Alliance for Internet of Things Innovation

Report on DLT-IoT-AI Technological Convergence

Release 2.0

AIOTI FG Distributed Ledger Technologies and Web3

February 2024

Table of Content

Table of Figures

1. Introduction

The integration of disruptive technologies is propelling society into a rapid and unparalleled digital transformation, erasing the boundaries between the physical and digital realms. To effectively navigate the intricacies of this transition, it is essential to possess a thorough understanding of the involved technologies and a comprehensive grasp of how these foundational components can synergize to create innovative platforms and practical applications.

This document is an advancement of the "Report on DLT-IoT Technological Convergence," published in May 2022, which offers the AIOTI's insights on the fusion of the Internet of Things (IoT) and Decentralized Ledger Technologies (DLT). It delves into the potentialities at the nexus of these technologies, aiming to delineate the overlapping layers of their respective tech stacks, thereby pinpointing promising zones for amalgamation and corresponding use case scenarios. The current report aims to further explore the potentialities at the intersection of Artificial Intelligence (AI), Distributed Ledger Technologies (DLTs), and the Internet of Things (IoT).

Our analysis commences with the articulation of three high-level technological stacks, serving as a foundational framework to decode the attributes of the constituent elements. This discourse then progresses to pinpointing domains and themes of significance at the technological intersections (DLT-AI and DTL-IoT), utilizing a Convergence Matrix. This matrix is designed to establish a unified platform for discussing open research topics and potential application opportunities.

Subsequently, we introduce the concept of the Convergence Prism, a tool designed to highlight opportunities at the tripartite intersection of DLT, IoT, and AI.

The final phase of this report seeks to bridge the theoretical analysis with tangible applications. This is achieved by selecting the most promising topics of convergence and associating them with extant applications, as identified within the AIOTI DLT Test Beds. This approach not only underscores the practical implications of our findings but also provides a tangible link to real-world implementations.

2. DLT Stack

A distributed ledger is an append-only store of distributed transactions across many nodes in a network, which provides auditing and ensuring long-lasting integrity. Therefore, a blockchain is a DLT implementation. It is structured into a linked list of blocks of ordered transactions, both cryptographically signed and secure, that operates without a central (trusted) authority in an adversarial environment[1,2].

Different solutions of a DLT stack have been proposed by both the academic world and the industry. These visions mainly focus on creating DLT stacks from a technological perspective, where modules, protocols, and solutions are grouped in broad layers (e.g., infrastructure, network, applications). For example, studies on such technological stacks have been proposed by Deloitte[3] and Outlier Ventures[4]. Our main goal differs from those practical solutions; we mainly focused on a stack in which each layer represents an irreplaceable building block of a modern DLT solution. A similar, more straightforward and less intuitive solution has been proposed by Radix[5].

Indeed, our vision of the DLT stack arises from the abstraction of the common traits of the different possible implementations of the DLT. As shown in **Error! Reference source not found.**, the six levels are arranged to include the needs of the complex solutions for diverse contexts, such as public or private deployments, various levels of I/O accessibility to the ledger and role-based permissions, and finding a balance for the trilemma among scalability, security, and decentralization.

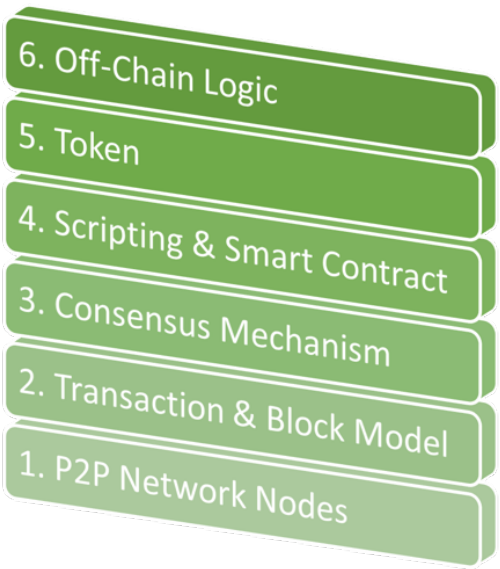


Figure 1. ***DLT Stack***

[1] X. Xiwei, I. Weber, and, M. Staples, (2018), "Architecture for Blockchain Applications", Blockchain Architecture Design, 14–58.

[2] M. Rauchs, A. Glidden, B. Gordon, G. C. Pieters, M. Recanatini, F. Rostand, K. Vagneur, and B. Zheng Zhang, "Distributed Ledger Technology Systems: A Conceptual Framework", 2019.

[3] Deloitte, "Blockchain Technology Stack", 2017.

[4] Outlier Ventures, "The Convergence Stack", 2019.

[5] Radix, "Introduction to DLT Stack", 2019.

P2P Network of Nodes. A network of physical or virtual machines (peers) maintaining a local copy of the ledger communicating over the internet (TCP/IP protocol). Peers are equally privileged, equipotent participants in the application. They share resources without a centralized administrative system or control in an untrusted environment[6].

Transaction & Block Models. The representation of the distributed ledger data structure is replicated across several nodes on the P2P network. Regardless of transactional taxonomy and block-level characteristics, we assume that the model is a cryptographically secure linked list of blocks where each block contains an ordered list of transactions.

Consensus Mechanism. A network protocol that defines rights, responsibilities, and means of communication, verification, validation, and consensus across the nodes in the network. This layer includes ensuring authorization and authentication of new transactions, appending new blocks, incentive mechanisms (if needed), and similar aspects[7]. A number of consensus mechanisms have been designed for blockchains, which include Proof of Work (PoW), Prof of State (PoS), Delegated Proof of State (DPoS), Proof of Elapsed Time (PoET), Practical Byzantine Fault Tolerance (PBFT), Directed Acyclic Graph (DAG), Proof of Authority (PoA), Tendermint, Ripple, Scalable Byzantine Consensus Protocol (SCP), Proof of Bandwidth (PoB), Proof-of-Importance (PoI), Proof of Burn, and Proof of Capacity[8] .

Scripting & Smart Contract (On-chain Logic). Smart contracts are programs (code) deployed as data in the ledger and executed throughout sending transactions to the network. Smart contracts can hold and transfer digital assets managed by the DLT and can invoke other smart contracts. Smart contract code is deterministic and immutable once deployed. This layer also includes not Turing-complete scripting systems for transactions (e.g., Bitcoin Script).

Token. Tokens allow to digitally represent (tokenize) fungible (i.e., money) and non-fungible (i.e., work of arts) assets. The tokens can be used to represent shares in a company, the right to benefit from future earnings, grant voice power for voting systems, uniquely represent real-world assets, and many others. The tokens can be created and exchanged, usually using smart contracts.

Off-chain Logic. In a DLT-based system, different architectural decisions that must be made regarding which piece of information might be stored on-chain and for what reason. The off-chain data and logic layer includes all parts of the data, and computation kept off-chain. As for the data, usual practices are to store large or private sets of data off-chain (e.g., replicated databases, sidechain, cloud) and to keep hashes, metadata, and small-sized public data on-chain. For logic, due to the "closed-world" logic (i.e., smart contracts can usually only examine state stored on the ledger), to interact with the external world, oracles are invoked to bring the external state into the ledger.

6 Antal, C.; Cioara, T.; Anghel, I.; Antal, M.; Salomie, I. Distributed Ledger Technology Review and Decentralized Applications Development Guidelines. Future Internet 2021, 13, 62.

7 Huaqun G., Xingjie Y., A survey on blockchain technology and its security, Blockchain: Research and Applications, Volume 3, Issue 2, 2022, 100067, ISSN 2096-7209.

8 Huaqun G., Xingjie Y., A survey on blockchain technology and its security, Blockchain: Research and Applications, Volume 3, Issue 2, 2022, 100067, ISSN 2096-7209

3. IoT Stack

Five levels have been proposed to cover the different abstraction levels from the field/edge to the internet/cloud, being able to deal with almost any technical architecture and environments, using public/private Clouds or plain traditional services. Communications are not listed in this layer concept because they play a transversal role connecting all levels of the stack.

Figure 2. IoT Stack

Sensors and Actuators. Sensors and Actuators are elements exposing either an analogue Interface or a digital Interface[9]. Most sensors are coupled with an embedded hub device in which case an internal bus technology is used to link both systems, such as I2C, RS232, RS485, SPI, SDI 12, 20mA etc. In a wired communications environment, no logical security provision is really necessary. On these cases the usage of physical devices such as an SCT-013 sensor can be used to tap the data line. Proper jamming protection avoiding wrong measure, and physical protection should be considered.

Hub Device. A Hub Device enables the collection of data through a multitude of standards and configurations. It creates a bridge between the IoT Gateway and the sensors and actuators[10]. The Hub device presents two Communication Interfaces (both bidirectional): one towards sensors (usually a wired analogue connection or a wired digital protocol as the ones mentioned previously) and a second wireless one towards the IoT Gateway. The goal of this devices is to group several sensors/actuators in a first level of processing power and can include different devices as mobile phones, PLCs, IoT platforms, etc. Computation at this level can be said that is happening on the edge. This second communication interface towards the gateway can be based either on ISM band network protocols (868MHz and 2.4GHz for Europe) such as LORA, 6LoWPan, Thread, Zigbee etc or mobile data (4G, NBIOT etc), or Low Earth Orbit Satellite Networks.

9 S. Moyer, "IoT Sensors and Actuators," in IEEE Internet of Things Magazine, vol. 2, no. 3, pp. 10-10, September 2019, doi: 10.1109/MIOT.2019.8950961.

10 Mahmoud Ammar, Giovanni Russello, Bruno Crispo, Internet of Things: A survey on the security of IoT frameworks, Journal of Information Security and Applications, Volume 38, 2018, Pages 8-27, ISSN 2214-2126.

Security is very important between Hub and Gateway and should cover not only data and commands transmissions but also OTA firmware updates of the Hub. DTLS is one possible example. Overall, the secure authentication and enrolment of devices in a service network is a really hot topic of cybersecurity, the more powerful of them should take into account the capacity of secure software update and EDR/anti-malware, as a complement to Gateway services.

Gateway. An IoT Gateway provides the means to bridge the gap between devices in the field (factory floor, home, etc.), the (corporative network, frequently in the) Cloud, where data is collected, stored and manipulated by enterprise applications, and the user equipment (smart phones, tablets etc.)[11]. The IoT Gateway, provides a communication link between the field and the network and can also offer local processing and storage capabilities to provide offline services and if required real time control over the devices in the field. In summary an IoT Gateway provides services covering:

- Data Management,
- Device Interfaces and Protocols,
- Algorithms and processing,
- QoS and collision management,
- Data Security and
- Firewall and Device Security.

This type of system usually doesn't involve long term storage or computationally intensive analysis, but stream or flow activities that must be performed as soon as data is gathered. The main difference between the lower level hubs, is that this level focuses on the aggregation of multimodal information received from several physical specialized devices, in a semantic second level of integration. Open source examples of such semantic tools include FIWARE's ORION and SCORPIO.

To achieve sustainable interoperability on the Internet of Things ecosystem today there are two dominant architectures for data exchange protocols (mostly between Gateways and Cloud): bus-based (DDS, REST, XMPP) and broker based (AMPQ, CoAP, MQTT, JMI). These protocols can also be classified as message-centric (AMQP, MQTT, JMS, REST) or data-centric (DDS, CoAP, XMPP). In order to use the full potential of IoT, interconnected devices must exhibit energy efficiency and thus communicate using lightweight protocols that don't require extensive CPU resources. C, Java, Python and some scripting languages are the preferred choices used in IoT applications.

To handle any needed protocol conversion, database storage or decision making (e.g. collision handling), IoT hubs (nodes) use separate IoT gateways in order to supplement the low-intelligence within the IoT hub. The gateway is responsible to control the access of internet operators and the data, firmware and fingerprinting of the devices.

11 Gunjan Beniwal, Anita Singhrova,"A systematic literature review on IoT gateways", Journal of King Saud University - Computer and Information Sciences, 2021, ISSN 1319-1578.

Computation servers. These types of system are designed to deal with Big Data (store and manage historical data) and provide complex computations on them, like Machine Learning algorithms. Particular architectures can be devoted to only one of these functions or all of them[12]. The amount of processing power expected at this level corresponds to CPD clustering systems or more frequently Cloud platforms. Communications between the gateway and the computation server is usually done through TCP/IP protocols. At this level we can provide firewalls, IDS, ADS, endpoint security, etc., tagging trustfulness of data, and identity management frameworks play an important role as well. Different authorization schemes are being proposed to deal with the fine-grained level of classification required to provide secure access of data to different users, and applications.

Services. This level covers the interaction between servers and users, representing man-machine interface technologies. Services provide a virtual/direct link between people and data, using infrastructure as a transparent tunnel. Currently the exploitation of information is based on web technologies, and visualization on mobile devices is strongly promoted, drawing a system where mobile devices participate in both end of the chain, as producers and as consumers. Security at this level is related to the identification of users, on one hand, and the protection of data transversing open channels on the other. This level deals with confidentiality of data, probably using the authentication environment, but also user-friendly cyphering frameworks. User rights provision is very important to protect the integrity of the analysed/fused/predicted data/results. Quality of service is a key concept here in the sense of access to processed data, but also taking into account their temporal validity.

12 Maggi Bansal, Inderveer Chana, and Siobhán Clarke. 2020. A Survey on IoT Big Data: Current Status, 13 V's Challenges, and Future Directions. ACM Comput. Surv. 53, 6, Article 131 (November 2021).

4. AI Stack

The Artificial Intelligence (AI) technology stack is a comprehensive framework that underpins the operational ecosystem of AI systems. This stack is integral to understanding and deploying AI solutions effectively, as it encompasses the entire journey from data acquisition and processing to the application of AI models for practical tasks. The AI stack consists of several critical components, each playing a distinct role in transforming raw data into actionable insights. This section delves into these components, elucidating their functions and interconnections within the broader AI landscape.

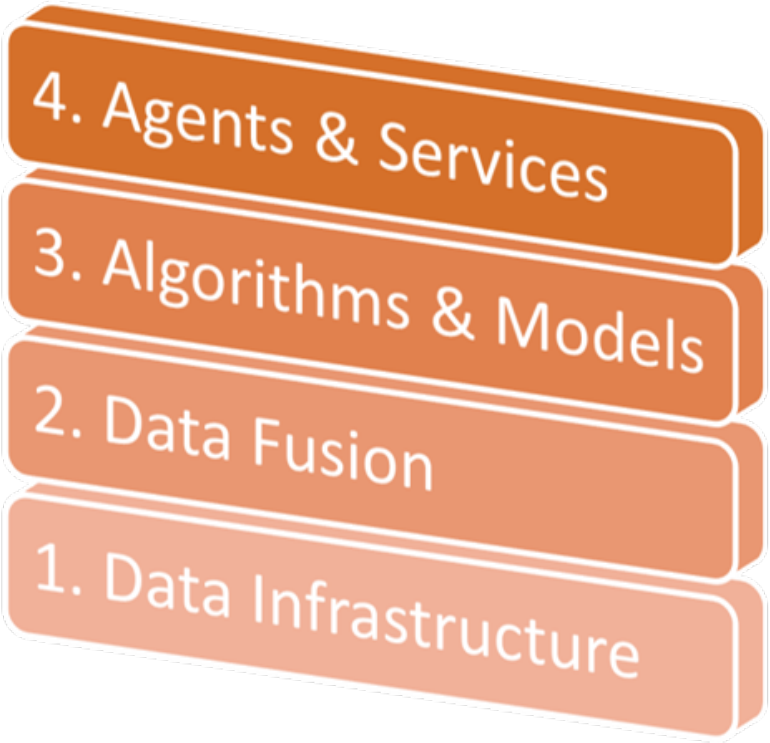


Figure 3. AI Stack

Data Infrastructure

The foundation of any AI system lies in its data infrastructure. This infrastructure comprises hardware resources, which can be either physical or virtualized, dedicated to storing vast amounts of data and processing them efficiently. Key elements include systems like Hadoop, which are designed for big data storage, and a variety of computing resources such as Virtual Machines (VMs), Containers, Central Processing Units (CPUs), and Graphics Processing Units (GPUs). These components are essential for handling the immense volume, velocity, and variety of data typically encountered in AI applications. The robustness and scalability of the data infrastructure directly influence the performance and capabilities of AI systems. This level can be matched with Computation Servers in the IoT stack, and in some use cases will be the same physical machines.

Data Fusion

Data fusion involves the integration of data from multiple sources and formats, making it a vital component of the AI stack. It employs software tools that interface with the storage and processing resources, such as SQL for structured data querying, NoSQL for unstructured data handling, and Apache Spark for large-scale data processing. These tools are responsible for the crucial steps of raw data cleaning and labelling, ensuring the creation of high-quality datasets. This pre-processing phase is critical as it lays the groundwork for effective model training, ensuring that the AI algorithms are fed with accurate and relevant data. Management of data trust is a key aspect associated with this issue.

Algorithms and Models

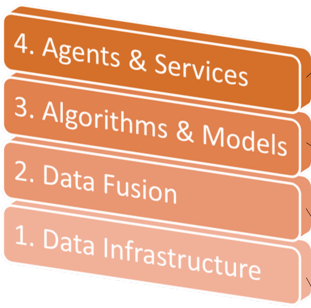
At the heart of the AI stack are the algorithms and models, the sophisticated mathematical tools that learn from data to make predictions or decisions. This layer includes a diverse array of tools and libraries, such as TensorFlow, Caffe, Torch, Scikit-learn, and CNTK, each offering unique functionalities for different types of AI applications. These tools facilitate various forms of model training, including supervised learning (learning from labelled data), unsupervised learning (learning from unlabelled data), and reinforcement learning (learning from interactions with the environment). The choice of algorithms and models is contingent upon the specific requirements and constraints of the AI application, including the nature of the task, the availability of data, and the desired outcome. Protection and resilience of AI models against AI threats should be strongly considered at this level.

Agents and Services

The final layer of the AI stack encompasses agents and services, which are applications that utilize the outcomes of AI model analyses to perform a wide range of data analysis operations. These operations can include natural language processing (NLP), image processing, and various predictive tasks such as classification and clustering. AI agents are autonomous systems capable of making decisions based on the analysis of vast amounts of data, while AI services are more focused on specific tasks, often accessible via APIs. This layer is where the practical application of AI becomes evident, as these agents directly interact with end-users using the services, providing intelligent solutions to complex problems.

In the context of the AI stack and its significance, as outlined in the generative AI tech stack model, we can draw a parallel (Figure 4) with the model proposed in the ACM paper[13]. The generative AI stack emphasizes foundational understanding, development guidance, interoperability, tool selection, future-proofing, specialization, and deployment. This mirrors the ACM's perspective, highlighting the structured approach necessary to build, develop, and deploy AI systems effectively. Both models stress the importance of an integrated and comprehensive tech stack that must evolve to accommodate the rapidly advancing field of AI, ensuring that applications remain relevant and functional over time.

13 Management and technology challenges of AI-enabled application projects. BY RUA-HUAN TSAIH, HSIN-LU CHANG, CHIH-CHUN HSU, AND DAVID C. YEN, The AI Tech-Stack Model, https://dl.acm.org/doi/pdf/10.1145/3568026



AI Tech Stack		Definitions	Functionalities
SaaS + AI-embedded functions	AI Solution	AI-enabled solutions to address business applications in a specific domain.	A variety of capabilities to deliver business intelligence in a specific function domain (for example, customer service) or industry domain (for example, banking).
	AI Service	Well-defined AI-enabled services that can be fulfilled by API function call request.	General-purpose API services such as recommendation, ranking, intelligent search, language translation, and object detection.
DaaS + DataOps	AI Data Pipeline	Data lifecycle-management platform to generate curated data and feature engineering for AI/ML model training.	DaaS, DataOps platform for data pipeline automation, orchestration, visualization and feature operations, and more.
AI software modules	AI Algorithm	Training methods by which the AI system conducts its learning task.	Supervised, unsupervised, and reinforcement learning.
	AI Framework	AI-related frameworks for defining AI/ML architectures and invoking algorithms, library, and accelerator drive on the hardware.	Tensor computing, AI libraries (for example, Torch, TensorFlow), prebuilding AI models (for example, neural network models), and so on.
PaaS + MLOps	AI Platform	A unified interface that facilitates communication between software and hardware throughout the ML lifecycle.	PaaS, AI/ML lifecycle management platform (for example, ML-Ops, IEP) to build, train, test, evaluate, serve, and monitor AI-enabled applications.
IaaS + Accelerator	AI Infrastructure	Hardware units that orchestrate and coordinate computations among accelerators	IaaS, AI accelerators for highly parallel operations (for example, GPU, TPU, FPGA), tools for monitoring, clustering, and so on.

Figure 4. AI Stack parallelism

5. Convergence Matrix

5.1 DLT-IoT Convergence Matrix

The DLT-IoT Convergence Matrix is a strategic framework designed to illustrate the synergistic potential between Distributed Ledger Technologies (DLT) and the Internet of Things (IoT). By mapping the intricate interplays between the stacks of both technologies, this matrix provides a comprehensive blueprint for identifying and leveraging convergence points. These points serve as the nexus for innovation, where the decentralized, secure, and transparent nature of DLT meets the interconnected and data-rich landscape of IoT. The following matrix visualizes these interactions, showcasing how combined, these technologies can unlock transformative solutions across various sectors.

<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></td><td rowspan="2">Securing Access management with access token</td><td>IoT Network Management</td><td rowspan="2">Gateway Brokers</td><td></td><td rowspan="2">Secure Data Exchange</td><td></td></tr>
<tr><td>Securing IoT with fingerprinting</td><td></td><td></td></tr>
<tr><td>Scalability</td><td rowspan="4">Autonomous identity</td><td>IoT network Management</td><td rowspan="4">Hub Devices</td><td>Decentralization</td><td rowspan="2">Scalability</td><td>Scalability</td></tr>
<tr><td rowspan="3">Interoperability</td><td>Autonomous Identity Management</td><td rowspan="3">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>

Figure 5. DLT-IoT Convergence Matrix

5.1.1 How DLT can assist or solve different issues related to IoT

Decentralization

Decentralization is a key feature of blockchain that can be further enhanced through the integration with IoT and edge computing. Decentralized smart Internet of Things (IoT) refers to future IoT powered by blockchain-enabled edge intelligence. The integration of blockchain and edge computing is mutually beneficial: on one hand, blockchain introduces security, privacy, and trust to edge devices, enabling efficient control and incentive of cooperation among edge devices and servers that are securely enabled by blockchain. Decentralized approach can reduce IoT costs associated with installing and maintaining large, centralized data centres. With DLTs computation and storage can be decentralized across the billions of devices that form the IoT network.

Interoperability

Fragmentation and lack of interoperability among different platforms is a major issue with Internet of Things (IoT). Currently, IoT platforms and systems are vertically oriented silos unable (or unwilling) to exchange data with, or perform actions across, each other. IoT devices, including wearable devices, are highly heterogeneous in terms of the underlying communication protocols, data formats, and technologies from different vendors. Such heterogeneous infrastructures, devices, and configurations have become a strong limitation for data integration and interoperability. This leads to multiple problems: reduced competition and vendor lock-ins, as it is difficult for customers to switch IoT providers, worse privacy as vendors usually forces their customers to move at least some of their data or metadata to the vendor's cloud, and reduced functionality compared to what better interoperability would afford. Since IoT systems are becoming prevalent in everyday life, lack of interoperability and limited use of relevant data is growing into a significant problem for the whole society. Distributed Ledger Technologies (DLTs) such as blockchains offer decentralized solutions for collaboration and interoperability. At the network and connectivity level, blockchain can help increasing IoT interoperability providing a common, trusted communications layer between devices of different types and manufacture.

Scalability

Scalability is a fundamental requirement of any IoT system to meet service and security requirements across a dynamic network of devices. With billions of IoT devices expected in the next few years, meet these requirements is becoming essential to run IoT especially in mission-critical scenarios. This is rapidly pushing IoT data processing, management and analytics to the "edge," where compute occurs locally, instead of relying on cloud connectivity. The introduction of Blockchain technology can enable fast processing of transactions and coordination among billions of connected devices. IoT edge devices can improve the scalability of blockchain in a distributed and efficient manner by delivering computing and cache resources to the blockchain-enabled IoT systems.

Secure Data Exchange

Data originated from billions of sensors pose significative privacy and security challenges. Secure data exchange has become crucial in achieving effective information sharing and promoting efficient use of valuable data in IoT ecosystems. Sharing of data in IoT is often rudimentary and can significantly increase the probability of an adversary gaining access of the data. Cloud and edge computing offers seamless services for data exchange, but security in cloud still represent a point of debate. DLT can address this challenge maintaining immutable, auditable, and single-version-of-truth data and providing provide a secure mechanism for data sharing among IoT devices so that the visibility, privacy, interoperability, and protection of data are accountable along the data exchange process.

IoT network security and Identity management

Implementing a distributed network into an IoT ecosystem has innate structural availability benefits. Centralized networks create a single point of failure for all connected services, while devices on a distributed network are more autonomous and not reliant on a core system. Any malicious attempts to alter or attack a distributed database would require penetration of a majority of connected nodes, out of potentially thousands, making it virtually impossible to hack. Security is an area within IoT that could potentially benefit from enabling certain aspects of blockchain that sets it apart from traditional DLT. A decentralize P2P network is more resilient to cyber-attacks or single points of failure. Any attempts attack a decentralized network would require the control of several connected nodes (depending on consensus algorithm), making it virtually impossible. Blockchain can also provide mechanisms for IoT devices identity authentication SSI.

Autonomous M2M interaction

One of the biggest issues with this is machine-to-machine communication. Over time, every manufacturer will come up with their own machine-to-machine (M2M) protocols. However, a lot of different M2M communication protocols may make it troublesome to integrate products and services. This is where blockchain technology could potentially help IoT. Blockchain can work with IoT in facilitating autonomous machine-to-machine transactions. Smart contracts can be deployed that allow machines to hold funds, make decisions based on complex business logic and carry out transactions.

Data monetization

DLT can act as a trusted broker to monetize IoT's data trading. DLT enables the creation of data marketplaces based on automated, reliable, and transparent monetization system, allowing IoT data users to exercise fine-grained control on shared data. Rising of Smart Legal Contracts is promising, but currently it is an immature technology.

Micro-payments

DLTs, and, in particular, layer 2 scalable solutions (e.g., Lightning Network) can be suitable as a micropayment solution for IoT. Incorporating micropayments into a full-scale IoT, having a device autonomously pay another device, could enable the machine-to-machine economy.

Voting & Negotiation

The matrix posits that DLT can empower IoT devices to make collective decisions. In a decentralized energy grid, devices could vote on the best energy source to use at a given moment, optimizing for cost and efficiency, and execute that decision autonomously.

5.2 DLT-AI Convergence Matrix

The nexus of Distributed Ledger Technology (DLT) and Artificial Intelligence (AI) heralds a new paradigm in technological advancement. The DLT-AI Convergence Matrix is a pivotal tool for dissecting and understanding how these two revolutionary technologies can mutually enhance and address each other's challenges. On one hand, DLT can fortify AI by introducing improved data integrity, transparency in decision-making processes, and secure data sharing mechanisms. On the other hand, AI can amplify the capabilities of DLT by optimizing consensus mechanisms, enabling predictive analytics for network health, and automating smart contract functionality.

This convergence matrix aims to delineate specific areas where DLT can contribute to solving inherent AI-related issues, such as data provenance, model accountability, and computational integrity. Conversely, it also explores how AI can resolve DLT-related challenges, including scalability constraints, security vulnerabilities, and the enhancement of autonomous decision-making in distributed networks. By systematically analysing the cross-pollination of DLT and AI, stakeholders can exploit the convergence matrix to identify opportunities for innovation, streamline operations, and cultivate new business models that capitalize on the strengths of both technologies.

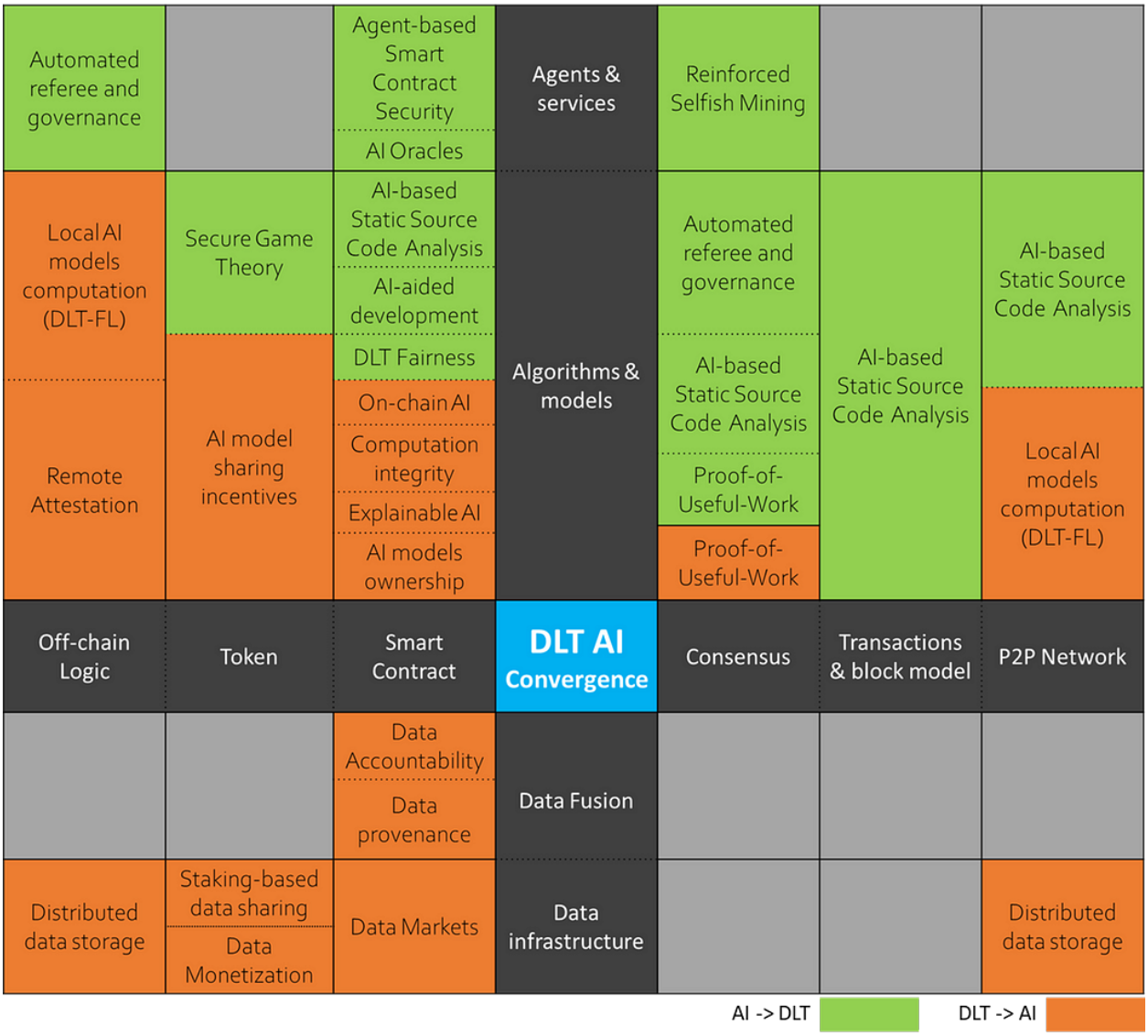


Figure 6. DLT-AI Convergence Matrix

5.2.1 How DLT can assist or solve different issues related to AI

AI models sharing incentives

By integrating AI with blockchain, data scientists and developers gain the capability to share their AI models on a decentralized public ledger, thereby opening avenues for remuneration in the form of cryptocurrencies. This model not only fosters a token-based reward system that compensates contributors when their models are utilized or positively evaluated but also enables the sale of rights to future earnings that these models may generate. The decentralization allows for a portion of the computational work to be offloaded to the community, incentivizing contributions through token rewards and creating a collaborative development environment.

On-chain AI

Blockchain technology enables the uploading of AI models onto the chain, allowing smart contracts and decentralized applications (DApps) to directly access and execute basic AI functions such as linear regression, classification, or clustering tasks. This method promotes transparency and democratization of AI by decentralizing the algorithms, thereby allowing a broader choice among AI providers and fostering trust through open-source collaboration.

Data accountability & data provenance

In AI, trust hinges on the end-user's confidence in the model, necessitating clear visibility into the training process and data sources. Blockchain's smart contracts offer a publicly auditable method to encode data usage policies and trace data provenance, effectively addressing the concerns surrounding sensitive data processing, ensuring data accountability, and tracking provenance in a privacy-conscious manner.

Remote attestation on Trusted Execution Environments

The deployment of authentic AI models is critical, ensuring that they are untampered and perform as intended. Within TEEs, blockchain can be used to attest to the integrity of the executing software, providing certification that is recorded on the ledger and offering a layer of security that bolsters user trust in AI applications.

Computational integrity

The integrity of AI is paramount for trust in its applications. By training machine learning models, especially when computed off-chain in TEEs, one can achieve both high computational performance (especially on GPUs) and maintain privacy and confidentiality, thus ensuring the integrity of computational processes.

DLT-based federated learning for AI models computation

Federated Learning, a technique for distributed machine learning, benefits from blockchain's decentralized infrastructure, which is resistant to inference attacks. This structure enhances data confidentiality, asserts AI model ownership, and adds an auditable layer to the training process, thus rendering the AI more trustworthy.

Data markets and data monetization

DLT opens the gates to democratized data markets by allowing users to share their data, retain ownership, and directly monetize it. This system could improve machine learning performance by broadening the datasets available for training, particularly improving tasks like classification accuracy.

AI Pipeline explainability, traceability and audibility

The complexity of machine learning pipelines demands transparency and explainability. Blockchain can solidify trust by recording the evaluation results of each training epoch on the chain, serving as a validation and auditing mechanism to certify the quality of AI models.

Staking-based data sharing

In staking-based data sharing systems, the quality of input data for training AI models is crucial. DLT systems reward data providers based on the quality of their datasets, as determined by the liquidity staked on them. This incentivizes the provision of high-quality data, with token earnings proportionate to the dataset's utilization.

Distributed data storage

Advanced solutions like IPFS or Swarm enable decentralized storage and communication, essential for distributing and managing encrypted, trained models. Participants can download initial models and contribute to their training, facilitated by a decentralized storage module.

AI models ownership

Ensuring the ownership and traceability of AI models is vital for confidential data sharing and addressing biases or fairness issues within models. Blockchain smart contracts enable the establishment of ownership and access controls, limiting use to authorized parties.

Proof-of-Useful-Work

To mitigate the energy inefficiencies of Proof-of-Work systems, AI-based consensus mechanisms have been proposed. These allow AI and ML models to optimize the computation resources, reducing the time and cost associated with model training, thus enhancing the blockchain's application potential without the associated energy waste.

5.2.2 How AI can assist or solve different issues related to DLT

AI-based Static Source Code Analysis

AI-based Static Source Code Analysis represents a paradigm shift in enhancing the security and robustness of DLT systems. It employs AI models, such as neural networks and reinforcement learning, to scrutinize various layers of the DLT stack without the need to run the actual programs. This includes identifying systemic faults and bugs within the P2P network, detecting vulnerabilities in transaction and block models, verifying smart contracts, and ensuring fairness in consensus protocols. For instance, AI can identify potential vulnerabilities in a blockchain's code that could lead to network fragmentation, or it could analyse transaction opcodes for anomalies that suggest security flaws.

Automated Referee and Governance

AI can function as an automated referee within DLT systems, resolving disputes and ensuring governance integrity. It can provide oversight for on-chain activities, such as the execution and outcomes of smart contracts, and assist in the adjustment of governance parameters. For example, in a blockchain network, AI could mediate in transaction disputes by analysing the ledger and applying pre-set rules to determine the rightful outcome, or it could help optimize the block production process based on network activity data.

Proof-of-Useful-Work

The concept of Proof-of-Useful-Work emerges as an AI-enhanced alternative to traditional consensus mechanisms like Proof-of-Work, which are criticized for their high energy consumption. By employing AI, blockchain networks can update governance parameters such as mining difficulty or validate miner activity more efficiently. AI could predict the optimal number of miners needed at any given time to maintain network integrity without excessive energy use. Cybersecurity of mining nodes should be considered also into the set of optimization parameters.

AI-Aided Development

AI-aided tools can revolutionize smart contract development by automatically analysing code to identify vulnerabilities and suggest best practices. For example, AI could scan a smart contract before it's deployed on the blockchain to ensure it doesn't contain any exploitable bugs or patterns that could lead to security breaches.

DLT Fairness

AI technologies can contribute to the fairness of DLT protocols by applying the principles of explainable AI (XAI). This can make the decision-making processes within the DLT more transparent and comprehensible, thus promoting trust among diverse participants. For instance, AI could provide justifications for decisions made by autonomous agents within a decentralized autonomous organization (DAO), making the process more auditable and fair.

Secure Game Theory

AI can apply reinforcement learning to analyse and secure smart contracts using game theory principles. This approach allows for the simulation and testing of various strategic scenarios that a smart contract might encounter, identifying potential security risks and strategic vulnerabilities.

Reinforced Selfish Mining

Reinforcement learning can also be used to understand and mitigate selfish mining strategies in blockchain. By simulating a blockchain environment, AI agents can learn the most effective strategies for miners, contributing to the security and stability of the mining process.

Agent-based Smart Contract Security

Agents empowered with AI can intelligently interact with smart contracts, identifying and rectifying security issues. Through pattern recognition and behavioural analysis, these AI agents can pre-emptively detect and address actions that might undermine the security of the blockchain.

AI Oracles

AI oracles represent the bridge between the blockchain and the external world, enabling smart contracts to interact with off-chain data. By automating the collection and verification of real-world data, AI oracles allow smart contracts to respond to external events accurately and reliably, expanding the scope of blockchain applications.

6. Convergence Prism

The "Convergence Prism: DLT - IoT - AI" stands as a ground breaking exploration into the synergistic integration of three pivotal technologies: Distributed Ledger Technology (DLT), the Internet of Things (IoT), and Artificial Intelligence (AI). This convergence represents a paradigm shift, melding the unique strengths and capabilities of each technology to forge innovative solutions and opportunities.

In this convergence prism, we delve into the myriad intersections where DLT, IoT, and AI dynamically interact, revealing how the amalgamation of these technologies enhances functionality, security, and efficiency far beyond what each could achieve independently. The convergence of these technologies heralds a new era of smart, interconnected systems that are secure, self-regulating, and highly intelligent.

This analysis spotlights key areas and topics where convergence is not only feasible but also transformative. It includes decentralized data management and enhanced security protocols offered by DLT, the extensive sensory networks and real-time data collection capabilities of IoT, and the predictive power and decision-making prowess of AI.

In the development of our IoT-DLT-AI Convergence Prism, we employed a systematic and layered approach to analyse and integrate the distinct technological stacks of Internet of Things (IoT), Distributed Ledger Technology (DLT), and Artificial Intelligence (AI). Our methodology unfolded in several strategic steps:

1. **Layered Analysis of Technological Stacks**: We began by dissecting the technological stacks of IoT, DLT, and AI into their respective layers. For IoT, this included Sensors & Actuators, Hub Device, Gateway Broker, Computational Server, and Services. The DLT stack was segmented into P2P Network Nodes, Transactions & Block Model, Consensus Mechanism, Token, and Off-Chain Logic. For AI, we identified key layers such as Data Infrastructure, Algorithms and Models, and Data Fusion.

2. **Three-Dimensional Prism Creation**: Utilizing the identified layers, we constructed a three-dimensional prism, where each side represented a layer from the IoT, DLT, and AI stacks. This geometric representation allowed us to visualize and systematically explore the intersections of these technologies.

3. **Investigation of Intersection Points**: At each intersection point within the prism, we conducted an in-depth examination to identify potential areas of convergence. This involved:

    a. **Assessing Technical Capabilities**: We evaluated the specific technical capabilities inherent in each layer at the intersection points, understanding how their individual attributes could potentially synergize.

    b. **Identifying Potential Benefits**: Our focus extended to recognizing the advantages that could emerge from combining the capabilities of the intersecting layers. This included envisaging new functionalities, enhanced efficiency, and broader applicability of integrated solutions.

    c. **Addressing Challenges for Convergence**: We acknowledged and analyzed the potential challenges and obstacles that might arise in realizing convergence at these intersections. This included technical limitations, integration complexities, and scalability concerns.

Through this comprehensive methodology, we aimed to uncover innovative convergence themes, paving the way for transformative solutions that harness the collective strengths of IoT, DLT, and AI technologies. This prism serves as a guide to exploring new frontiers in technological integration, highlighting the vast potential for cross-disciplinary innovation and advancement.

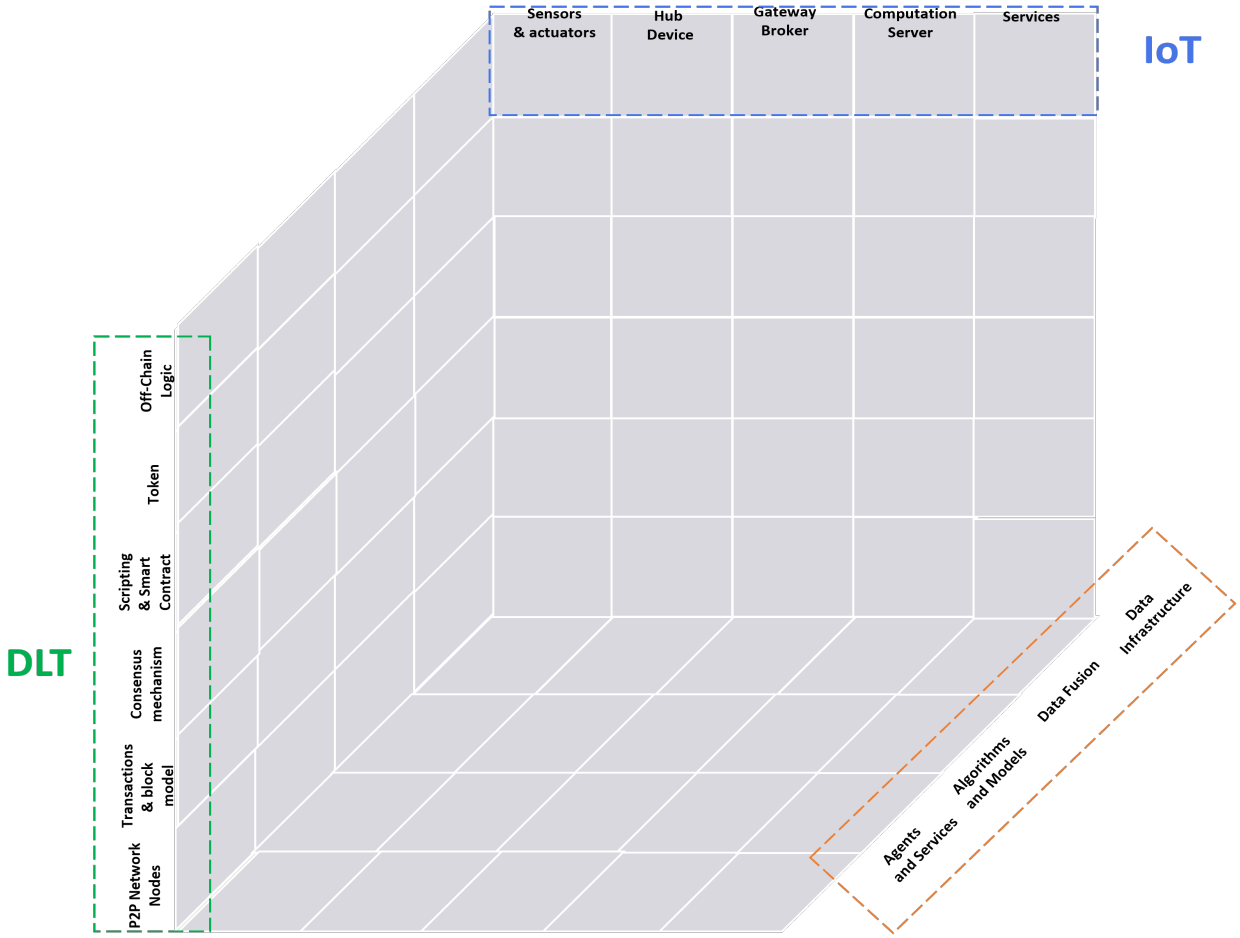


Figure 7. IoT-DLT-AI Convergence Prism

6.2 IoT devices for on-chain AI

In the comprehensive exploration of the IoT-DLT-AI Convergence Prism, the "IoT Devices for On-Chain AI" cube emerges as a crucial intersection point. This convergence cube integrates the Smart Contract layer from Distributed Ledger Technology (DLT), the Sensors and Actuators layer from the Internet of Things (IoT), and the Algorithms and Models layer from Artificial Intelligence (AI).

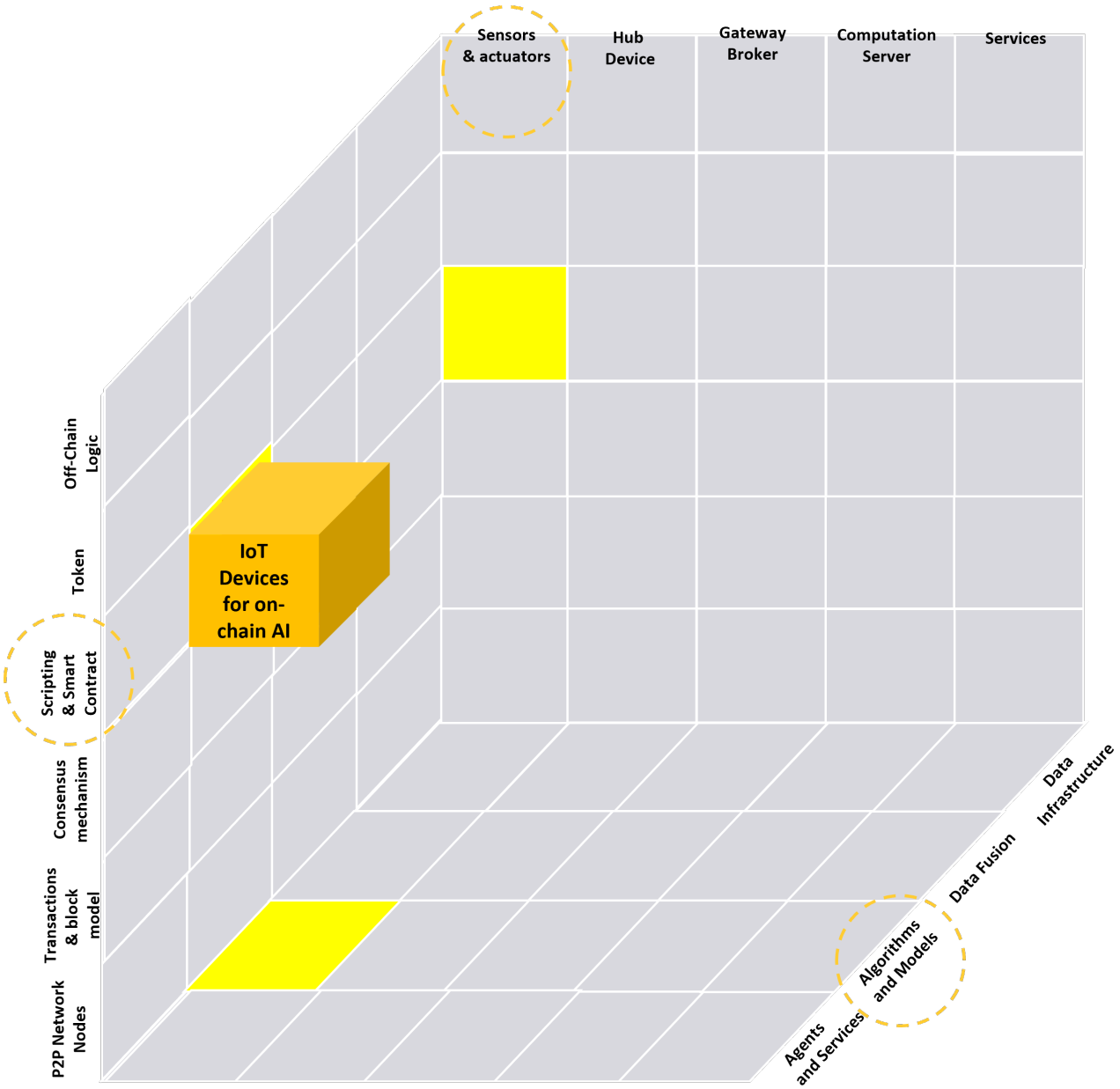


Figure 8. IoT Devices for on-chain AI

AI-DLT Synergy

- **Blockchain Integration of AI Models**: AI models, including but not limited to linear regressions, classification, and clustering tasks, can be uploaded onto the blockchain. This integration facilitates the accessibility and execution of these models via smart contracts and decentralized applications (DApps).

- **Enhanced Transparency and Diversity in AI**: By decentralizing AI algorithms and making them available through blockchain technology, there's a paradigm shift towards a more transparent AI ecosystem. This openness allows users to select from a diverse array of AI providers, enhancing the accountability and trustworthiness of AI systems.

IoT-AI Interaction

- **Data Acquisition for AI Training**: IoT devices serve as pivotal data collection tools, gathering vital information including sensor readings and actuator control signals. This data forms the backbone for training robust AI models devoted to anomaly detection or time-series prediction.

- **Application of Trained AI Models**: These AI models, once trained, are deployed to execute real-world tasks. Applications vary widely, from managing autonomous vehicles and optimizing manufacturing processes to enhancing customer service.

Practical Use-Cases

1. **Smart City Traffic Optimization:** In urban settings, AI models can optimize traffic management by processing data from various city sensors, such as traffic cameras and parking sensors. These AI-driven decisions can effectively regulate traffic lights, manage parking, and optimize city resource allocation.

2. **Manufacturing Quality Assurance**: AI models can significantly improve manufacturing quality control by analyzing data from production line sensors. This proactive approach allows for early identification of product defects, ensuring quality assurance before shipment.

3. **Enhanced Healthcare Services**: In healthcare, AI models, trained on data from medical devices and health records, can assist in disease diagnosis, patient outcome prediction, and personalization of treatment plans, thereby elevating the standard of patient care.

6.2 Remote attestation on Trusted Execution Environment

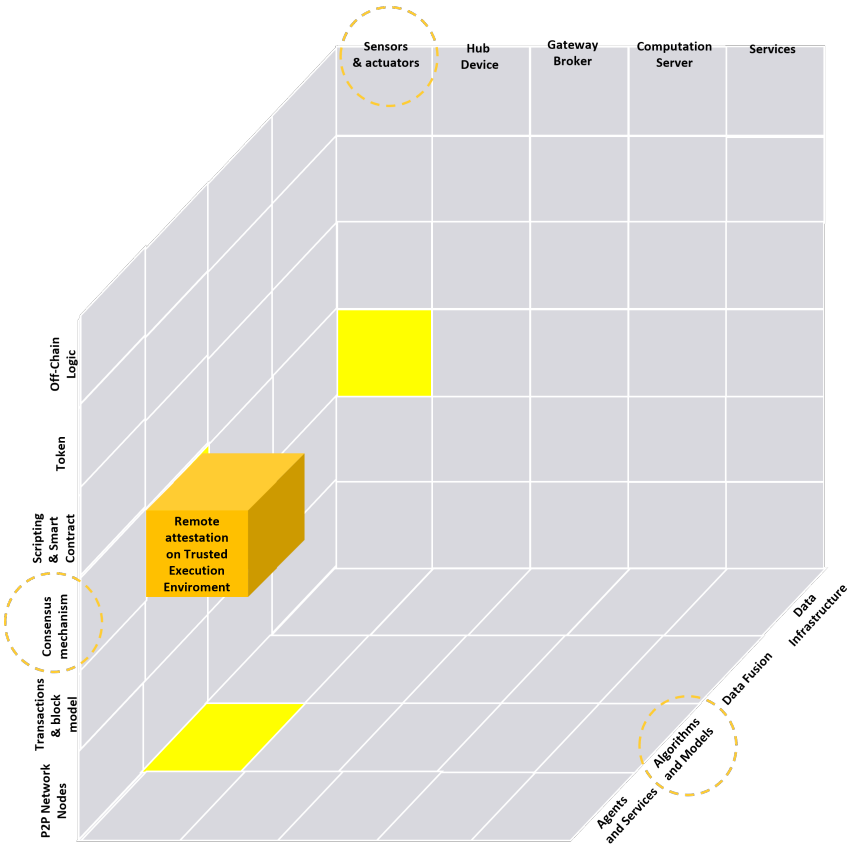


Figure 9. Remote attestation on Trusted Execution Environment

In the "Remote Attestation on Trusted Execution Environments (TEE)" cube within the IoT-DLT-AI Convergence Prism, the interaction amongst AI, DLT, and IoT devices can be analyzed and understood through a multi-faceted approach:

AI-DLT Synergy

- **Certificate Management via DLT**: DLT serves a pivotal role in managing the certificates of AI models, ensuring their authenticity. This mechanism guarantees that AI models are genuine and their code remains untampered, thereby maintaining integrity.

- **Proof of Attestation via DLT**: DLT can generate proofs of attestation, crucial for verifying that AI models are operating on the intended hardware without any tampering. This enhances the trustworthiness of AI systems, particularly in critical applications.

AI-IoT Interaction

- **Data Acquisition for AI Training**: IoT devices are instrumental in collecting data necessary for training AI models. This data encompasses a wide range of inputs, from sensor readings to actuator signals, capturing diverse aspects of the physical world.

- **Real-World AI Application**: The AI models, once trained, can be utilized to make informed decisions and perform actions in the real world, such as controlling autonomous vehicles, optimizing manufacturing processes, or enhancing customer service.

Integrated Workflow in the Cube

1. **Data Collection**: IoT devices gather data from the physical environment.

2. **Data Management**: This data is then transmitted to the DLT network for secure storage and management.

3. **Attestation Proof Generation**: The DLT network produces a proof of attestation for the AI model.

4. **Deployment on TEE**: The AI model is deployed onto the TEE.

5. **Verification by TEE**: The TEE verifies the proof of attestation, ensuring the AI model's integrity and confirming it is operating on the designated hardware without tampering.

6. **Decision Making**: Utilizing the IoT-collected data, the AI model executes decisions or actions in real-world scenarios.

This interaction within the cube not only guarantees the deployment of genuine AI models but also assures their operation on the intended hardware, significantly enhancing the security and reliability of AI systems.

Practical Applications

1. Smart City Infrastructure: This cube can be employed in smart cities to ensure the deployment of authenticated AI models for controlling traffic lights and other critical infrastructures, thereby enhancing urban management and safety.

2. Manufacturing Quality Control: Manufacturing plants can leverage this cube to confirm the authenticity of AI models used in monitoring production lines and detecting potential defects, ensuring product quality and operational efficiency.

3. Healthcare Diagnostics: Healthcare providers can utilize this cube to validate AI models used in diagnosing diseases and formulating treatment plans, thus ensuring accuracy and reliability in medical care.

6.3 Sensor data monetization

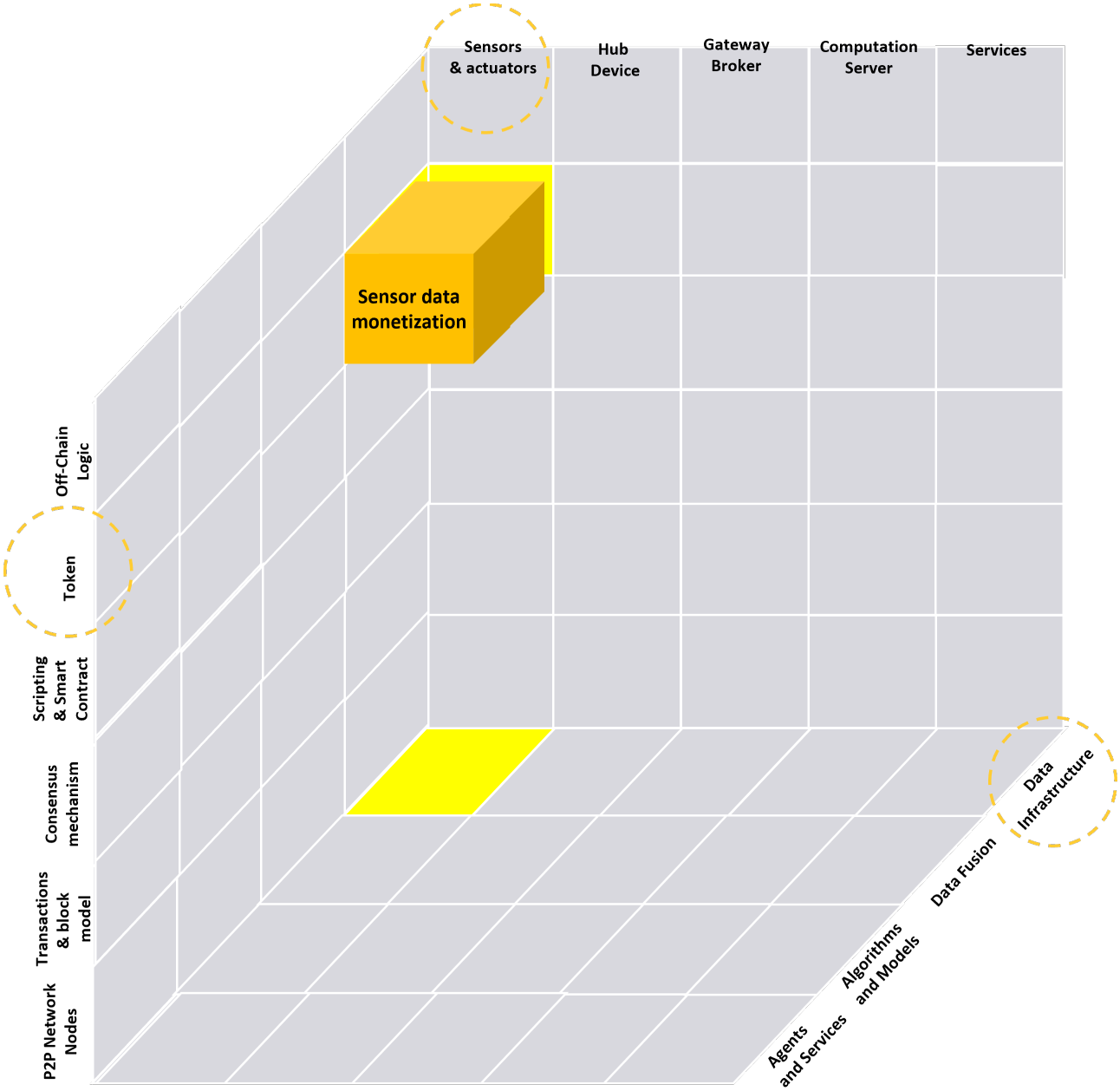


Figure 10. Sensor data monetization

In the "Sensor Data Monetization" cube of the IoT-DLT-AI Convergence Prism, the intricate interactions among AI, DLT, and IoT devices can be dissected into specific functionalities and processes, suitable for a technical report:

AI-DLT Interaction

- **Creation of a DLT-Based Data Market**: DLT is instrumental in establishing a marketplace for data transactions. This platform facilitates the sale of data from individuals or entities (data sellers) to parties interested in acquiring data for AI model training or other analytical purposes (data buyers).

- **Revenue Generation for Data Sellers**: Individuals or entities that generate data, potentially through IoT devices, can monetize their data assets by selling them in this DLT-driven market. This opens a new revenue stream for data providers.

- **Data Acquisition for AI Developers**: AI developers or companies requiring diverse datasets for model training can purchase this data, thereby gaining access to a broader range of real-world data, which can enhance the effectiveness of AI models.

AI-IoT Interaction

- **Data Collection by IoT Devices**: IoT devices play a pivotal role in gathering data from various physical environments. This data can encompass a wide array of information, crucial for training AI models.

- **Application of AI Models**: The data collected and processed by IoT devices can be employed to train AI models, which are then utilized to execute decisions or actions in real-world scenarios, such as optimizing manufacturing processes or improving urban infrastructure management.

Integrated Workflow in the Cube

1. Data Harvesting: IoT devices collect data from diverse physical environments.

2. Data Tokenization and Transmission: This data is then tokenized and transferred to the DLT network.

3. Data Trading on DLT Market: The tokenized data is made available for purchase on a DLT-based marketplace.

4. Data Utilization by Buyers: Data buyers, such as AI developers, purchase this data to train and refine AI models.

5. Real-World AI Implementation: These AI models, bolstered by comprehensive and varied datasets, are then applied to practical tasks in various sectors.

Practical Applications

1. Smart City Participation: Residents in a smart city could sell environmental, traffic, or other urban data to entities seeking to enhance city management systems.

2. Manufacturing Insights: Employees in a manufacturing setting could monetize operational data, contributing to the refinement of AI models for industrial efficiency.

3. Healthcare Data Utilization: Patients could opt to sell their health data, aiding in the development of more sophisticated AI-driven diagnostic tools.

Enhanced Data Control

Beyond monetization, this DLT-based market offers enhanced data control, allowing users to selectively sell data to preferred buyers or use their data for personal AI model training. This aspect not only fosters a new economic model for data but also ensures greater privacy and security for the data providers.

6.4 Next Generation Digital Twin

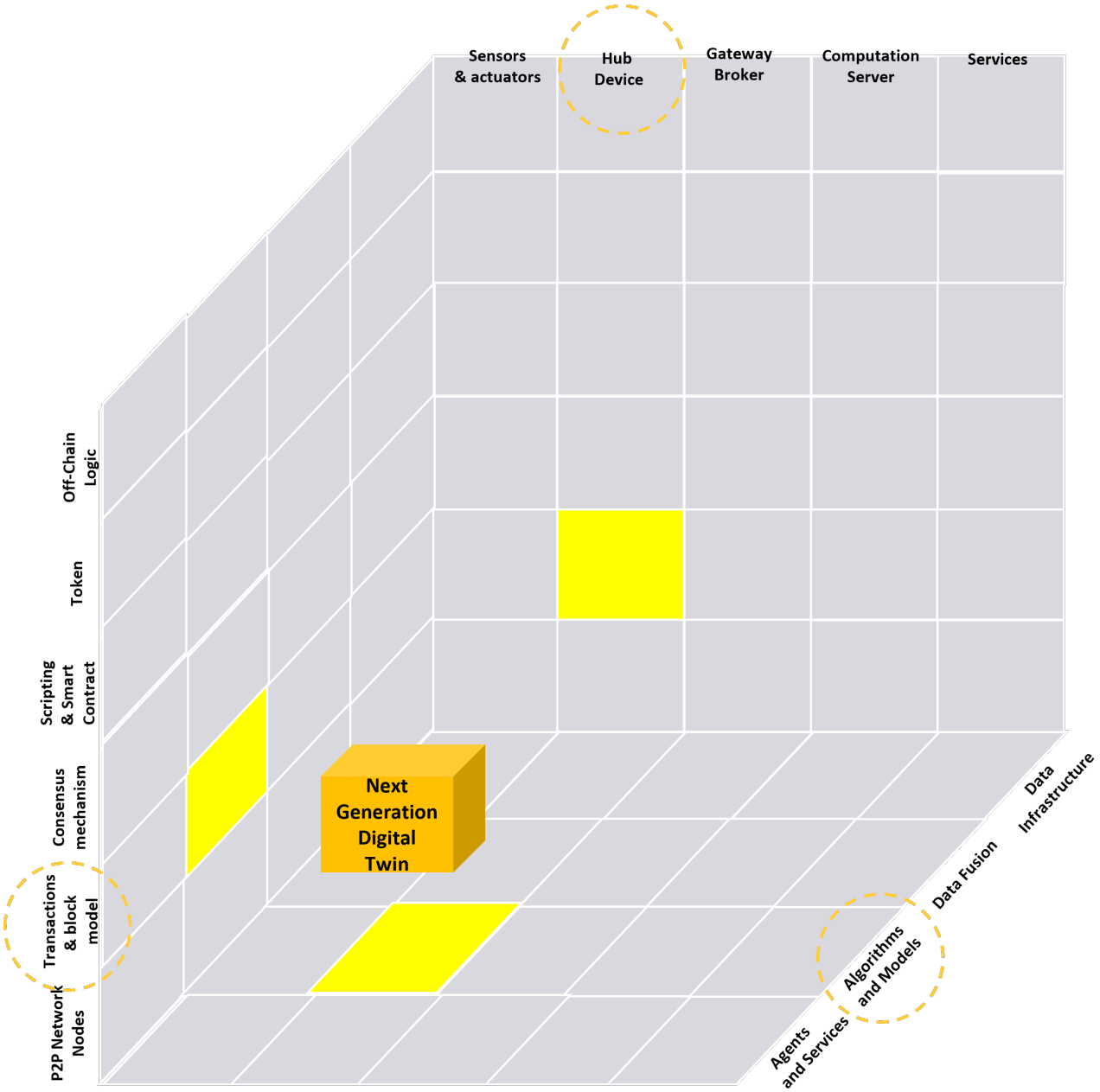


Figure 11. Next Generation Digital Twin

In the "Next-Generation Digital Twins" intersection of the IoT-DLT-AI Convergence Prism, we explore how the synergistic combination of Artificial Intelligence (AI), Distributed Ledger Technology (DLT), and the Internet of Things (IoT) enhances the development of advanced digital twins. Digital twins represent virtual models of physical objects or systems, capable of monitoring, analyzing, and optimizing their real-world counterparts.

Enhancements through AI, DLT, and IoT Convergence

1. **AI-Enhanced Accuracy and Reliability**:

    a. AI algorithms analyze sensor data to uncover patterns and trends, which might be elusive to human observation.

    b. This advanced analysis leads to more precise and reliable digital twin models, making them capable of more accurately reflecting the physical entities they represent.

2. **DLT for Security and Trustworthiness**:

    a. DLT is utilized to securely store and manage data collected from various IoT devices in a decentralized fashion.

    b. This decentralization enhances the security of digital twins by making data manipulation or unauthorized access more challenging, ensuring data integrity and reliability.

3. **IoT for Comprehensive and Real-Time Updates**:

    a. IoT devices continuously gather real-time data from the physical environment.

    b. This real-time data flow keeps the digital twin models updated, offering a current and comprehensive virtual representation of the physical objects or systems.

Practical Applications of Next-Generation Digital Twins

1. **Manufacturing Optimization**:

    a. AI algorithms analyze data from manufacturing line sensors to detect potential defects or inefficiencies.

    b. Insights gained are used to refine the manufacturing process, improving efficiency and product quality.

2. **Healthcare Patient Monitoring**:

    a. IoT devices collect various health metrics from patients, like heart rate, blood pressure, and glucose levels.

    b. This data forms the basis of a patient's digital twin, which is then analyzed by AI to identify health trends or potential issues, enabling proactive healthcare management.

3. **Transportation Safety and Efficiency**:

    a. Data on vehicle speed, location, and engine performance is collected by IoT devices.

    b. Creating a digital twin of the vehicle allows AI algorithms to analyze this data, identifying potential safety hazards and areas for efficiency improvement.

6.5 AI Oracle based IoT data

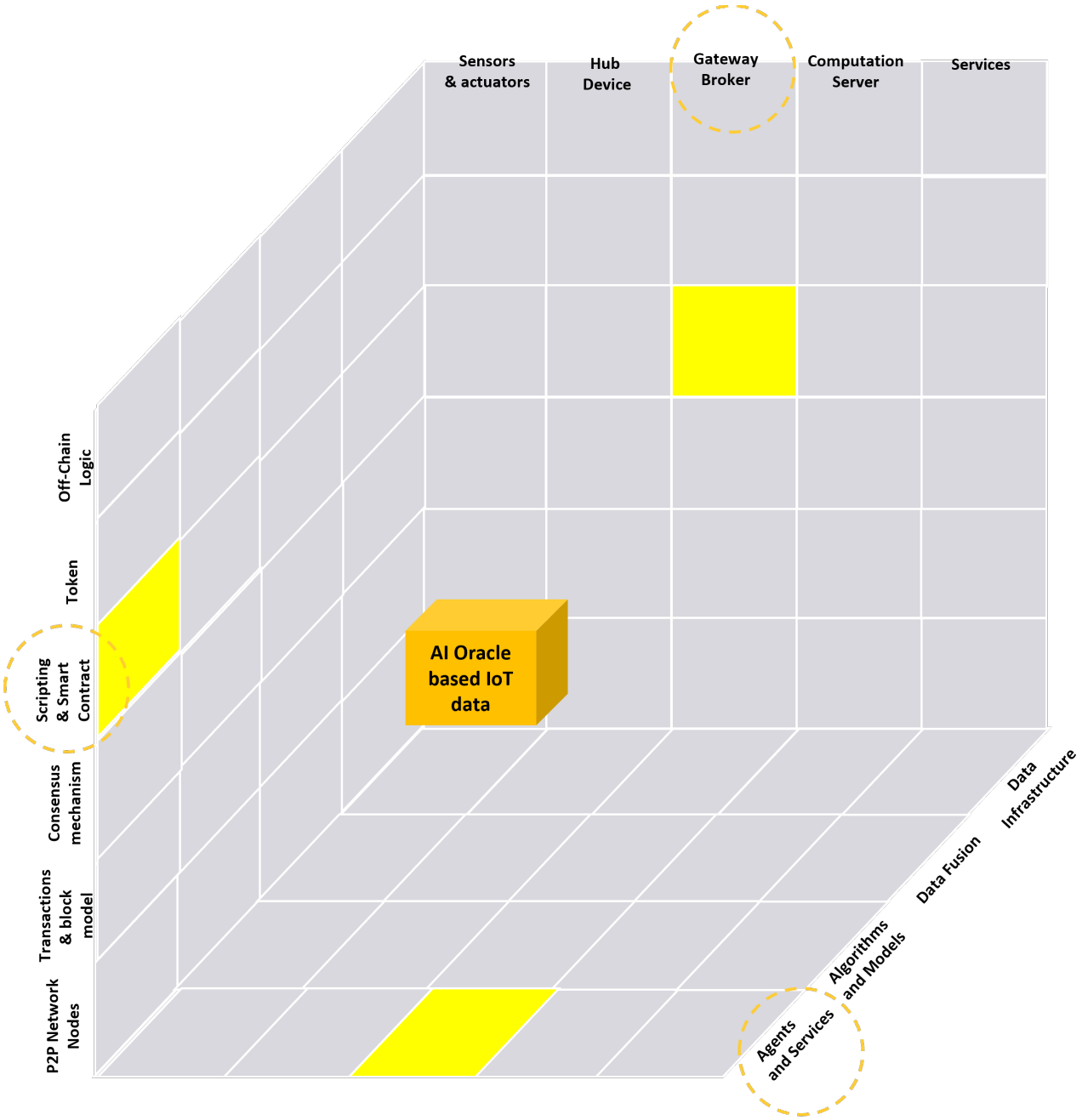


Figure 12. AI Oracle based IoT data

In the "Blockchain Oracles with IoT Integration" intersection of the IoT-DLT-AI Convergence Prism, we examine how the integration of IoT, specifically through the Gateway Broker layer, with blockchain oracles and smart contracts leads to enhanced functionalities in blockchain applications. This intersection is crucial for enabling smart contracts to interact with real-world data, thus extending their applicability beyond the blockchain.

Blockchain Oracles and Smart Contracts

- Role of Oracles in Blockchain: Oracles serve as intermediaries, providing real-world data to smart contracts on the blockchain. Smart contracts, being self-executing contracts stored on a blockchain, inherently lack the capability to access off-chain data.

- Limitations of Smart Contracts: Smart contracts are restricted to using data available on the blockchain, thereby unable to directly interact with external data like weather conditions, stock market fluctuations, or product pricing. Oracles bridge this gap by supplying such external data to smart contracts.

IoT Gateway Broker as an Oracle

- Function of the Gateway Broker: The Gateway Broker acts as a critical conduit between field devices (IoT devices) and the cloud. It collects data from IoT devices, processes it, and then relays it to the cloud. Conversely, it can transmit data from the cloud to IoT devices.

- Gateway Broker as an Oracle: In this context, the Gateway Broker can be conceptualized as an oracle. It provides essential real-world data to smart contracts, thereby enhancing their functionality and utility. For instance, a smart contract managing a building's temperature control system could utilize external temperature data provided by the Gateway Broker to make intelligent adjustments to the building's heating or cooling systems.

Enhanced Versatility of Smart Contracts with Oracles

- Real-World Data Utilization: By integrating real-world data through oracles, smart contracts can be employed in a broader range of applications, becoming more versatile and contextually relevant.

- Innovative Applications: As blockchain technology evolves, the use of oracles, especially in conjunction with IoT data, is expected to lead to more innovative and sophisticated applications of smart contracts.

6.6 AI-driven automatic sensors firmware update

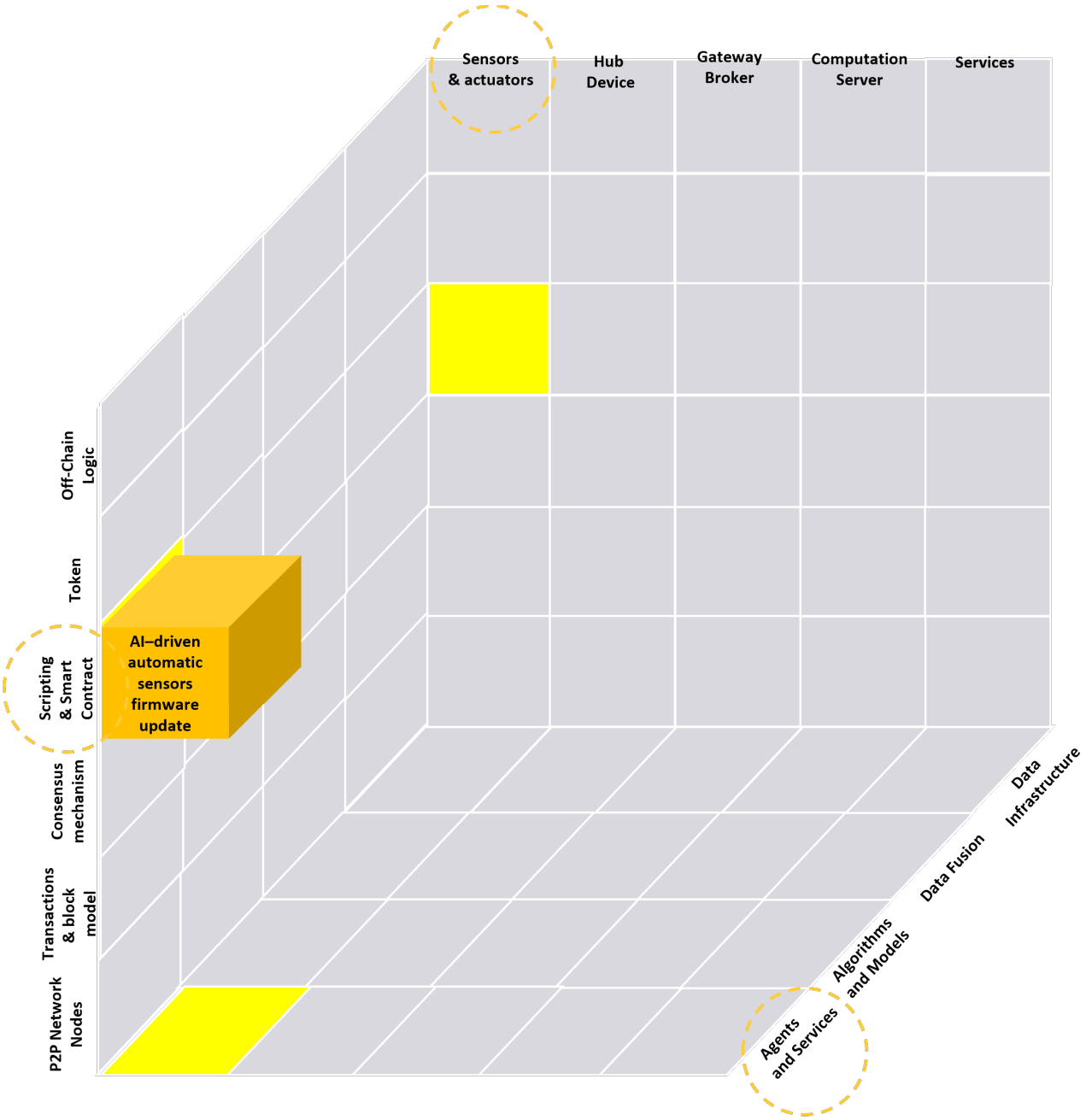


Figure 13. AI-driven automatic sensors firmware update

In the "AI-Driven Automatic Sensors Firmware Update" block of the IoT-DLT-AI Convergence Prism, we explore the integration of Distributed Ledger Technology (DLT), the Internet of Things (IoT), and Artificial Intelligence (AI) in enhancing the process of firmware updates in sensors. This convergence facilitates automatic, secure, and efficient firmware updates, leveraging the strengths of each technology.

Role of DLT, IoT, and AI in Firmware Updates

1. DLT for Firmware Update Management:
    a. DLT acts as a secure and reliable repository for storing firmware update information.
    b. It ensures the availability and secure distribution of firmware updates to all relevant sensors, mitigating risks of unauthorized access or tampering.
2. IoT for Data Collection and Monitoring:
    a. IoT devices, specifically sensors, collect critical operational data.
    b. This data is essential for monitoring sensor performance and identifying the need for firmware updates.
3. AI for Data Analysis and Update Decision-Making:
    a. AI algorithms analyze the data collected from sensors to assess their current state and performance.
    b. AI determines the necessity of a firmware update and can also generate specific instructions or algorithms for the update process.

Enhancing Sensor Efficiency and Security

- Automated Firmware Update Process: The integration of AI with IoT and DLT enables an automated approach to firmware updates. AI-driven analysis can pre-emptively identify the need for updates, enhancing sensor efficiency and accuracy.
- Security and Reliability: By leveraging DLT, the firmware update process becomes more secure and reliable, ensuring that updates are authentic and distributed effectively.

Practical Application Example

- Factory Temperature Sensor Management:
    - In a factory setting, AI can analyze data from temperature sensors to detect abnormal temperature rises in machinery.
    - Upon detecting a potential issue, AI can initiate a firmware update for the temperature sensor, potentially incorporating a more refined algorithm for temperature detection.
    - Such AI-driven updates can enhance sensor accuracy and responsiveness, potentially preventing machinery damage or failures.

6.7 Smart Data Management

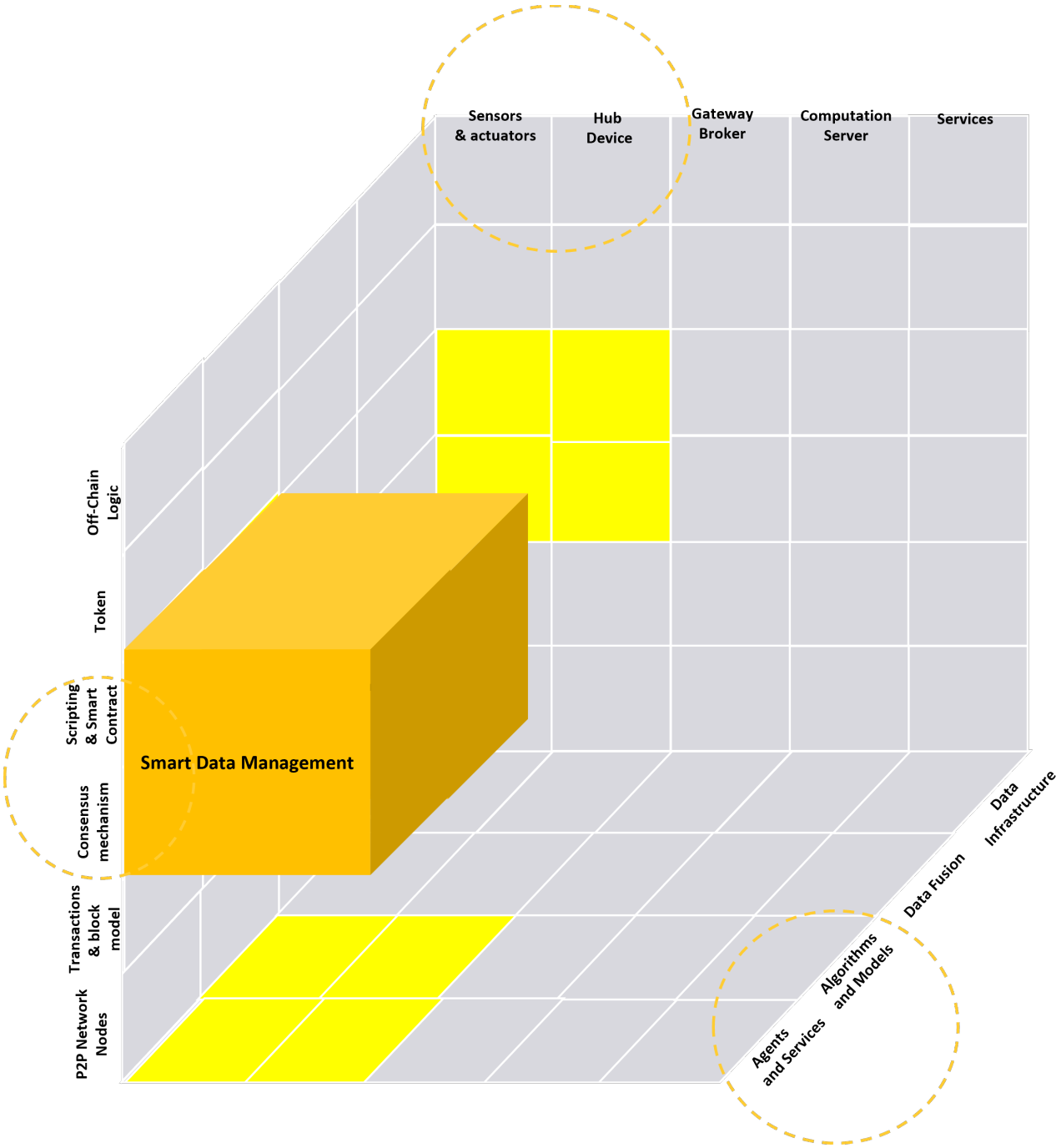


Figure 14. Smart Data Management

In the "Blockchain and AI for IoT Data Management" section of our IoT-DLT-AI Convergence Prism report, we address the integration of Blockchain and Artificial Intelligence (AI) technologies to enhance the management, storage, and security of data collected by IoT devices. This convergence offers a robust solution to the challenges of standardizing, securing, and efficiently managing the vast amounts of data generated by IoT devices.

Standardization and Interoperability

- IoT devices (e.g., smart home devices, sensors, machines) collect substantial amounts of data, traditionally stored on centralized servers without standardization.

- Blockchain technology can facilitate the standardization of data formats across various platforms, promoting harmonized data storage and increased interoperability.

Data Storage Options

- On-Chain Storage: Offers the advantage of permanent availability but can lead to significant storage demands, potentially impacting the blockchain's throughput and scalability.

- Off-Chain Storage: Involves storing actual data off the blockchain, with only aggregated metadata maintained on-chain, enhancing scalability but potentially reducing transparency.

Privacy and Security

- Blockchain platforms enable a high degree of data privacy through cryptography. Transactions can be pseudonymous or entirely anonymous, depending on the blockchain system.

- The architecture permits full encryption of stored and transmitted data, ensuring privacy and security, particularly vital for sensitive IoT data.

- However, complete anonymity can lead to potential misuse for illicit activities.

AI Integration for Enhanced Security

- AI can be employed to mitigate risks associated with transaction anonymity on blockchain platforms, using data analytics to detect and prevent illicit activities.

- AI algorithms, benefiting from extensive IoT data, improve in performance with more data, offering robust security solutions.

Scalability Challenges and Solutions

- Traditional concerns about blockchain's scalability, particularly with energy-intensive consensus mechanisms like proof-of-work, are being addressed with more efficient alternatives like proof-of-stake or proof-of-authority.

- AI, particularly through deep reinforcement learning (DRL), can optimize blockchain-enabled IoT systems, dynamically adjusting parameters like block producers and block size for improved throughput.

7. Use Cases

7.1 Development of Aquaculture (POAY in Greece)

Domain: Rural Development

Scope: POAYs are organized supervisory bodies for industrial activities that extend on land and sea and relate to existing or to be established, without environmental and spatial problems, aquaculture infrastructures (fish farms, packaging, fish food production etc). POAYs have been instituted by EU legislation and are compulsory for member states that include coastal lines at which industrial/commercial activities are established. For Greece a total of 23 such establishments are planned and expected to become operational in 2021. Their main role is the monitoring of environmental impact of aquaculture activities at the respective areas, in order to ensure that the foreseen sea activity planning progresses according to the national and EU policies. This involves measurements at frequent intervals of both sea water and air quality, proven validation and authenticity of these measurements, and final analysis to be delivered periodically to the central government. The above requirements can only be achieved if a robust IoT infrastructure combined with a proven DLT framework is provided to the POAYs and the respective organizations of other EU member states.

Area of convergence: (Data integrity) Interoperability and secure data exchange

Role of IoT: sensors and infrastructure

Role of DLT: device identity, secure data collection, monitoring, and certification.

7.2 VERSES DLT HSTP Spatial Web

Domain: Transversal

Scope: demonstrate the Hyper Spatial Modelling Language (HSML) and Hyperspace Transaction Protocol (HSTP) using COSM (Spatial Operating system) that enables interoperable, semantically compatible connections between connected software and hardware and includes specifications for: 1) a spatial range query format and response language for requesting data about objects within a dimensional range (spatial, temperature, pressure, motion) and their content; 2) a semantic data ontology schema for describing objects, relations, and actions in a standardized way; 3) a verifiable credentialing and certification method for permissioned create, retrieve, update, and delete (CRUD) access to devices, locations, users, and data; and 4) a human and machine-readable contracting language that enables the expression and automated execution of legal, financial and physical activities.

Area of convergence: verifiable credentialing and certification method for permissioned create, retrieve, update, and delete (CRUD) access to devices

Role of IoT: Autonomous drones, sensors, smart devices, and robots

Role of DLT: Certification methods for permissioned CRUD operations, access to devices data, human and machine-readable smart contracts for automated execution of legal, financial and physical activities

7.3 Bovlabs DLT PoC

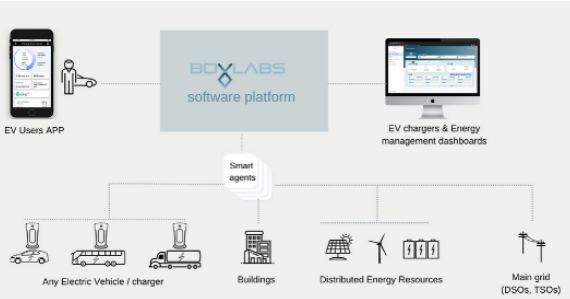
Domain: Energy, Mobility

Scope: platform to manage and control EV chargers. Our goal is to maximize utility for operators and EV owners. In doing so, charging cycles are optimized based on energy price, demand chargers, demand response programmers, along with driver inputs (for example, parking duration). Bovlabs PoC is set to demonstrate Ethereum Blockchain. Proof of Authority Based Consensus; 3 million transactions recorded in the first project; 450 transactions per second are supported; Smart agents uses light nodes to transact energy transactions; Smart contracts used for trade and execution (written using Solidity); ERC 20 Tokens used for transacting energy peer to peer.

Area of convergence: decentralization, scalability, micropayments, new business models.

Role of IoT: Smart agents integrate with any DERs (like solar, battery storage, EVSE) to record secure P2P energy transactions within the blockchain node embedded within the agent. This creates a distributed, decentralized dataset and with distributed intelligence at edges (ML) creates Virtual Power Plant

Role of DLT: Proof-of-authority consensus, smart contracts, tokens



7.4 VizLore DLT Labs

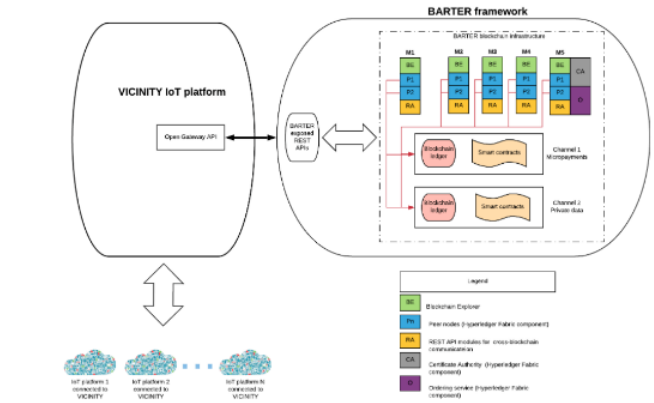
Domain: Smart city, smart buildings, e-mobility, agri-food, supply chain

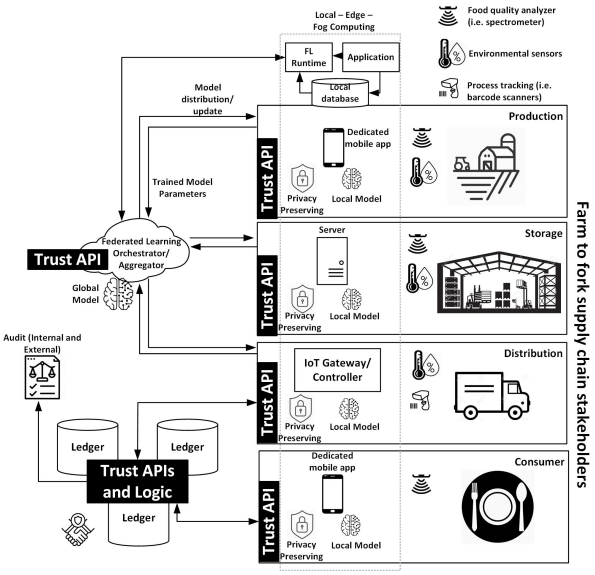
Scope: The DLT labs include two testbeds. The first is a micro-payment enabler service that can be exploited to support a range of use-cases that need a secure and scalable M2M micropayment solution, specifically designed for the IoT. The second is the FT-CHAIN testbed. This testbed is built by Freie University of Berlin and VizLore Labs Foundation in a bilateral research project – set to demonstrate quality and safety tracking of food through complex food supply chains combining federated learning, DLT and IoT.

Area of convergence: Autonomous M2M interaction, micropayments, smart sensing, trusted federated learning.

Role of IoT: M2M IoT Systems, Smart Sensing.

Role of DLT: Automated micro-payments and data storage. Smart contracts for regulations, ethics and business rules compliancy. Trusted data exchange. Trusted Federated Learning.





7.5 AIRQ DAO

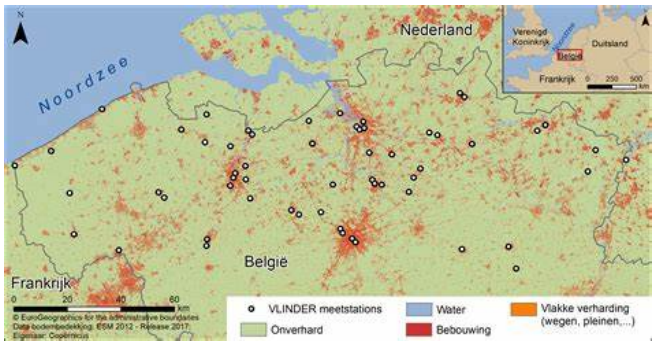
Domain: Smart city, Climate action

Scope: demonstrate the convergence of IoT and DLT into an autonomous system based on the AIOTI High Level Architecture (HLA) for data markets. Co-creation, micropayments and (smart contract) revenue-splits enable a 'self-sustaining' and financially autonomous IoT sensor network. Each air quality sensor integrates with the DLT network via a dedicated wallet. Local engaged citizens subscribe to notification services via micropayments. The sensor receives monthly payments, and an automated revenue split rewards the data aggregator, service providers and the AIRQ DAO foundation. If the sensor can earn its own value after two years, a smart contract orders his replacement. As such, only valuable sensors are maintained, and the network becomes (financially) self-sustainable.

Area of convergence: Decentralization, scalability, data monetization.

Role of IoT: Air quality monitoring stations.

Role of DLT: Automated micro-payments, smart contracts



7.6 BEIA PimeoAI

Domain: AI, Unmanned Surface Vehicle, water pollution

Scope: An artificial intelligence (AI) powered unmanned surface vehicle (USV) capable of performing a full range of water quality tests in all types of sensitive aquatic ecosystems is developed and tested in several representative situations. The PIMEO AI USV that results will be a cutting-edge advanced analysis tool for analyzing fragile ecosystems, identifying pollution sources, and mapping their environmental impact. It will meet a critical market demand for complete water quality USVs, which are currently scarce and mostly used in hydrology research.

Area of convergence: IoT Network Security & Identity Management, Autonomous M2M interaction

Role of IoT: The USVs will be integrated with water quality sensors that will measure different water parameters (Temperature, Conductivity, pH, Turbidity, Chlorophyll) and record GPS coordinates.

Role of DLT: The blockchain technology will be utilized to provide trust and traceability, such as securely handling sensor data information and stakeholders' identities. Implementing reliable, secure data transfer and access will enable GDPR compliance in terms of security and privacy.

7.7 FarmSustainaBL

Domain: Smart Farming, GHG emissions reduction

Scope: The project's major goal is to use a holistic strategy to reduce GHG emissions associated with intensive livestock farming by optimizing livestock production. The collaboration will accomplish so by keeping an eye on the animal diet, animal behaviour and traits, and a stable environment. A web-based platform will be established to collect and analyse all of the above data in order to provide suggestions to livestock farming stakeholders (farmers, consultants, etc.) so that management decisions may be made to reduce GHG emissions.

Area of convergence: decentralization, IoT Network Security & Identity Management

Role of IoT: IoT devices will be installed in the farm for monitoring key parameters of the animal (motion sensor, accelerometer, weight sensor etc.), the stable environment (gas sensors (CH4, NH3, NOx, COx and others), humidity, temperature) and the feed (weight sensor, humidity sensor, flow sensor, etc.).

Role of DLT: The platform will employ Blockchain Technology to provide features like data protection, data privacy, data sharing, traceability, and smart contracts among livestock farming players. The platform's smart contracts functionality, in particular, will assist livestock farming players in obtaining contracts with better prices due to lower GHG emissions.

7.8 SMARDY Open Science

Domain: Data Exchange, Data Security, Blockchain

Scope: Smardy is developing a research data marketplace for technology transfer based on software and data carpentry (i.e., developing and teaching workshops on the core data skills required to conduct research) where academia, industry, and government can share datasets, technology, and curated tools to promote economic and social development. A marketplace like this puts together data producers and data consumers to support the implementation of cross-cutting solutions based on an open innovation approach.

Area of convergence: interoperability, Secure Data Exchange

Role of DLT: One of the main objectives of the SMARDY project is data security and data protection in the online environment. Smardy integrates blockchain technology to meet this objective. The exposure of data to customers for use in various research must guarantee its authenticity in a secure, decentralized and uneditable environment. These features are the characteristics with which blockchain technology has entered the technology market. For the exchanging actions, the guarantee of data exposure security is achieved by Ethereum, one of the most popular and secure blockchain environments.

7.9 ERATOSTHENES Smart Health

Domain: Personalized devices, data exchange, data security, blockchain

Scope: The Smart Health use case is a Remote patient monitoring system. It facilitates remote assistance and follow up on patients suffering from chronic diseases such as diabetes, COPD or other diseases where patients at least partly can stay at home such as COVID-19. In general, the eHealth use case enables patients to stay home during treatment and care and foster self-care. It includes a Personal Health Gateway, which is deployed in every patient's home, that is responsible for collecting data from various medical sensors and sending them to the back-end Cloud services. The services provide data to health personnel allowing for remote patient monitoring, data is recorded in the patient's electronic health journal, and it normalizes data according to standard eHealth ontologies to allow for performing various data analysis.

Area of convergence: interoperability, Secure Data Exchange

Role of DLT: The DLT utilizes blockchain technology to provide decentralized solution for the transparent and immutable storage of the information that will be used by the ERATOSTHENES and its components. Basically, it is a distributed storage that is immutable and cannot be altered and everything which is stored in this space like identity management or the trust score information is verifiable by the peers in the network. In this use case, DLT is used for storing the DID created during the process of onboarding of Tellu gateway. It will also be used for storing the Trust score by the TMB/TMRA component.

7.10 ERATOSTHENES Automotive

Domain: Automotive, car on-board units, V2I/V2V communications

Scope: In the automotive world, the number of IoT devices involved has increased drastically in the latest years due to the evolution of the environment to a smarter one. In this new smart environment, all the actors are interacting between themselves and making decisions by themselves. Due to this tendency, increasing the cybersecurity in this field is a requirement. Two use-cases are suggested here, the first one is about the interaction with the infrastructure and the second one wants to cover a key topic in the automotive world, a software update of the vehicle units. Specifically, this use case tests the prospective benefits for connected vehicles that interact not only with other vehicles but also with external roadside elements, such as smart traffic lights. These vehicles need to ascertain the trustworthiness of these elements, aiming not only to prevent potential accidents but also to safeguard the privacy of the vehicle's driver or owner.

Area of convergence: interoperability, Secure Data Exchange, Firmware update, OS security

Role of DLT: The 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.

8. Conclusions

In conclusion, it is essential to recognize the transformative potential of integrating Distributed Ledger Technology (DLT), the Internet of Things (IoT), and Artificial Intelligence (AI).

The convergence of these technologies heralds an era of smart, interconnected systems that are secure, self-regulating, and highly intelligent. The Convergence Prism highlights the synergistic integration of DLT, IoT, and AI, showing how this convergence could significantly enhance functionality, security, and efficiency, paving the way for innovative solutions across various sectors.

The future holds immense potential for further exploration and exploitation of these convergences, promising to revolutionize numerous aspects of technology and society. This report serves as a foundation for understanding and leveraging these convergences, stimulating further research and development in this promising and rapidly evolving field.

Contributors

Editors:

Alfredo Favenza (Fondazione Links)

Silvio Meneguzzo (Fondazione Links, University of Turin, ISAS)

Reviewers:

Damir Filipovic (AIOTI)

Tom De Block (Nearcom)

Contributors:

Raúl Orduna (Vicomtech)

Tasos Charissis (Nydor System Technologies)

Tom De Block (Nearcom)

Philippe Sayegh (Verses)

JK Pillai (BovLabs)

Milenko Tosic (VizLore Labs)

George Suciu (BEIA)

Theodor Bratu (BEIA)

Konstantinos Loupos (INLECOM)

Konstantinos Dafloukas (INLECOM)

Acknowledgements

About AIOTI

AIOTI is the multi-stakeholder platform for stimulating IoT Innovation in Europe, bringing together small and large companies, start-ups and scale-ups, academia, policy makers and end-users and representatives of society in an end-to-end approach. We work with partners in a global context. We strive to leverage, share and promote best practices in the IoT ecosystems, be a one-stop point of information on all relevant aspects of IoT Innovation to its members while proactively addressing key issues and roadblocks for economic growth, acceptance and adoption of IoT Innovation in society.

AIOTI's contribution goes beyond technology and addresses horizontal elements across application domains, such as matchmaking and stimulating cooperation in IoT ecosystems, creating joint research roadmaps, driving convergence of standards and interoperability and defining policies. We also put them in practice in vertical application domains with societal and economic relevance.