Alliance for Internet of Things Innovation

Report on DLT-IoT Technological Convergence

Release 1.0

AIOTI IG Distributed Ledger Technologies

27 May 2022

Table of Content

Table of Figures

1. Introduction

Convergence of disruptive technologies is driving the society towards a fast and unprecedented digital transition, breaking the barriers between the physical and the digital world. Framing the complexity of this phenomenon requires a deep understanding of involved technologies and a clear comprehension of how the underlying building blocks could work together to build new platforms and real-world applications.

This report presents the AIOTI perspective on the convergence of the Internet of Things (IoT) and the Decentralized Ledger Technologies (DLT) exploring the opportunities lying at the intersection connecting the different layers of the two technological stack to identify promising areas of integration and related use cases.

The analysis begins with the definition of two high-level technological stacks as a steppingstone to understand the characteristic of the underlying building blocks. Subsequently, the discussion will move to the identification of areas and topics of interest by means of a Convergence Matrix aiming to set a common ground of open research topics and applications opportunities. Finally, to connect the theoretical analysis to real use cases, the most promising convergence' topics will be selected and linked to the existing applications identified among the AIOTI DLT Testbeds.

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 **Figure 1.**, 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[6].

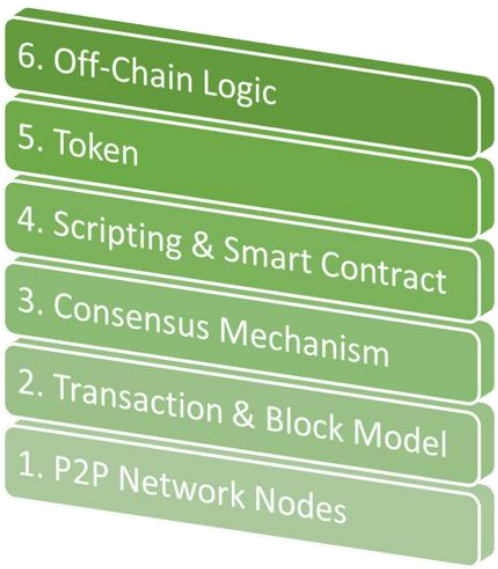


Figure 2. ***DLT Stack***

[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.
[6] Medium.com, "Exponential Technologies Convergence: Can AI help Shaping a New Breed of DLTs?", 2020

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[7].

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[8]. 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[9] .

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.

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

Sensors and Actuators. Sensors and Actuators are elements exposing either an analogue Interface or a digital Interface[10]. 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 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[11]. 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.

10 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.
11 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.

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. 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.

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.)[12]. 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 users and the data or firmware of the devices.

12 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[13].

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. identity provider 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. 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.

13 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. Convergence Topics

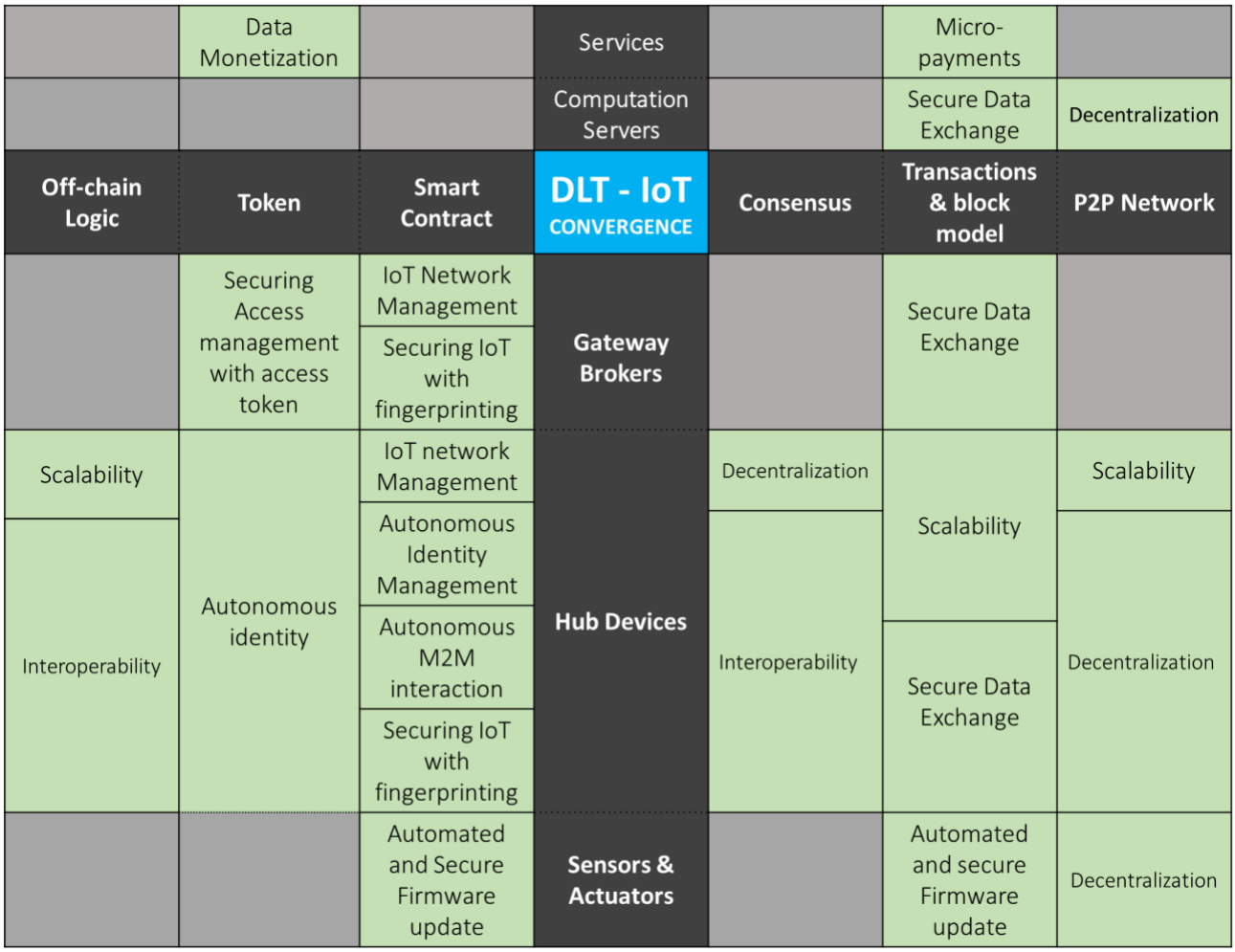


Figure 4. DLT-IoT Convergence Matrix

Decentralization

Decentralization is a key feature of DLTs 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 DLT-enabled edge intelligence. The integration of DLT and edge computing can introduce 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.

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 force 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. DLTs 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 DLT-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 & Identity Management

Implementing a distributed network into an IoT ecosystem has innate structural security 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 penetration of a majority of connected nodes, making it virtually impossible. Blockchain can also provide mechanisms for IoT devices identity authentication SSI.

Autonomous M2M interaction

One of the biggest issues of machine-to-machine communication is that, over time, every manufacturer will come up with their own machine-to-machine (M2M) protocol, making it troublesome to integrate products and services. Leveraging transactions and Smart Contracts, DLTs can allow machines to hold funds, make decisions based on complex business logic and carry out transactions.

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.

Data monetisation

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.

Voting and negotiation

Voting systems are widely adopted in IoT, for many applications, for example: (i) for the election of a leader in wireless sensor networks; (ii) for autonomous and distributed decision making; (iii) to decide if a new device is a trusted one which can join the network and ask for services; (iv) to choose which is the most trustworthy provider when there are multiple devices that provide the same service. DLTs, through consensus and tokenization mechanisms can enable IoT networks to autonomously negotiate and reach a common agreement through a voting process. The system can perform a simple majority voting, or a more complex voting process by exploiting the specific characteristics of the different consensus protocols and tokenization mechanism (as described in section 2).

5. Use Cases

5.1 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: Interoperability and secure data exchange

Role of IoT: sensors and infrastructure

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

5.2 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

5.3 Blue Future Organization DAO

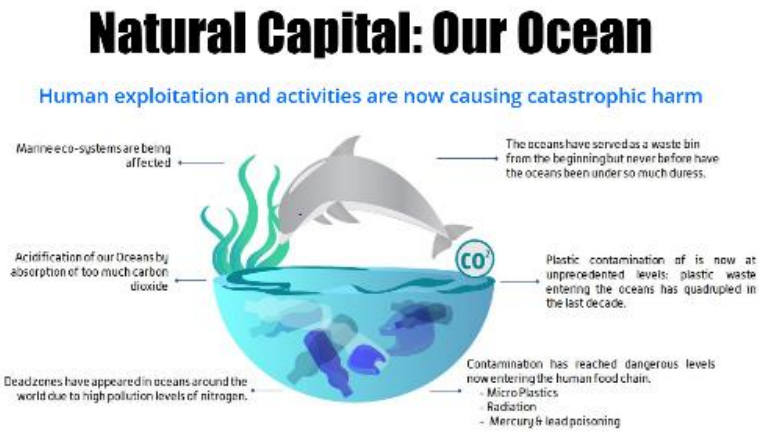
Domain: Farm-to-Fork, Farm-to-Finance, Climate action

Scope: demonstrate how Distributed Ledger Technologies enables "Farm-to-Fork" in aquaculture as a foundation to enable financial instruments and investments for acceleration into the blue economy. BFO is set to provide insights into the technical layers allowing observers to properly understand how the DLT is applied into the IT stack. BFO also demonstrates the autonomous reporting mechanism with XBRL as facilitator for financial and non-financial information.

Area of convergence: Secure data exchange, interoperability, data monetization, new business models

Role of IoT: Water quality sensors, data collect, surveillance

Role of DLT: DAO, Voting, Certification



5.4 Bovlabs DLT PoC

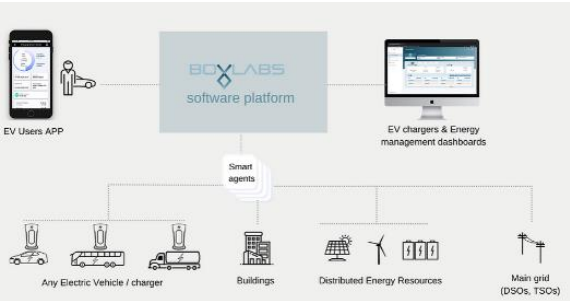
Domain: Energy, Mobility

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



5.5 VizLore DLT Labs - Blockchain-Assisted Real-time Transaction Execution and Repository framework (BARTER) Testbed

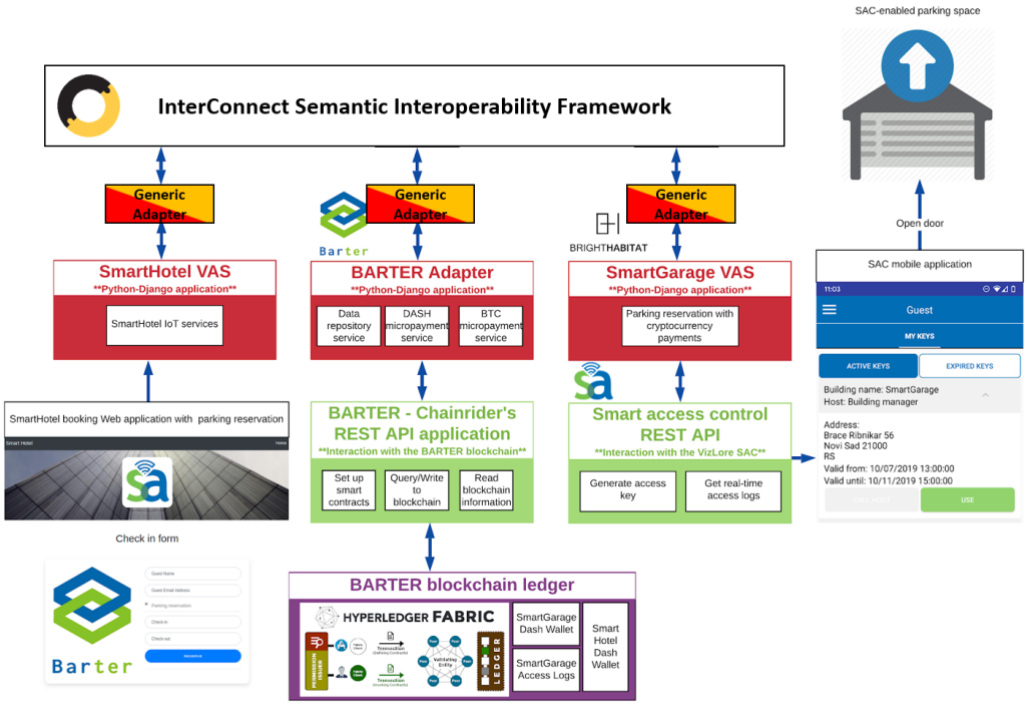
Domain: Smart city, smart buildings, e-mobility

Scope: Testbed is set to demonstrate a blockchain framework built on top of Hyperledger Fabric, Dash, Bitcoin and VizLore's ChainRider service. It is a micro-payment enabler service that can be exploited to support a range of use-cases that need a secure and scalable M2M micro-payment solution, specifically designed for the IoT. The testbed includes parking reservation emulation and IoT system for access control. The testbed utilizes semantic interoperability framework of the InterConnect project for interconnecting different services.

Area of convergence: Autonomous M2M interaction, micropayments, interoperability.

Role of IoT: M2M IoT Systems, smart sensing and actuation.

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



5.6 VizLore DLT Labs - Federated and Trusted Food Supply Chains (FT-Chain) Testbed

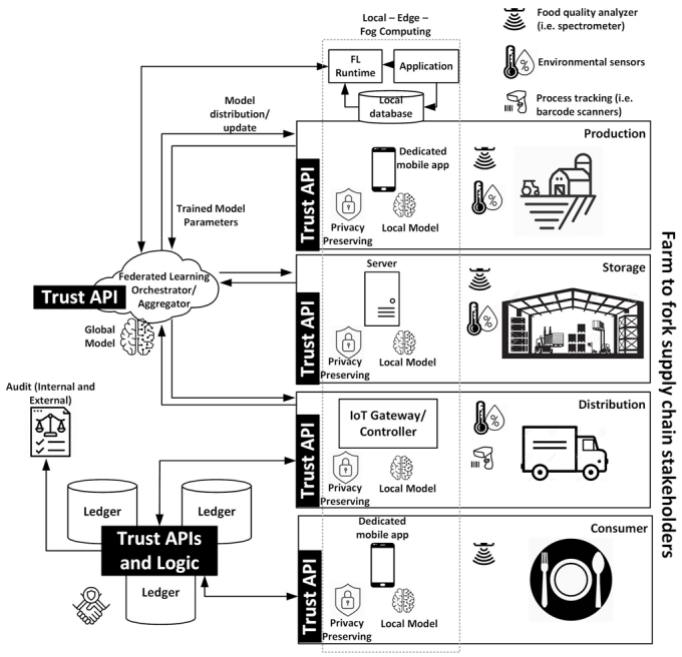
Domain: food supply chains

Scope: FT-Chain combines IoT system for food quality measurements (spectrometry methods), IOT system for environmental sensing, Hyperledger Fabric based ledger for trusted data sharing between parties and federated learning framework for high performance data analysis and decision making. The goal is to emulate complex processes and dependencies in food supply chains that might result in food quality degradation and contamination.

Area of convergence: decentralization, trust management.

Role of IoT: environmental sensing, field spectrometry, smart actuation.

Role of DLT: smart contracts for supply chain process automation, trusted federated learning and local/global ML model alignment, auditing and reporting.



5.7 AIRQ DAO

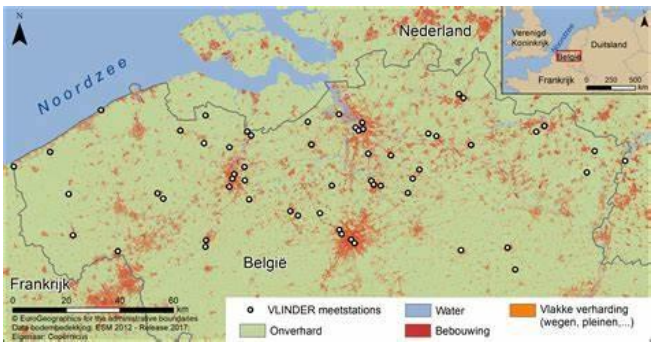
Domain: Smart city, Climate action

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



5.8 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 analysing 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.

5.9 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.

5.10 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.

6. Conclusions

IoT and DLT are both following a very steep hype curve. We will probably witness a progressive convergence between these two technologies, producing a new wave of creative destruction in many industries. It is thus essential to understand how to take advantage of the opportunities arising from this technological trajectory.

As for the advantages that DLT could bring to IoT, our analysis highlights innovation opportunities in increasing interoperability at device and network levels, improving security and identity management, enabling M2M autonomous interaction, micro-payments and data monetisation. IoT could aid DLT by delivering computing and cache resources to the DLT on edge devices.

This concludes the first version of this report that we intend to further extend with the emergence of new test beds and use cases that could give space to other topics of technical and social relevance such as the energy efficiency of DLTs, consensus mechanisms and of automatic voting for IoT sensor networks, and new business models that leverage the convergence of IoT and DLT.

7. Contributors

Editors:

Alfredo Favenza (Fondazione Links)

Reviewers:

Damir Filipovic (AIOTI)

Contributors:

Alfredo Favenza (Fondazione Links)

Giacomo Corrias (Fondazione Links)

Raúl Orduna (Vicomtech)

Tasos Charissis (Nydor System Technologies)

Tom De Block (Nearcom)

Philippe Sayegh (Verses)

JK Pillai (BovLabs)

Milenko Tošić (VizLore Labs)

Ismail Arribas (Blue Future Organisation)

George Suciu (BEIA)

Theodor Bratu (BEIA)

Acknowledgments

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.