Alliance for IoT
and Edge Computing
Innovation

Online • 8 May 2024

Presentation of the Report on DLT-IoT-AI Technological Convergence

Agenda

AICTI

Agenda

15:00h **Opening and Welcome**
Damir Filipovic, AIOTI Secretary General
Introduction of the AIOTI FG DLT & Web3
Tom De Block, AIOTI FG DLT & Web3 Chair

15.10h **Presentation of the Report on DLT-IoT Technological Convergence (20 min)**
Alfredo Favenza, AIOTI FG DLT & Web3 Co-Chair, Fondazione LINKS
Silvio Meneguzzo, PhD in Blockchain & DLT, University of Turin – Fondazione LINKS

15.30h **Use Case presentation Examples (20 min)**
Konstantinos Ntafloukas, INLECOM

15.50h **Questions and open discussions (10 min)**

16.00h **Wrap-up and end of Webinar**
Tom De Block, AIOTI FG DLT & Web3 Chair

About AIOTI
FG DLT & Web3

AIOTI

Focus Group DLT and Web3

Chair
Tom De Block
Nearcom

Co-Chair
Alfredo Favenza
Fondazione LINKS

Vision: To represent the DLT aka 'Blockchain' enabling technology. Opening new business models that will allow IoT infrastructures to become trustful and sustainable

Scope: To bring knowledge and awareness, starting with AIOTI verticals. To assist members to work towards deployments

Highlights

Relevant facts

54 member organisations

71 participants

Main achievements

Deliverables	Collaborations	Events
• Updated AIOTI Testbeds catalogue with over 60 testbeds • Updated AIOTI Testbeds methodology • DLT PET methodology • Report on DLT-IoT Technological Convergence R2	• Innovation Ecosystems • INATBA • CCC	• Webinar promoting convergence paper • AIOTI Signature Event 2023 • Two successful hackathons

Introduction and Overview of the Report

Alfredo Favenza
AIOTI FG DLT & Web3 Co-Chair, Fondazione LINKS

AIOTI

Background

- In **2022 AIOTI** released the «**Report on DLT-IoT Convergence"**, led by LINKS Foundation with the collaboration of members from the AIOTI DLT Interest Group including Nearcom, Vicomtech, Nydor System Technologies, Verses, BovLabs, VizLore Labs, Blue Future Organisation, BEIA)
- **2023.** The AIOTI established a roadmap for the evolution of the Technology Convergence Topic to extend the analysis to the opportunity lying at the intersection of three technology stack, IoT, DLT and AI.
- By **2024**, the AIOTI unveiled the "**Report on DLT-IoT-AI Convergence.**" This effort, continued under the leadership of the LINKS Foundation, emphasized the significant potential for new services and applications. These innovations aim to fully leverage the combined capabilities of these three transformative technologies.

Webinar's Objectives

- **Introducing the three-technology stack**, including IoT, DLT and the new AI stack.
- **Explore areas and topics of convergence** lying at the bilateral intersection of IoT-DLT and AI-DLT stacks through the convergence matrix.
- **Explore the trilateral intersections between IoT-DLT-AI stacks** through the convergence prism, to discover promising areas and topics of convergence where DLT IoT and AI can help solving respective challenges.

Technology Stacks

Silvio Meneguzzo, PhD in Blockchain & DLT, University of Turin – Fondazione LINKS

IoT technology stack

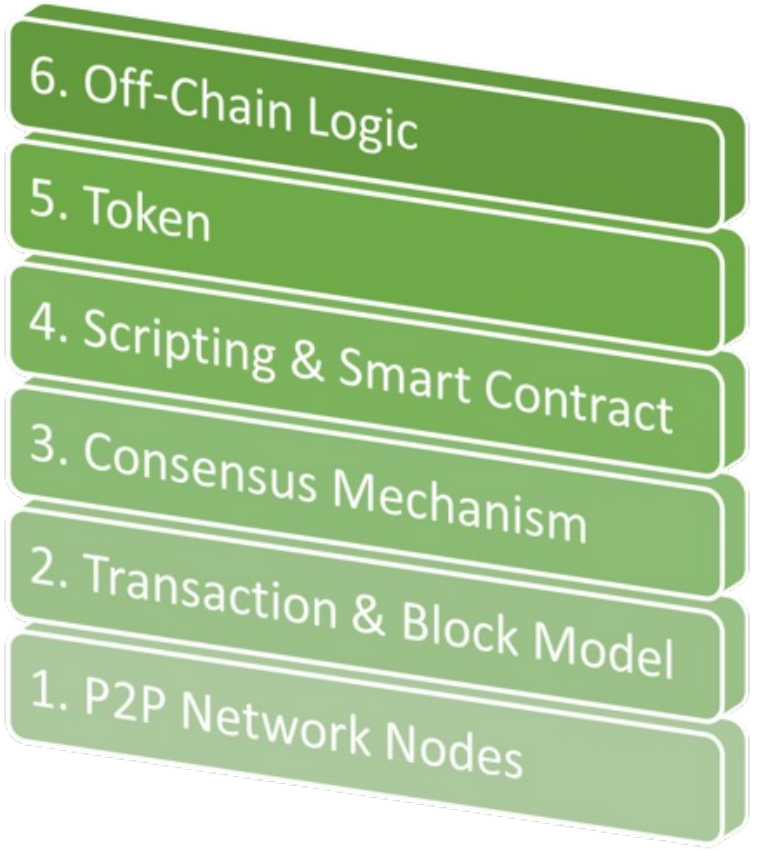
- **Sensors and Actuators.** Devices with analogue or digital interfaces that detect or ac upon physical conditions. Typically, these sensors are connected through various bu technologies like I2C, RS232, and SPI to facilitate data transmission
- **Hub Device.** A central device that collects data from sensors and actuators, creatin a bridge to the IoT Gateway. It includes two bidirectional communication interface one for sensors and another wireless interface for connectivity with the IoT Gateway.
- **Gateway.** Serves as the intermediary that connects devices on the field (like in home or factories) to cloud-based systems where data is stored and processed. It suppor local processing and storage capabilities, providing a crucial link for both online an offline services.
- **Computation** Servers. Dedicated systems designed to process large datasets an perform complex computations, such as machine learning algorithms. These serve are usually part of cloud platforms and communicate through TCP/IP protocols.
- **Services.** This layer manages the interaction between computation servers and user facilitating access to processed data through web technologies and mobile devic visualization. It ensures quality of service and considers the temporal validity of data.

AIOTI

Ref: «Report on DLT-IoT Convergence», AITOI, 2022

DLT technology stack

- **P2P Network of Nodes.** A decentralized network where peers with equal status maintain and communicate a ledger copy via the internet.
- **Transaction & Block Models.** Data structures within the distributed ledger; a secure chain of blocks containing transactions.
- **Consensus Mechanism.** Protocol ensuring rights and communication for verification, consensus, and authentication within the network.
- **Scripting & Smart Contract (On-chain Logic).** Code within the ledger for executing transactions and managing digital assets through smart contracts.
- **Token.** Digital representations of assets, either fungible or non-fungible, used for company shares or voting power.
- **Off-chain Logic.** Data and computations conducted outside the chain, using off-chain storage for privacy and on-chain for public data; oracles link external information to the ledger.

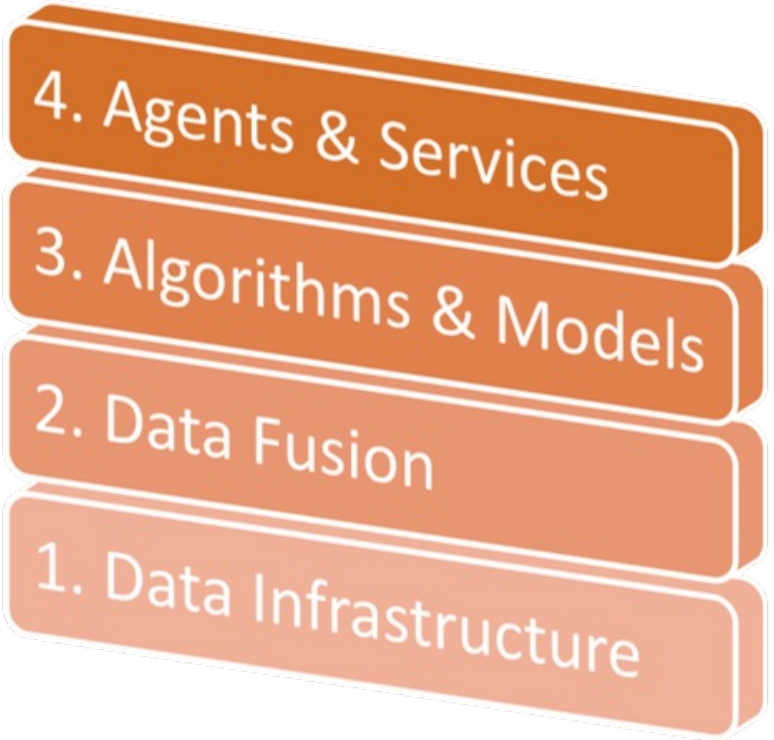


AITOI

Ref: «Report on DLT-IoT Convergence», AITOI, 2022

AI technology stack

- **Data Infrastructure.** Consists of the hardware resources, both physical and virtualized, used for storing and processing data, such as Hadoop systems, and computing resources like VMs, CPUs, and GPUs.
- **Data Fusion.** Software tools that interact with storage and processing resources to perform tasks like cleaning and labelling raw data, ensuring the preparation of high-quality datasets for machine learning models.
- **Algorithms and Models.** Comprise the tools and libraries used to train models on datasets, involving feature selection and various training methodologies like supervised and unsupervised learning, with tools such as TensorFlow and Scikit-learn.
- **Agents and services.** Refer to the applications that use model outcomes to conduct data analysis tasks including natural language processing, image processing, and various prediction and classification activities.

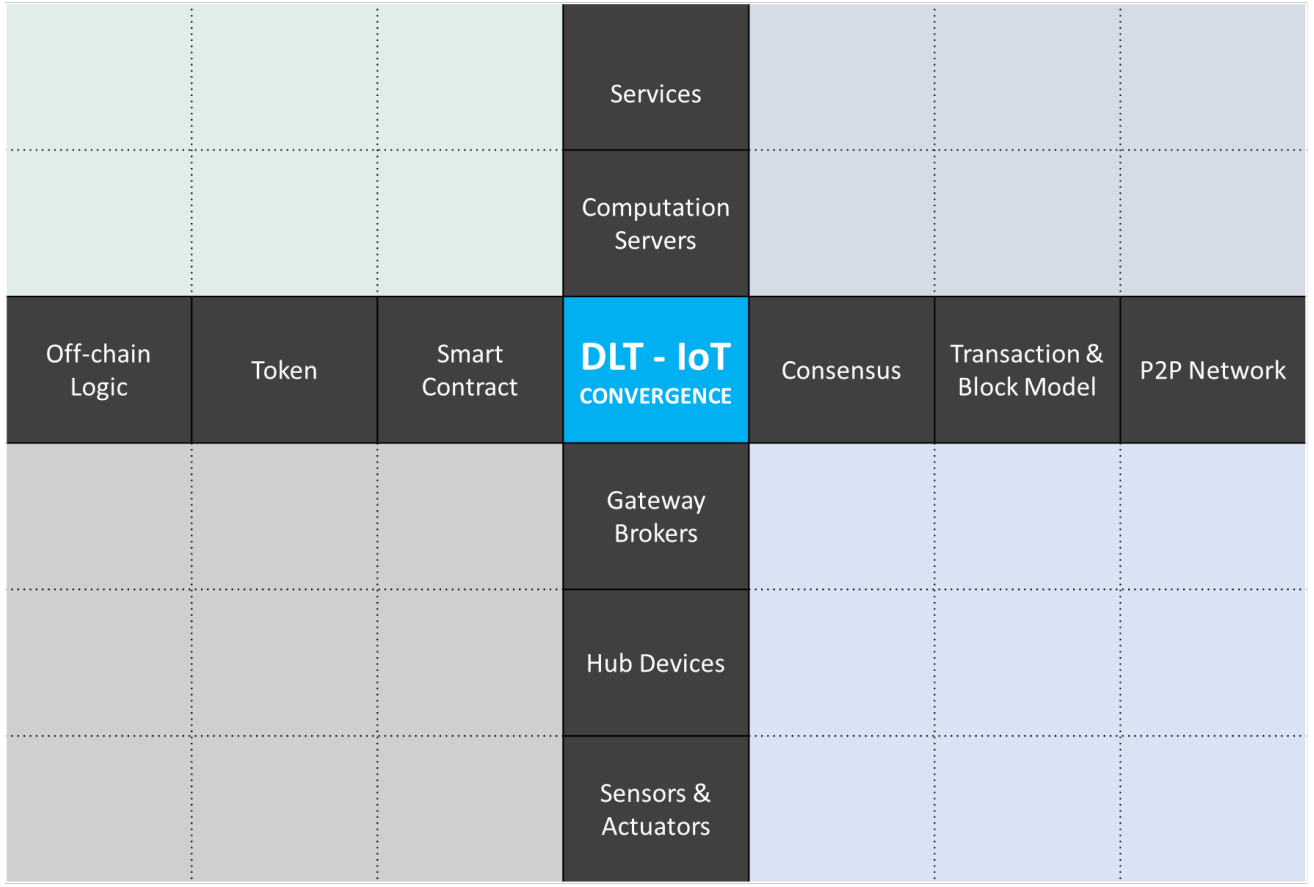


Convergence Matrix

Silvio Meneguzzo, PhD in Blockchain & DLT, University of Turin – Fondazione LINKS

DLT-IoT Convergence Matrix

- **Report on DLT-IoT Convergence** (AIOTI, 2022)
- Highlights the possible **areas and topics of convergence** lying at the **intersection of the building blocks** of the DLT and the IoT stacks.



DLT-IoT Convergence Areas

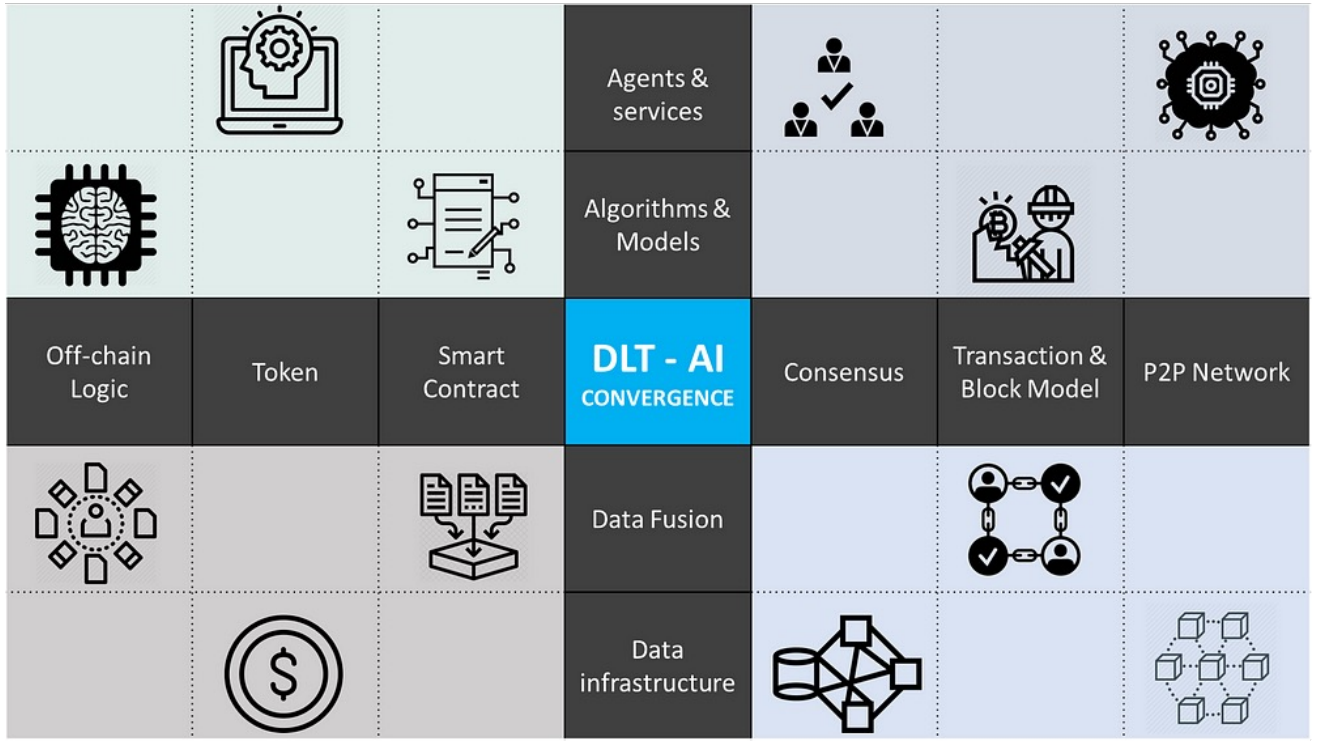
- Decentralization
- Interoperability
- Scalability
- Secure Data Exchange
- IoT network security and Identity management
- Autonomous M2M interaction
- Data monetization
- Micro-payments
- Voting & Negotiation

<table>
<tr><td></td><td>Data Monetization</td><td></td><td>Services</td><td></td><td>Micro-payments</td><td></td></tr>
<tr><td></td><td></td><td></td><td>Computation Servers</td><td></td><td>Secure Data Exchange</td><td>Decentralization</td></tr>
<tr><td>Off-chain Logic</td><td>Token</td><td>Smart Contract</td><td>DLT - IoT
CONVERGENCE</td><td>Consensus</td><td>Transactions & block model</td><td>P2P Network</td></tr>
<tr><td rowspan="2"></td><td rowspan="2">Securing Access management with access token</td><td>IoT Network Management</td><td rowspan="2">Gateway Brokers</td><td rowspan="2"></td><td rowspan="2">Secure Data Exchange</td><td rowspan="2"></td></tr>
<tr><td>Securing IoT with fingerprinting</td></tr>
<tr><td>Scalability</td><td rowspan="5">Autonomous identity</td><td>IoT network Management</td><td rowspan="5">Hub Devices</td><td>Decentralization</td><td rowspan="2">Scalability</td><td>Scalability</td></tr>
<tr><td rowspan="4">Interoperability</td><td>Autonomous Identity Management</td><td rowspan="4">Interoperability</td><td rowspan="3">Decentralization</td></tr>
<tr><td>Autonomous M2M interaction</td><td rowspan="2">Secure Data Exchange</td></tr>
<tr><td>Securing IoT with fingerprinting</td></tr>
<tr><td></td><td></td><td>Automated and Secure Firmware update</td><td>Sensors & Actuators</td><td></td><td>Automated and secure Firmware update</td><td>Decentralization</td></tr>
</table>

Ref: «Report on DLT-IoT Convergence», AITOI, 2022

DLT-AI Convergence Matrix

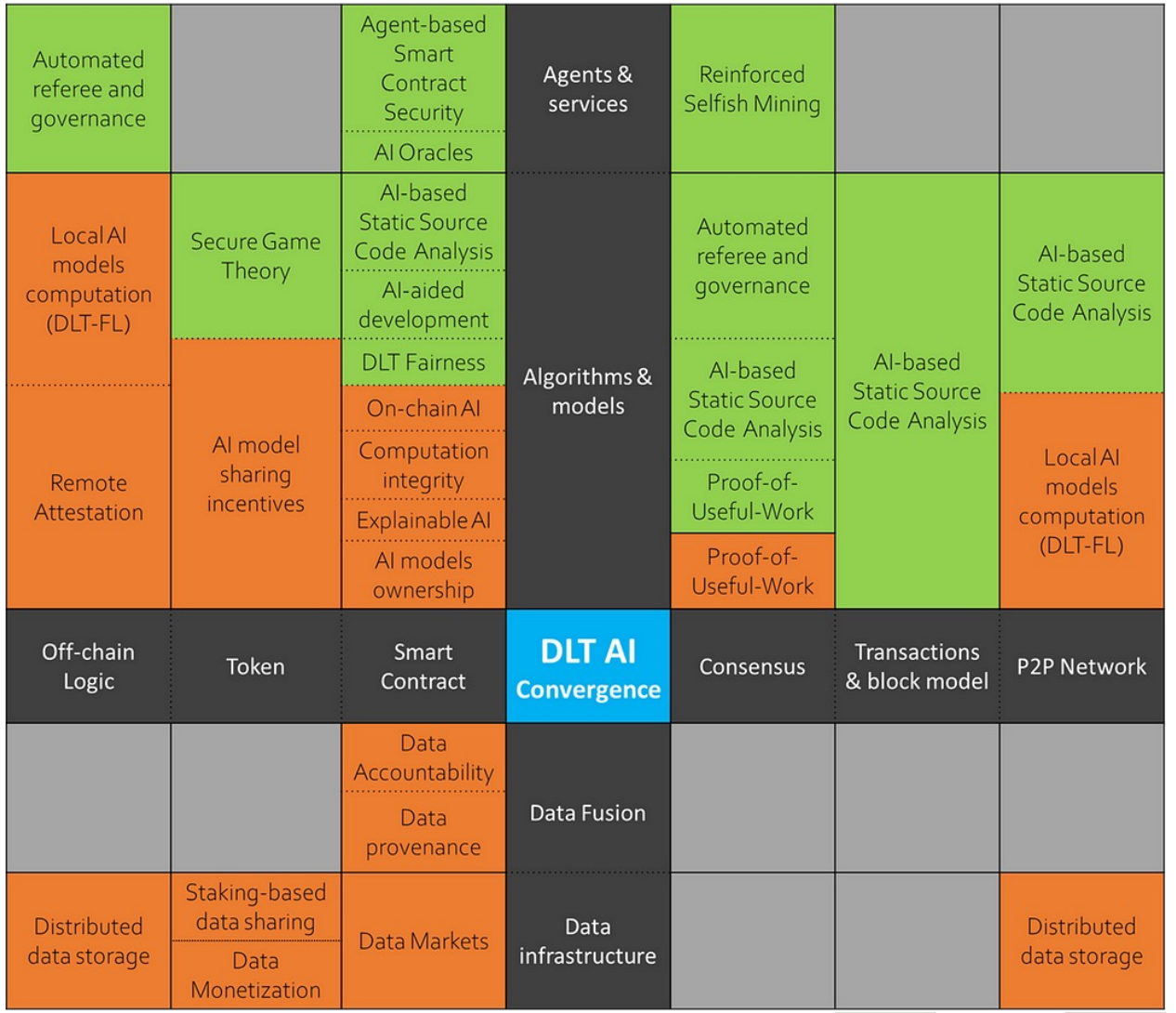
- Highlights the possible **areas and topics of convergence** lying at the **intersection of the building blocks** of the DLT and the AI stacks.



DLT-AI Convergence Areas

DLT -> AI

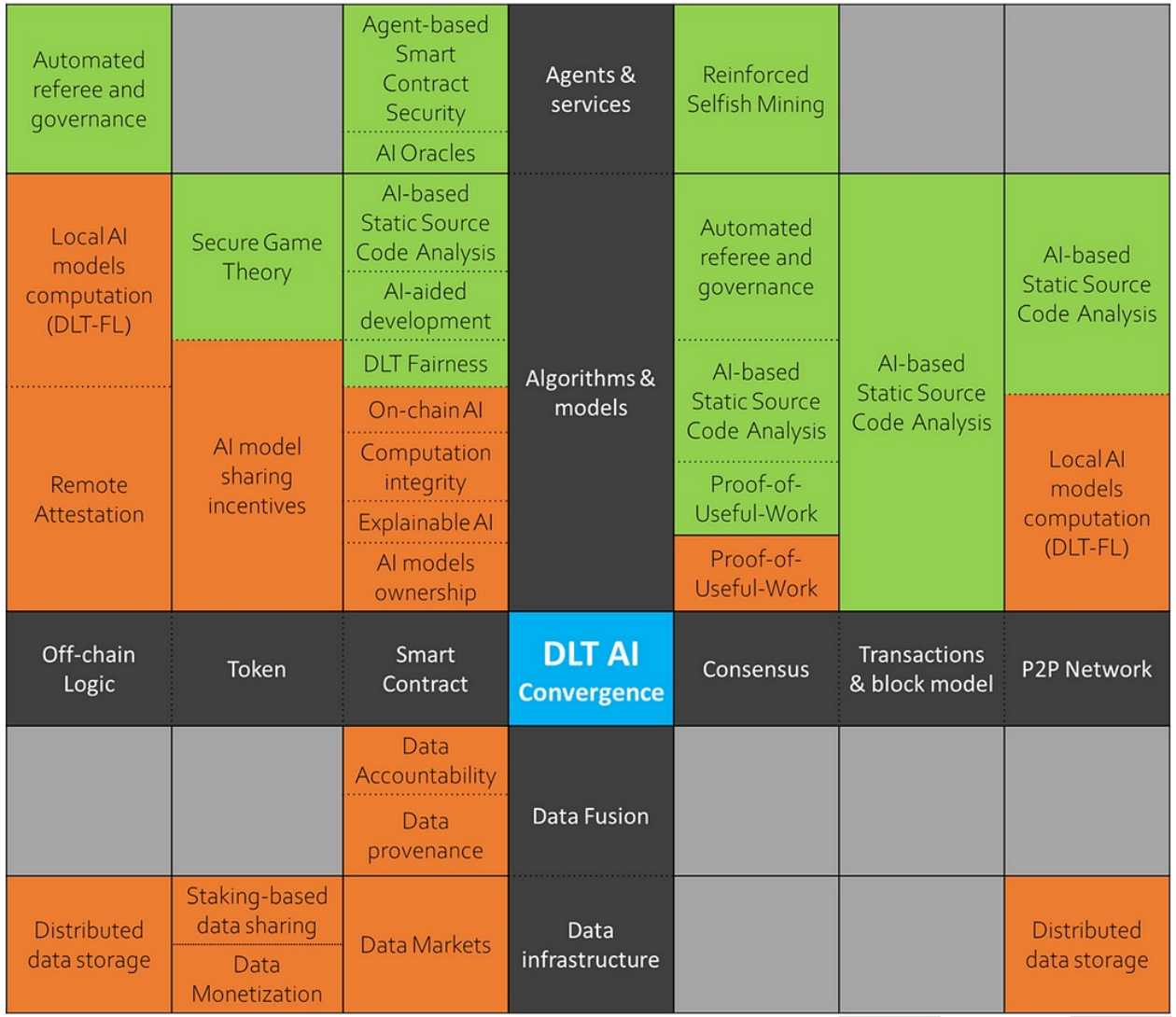
- AI models sharing incentives
- On-chain AI
- Data accountability & data provenance
- Remote attestation on Trusted Execution Environments
- Computational integrity
- DLT-based federated learning for AI models computation
- Data markets and data monetization
- AI Pipeline explainability, traceability and audibility
- Staking-based data sharing
- Distributed data storage
- AI models ownership
- Proof-of-Useful-Work



DLT-AI Convergence Areas

AI -> DLT

- AI-based Static Source Code Analysis
- Automated Referee and Governance
- Proof-of-Useful-Work
- AI-Aided Development
- DLT Fairness
- Secure Game Theory
- Reinforced Selfish Mining
- Agent-based Smart Contract Security
- AI Oracles



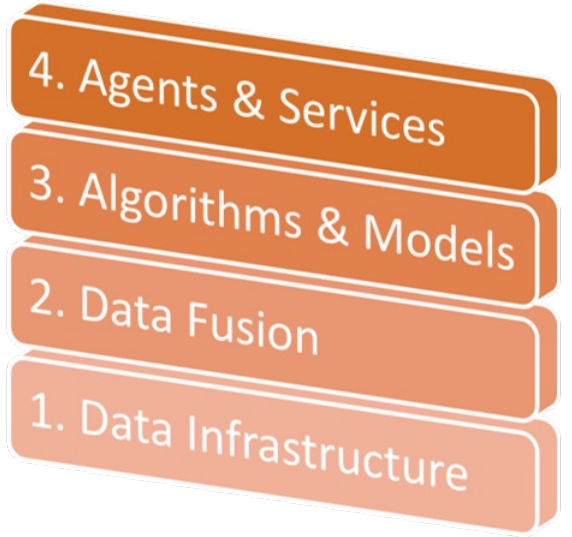
IoT-DLT-AI Convergence Prism

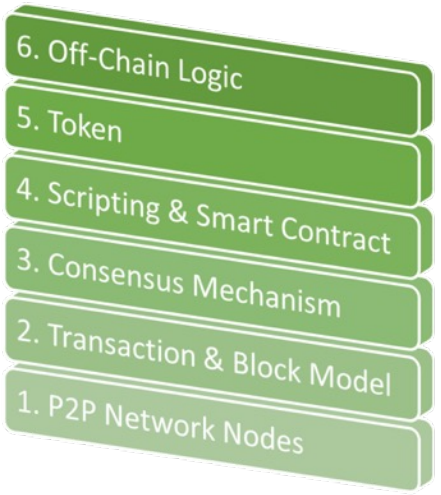
Silvio Meneguzzo, PhD in Blockchain & DLT, University of Turin – Fondazione LINKS

AI@TI

DLT-IOT- AI Convergence Prism

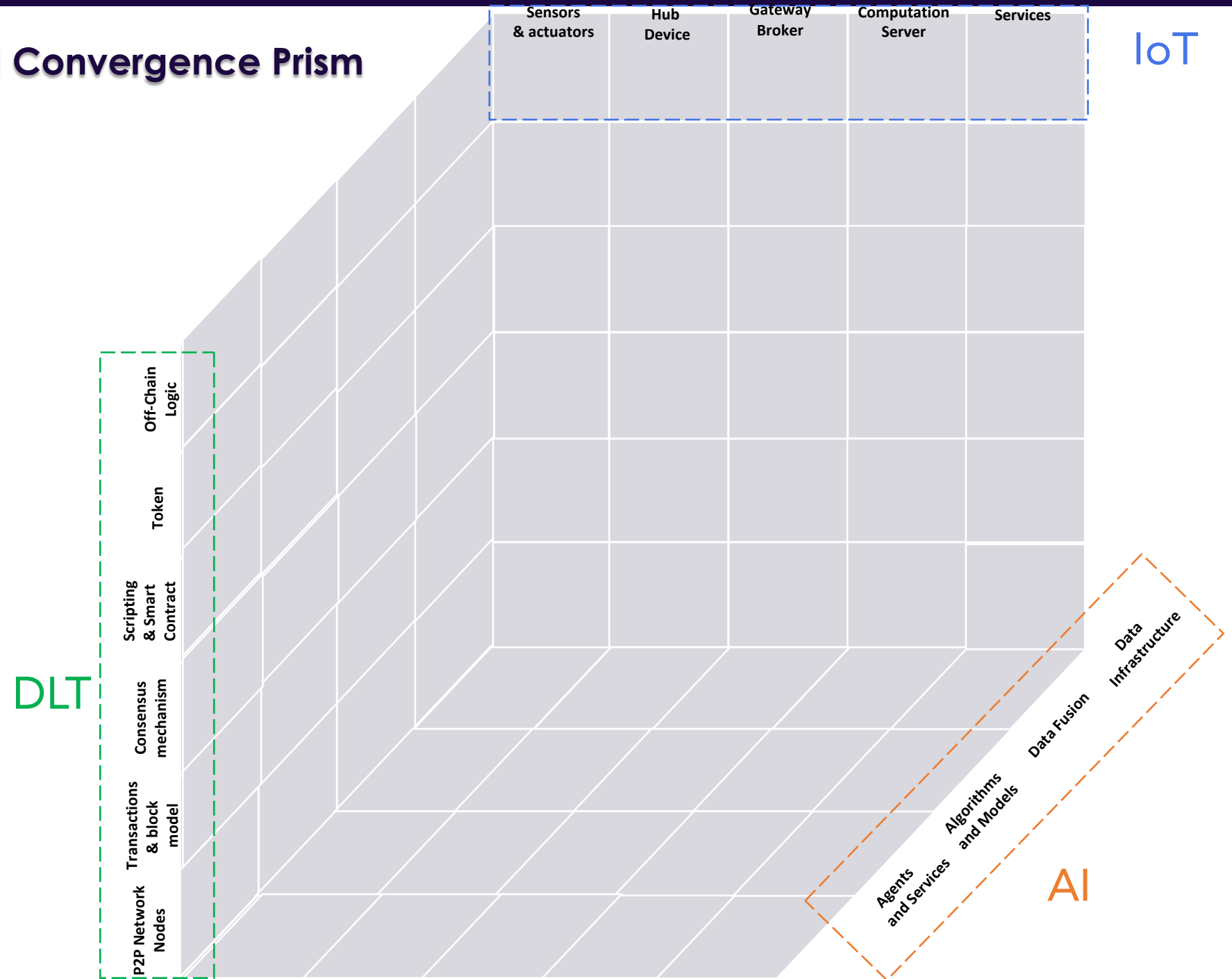
Highlights the possible **areas and topics of convergence** lying at the **intersection of the building blocks** of the DLT, IoT and the AI stacks.





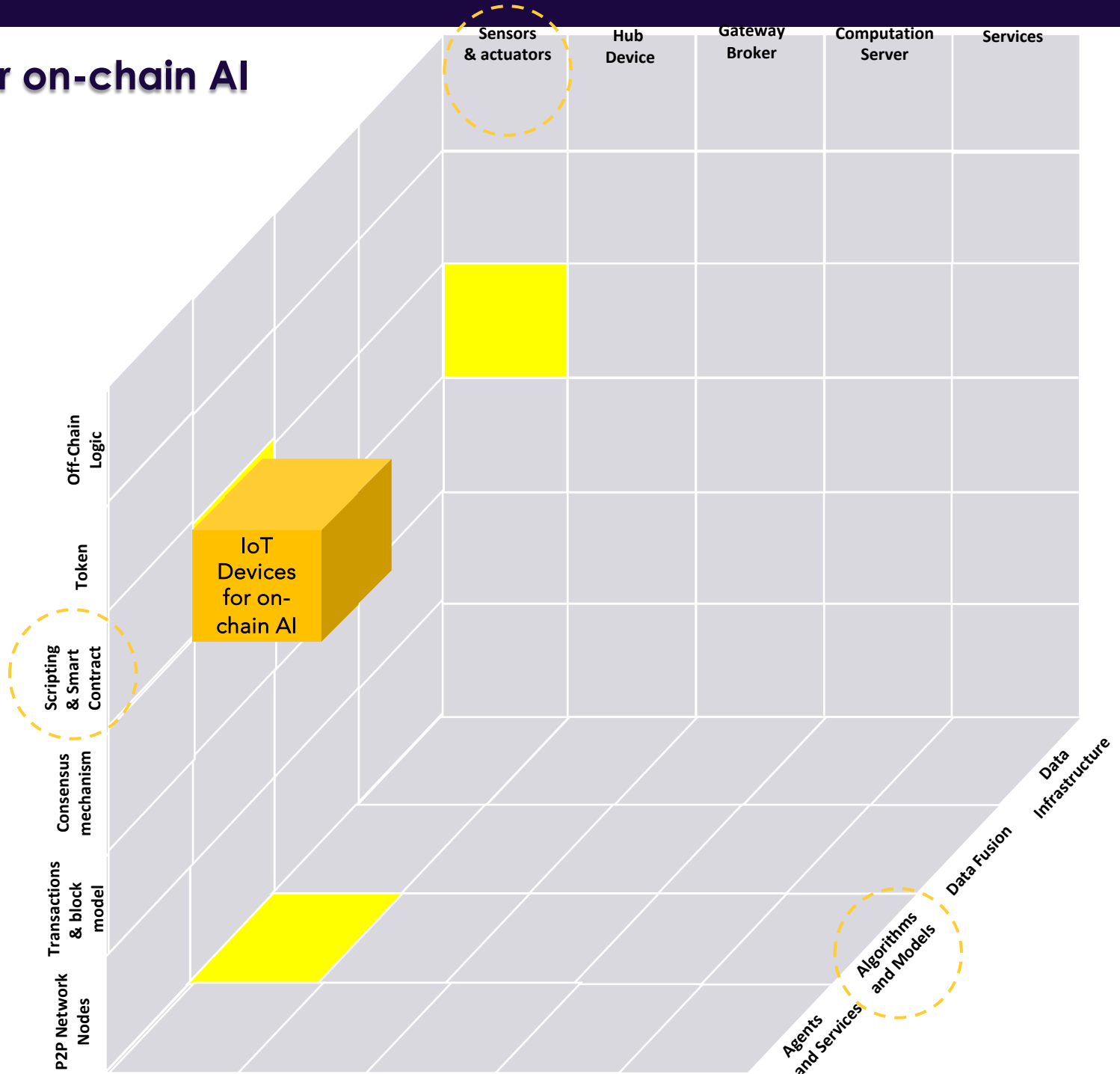
AIOTI

IoT-DLT-AI Convergence Prism



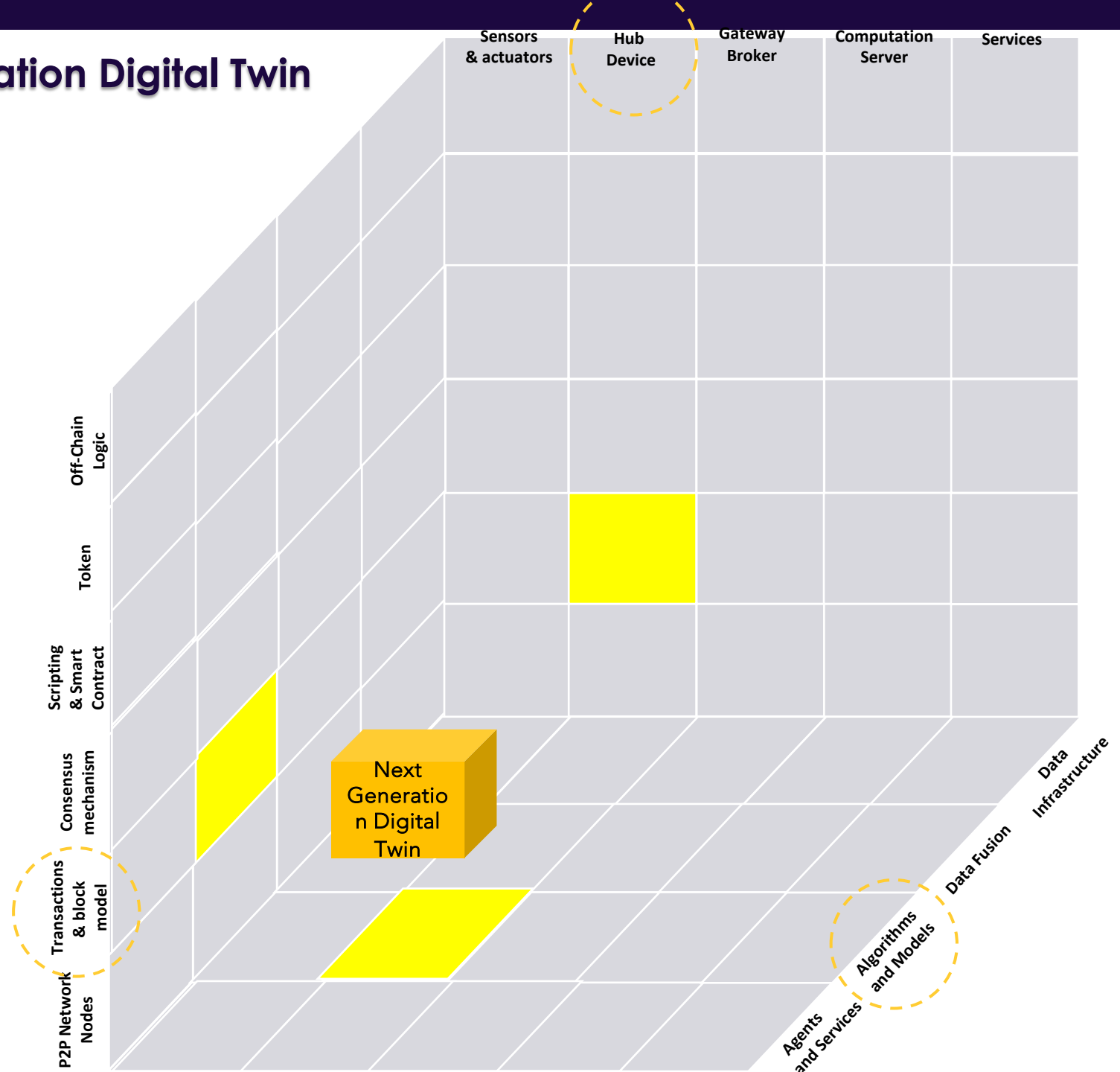
AIOTI

IoT Devices for on-chain AI



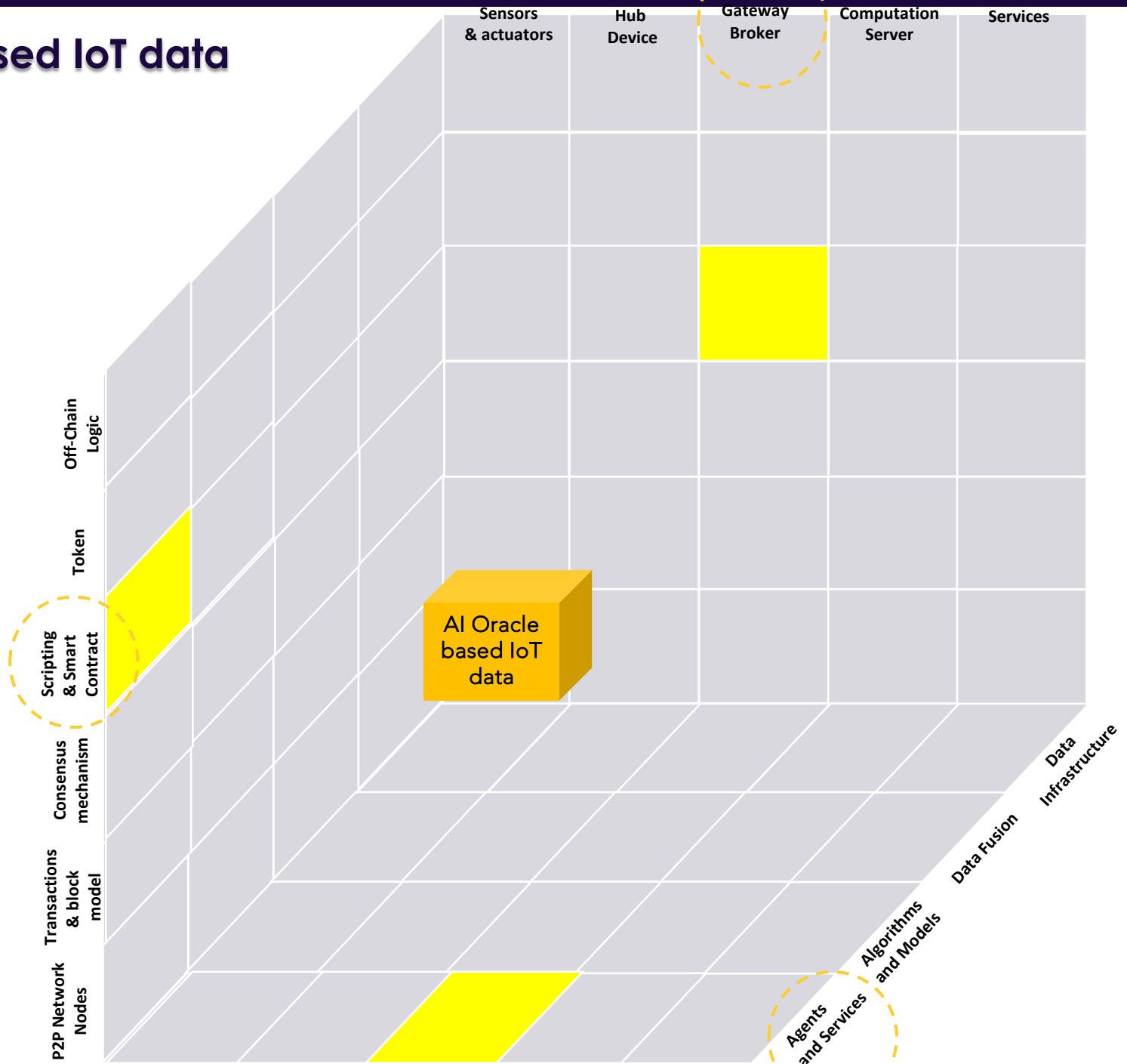
AIOTI

Next Generation Digital Twin



AICTI

AI Oracle based IoT data



AIOTI

Summary of IoT-DLT-AI Convergence Areas

- IoT Devices for on-chain AI
- Remote attestation AI algorithm on Trusted Execution Environment
- Smart Sensor data monetization
- Next Generation Digital Twin
- AI Oracle based IoT data
- AI-driven automatic sensors firmware update
- Supply Chain Transparency and Optimization Platform
- Smart Data Management

Presentation of the Use-Cases

Konstantinos Ntafloukas (Inlecom)

About the Team

inlecom

Enhancing innovation capacity through digital ecosystems
Research. Advancing Technology. Disruptive Business Models

Research & Innovation Consultants.
Established in 1996 with presence in Greece, Belgium, Ireland and the UK

Strong participation in Research Projects. Bringing innovation to industry.

25 ongoing projects, 7 coordinating.
> 40% proposal success rate vs EU <10% average.
> 35 EU-funded completed projects.
> successfully granted patents (80% success rate).

- **Applied ICT and Internet of Things**
- **Transport & Logistics**
- **Food & Circular economy**
- **Security**
- **Energy**
- **Green buildings & Smart Cities**
- **Health**
- **Manufacturing**

Background and Industrial/Scientific Challenges

ERATOSTHENES
(14 Partners - 8 Countries)

IoT industrial/scientific gaps & Focus

- Lack of security visibility
- Lack **of effective information sharing** between organisations and availability of tools to the CERTs/CSIRTs
- **Heterogeneity of IoT devices** extremely challenging to establish a trustworthy environment
- Lack of a **common trust enforcement mechanism and relevant standards**. Available mechanisms address only security and privacy aspects and rely on centralised authorities while remain vulnerable to threats
  - Not that easy in an artificial society such as IoT
  - Important to **quantify "trust" such that it can be understood by the artificial agents**
- **Firmware and security updates are infrequent** and **difficult** or even **impossible**
- **Lack of a transparent identity and privacy framework** to allow the users to maintain full control of their identity and data at the device level
- **Lacking security training and security protocols' adoption for** persons and devices

ERATOSTHENES Summary

Innovation & Technical Outcomes

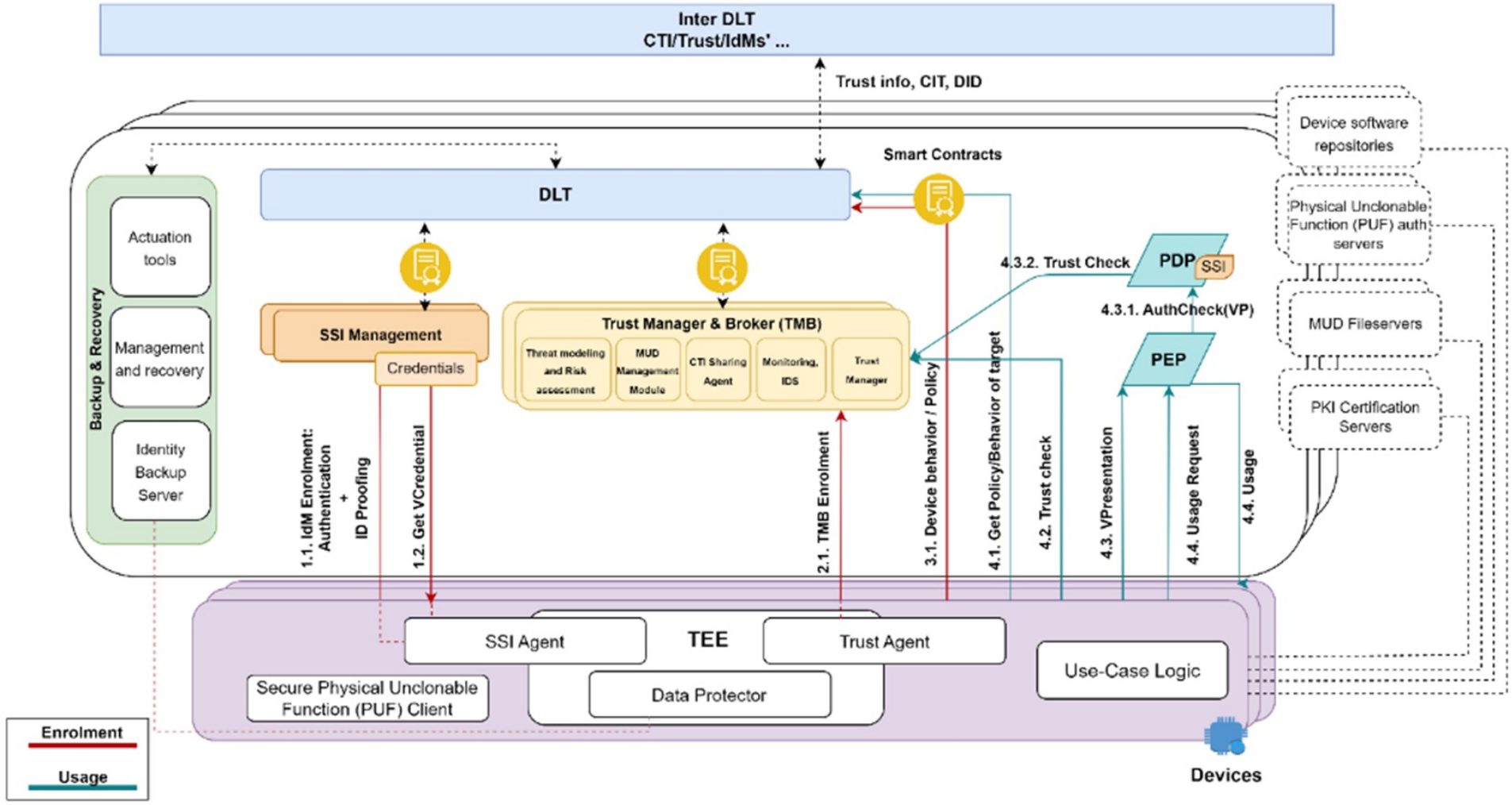
- A distributed, automated, auditable, privacy-respectful, **Trust and Identity Management Framework** to manage the lifecycle of IoT devices
- First-ever enclosure of **cybersecurity features in IoT devices** through deployment of Trust Agents
- **Decentralized identity management** mechanisms
- **Self-encryption/decryption** with an automated recovery process
- **Threat analysis models** based on federated learning Integration of Physical Unclonable Functions in trust framework

ERATOSTHENES Summary

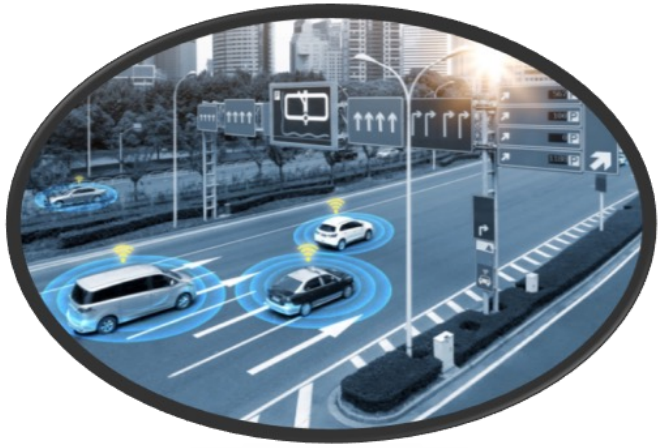
Innovation & Technical Outcomes

- First-ever enclosure of cybersecurity features in IoT devices through deployment of **Trust Agents** and **continuous trust evaluation**
- **Decentralised identity management** mechanisms to conciliate requirements of self-sovereignty and privacy preservation in a distributed/transparent trust model
- **Self-encryption/decryption at device-level** with a whole system **automated recovery** process
- **Threat-analysis models** based on federated learning and edge execution
- **Collaborative IoT threat intelligence** sharing across ledgers to adapt detection/defence mechanisms
- **Integration of Physical Unclonable Functions** in trust framework and distributed ledgers
- Support **enforcement of the NIS directive** information sharing based on inter-ledger technologies

ERATOSTHENES Architecture



Pilots and Use Cases

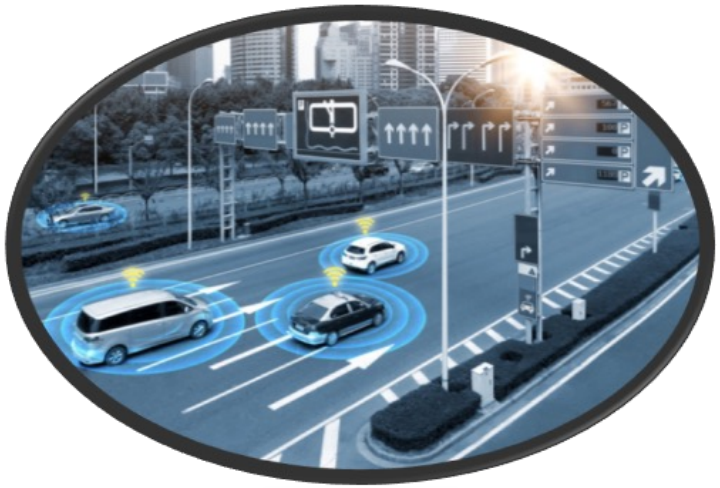


Applus IDIADA

Pilot 1: Connected Vehicles

- Interaction with vehicle (V2V) and road infrastructure (traffic lights).
- Software updates in the vehicle's units.
- Evaluation of the prospective benefits for connected vehicles, that interact both with other vehicles and external roadside elements, such as smart traffic lights.
- These vehicles need to ascertain the trustworthiness of these elements, aiming to prevent potential accidents and safeguard the privacy of the vehicle's driver or owner.

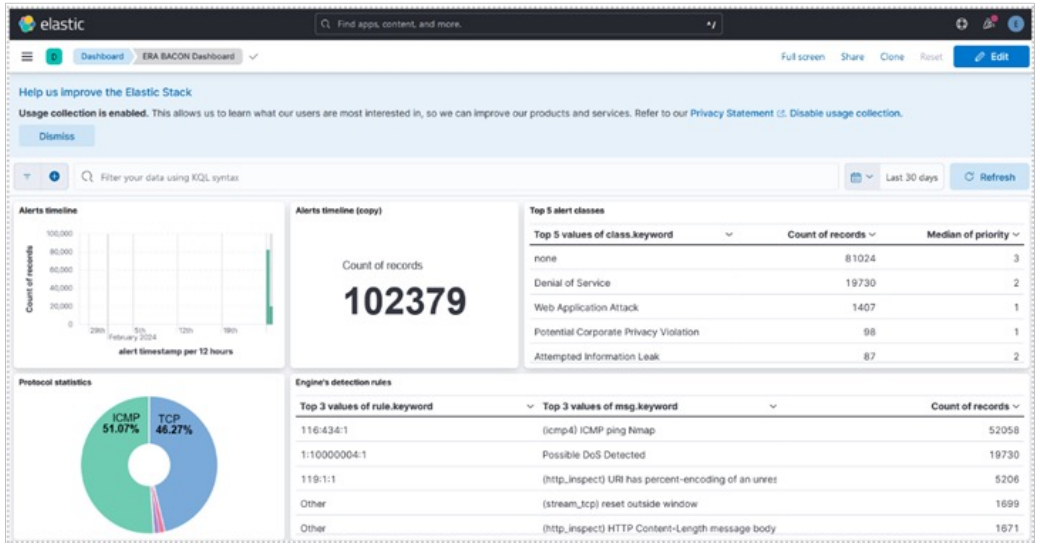
Pilots and Use Cases



Role of the DLT in Pilot 1

- DLT, in this use case uses blockchain technologies to store information that is used by the modules in the ERATOSTHENES network.
- Everything stored in this solution can be verified by members of the network but cannot be modified.

IDS Detection test



Pilots and Use Cases

tell.u

Pilot 2: Smart Health

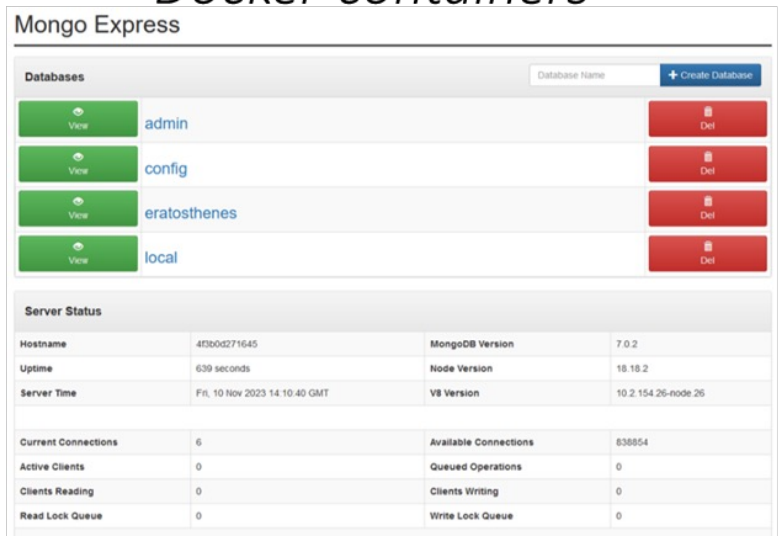
- eHealth Remote Patient monitoring use cases.
- Zero-contact enrolment of users and devices
- Integrate with third-party services.
- Extending the platform with private devices
- Emergency situations
- Continuous monitoring and lifecycle management of the Tellu service

Pilots and Use Cases

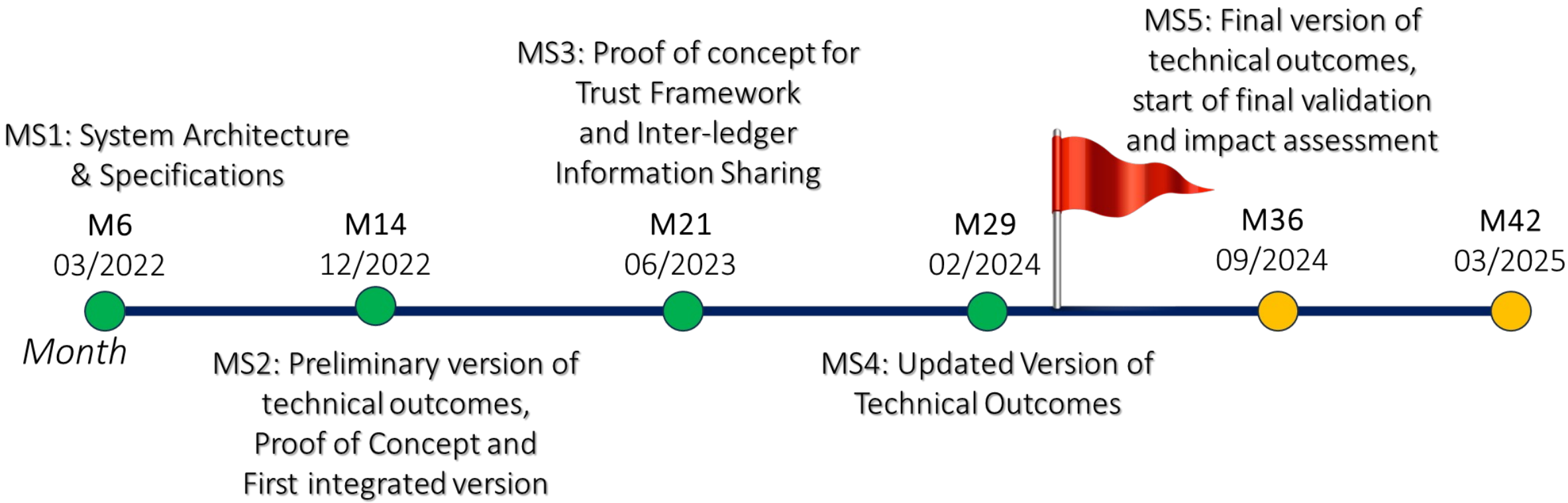
Role of the DLT in Pilot 1

- DLT, in this use case uses blockchain technologies to store information that is used by the modules in the ERATOSTHENES network.
- Everything stored in this solution can be verified by members of the network but cannot be modified.

Trust Manager and Broker component & Docker containers



Technical Milestones



Scientific, Social and Economic Impact

- Reduced number and impact of cybersecurity incidents
- Efficient and low-cost implementation of the NIS Directive and General Data Protection Regulation
- Effective and timely co-operation and information sharing between and within organisations as well as self-recovery
- Availability of comprehensive, resource-efficient, and flexible security analytics and threat intelligence
- Self–recovering, interoperable, scalable, dynamic privacy-respecting identity management schemes
- Better standardisation and automated assessment frameworks for secure networks and systems, allowing better-informed investment decisions related to security and privacy
- Availability and widespread adoption of distributed, enhanced trust management schemes including people, smart objects
- Availability of user-friendly and trustworthy on-line products, services and business
- A more competitive offering of secure products and services by European providers in the Digital Single Market

Questions from the Audience

Moderated by:
Tom De Block, AIOTI FG DLT and Web3 Chair

Wrap up and end of the Workshop

Tom De Block, AIOTI FG DLT and Web3 Chair

AIOTI

Thank you for listening

Any questions?

You can find us at @AIOTI_EU or email sg@aioti.eu

AIOTI