Genova Ricerche

HayGroup®

GIUNTI labs
the X learning Company

sedApta
smart manufacturing made easy

skillaware
Workflow based Performance Support & Learning Analytics

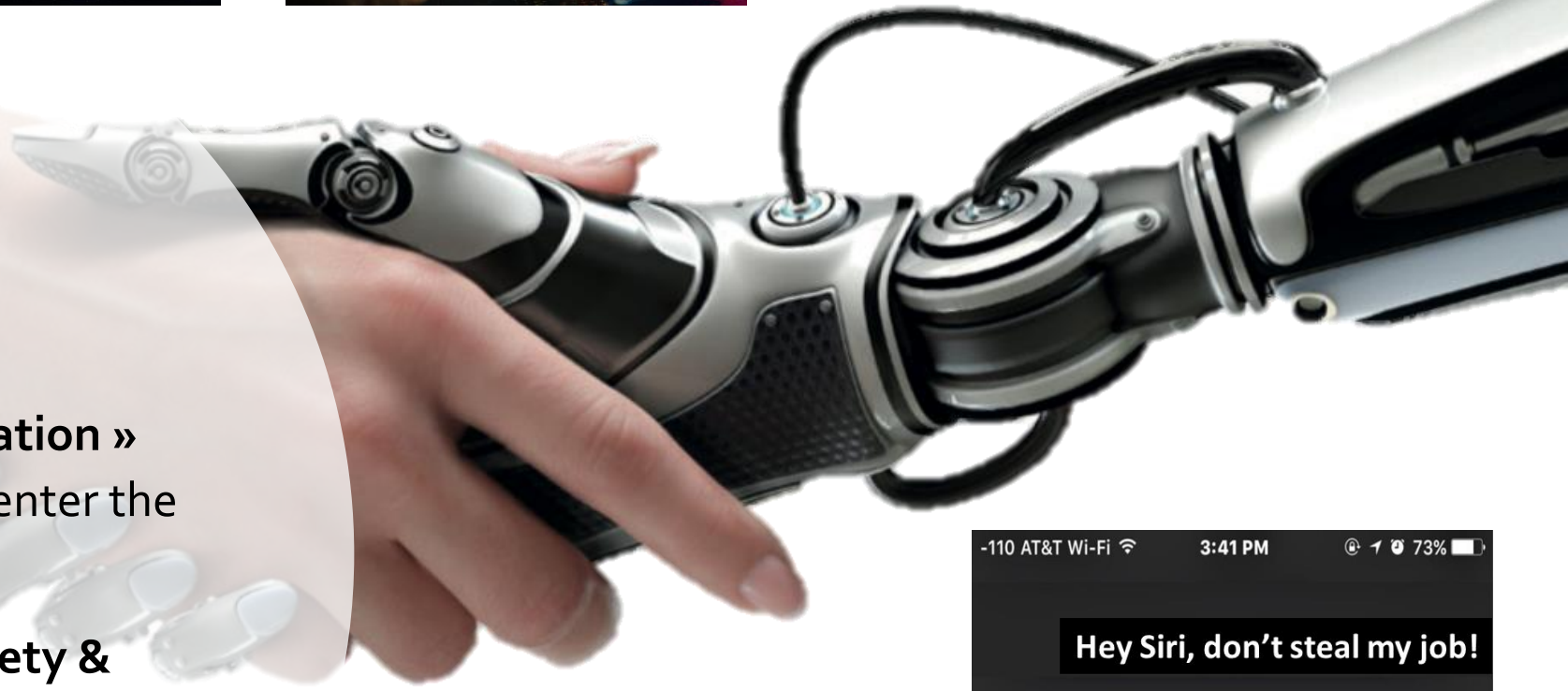
SMART TRACK

MYW.AI™
Edge Intelligence for All

WAVENURE

knowhedge

your edge to know how



WHAT we do?

knowhedge™ is a « **Open Innovation »** consulting firm helping clients to enter the **«machine economy ».**

Whilst improving **Training, Safety & Performance Support** of their « human Resources » using new **« exponential technologies » such as AI, IOT and Blockchain @ the EDGE of new digital workplaces.**

MYW.AI™
EDGE INTELLIGENCE FOR ALL

knowhedge
your edge to know how

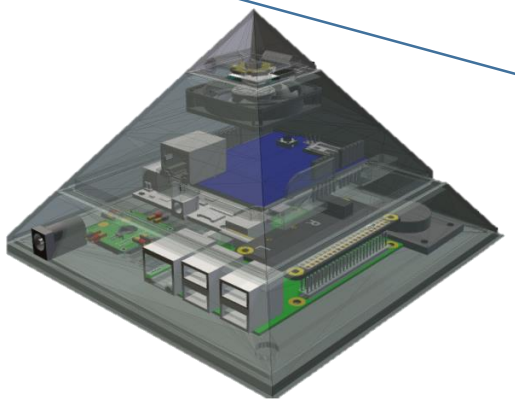
Giancarlo Bo
(former Giunti Labs)
SOA & Microservices

Luca Marchese
(former Ericsson)
Neural Networks

Giorgio Cantarini
(AI student)

Marco Migliorati
(BioEngineer)

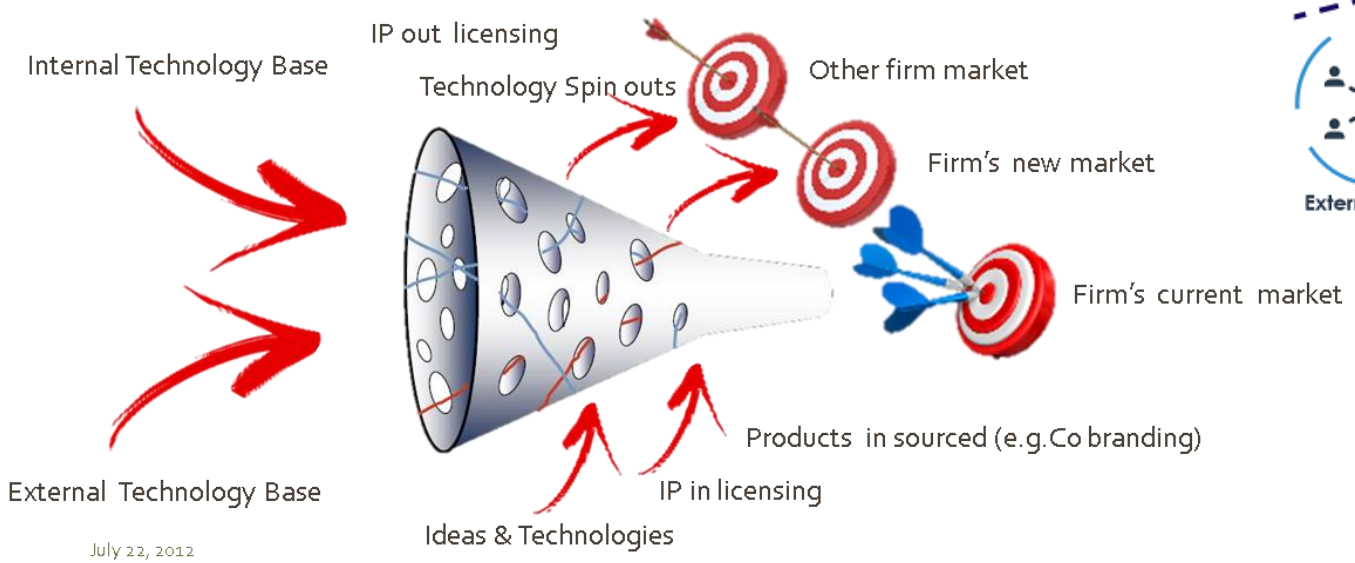
Andrea DeCamilli
Blockchain, DLT & IOTA

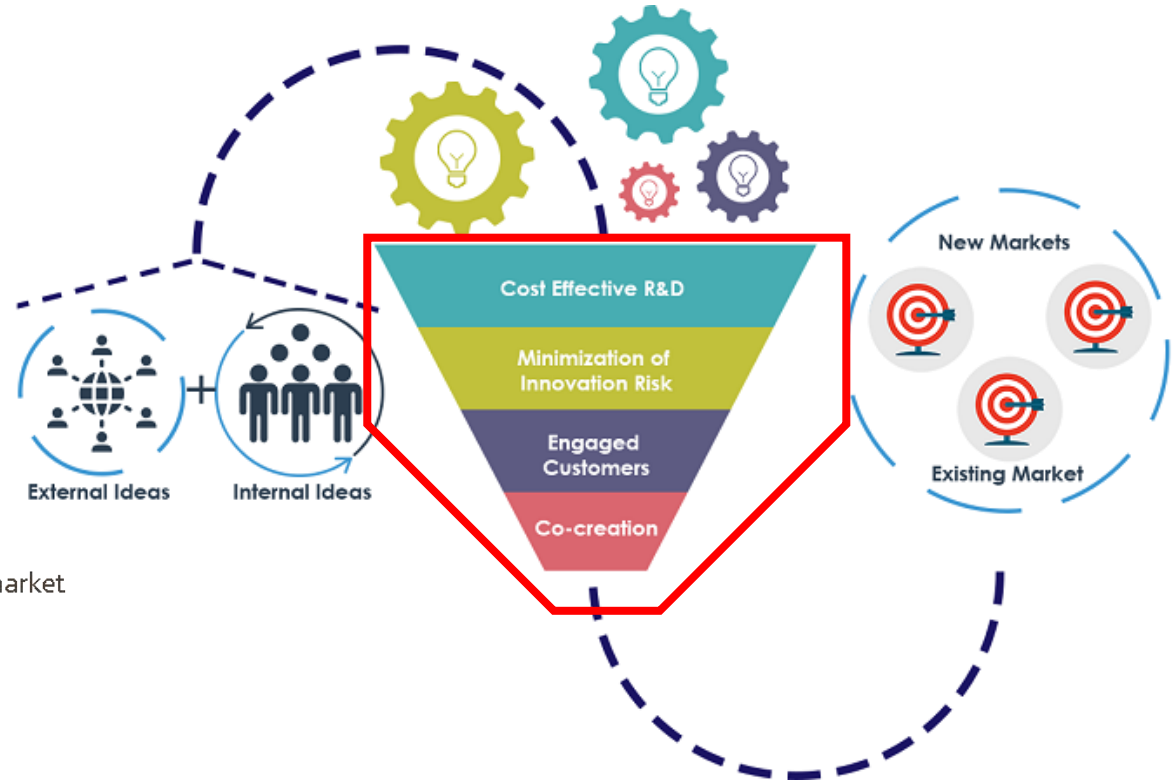


Open Innovation

knowhedge
your edge to know how

Open innovation is a term promoted by Henry Chesbrough, adjunct professor and faculty director of the Center for Open Innovation at the Haas School of Business at the University of California.

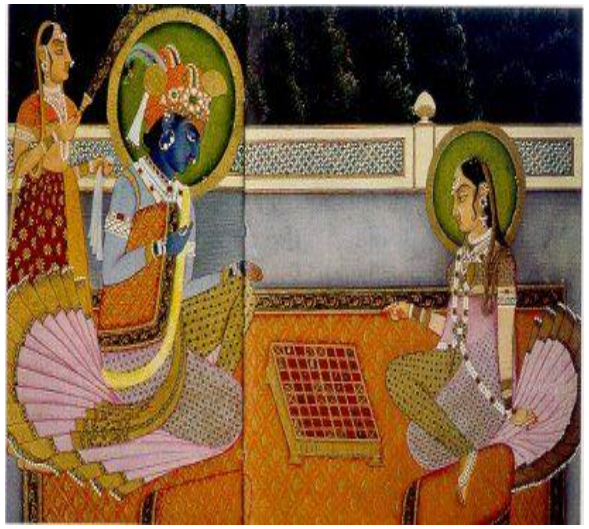


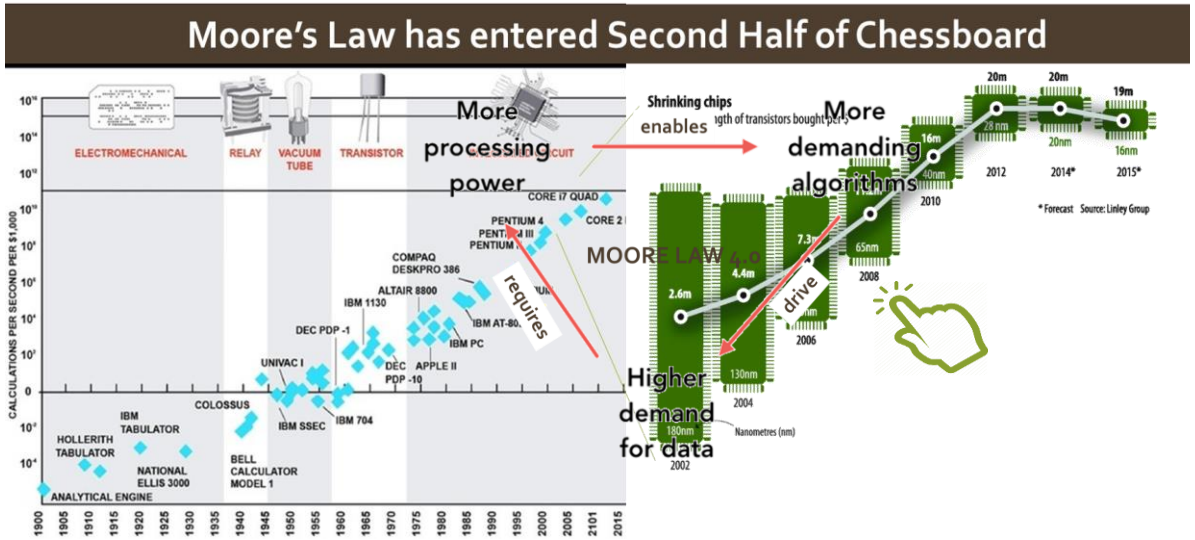


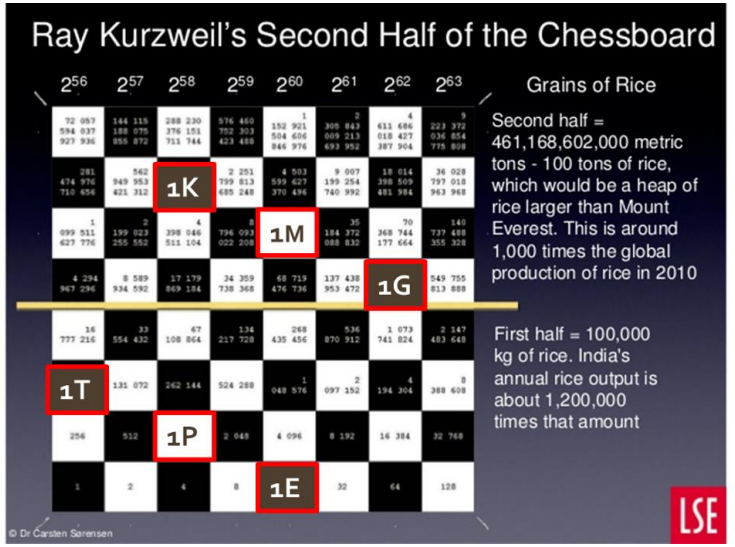
Exponential Technologies…

knowhedge

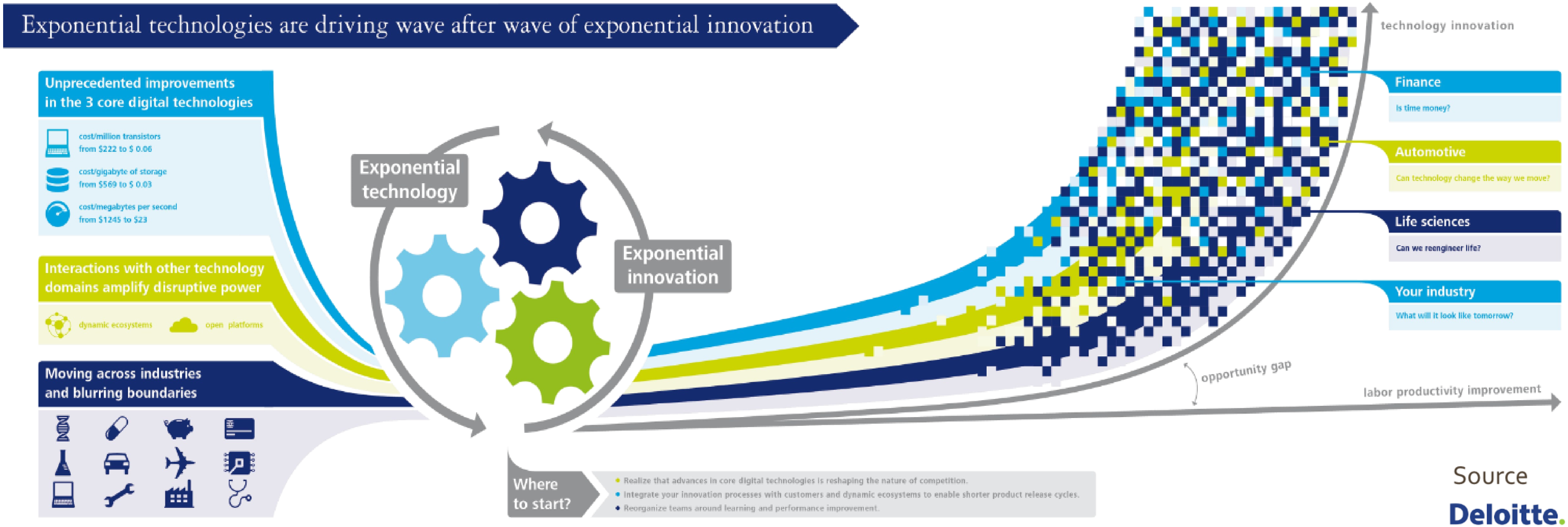
your edge to know how







Exponential Technologies…



Source

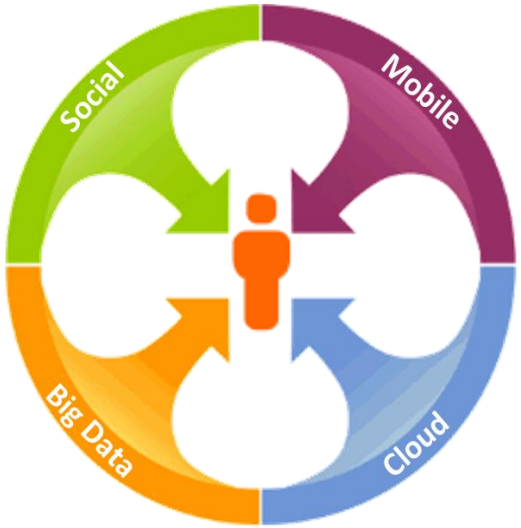
Deloitte.

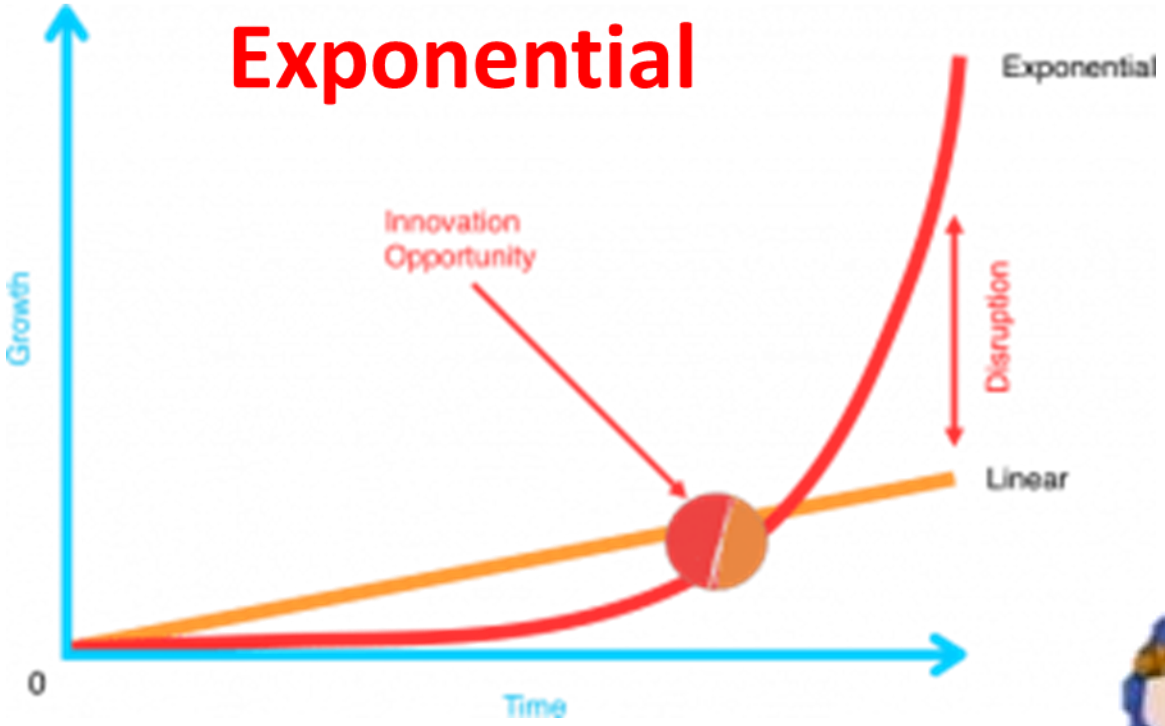
The (next) digital revolution

knowhedge

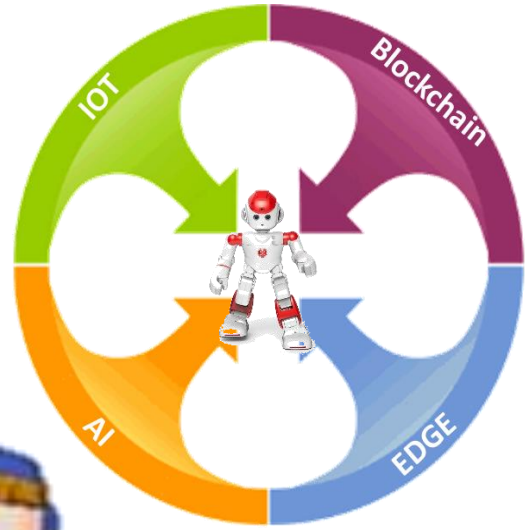
your edge to know how

The Digital Transformation Nexus
(2000-2018)

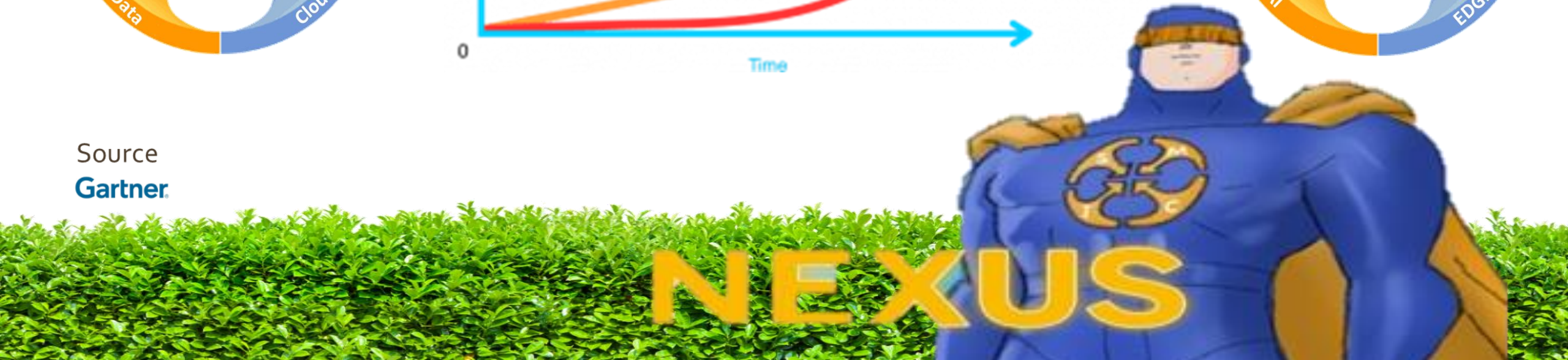




The Digital Disruption Nexus
(2018-2030)



Source
Gartner

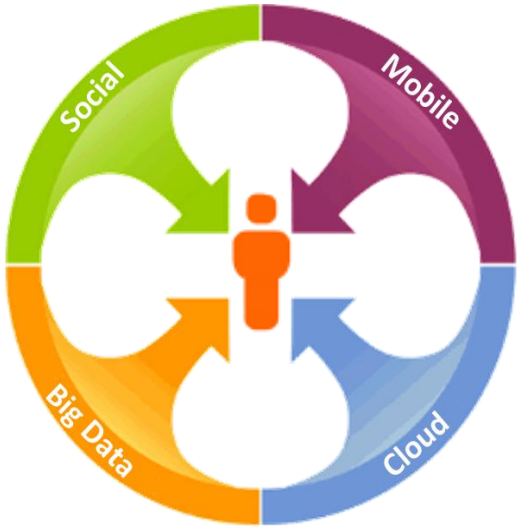


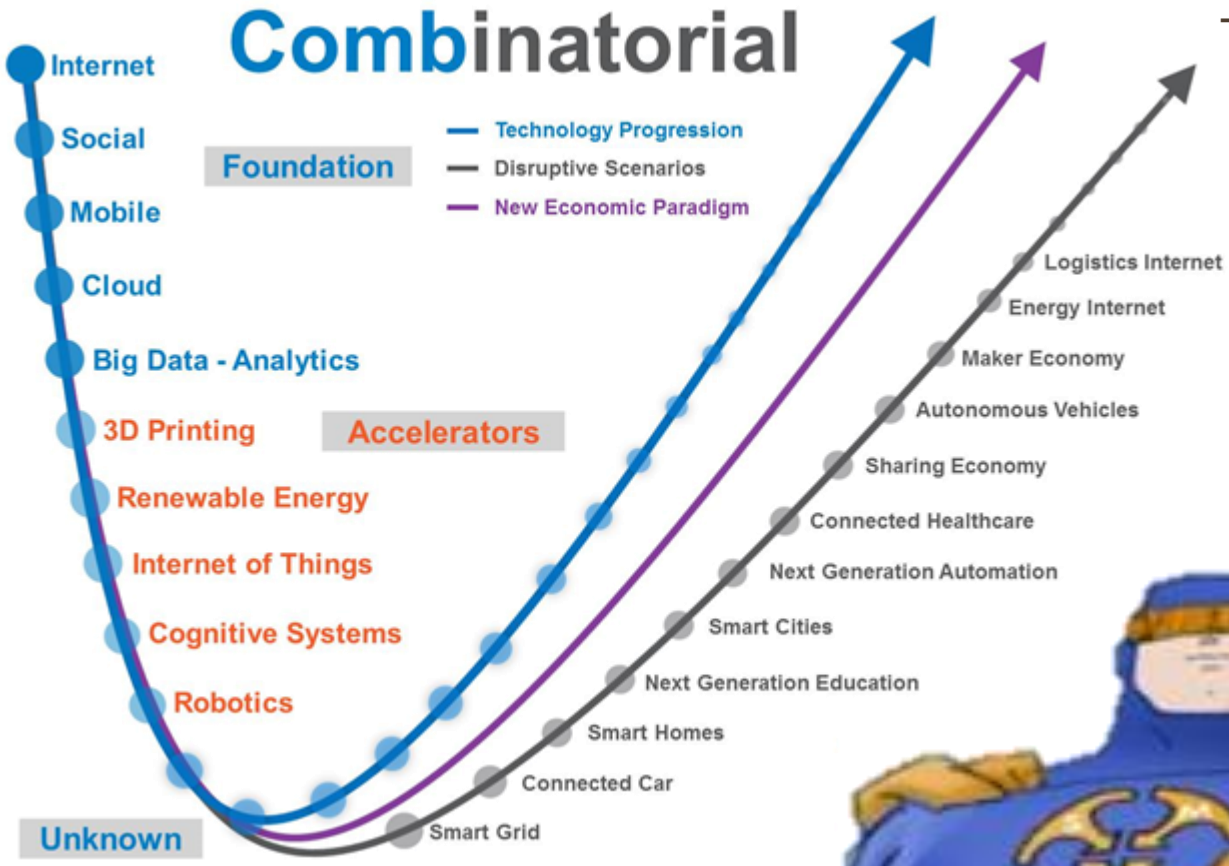
The (next) digital revolution

knowhedge

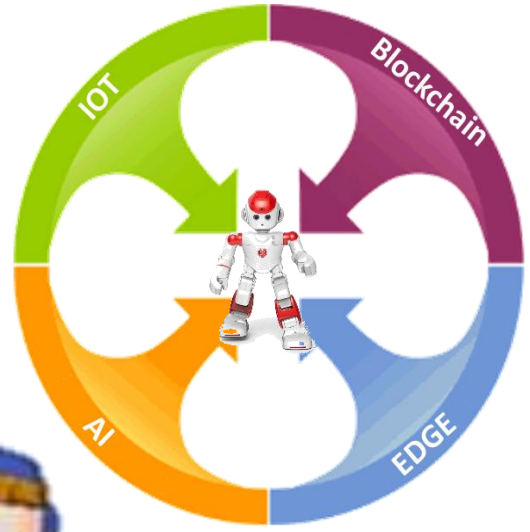
your edge to know how

The Digital Transformation Nexus
(2000-2018)





The Digital Disruption Nexus
(2018-2030)



Source
Gartner

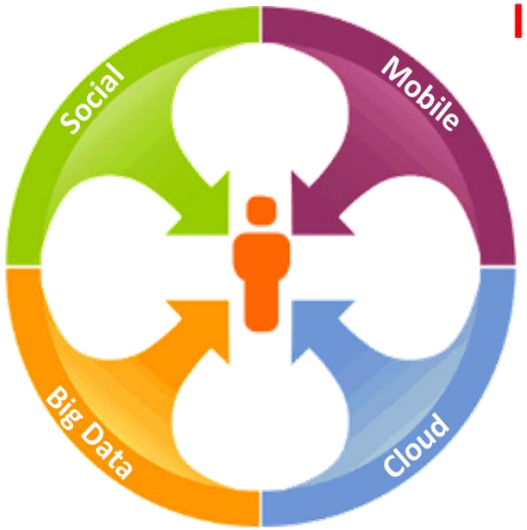
The (next) digital revolution

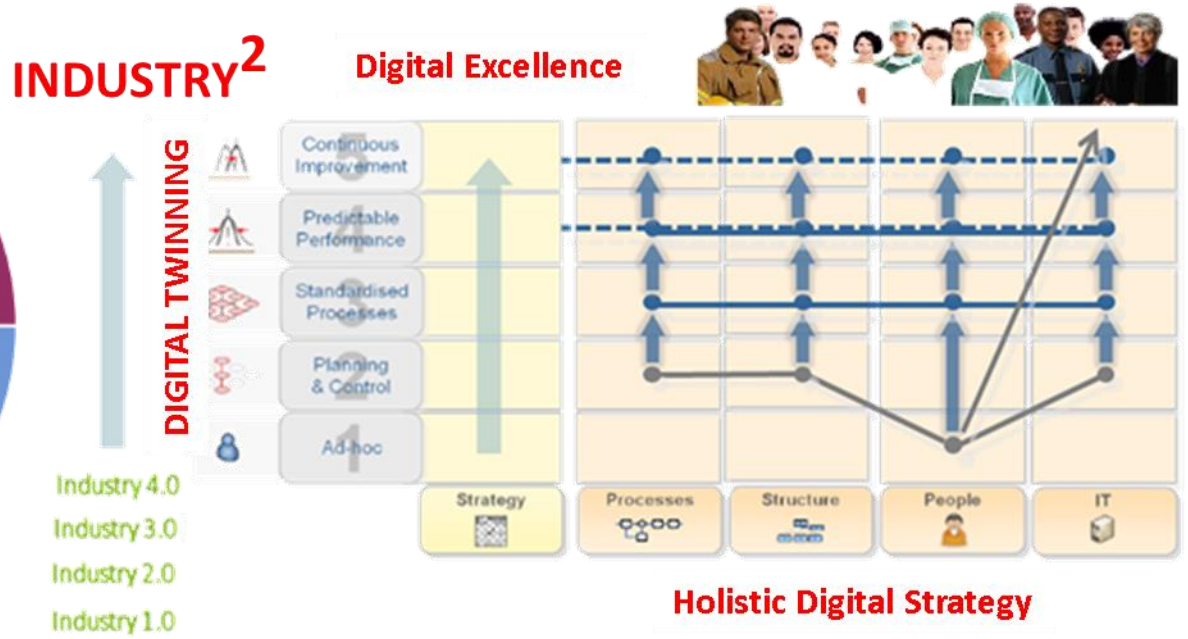
knowhedge

your edge to know how

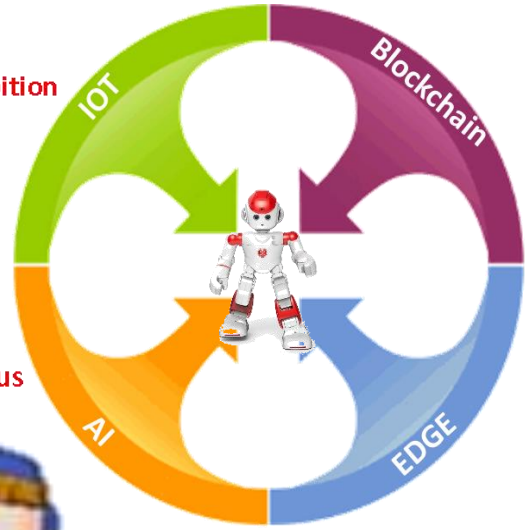
Holistic

The Digital Transformation Nexus
(2000-2018)





The Digital Disruption Nexus
(2018-2030)



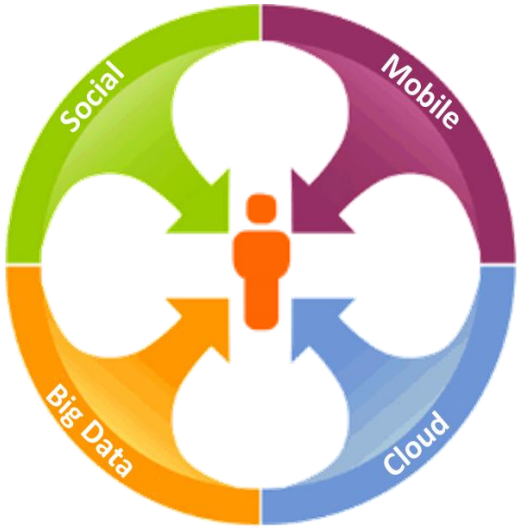
Source
Gartner

The (next) digital revolution

knowhedge

your edge to know how

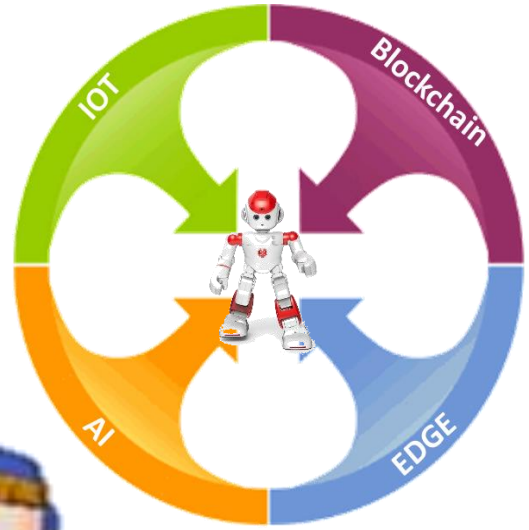
The Digital Transformation Nexus
(2000-2018)



European Parliament

Regulated

The Digital Disruption Nexus
(2018-2030)



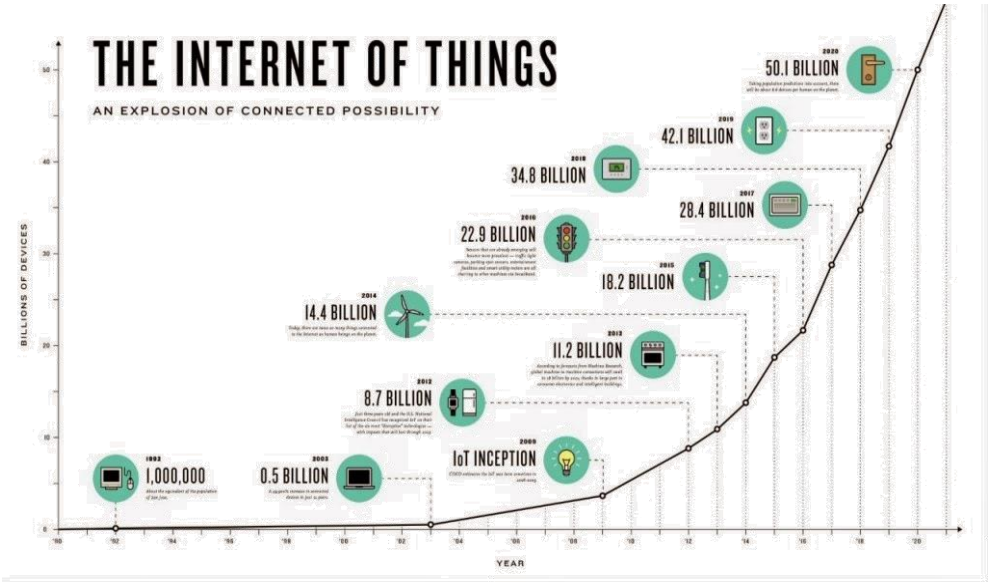
GDPR

> "The most sophisticated autonomous robots could be established as having the status of electronic persons with specific rights and obligations."
>
> —A draft motion from the European Parliament's Committee on Legal Affairs calls on the European Commission to consider civil law for robotics.

UNCONDITIONAL
BASIC INCOME
EUROPE

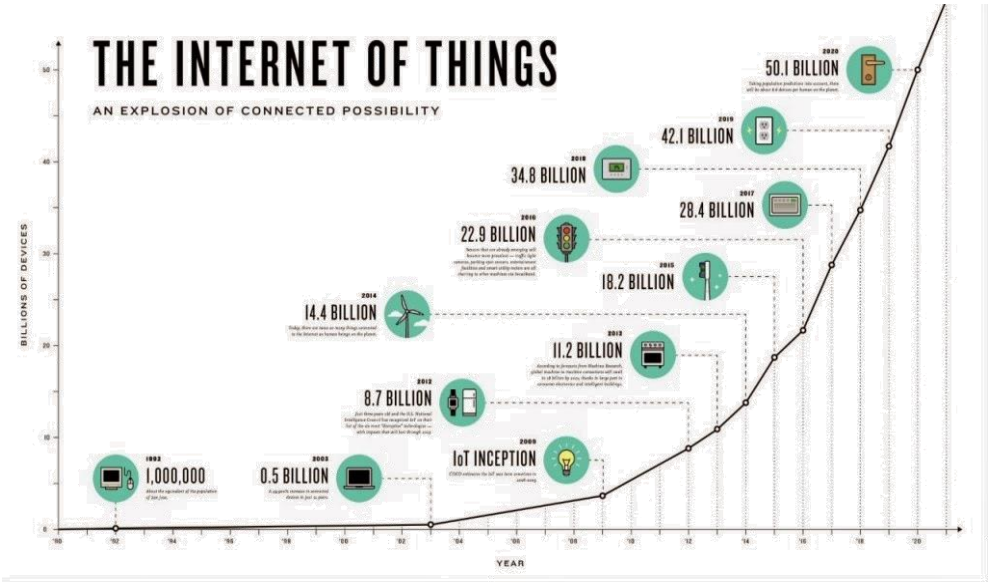
Source
Gartner

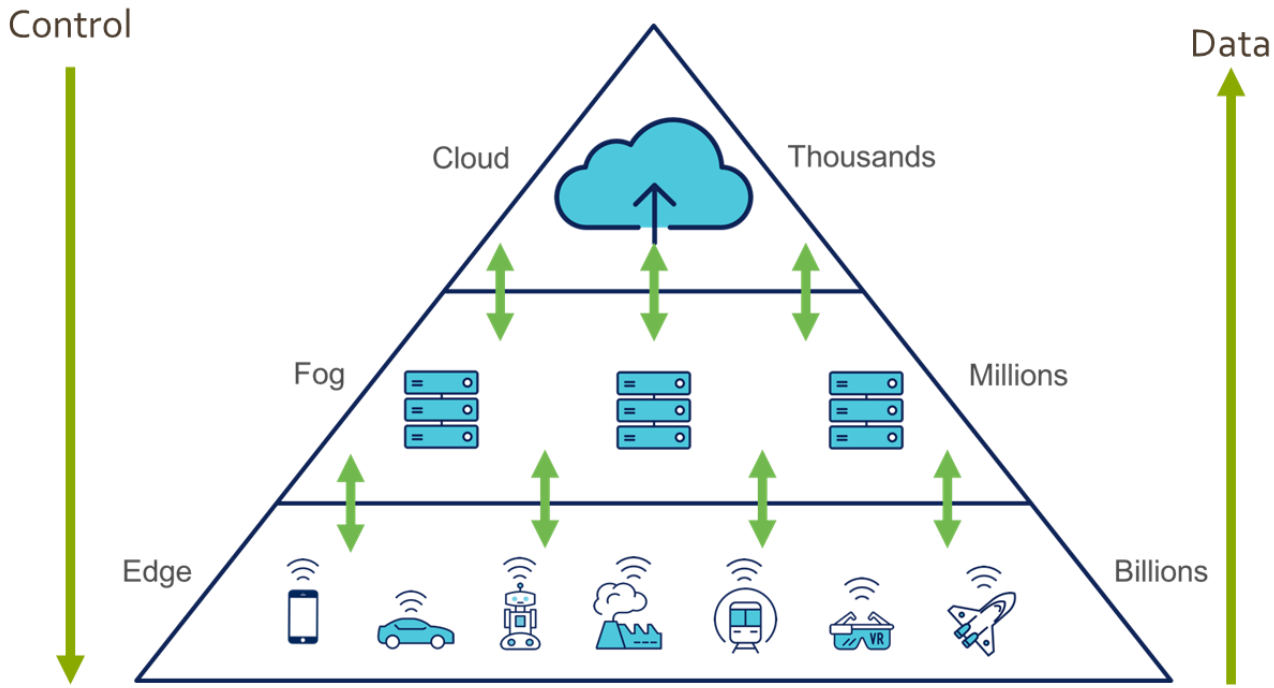
The Internet of (every) thing.



BOSCH
Invented for life

The Internet of (every) thing.

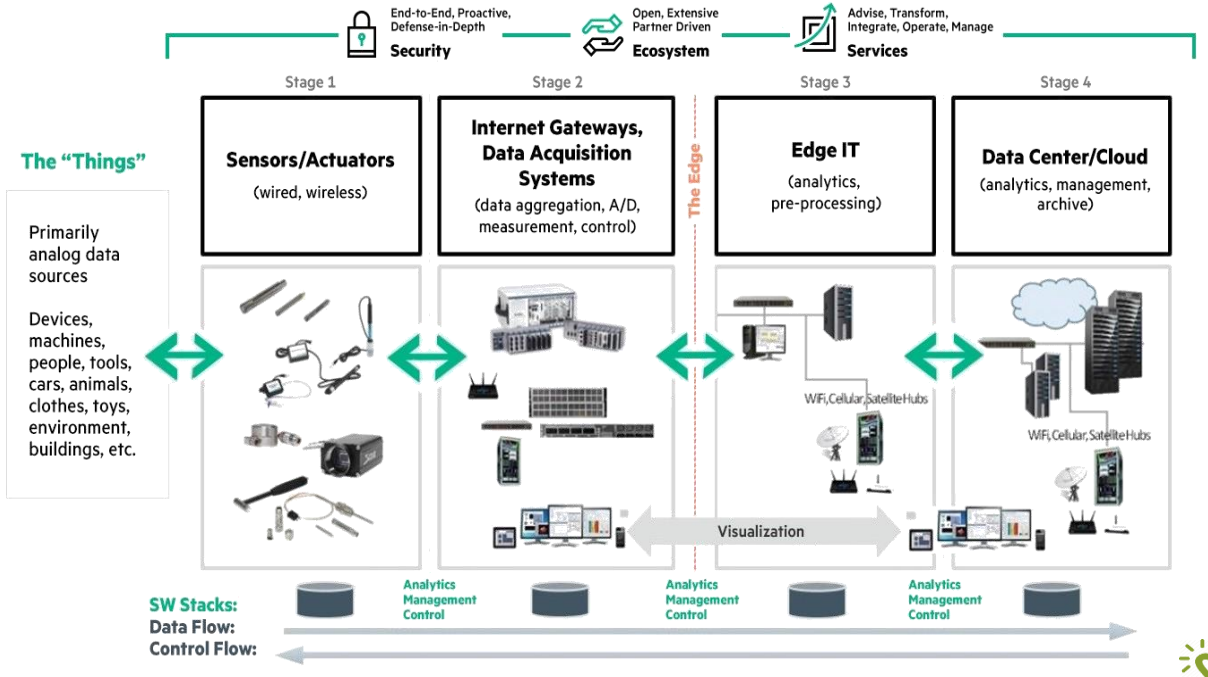


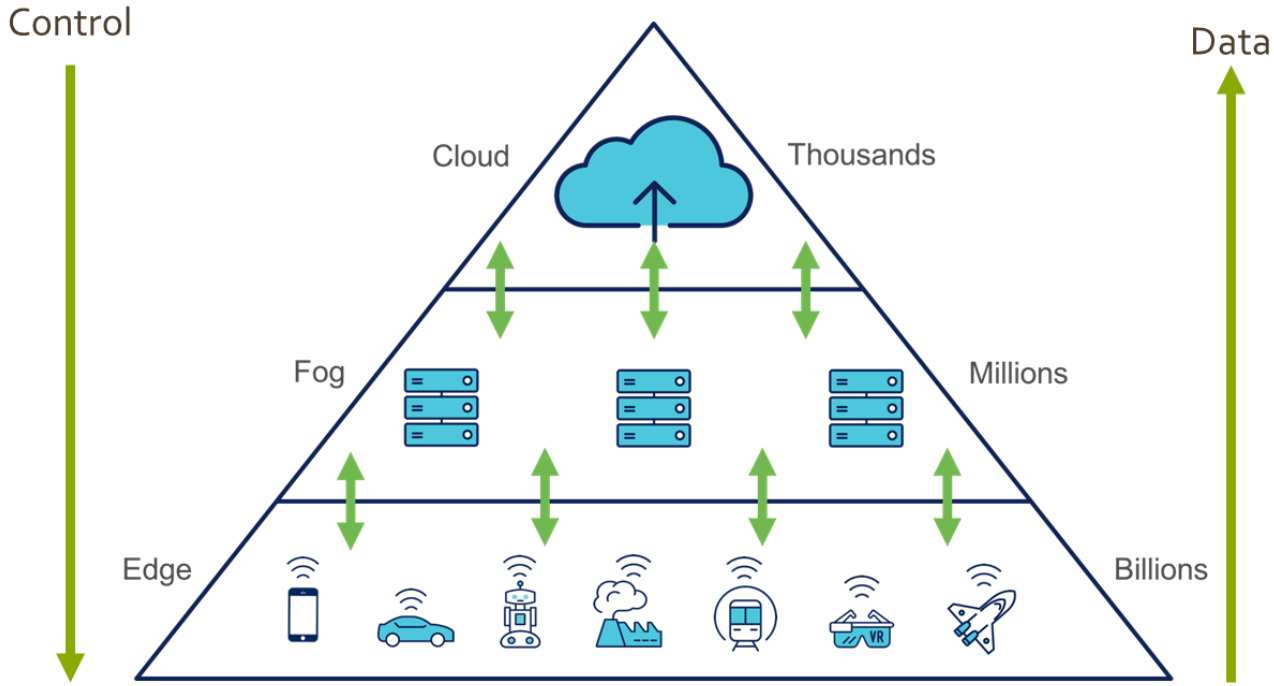


EDGE Computing

Hewlett Packard Enterprise

The 4-Stage IoT Solutions Architecture

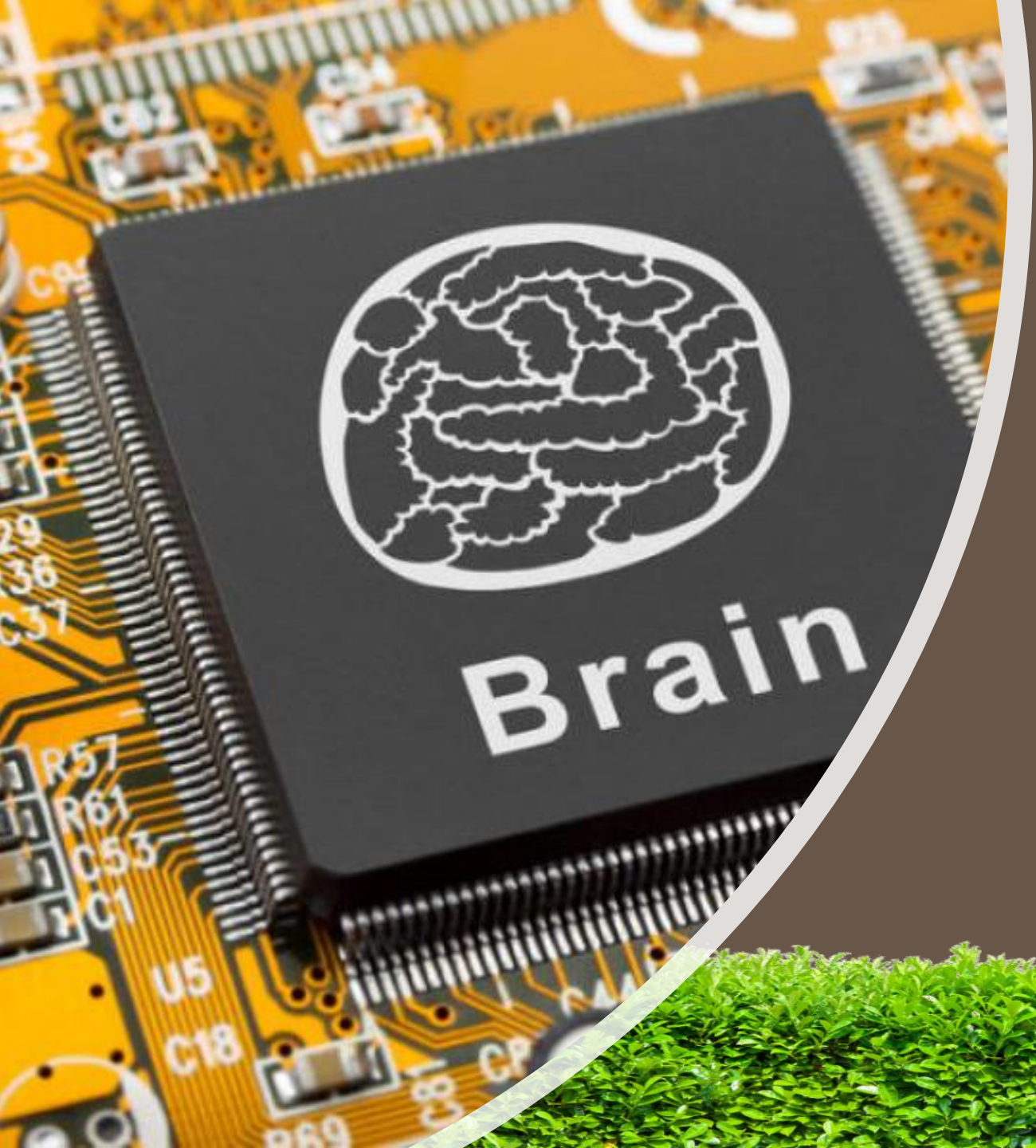




Latency · Bandwidth · Cost · Threats · Duplication · Reliability · Compliance

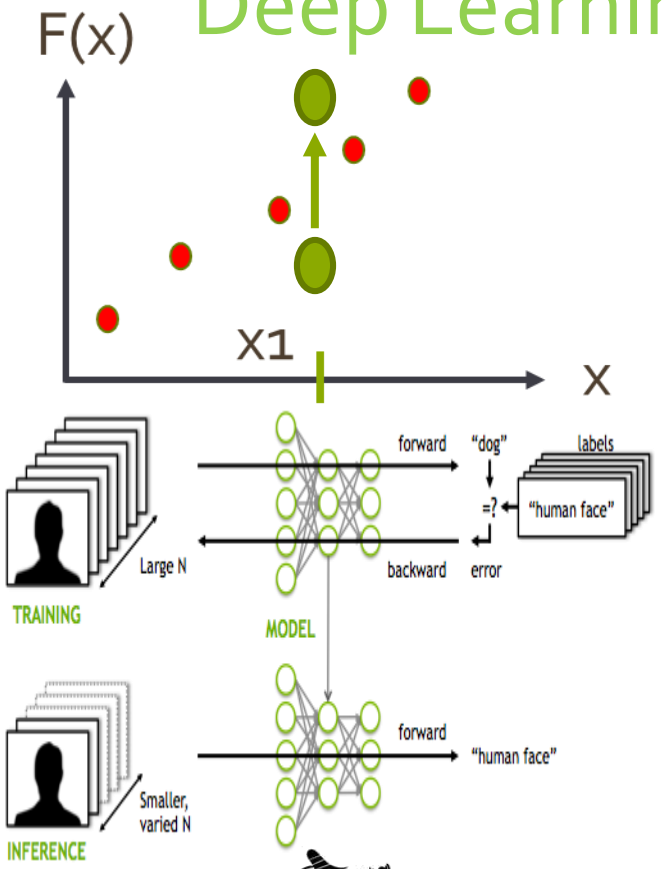
Intelligence

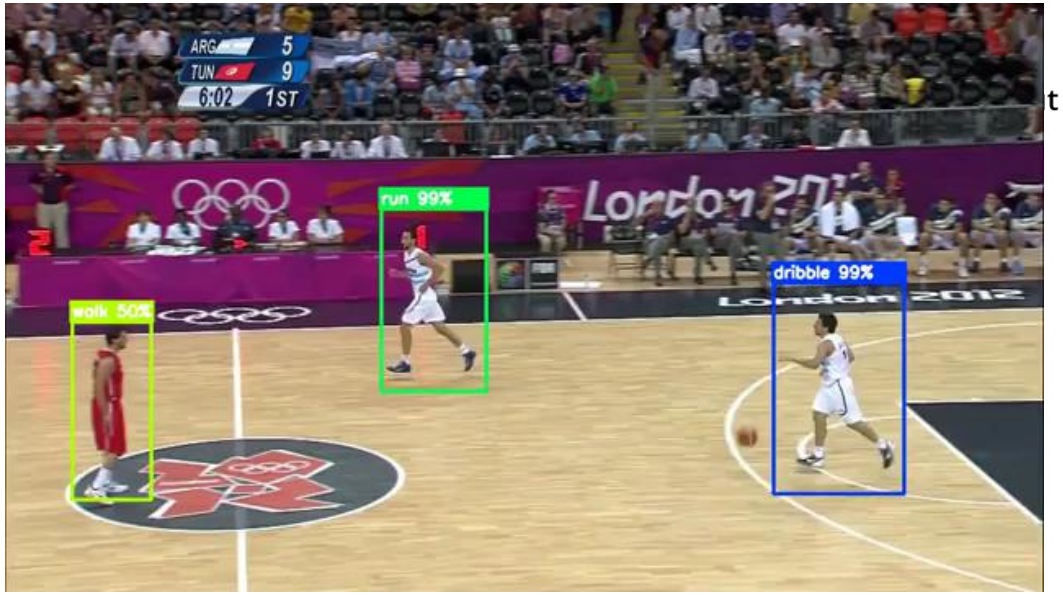
Trust



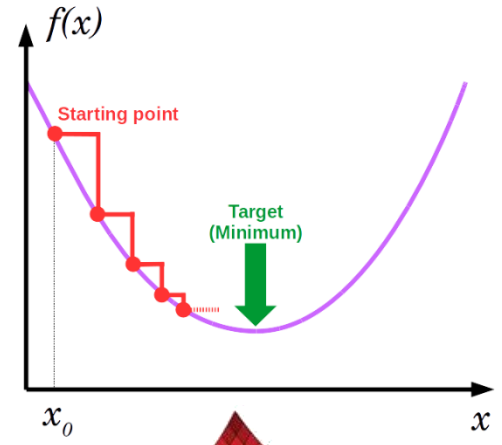
Edge Intelligence

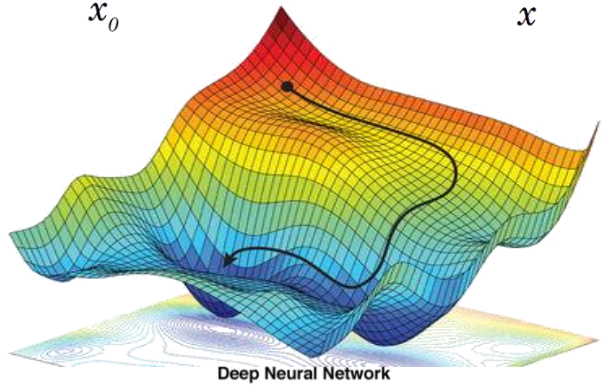
Deep Learning





t





$$J(\theta) = \frac{1}{m}\sum_{i=1}^{m}\left(h_\theta\left(x^{(i)}\right) - y^{(i)}\right)^2$$

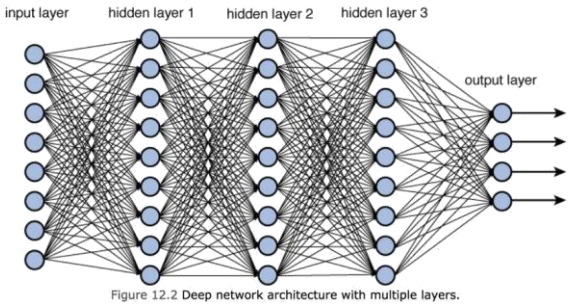
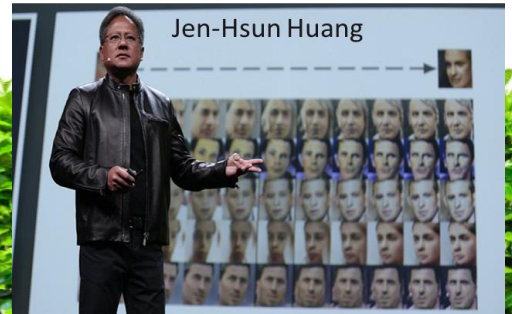
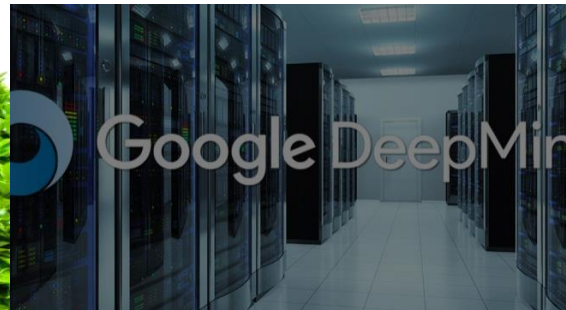


Figure 12.2 Deep network architecture with multiple layers.





Limits of Deep Learning @ the Edge

1. Asymmetric
2. Heavy
3. Black Boxed

+

4. HACKABLE

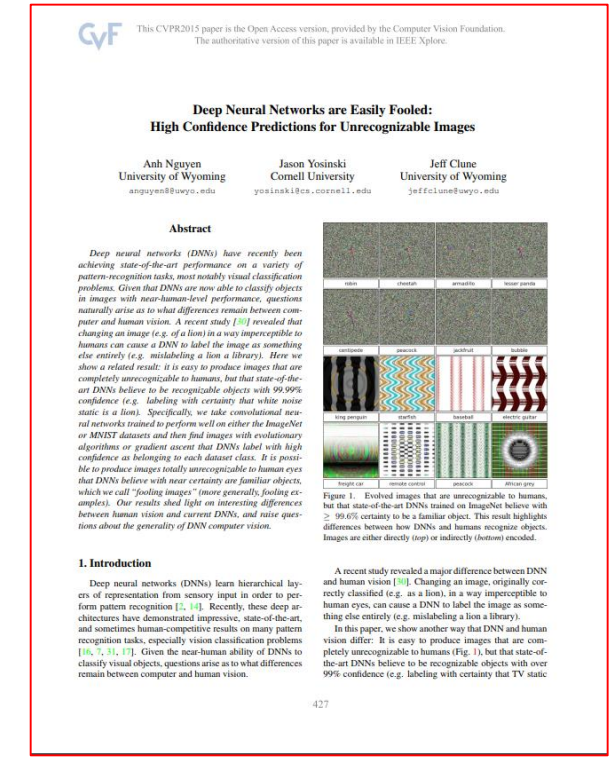
A. Catastrophic forgetting

B. One Pixel Attacking

C. Generative Adversarial Attacking

Deep Neural Networks are Easily Fooled

High Prediction Scores for Unrecognizable Images



This CVPR2015 paper is the Open Access version, provided by the Computer Vision Foundation.
The authoritative version of this paper is available in IEEE Xplore.

Deep Neural Networks are Easily Fooled:
High Confidence Predictions for Unrecognizable Images

Anh Nguyen
University of Wyoming
anguyen8@uwyo.edu

Jason Yosinski
Cornell University
yosinski@cs.cornell.edu

Jeff Clune
University of Wyoming
jeffclune@uwyo.edu

Abstract

Deep neural networks (DNNs) have recently been achieving state-of-the-art performance on a variety of pattern-recognition tasks, most notably visual classification problems. Given that DNNs are now able to classify objects in images with near-human-level performance, questions naturally arise as to what differences remain between computer and human vision. A recent study [30] revealed that changing an image (e.g. of a lion) in a way imperceptible to humans can cause a DNN to label the image as something else entirely (e.g. mislabeling a lion a library). Here we show a related result: it is easy to produce images that are completely unrecognizable to humans, but that state-of-the-art DNNs believe to be recognizable objects with 99.99% confidence (e.g. labeling with certainty that white noise static is a lion). Specifically, we take convolutional neural networks trained to perform well on either the ImageNet or MNIST datasets and then find images with evolutionary algorithms or gradient ascent that DNNs label with high confidence as belonging to each dataset class. It is possible to produce images totally unrecognizable to human eyes that DNNs believe with near certainty are familiar objects, which we call "fooling images" (more generally, fooling examples). Our results shed light on interesting differences between human vision and current DNNs, and raise questions about the generality of DNN computer vision.

Figure 1. Evolved images that are unrecognizable to humans, but that state-of-the-art DNNs trained on ImageNet believe with $\geq$ 99.6% certainty to be a familiar object. This result highlights differences between how DNNs and humans recognize objects. Images are either directly (*top*) or indirectly (*bottom*) encoded.

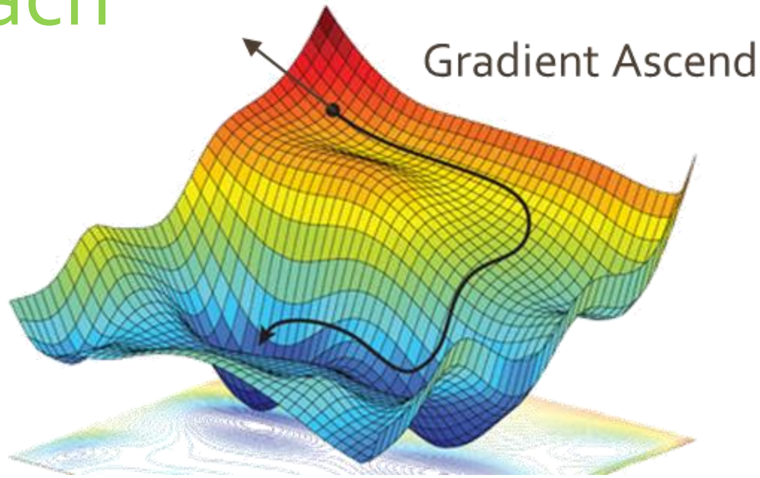
1. Introduction

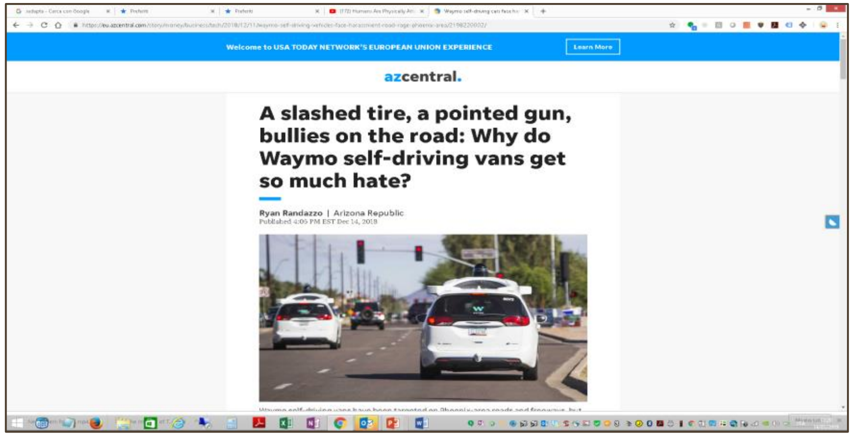
Deep neural networks (DNNs) learn hierarchical layers of representation from sensory input in order to perform pattern recognition [2, 14]. Recently, these deep architectures have demonstrated impressive, state-of-the-art, and sometimes human-competitive results on many pattern recognition tasks, especially vision classification problems [16, 7, 31, 17]. Given the near-human ability of DNNs to classify visual objects, questions arise as to what differences remain between computer and human vision.

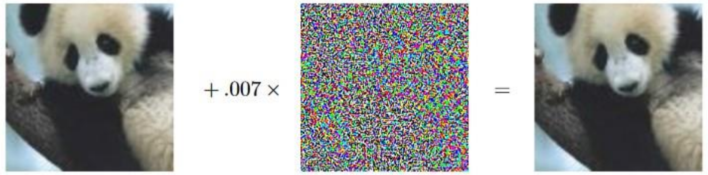
A recent study revealed a major difference between DNN and human vision [30]. Changing an image, originally correctly classified (e.g. as a lion), in a way imperceptible to human eyes, can cause a DNN to label the image as something else entirely (e.g. mislabeling a lion a library).

In this paper, we show another way that DNN and human vision differ: It is easy to produce images that are completely unrecognizable to humans (Fig. 1), but that state-of-the-art DNNs believe to be recognizable objects with over 99% confidence (e.g. labeling with certainty that TV static

1 Pixel Attach







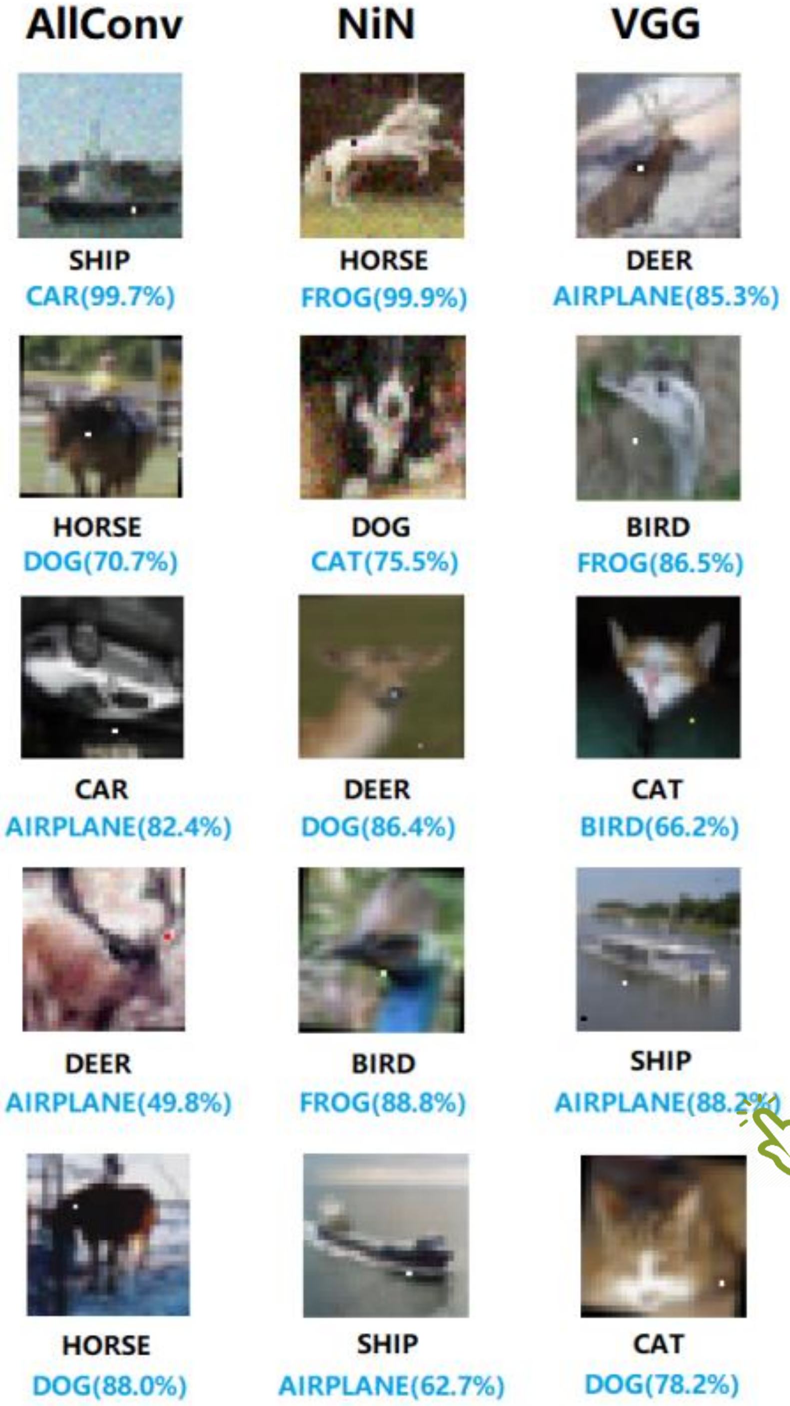
x
"panda"
57.7% confidence

$+ .007 \times$

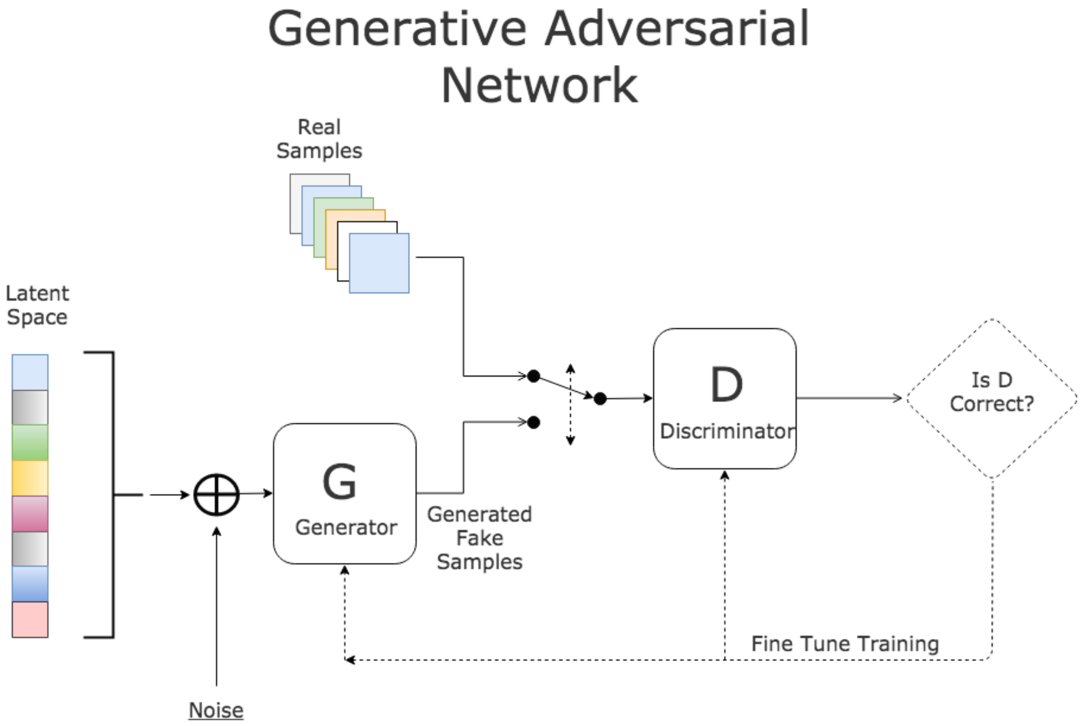
$\text{sign}(\nabla_x J(\theta, x, y))$
"nematode"
8.2% confidence

$=$

$x + \epsilon\text{sign}(\nabla_x J(\theta, x, y))$
"gibbon"
99.3 % confidence

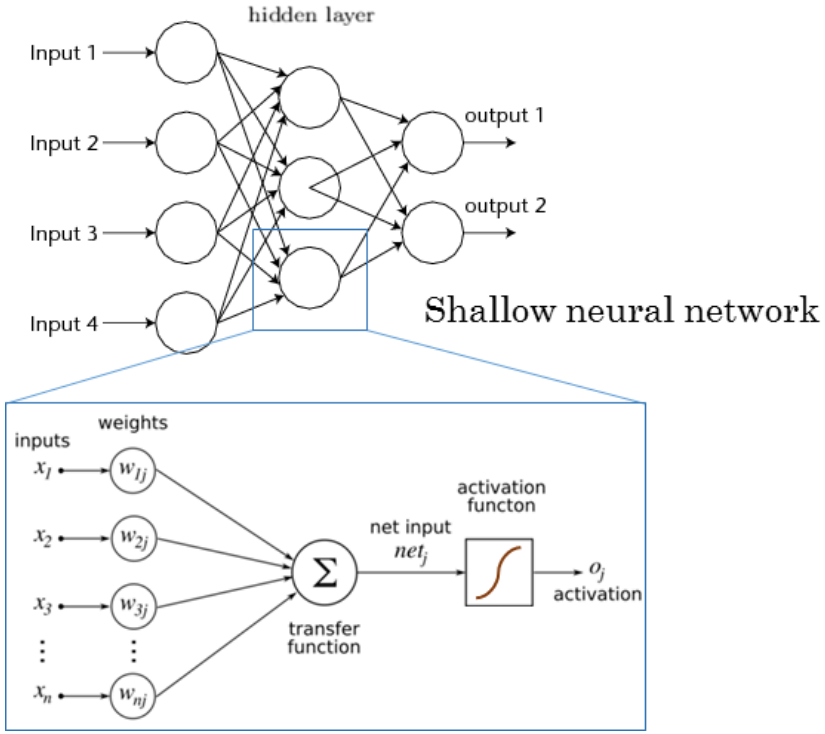


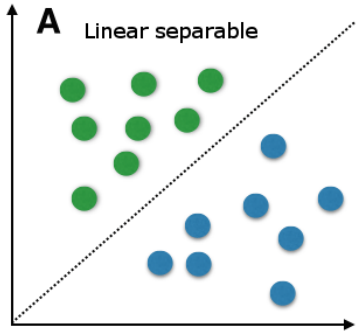
DeepFake & Generative Adversarial Attacks

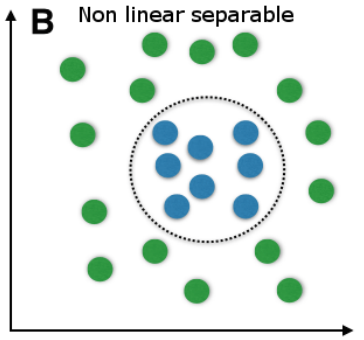


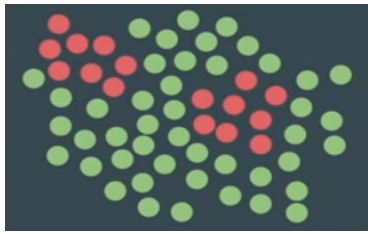
Shallow Learning

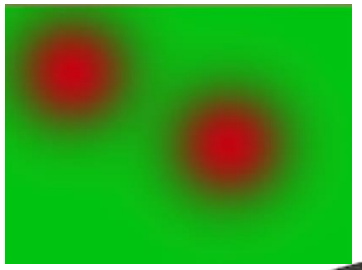
1. Lite & Rapid
2. Explainable
3. (Re)Trainable



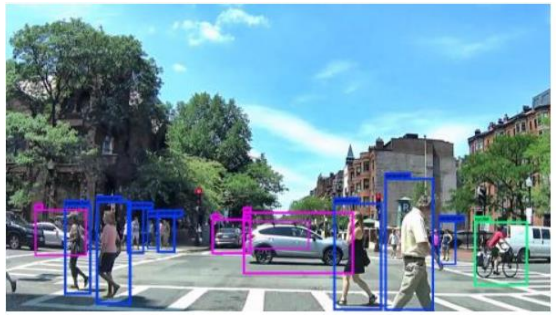




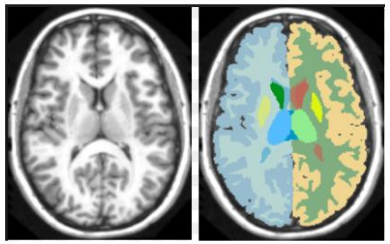




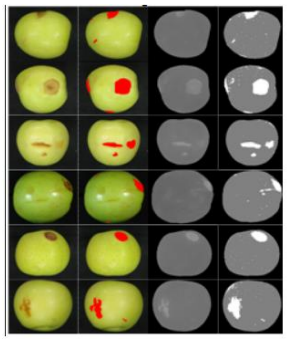
Deep or Shallow?



complex scene analysis with multiscale object recognition



medical images



product quality control

DEEP
(CNN starting from pixels)

SHALLOW
(features extraction)

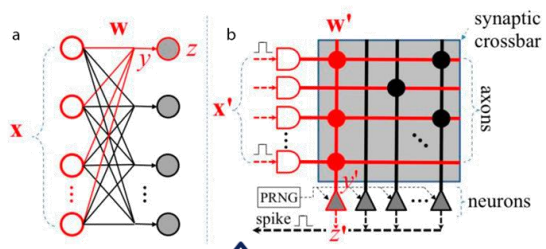
SHALLOW (RBF)	DEEP (BP)
+ FAST TRAINING	- SLOW TRAINING (BACK-PROPAGATION)
+ CONTINUOUS LEARNING	- NEED RECYCLING ON ENTIRE DATASET
+ LEARNING FROM SMALL DATA	- NEED BIG DATA
+ PERSONALIZED DATASET	- PUBLIC DATASET
+ EXPLAINABLE DECISIONS (GDPR)	- BLACK BOX
+ LOW POWER COMPUTATIONAL RESOURCES	- HIGH POWER COMPUTATIONAL RESOURCES
- IMAGE REC: NEED FEATURES EXTRACTION	+ IMAGE REC: START FROM PIXELS (CNN)
- IMAGE REC: RESTRICTED CONTEXT	+ IMAGE REC: WIDE CONTEXT
- IMAGE REC PERF: DEPENDING BY FEAT.EXTR.	+ IMAGE REC: HIGH PERFORMANCE
+ IMAGE REC: RELIABLE	- IMAGE REC: EASILY FOOLED

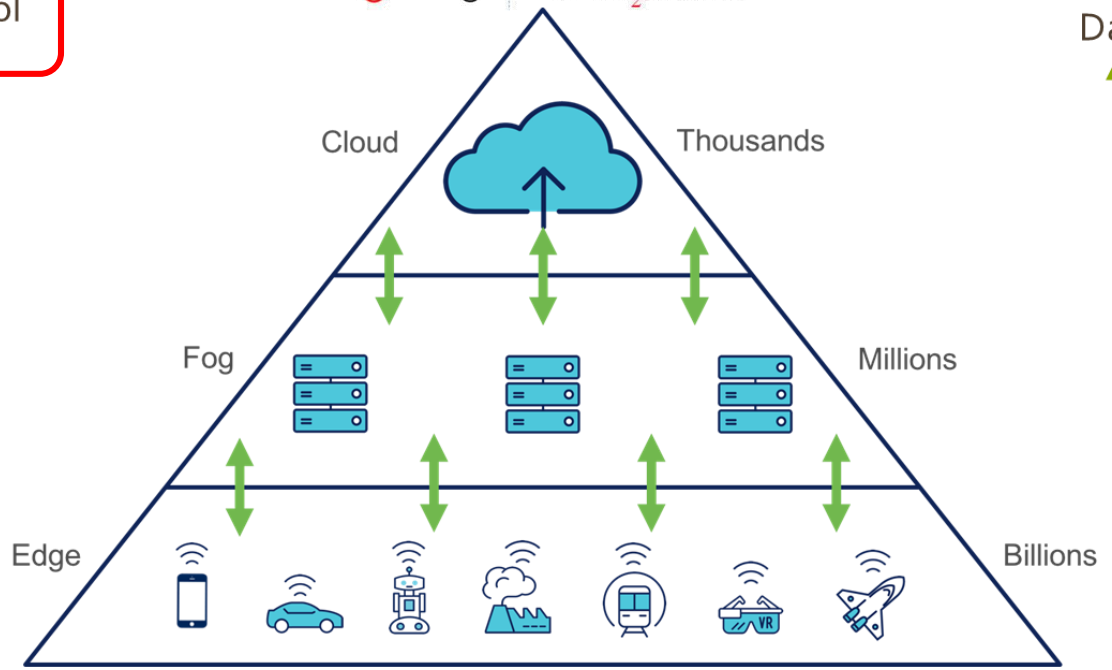
Edge AI

Flexibility

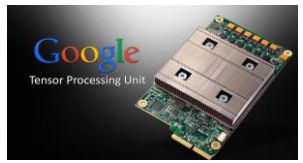
Efficiency

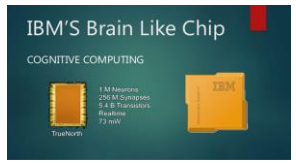
Control





Da





Big Corps AI Chips Strategy

NVIDIA
2017, 05
NVIDIA launches its Volta GPU computing architecture to boost AI inference, training and HPC.

IBM
2017, 07
IBM and the US AFRL announce a collaboration on a brain-inspired supercomputing system.

HUAWEI
2017, 09
Huawei introduces Kirin 970, its new flagship SoC with AI capabilities.

AMAZON
2018, 02
Amazon is developing a new processor for its virtual assistant Echo to make Alexa faster and smarter.

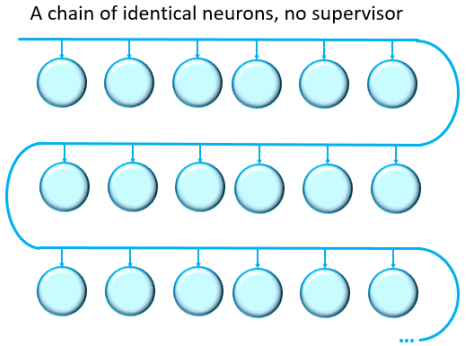
GOOGLE
2017,06
Google introduces its TPU (Tensor Processing Units) which accelerate the TensorFlow framework in machine learning.

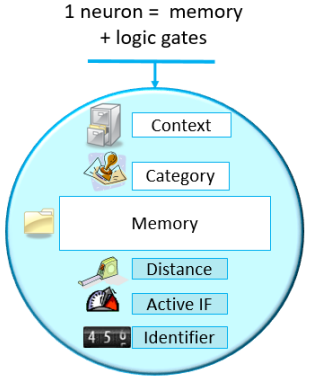
MICROSOFT
2017, 07
Microsoft announces that it is working on a processor for the second generation of HoloLens. The chip will enhance the AR headset's image recognition feature.

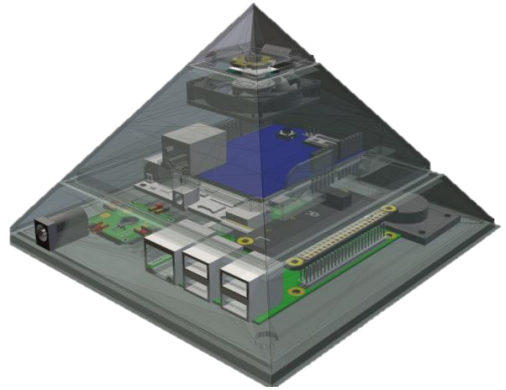
INTEL
2017, 09
Intel announces the acquisition of Movidius. Intel will leverage its existing assets and Movidius technology in the development of new AI chips for devices such as drones, robots, VR and etc.

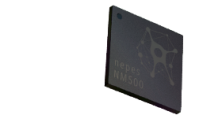
Shallow Learning @ the Edge

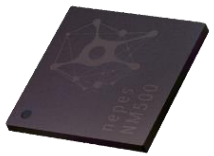
MYW.AI™
EDGE INTELLIGENCE FOR ALL

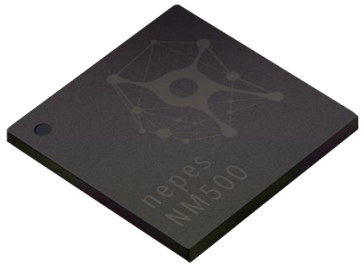


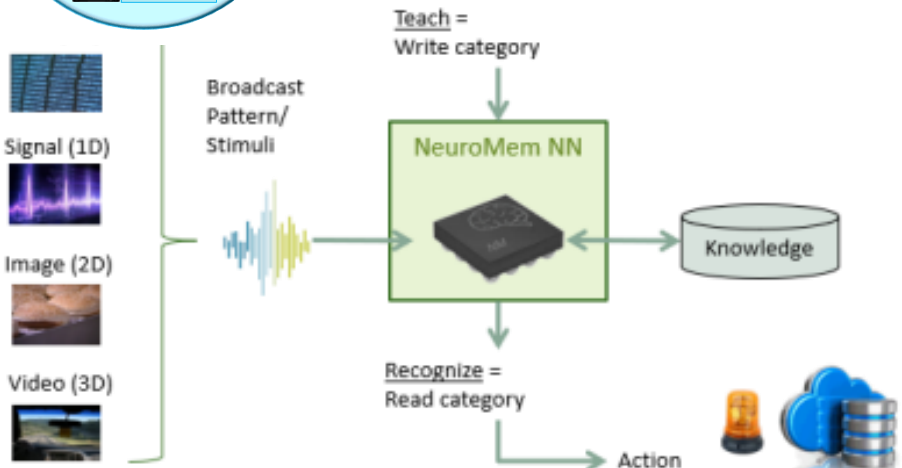












GENERAL VISION

NM500 NEUROBRICK NEUROSHIELD

coming soon

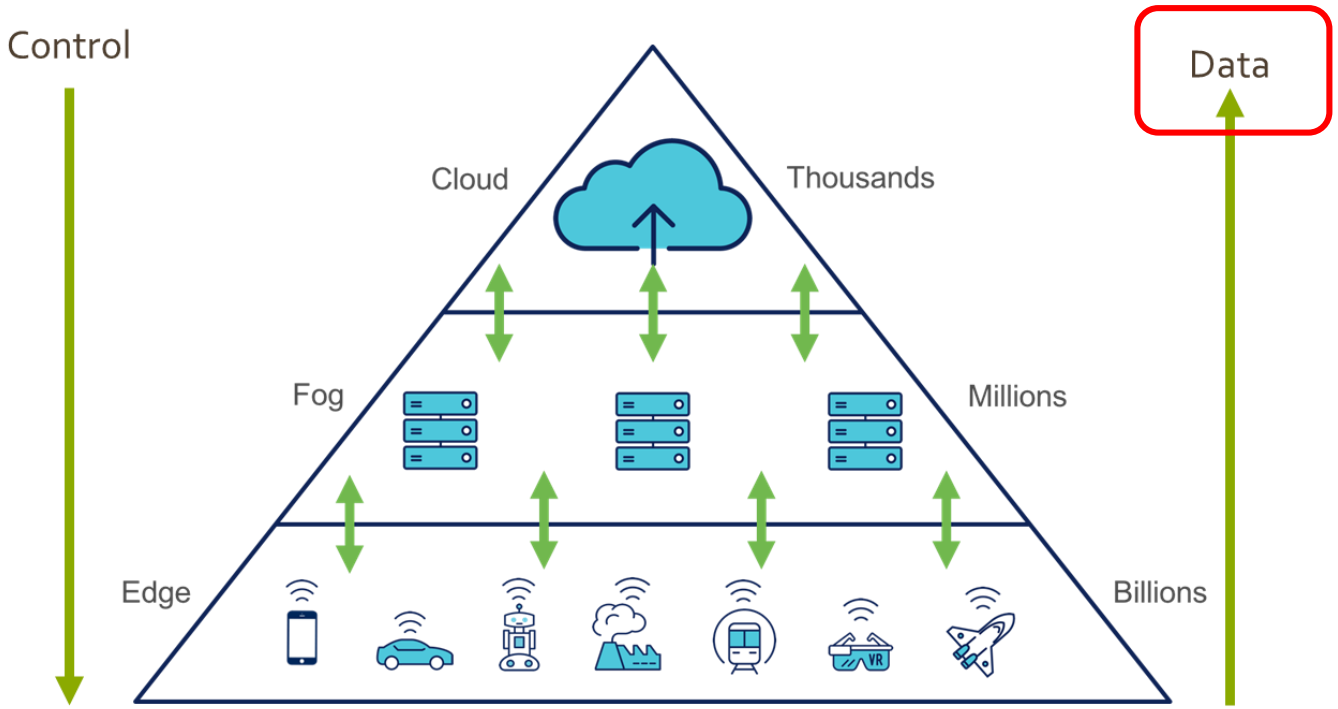
PRODIGY BOARD

coming soon

Brilliant USB

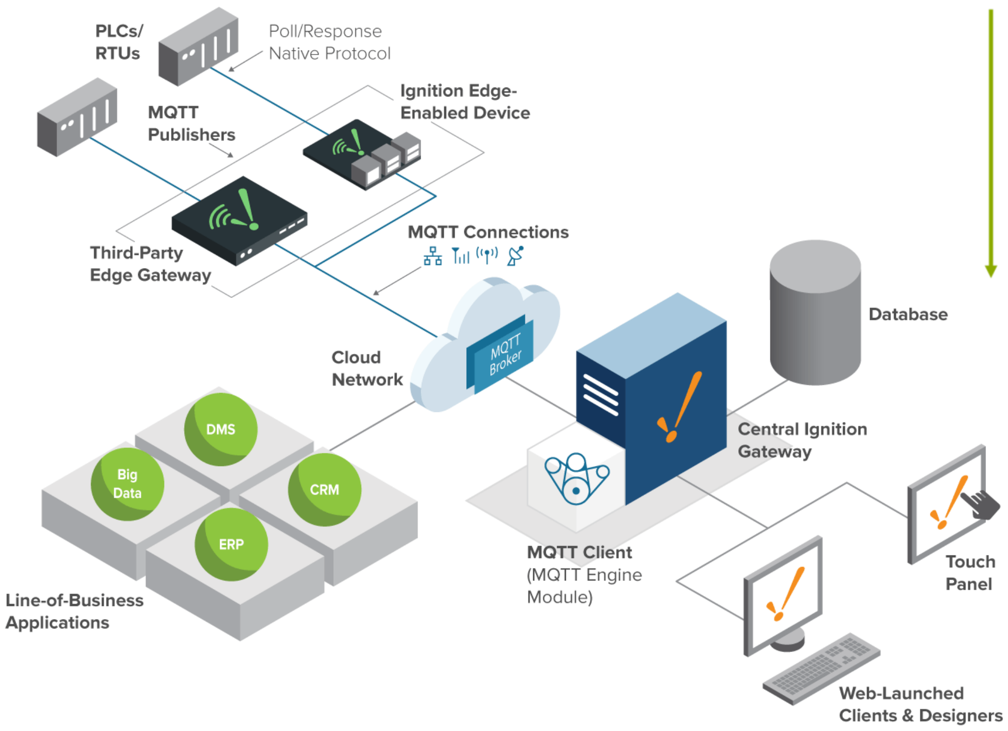
Edge Trust

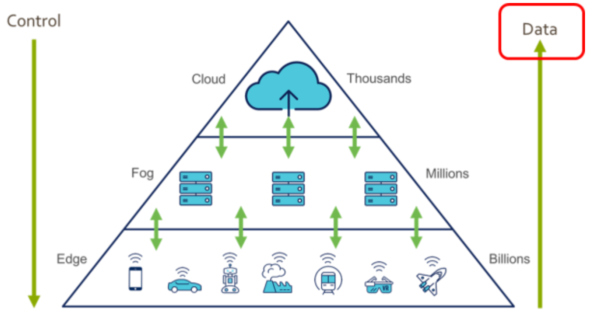
Edge AI



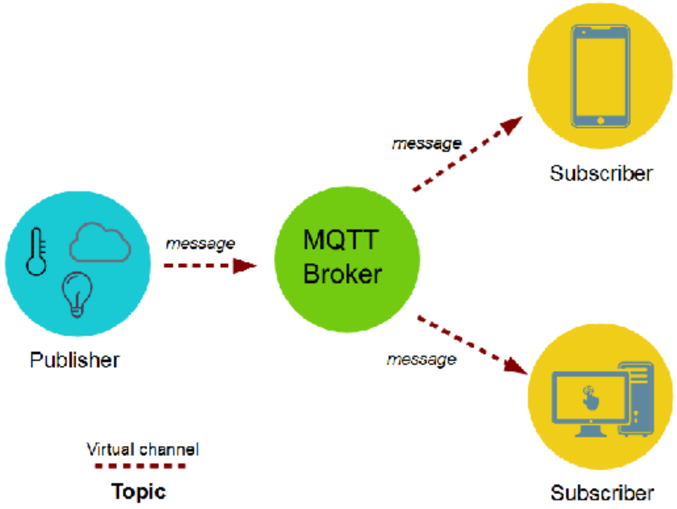
How Can We Trust Data in a distributed Supply Chain ?

IOT Data transport, verification & rendering



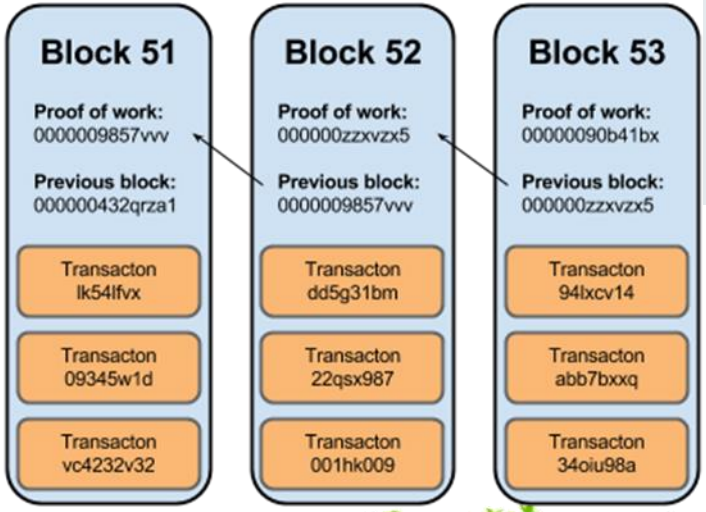


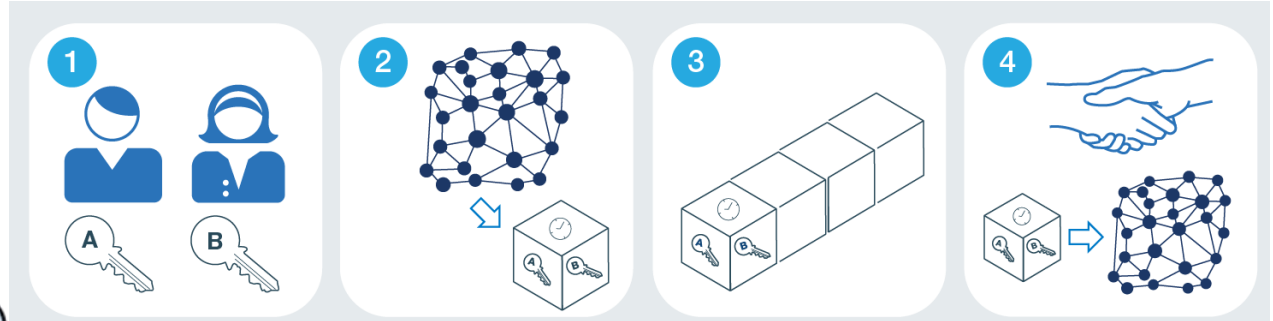
PRESENT
MQTT
(Message Queue Telemetry Transport)



Improving Trust @ the EDGE

BLOCKCHAIN ethereum HYPERLEDGER





When 2 parties initiate a transaction, blockchain assigns an encryption

Blockchain verifies the transaction and creates a block

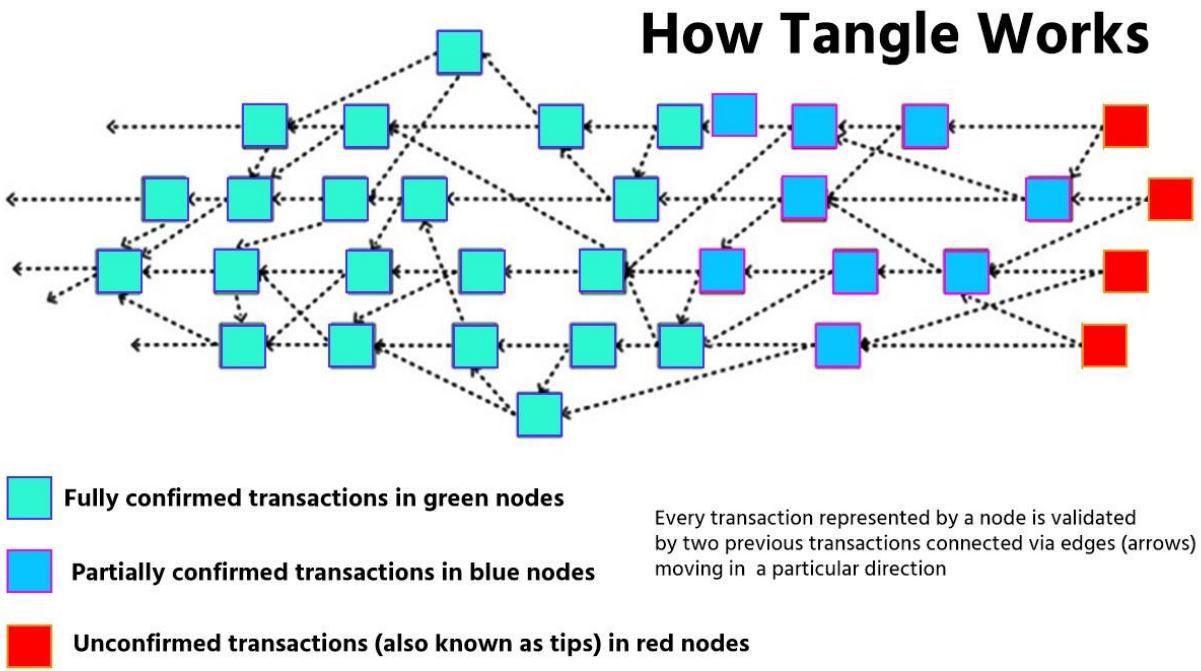
The new block is appended to the blockchain

The blockchain transaction is now complete and the ledger is updated

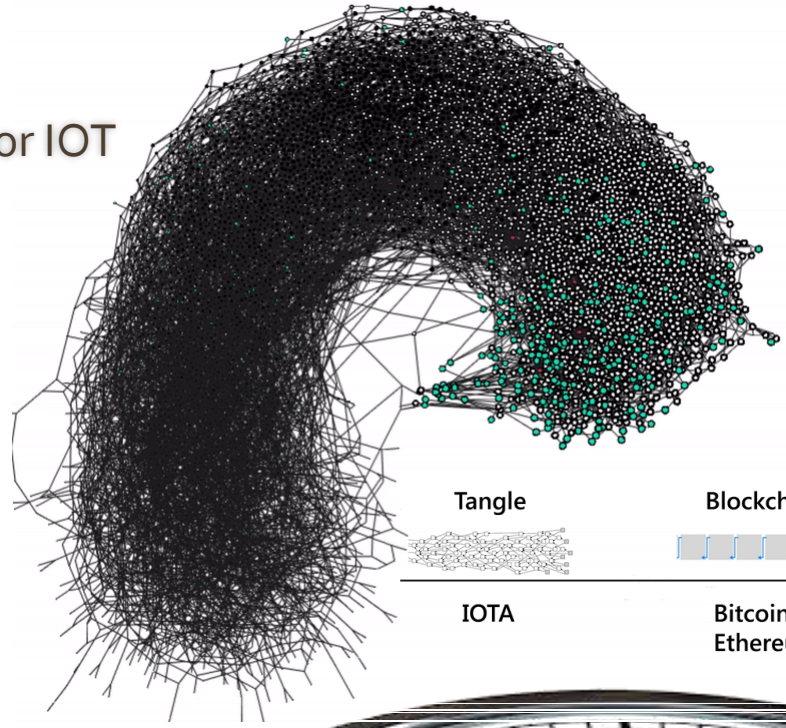
- Made for financial transactions between humans
- Not scalable
- Not free

IOTA – Blockchain for IOT

knowhedge
your edge to know how



- SCALABLE
- FREE
- Made for IOT



IDEAL FOR MONETIZING IOT DATA STREAMS IN THE MACHINE ECONOMY !

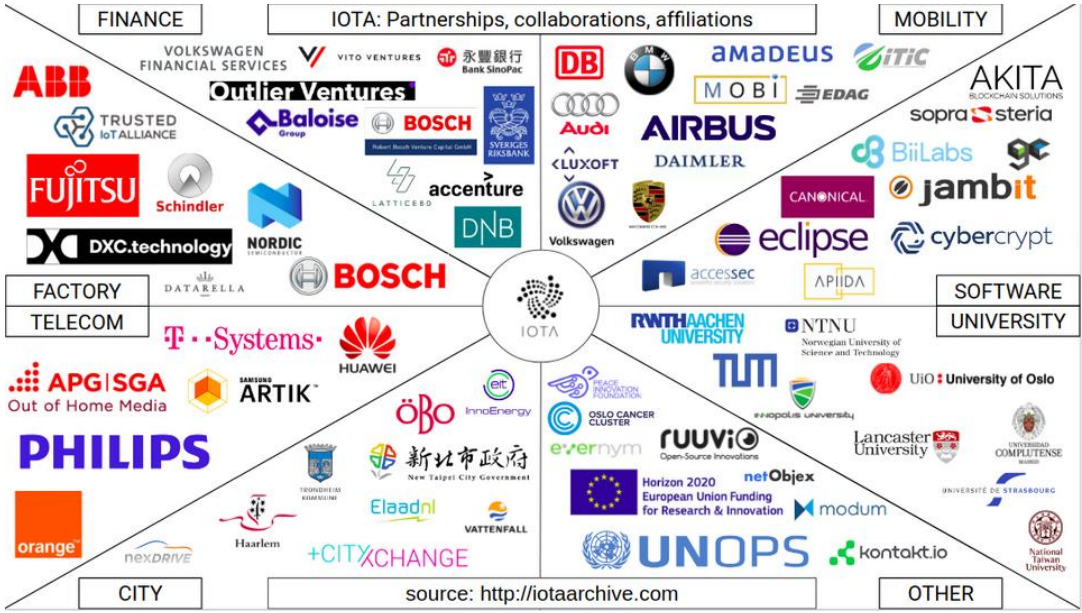
2015: David Sønstebø & Dominik Schiener found IOTA
2017: 12 Billion USD valorization (4° ICO ever)

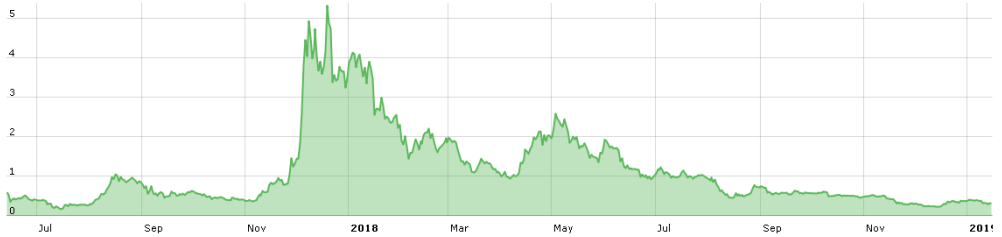
IOTA – Blockchain for IOT

knowhedge

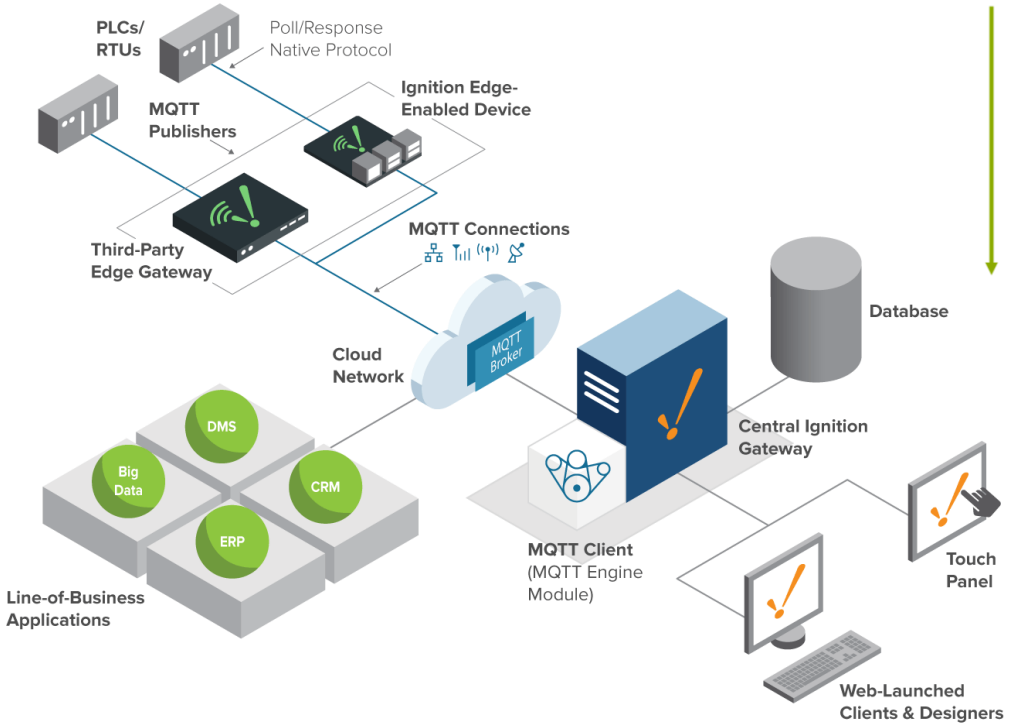
your edge to know how

- No limits to scale (DAG vs CHAINS)
- No mining , no transaction fees (user=verifier)
- IDEAL FOR IOT (miota based M2M transactions)



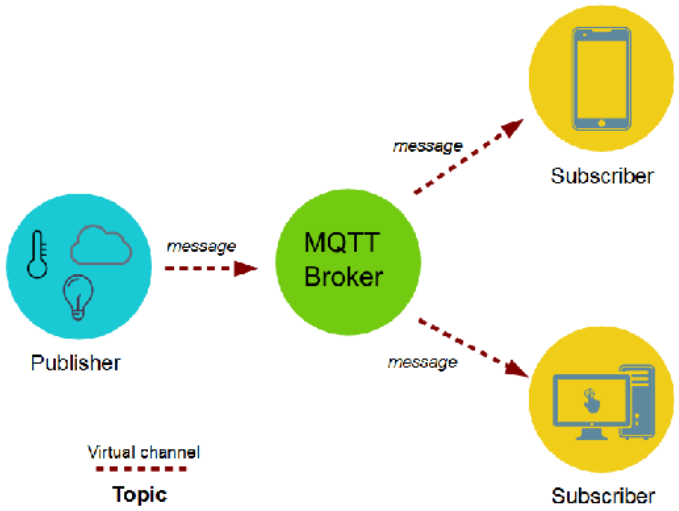


IOTA – MAM (Masked Authentication Messaging)
The future of IOT messaging format?

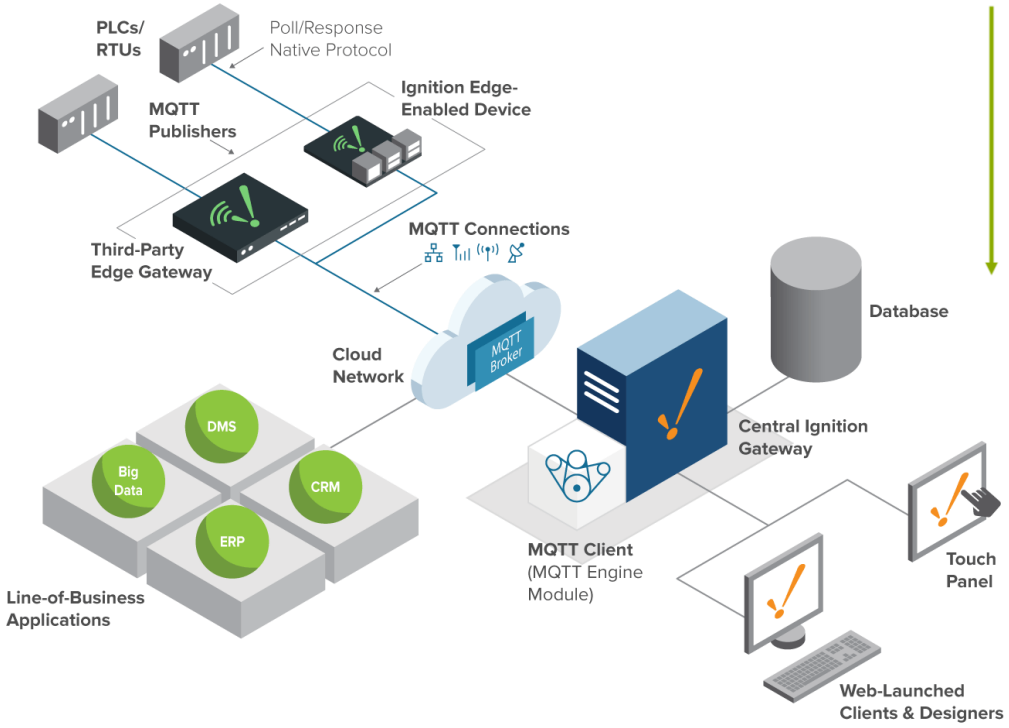


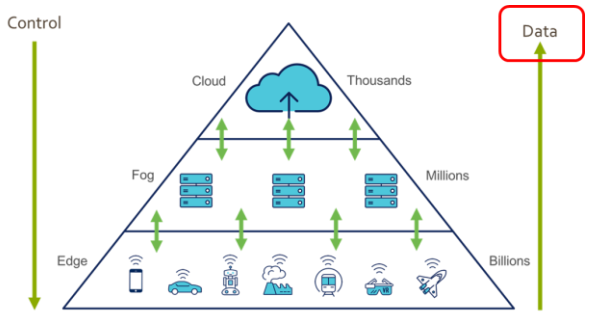
MQTT PROTOCOL

PRESENT
MQTT
(Message Queue Telemetry Transport)



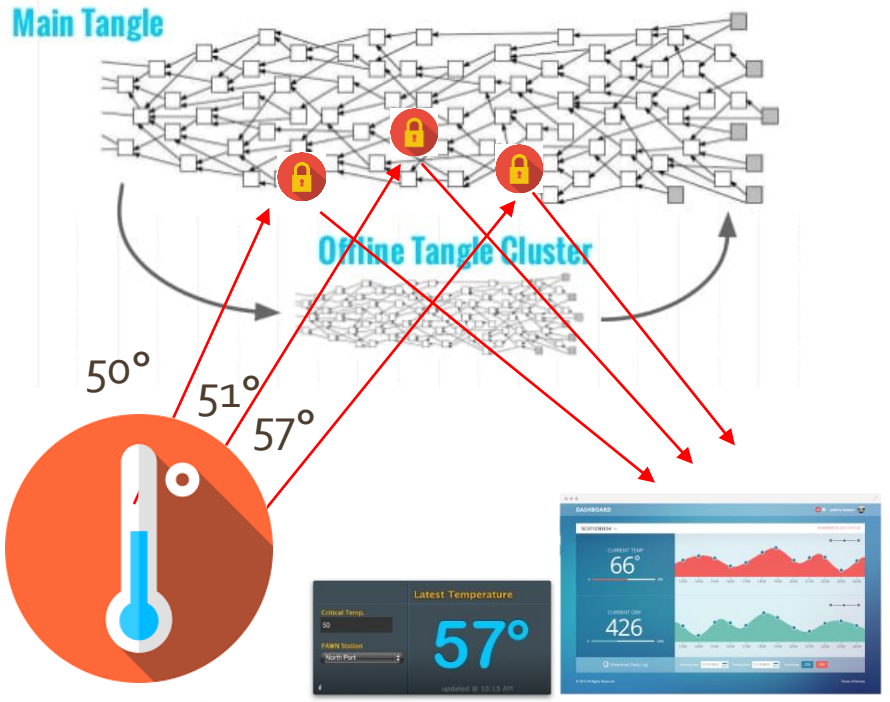
IOTA – MAM (Masked Authentication Messaging)
The future of IOT messaging format?





GOSSIP PROTOCOL

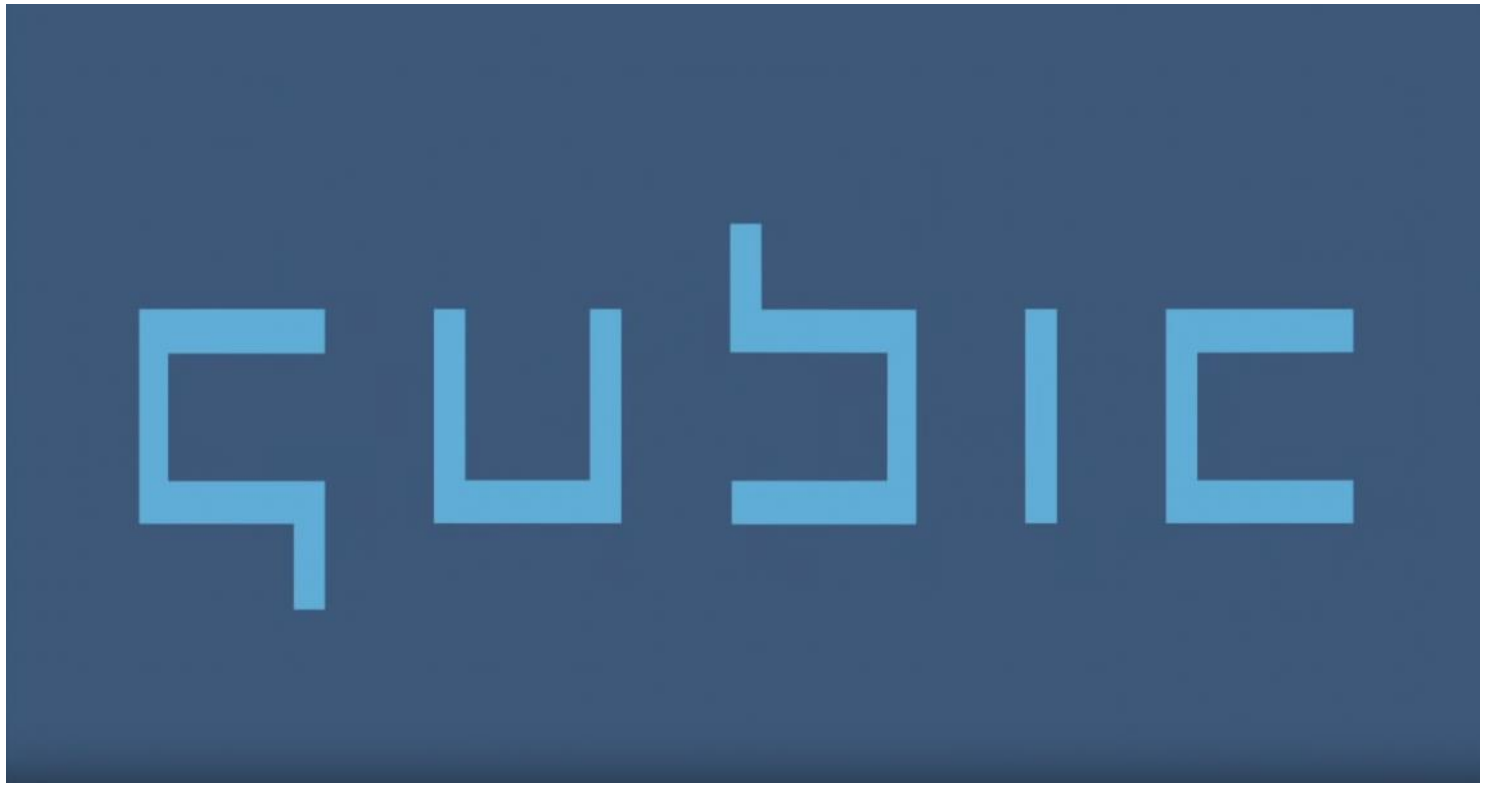
Future
MAM
(Masked Authentication Messaging)



IOTA – WHAT's NEXT @ The EDGE?

Future 2nd level IOTA protocols (QUBIC)

- Smart (IOT) Contracts
- External (IOT) Oracles
- Distributed (IOT) Computing

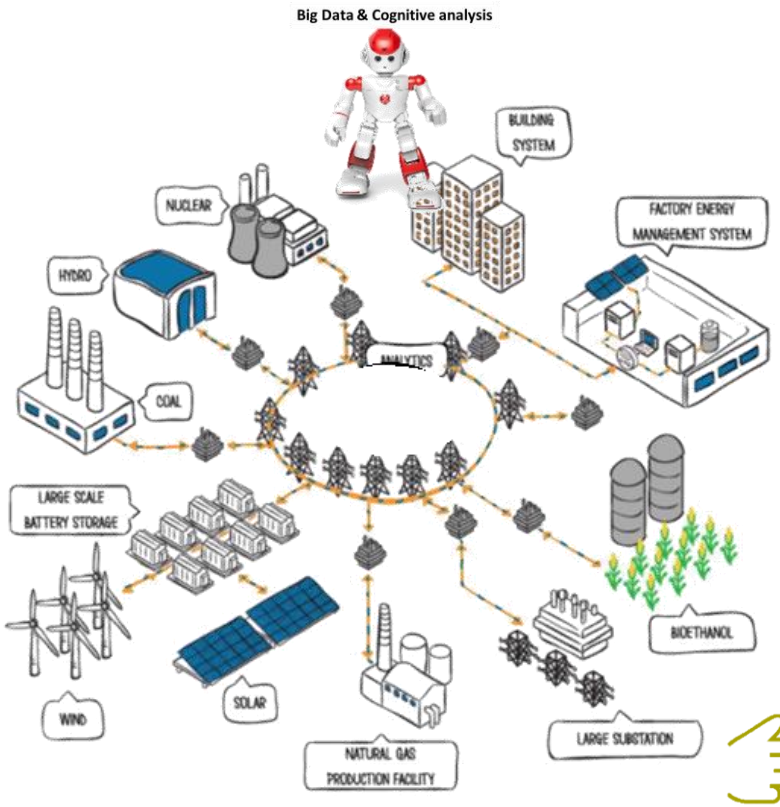


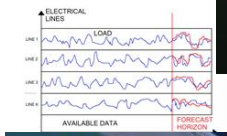
Future Edge Scenario 1 (trusted plant control by Bosch)

BOSCH
Invented for life

XDK2M.AM

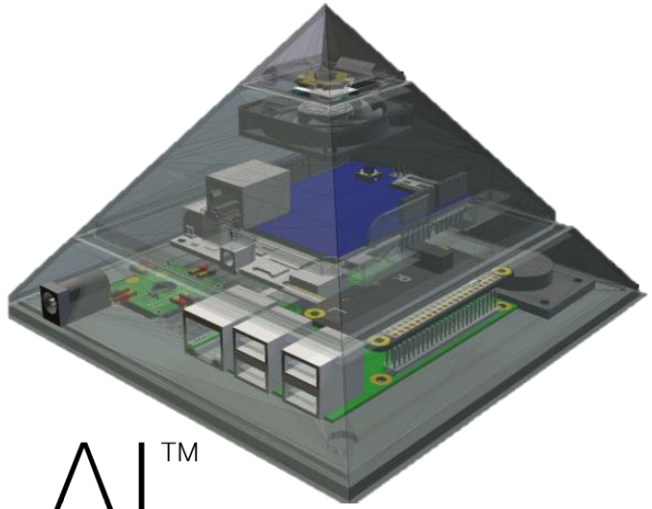
Future Edge Scenario 2





Future Edge Scenario 2 (Edge Intelligence 4 all by MYWAI)

MYW.AI™ is a new EDGE AI and IOTA appliance currently under engineering at Digital Tree, the AI Hub and startup incubator founded by SoftJam and Mixura with the support of Microsoft Italy.



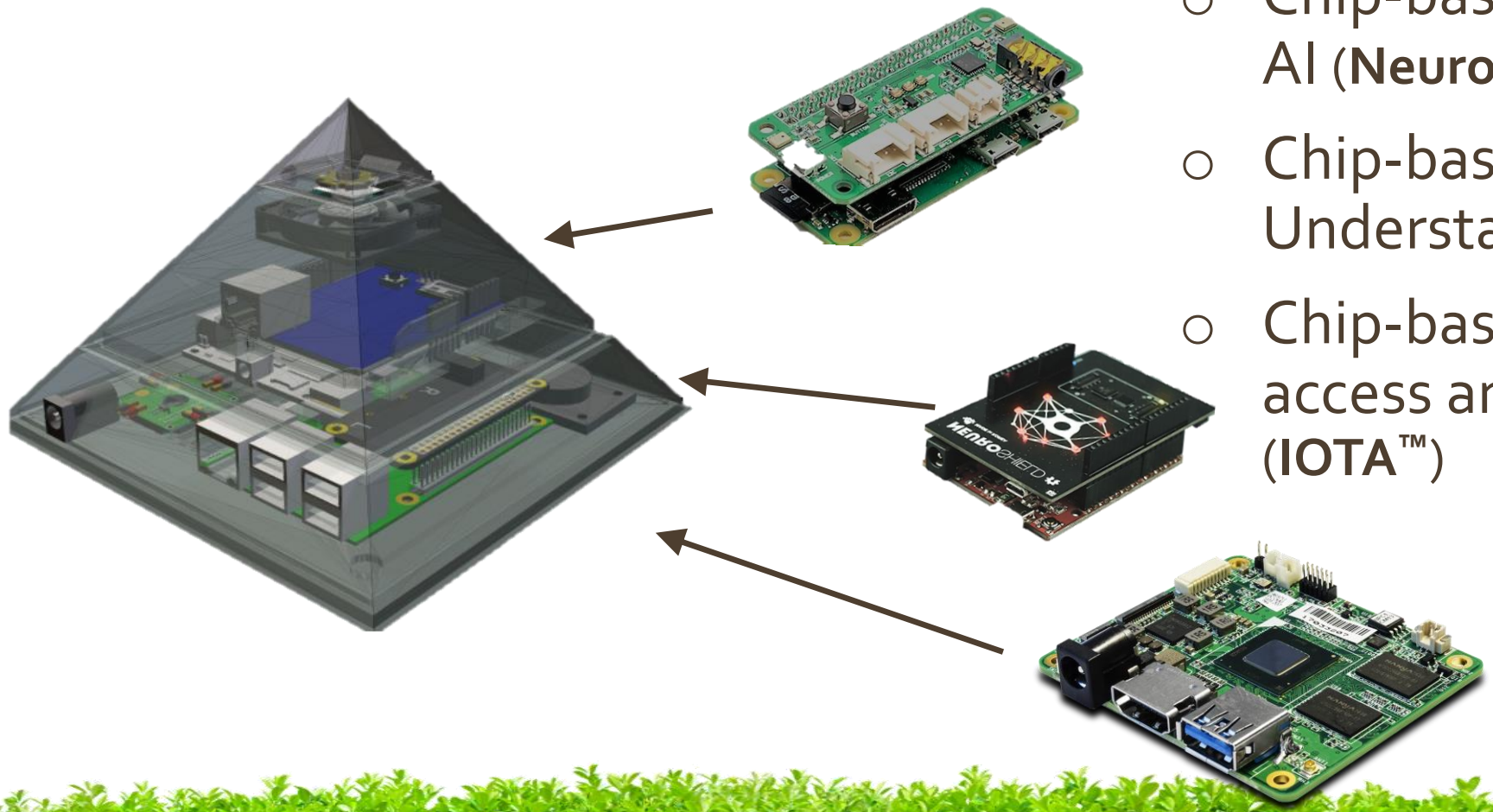
MYW.AI™
EDGE INTELLIGENCE FOR ALL

Click to access the Industry 4 Light House Plant Project Portal & Videos

MYW.AI™
EDGE INTELLIGENCE FOR ALL

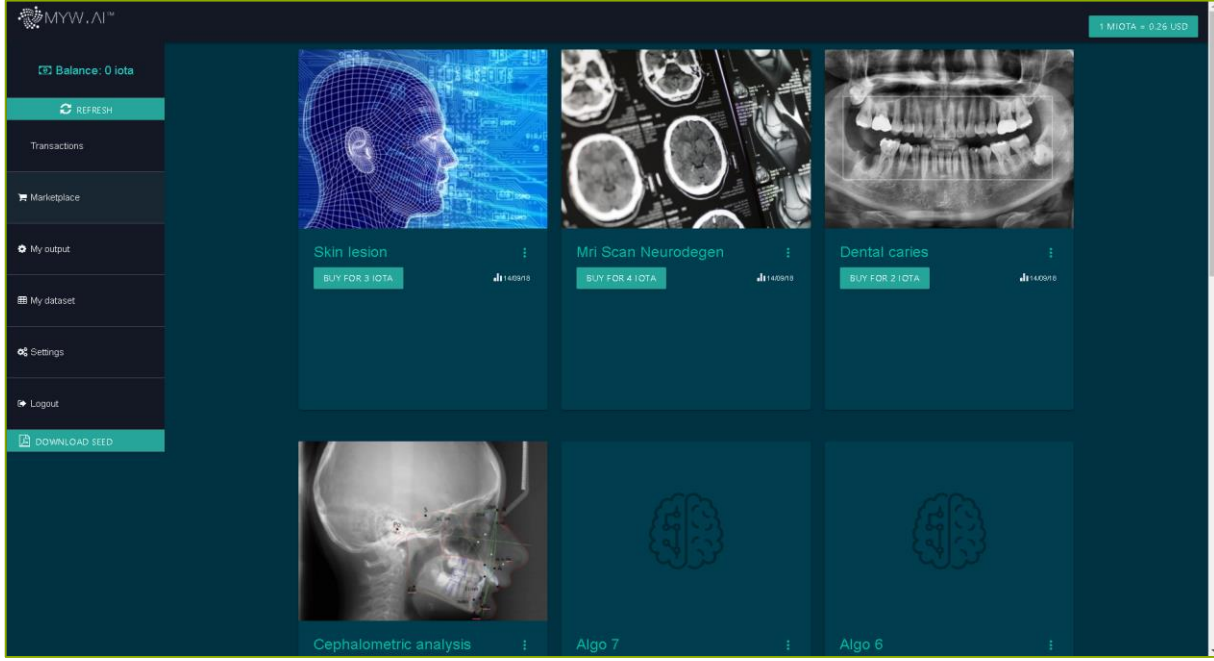
The MYW.AI Edge integrates

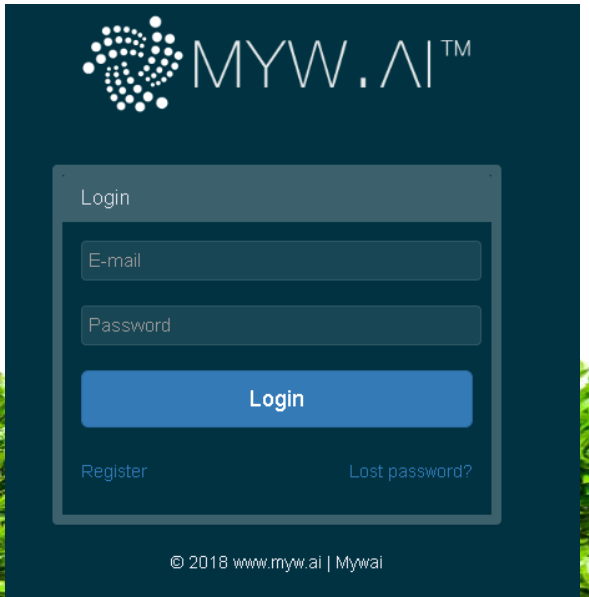
- Chip-based Shallow Learning AI (**Neuromem™**)
- Chip-based Natural Language Understanding (**SNIPS™**)
- Chip-based DLT hashtagging, access and MQTT2MAM (**IOTA™**)

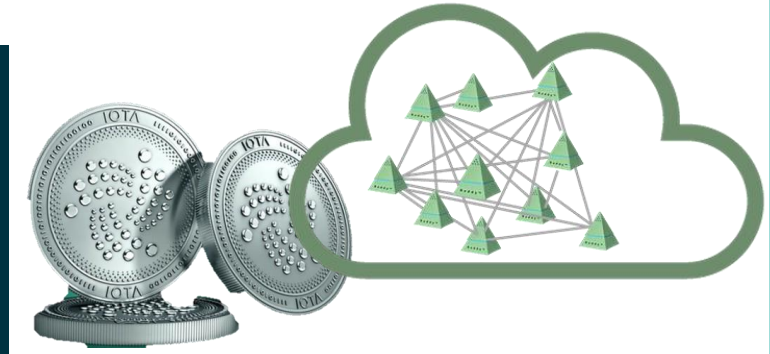


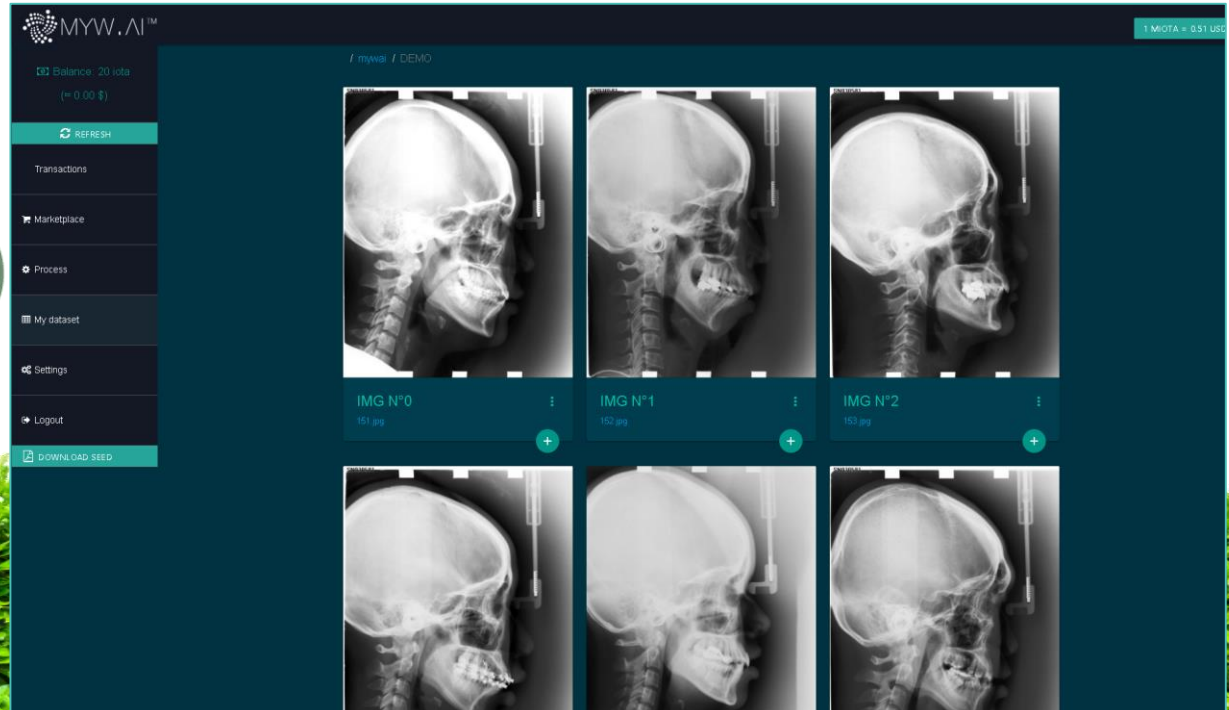
MYW.AI™ MARKETPLACE

- IOTA Network of certified MYW.AI edge appliances
- Community of AI ALGO developers & users
- DLT based certification
- Crypto market









MYW.AI™
Healthcare

HEY MYWAI

Hey my way

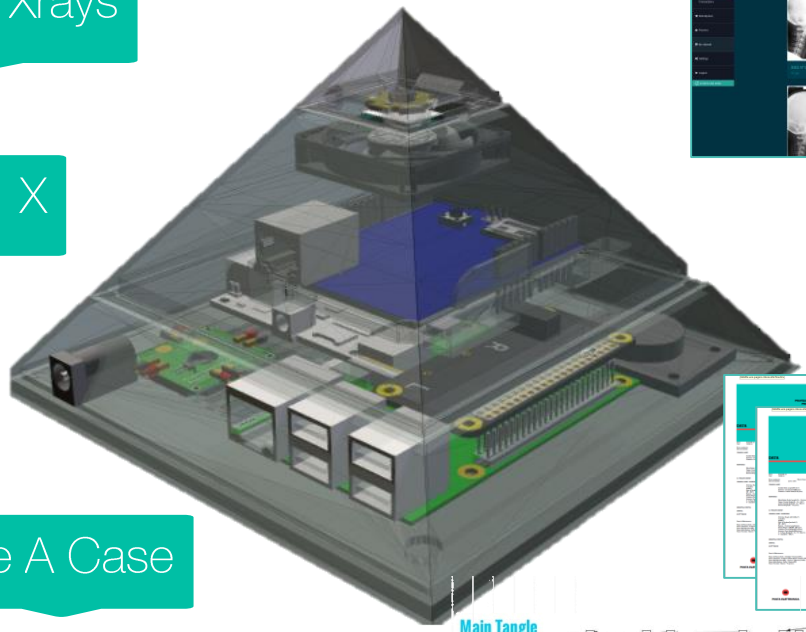
Please load cephalometric Xrays

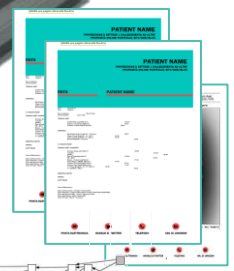
Please select patient X

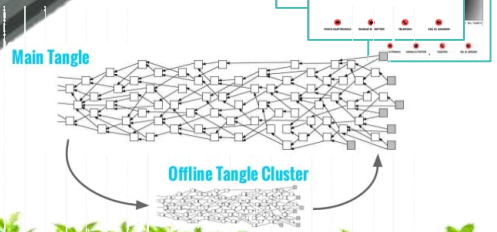
Please classify patient

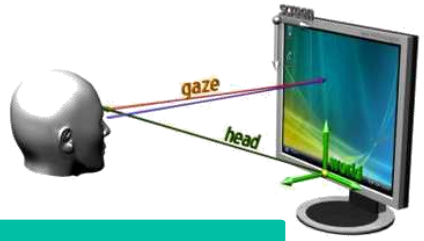
Patient X is a Type A Case

Please publish report



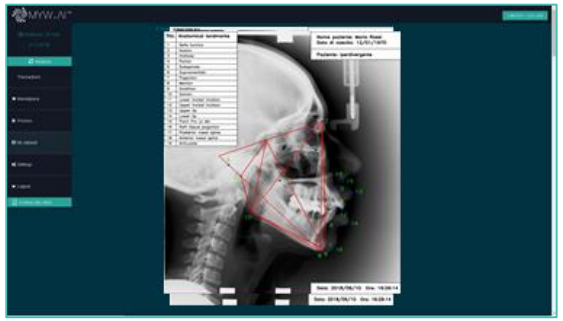






Hey Manager

TRUST
LINEAGE
INTEGRITY
ORIGIN
DATA



MYW.AI™
Quality Manager

IOT 4 INDUSTRY

HEY MYWAI

Hey my way

Please load my production alerts

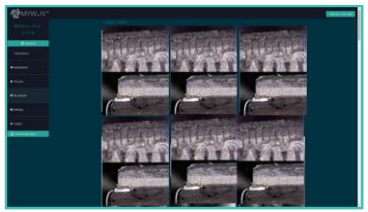
Please train defect class X

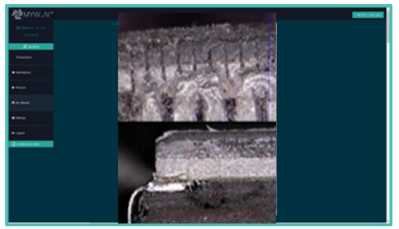
Please classify defect

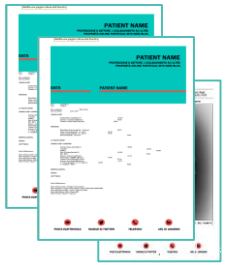
Product X has defectType A

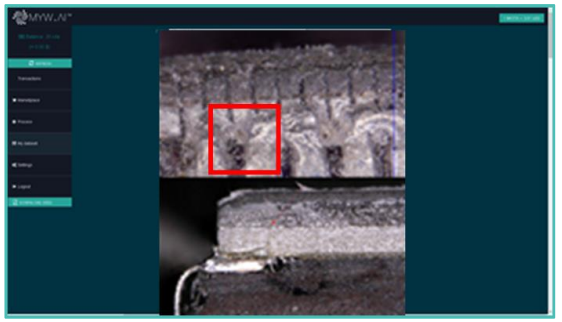
Please publish report

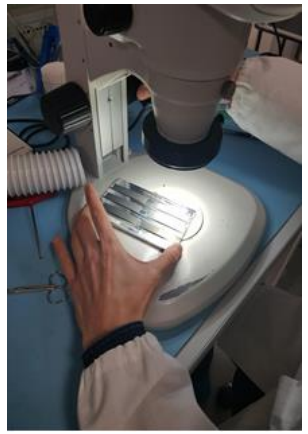
Hey Manager











MYW.AI™
Edge Intelligence for All

knowhedge
your edge to know how

Fabrizio Cardinali (Kowhedge CEO)
BA & Investor

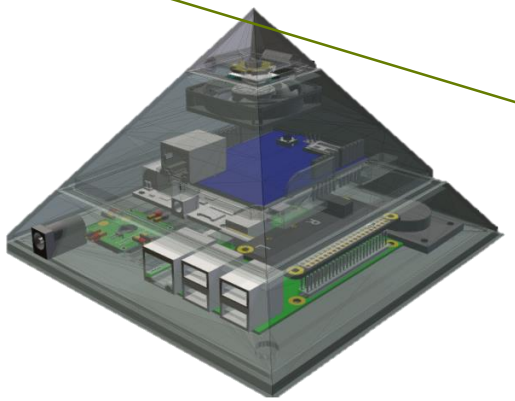
Giancarlo Bo
(former Giunti Labs)
SOA & Microservices

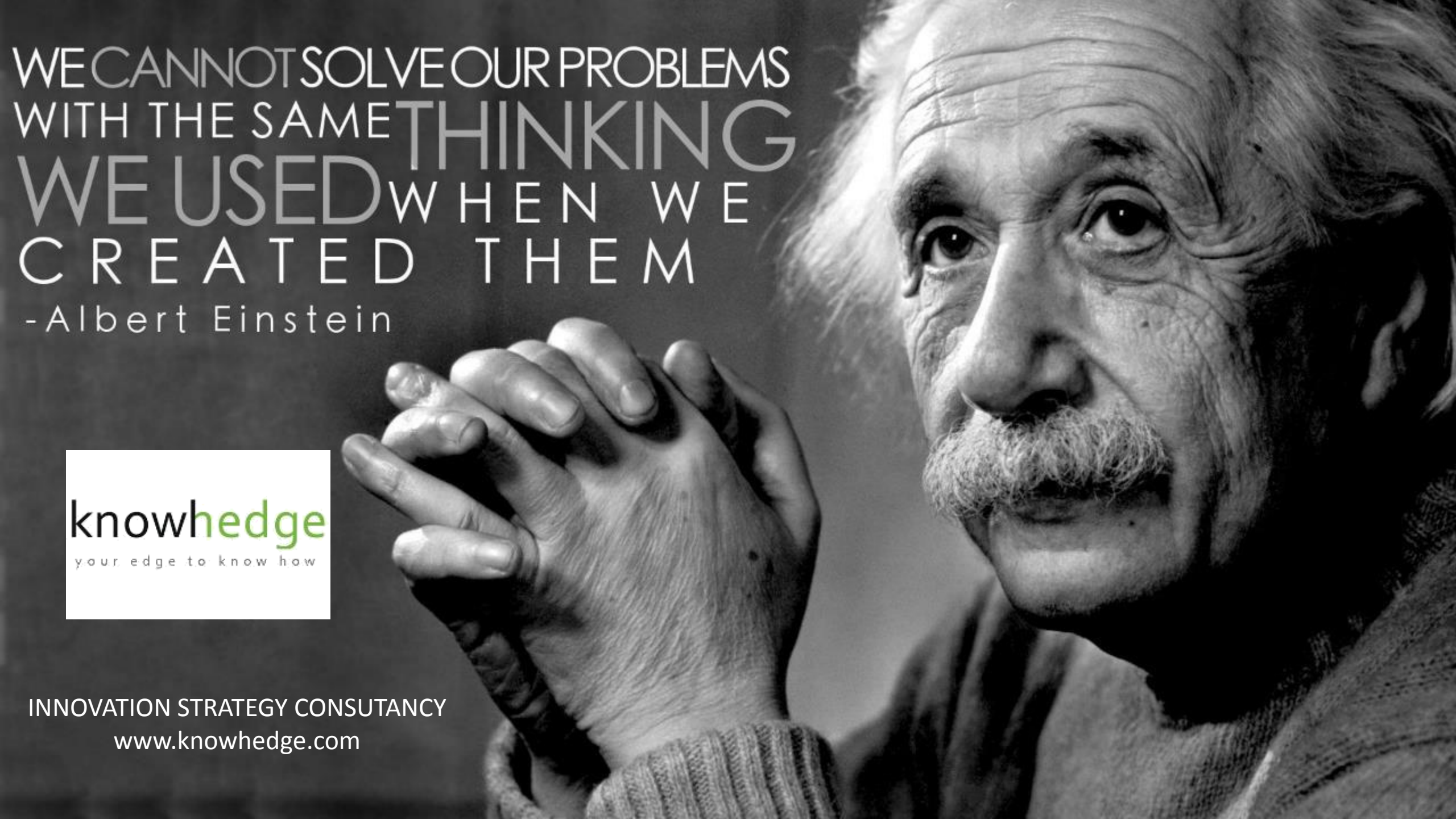
Luca Marchese
(former Ericsson)
Neural Networks

Giorgio Cantarini
(AI student)

Marco Migliorati
(BioEngineer)

Andrea DeCamilli
Blockchain, DLT & IOTA





knowhedge

your edge to know how

INNOVATION STRATEGY CONSUTANCY

www.knowhedge.com