EUROPEAN COMMITTEE FOR STANDARDIZATION

EUROPEAN COMMITTEE FOR ELECTROTECHNICAL STANDARDIZATION

Recommendations for Successful Adoption in Europe of Emerging Technical Standards on Distributed Ledger / Blockchain Technologies

CEN-CENELEC Focus Group on

Blockchain and Distributed Ledger Technologies (FG-BDLT)

White Paper Subgroup: N 001

Document Title	Recommendations for Successful Adoption in Europe of Emerging Technical Standards on Distributed Ledger/Blockchain Technologies
Last modification	20th September 2018
Document Version	1.1

SECRETARIAT UNI/UNINFO

Via Sanfront, 1/C • 10138 TORINO ITALY

Tel: +39 011 501027 email: sirocchi@uninfo.it

Subgroup Convenor: Pietro Marchionni

Convenor: pietro.marchionni@agid.gov.it

(This page is intentionally left blank.)

Contents

1. Introduction

CEN and CENELEC created a new Focus Group on Blockchain and Distributed Ledger Technologies (FG-Blockchain-DLT), with objectives to support the standardization work carried on in ISO/TC 307, to identify potential European needs for Blockchain and DLT standardization (e.g. for the European implementation of ISO/TC 307 standards), and to encourage further European participation in ISO/TC 307.

The European Commission contacted CEN and CENELEC to consider the possibility to draft a white paper on European Blockchain standardization, which would highlight some European specificities, notably when it comes to the particular legislative and policy context, or specific use cases. It was commonly agreed that CEN-CENELEC FG-Blockchain-DLT would take ownership of this white paper project, to assign it to a dedicated sub-group, and to organise regular stakeholder engagement meetings to support the work of the Focus Group.

The objective of this white paper is to identify potential and European specific needs in standardization, i.e. provide recommendations on how best to standardize Blockchain and DLT within Europe.

The adoption of common standards contributes to avoiding market fragmentation and customers being locked in proprietary solutions, increases competition, and when adopted in (public) procurement, offers SMEs better opportunities to compete with major vendors. It may also improve the quality of the technology used as problems of asymmetric information and market failure can be addressed through standardization.

2. Rationale

The European Commission ICT Strategy for the creation of an inclusive digital society ('Digital Society') finds application in the creation of a digital single market to ensure access to online activities for individuals and businesses under conditions of fair competition, consumer and data protection, sustainable development, inclusiveness, removing geo-blocking and copyright issues.

Key policy areas to develop the digital market include the digitisation of industry and modernisation of public services; the strategy of the Digital Society requires building blocks on which such a strategy can be built. Digital identity, data protection and integrity, security, cross border data sharing, interoperability, electronic signatures, and process automation are some of the base elements and have been identified as topics requiring particular attention at European level.

Blockchain and Distributed Ledger Technologies, with their characteristics of tamper resistance, security, shared consensus, distribution of resources and disintermediation, instant availability of data updates to connected parties, can address and contribute to the implementation of the building blocks of the Digital Society.

These technologies will likely lead to a major breakthrough that will transform the way information or assets are exchanged, validated, shared and accessed through digital networks. They are likely to continue to develop in the coming years and become a key component of the digital economy and society.

To support the European Commission initiatives within this strategy, the CEN and CENELEC Focus Group on Blockchain and Distributed Ledger Technologies (FDLT) was established and will maintain a white paper collecting identified specific European needs on these technologies, in a European normative and technological context.

The Focus Group aims then to support the European Commission and standardization bodies at international level (as indicated in the References section), specifically ISO/TC 307.

This will be achieved by raising awareness on ISO's activities and encouraging a broader European participation in ISO/TC 307 and other international bodies.

3. European Commission Initiatives Highlights

Blockchain and Distributed Ledger Technologies (DLT) can change the way citizens and organisations collaborate, share information, execute transactions and deliver services.

The technology promotes user 'trust', making it possible to share on-line information, agree on and record transactions in a verifiable, secure and permanent way. Today, the technology is being used in mainly financial services but will be increasingly integrated into other digital services (such as regulatory reporting, energy and logistics).

This technology is an opportunity for Europe and its Member States to re-think information systems, to promote user 'trust' and the protection of personal data, to help create new business opportunities and to establish new areas of leadership for digital applications that benefit citizens, public services and companies.

Europe is well placed to take a global leadership position in the development of new trusted services and applications based on blockchain and distributed ledger technologies.

The European Commission launched the EU Blockchain Observatory and Forum in February 2018[1] involving private stakeholders and public authorities in technical and regulatory discussions about the future development and applications of blockchain technology. Among its important tasks, it will gather the best European experts in thematic workshops on important subjects such as Blockchain and GDPR, or blockchain innovation, and produce reports, which will help European stakeholders to deploy blockchain based services in Europe[2].

On the 10th of April 2018, the European Blockchain Partnership was launched[3], with 22 European countries agreeing, through a joint declaration to cooperate in the establishment of a European blockchain services infrastructure that will support the

[1] https://www.eublockchainforum.eu/

[2] https://www.eublockchainforum.eu/reports

[3] https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership

delivery of cross-border public services, through interoperability and open interfaces and with the highest standards of security.

The European Commission has already invested more than € 80 million in projects supporting the use of blockchain in technical and societal areas. Up to € 300 million is expected to be further invested until the end of the EU funding programme Horizon 2020[4].

In its Communication on ICT standardization priorities, adopted in April 2016[5], the Commission explained why the development and adoption of international standards in emerging technologies is an important element of the Digital Single Market Strategy.

The adoption of common standards contribute to avoiding market fragmentation and customers being locked in proprietary solutions, increases competition, and when adopted in (public) procurement, offers SMEs better opportunities to compete with major vendors. Through its liaison with ISO Technical Committee 307 on Blockchain and Distributed Ledger Technologies, the Commission is contributing to international standardization in important areas such as smart contracts, identity, security and privacy, governance, use cases, etc.

Within this process there is also a need to identify potential specificities related to the European market, whether they relate to regulations and policies, such as the GDPR or eIDAS, to priority use cases, for example in the public sector, or to specific development of the European market.

[4] https://ec.europa.eu/digital-single-market/en/news/h2020-information-day-blockchain-and-distributed-ledger-technologies-topics-follow

[5] https://ec.europa.eu/digital-single-market/en/news/communication-ict-standardisation-priorities-digital-single-market

4. The CEN and CENELEC Focus Group 'Blockchain and Distributed Ledger Technologies' recommendations

4.1 Support for European industrial priorities (e.g. Digitising European Industry initiative)

Rationale

The European Commission launched the Digitising European Industry initiative (DEI) with the objective to reinforce the EU's competitiveness in digital technologies and ensure that its citizens and businesses can draw the full benefits from digital innovation in the so-called **4th Industrial Revolution** in an environmentally sustainable way.

At the same time, consideration must be given in order to anticipate and dampen the disruptive effects that may harm the livelihood of certain individuals without the proper training and sectors that are rendered obsolete by the sudden changes.

On this basis, this section identifies and recommends specific technical standards that in FG-BDLT's opinion will hasten and encourage the widespread adoption of digitisation and a Single Digital Market by industrial companies within the EU, while protecting citizens' individual privacy concerns and providing effective security against malicious and intentional attacks.

The objective is greater efficiency, productivity and competitiveness of EU industrial companies, and their full integration within the global digital market.

Context

Building on and complementing the various national initiatives for digitising industry, the DEI actions are structured around five main pillars:

Figure 1 DEI pillars
© European Commission

1. European platform of national initiatives on digitising industry

This EU coordination forum brings together all Member States to ensure coherence and collective steer. The goal is to build a critical mass of initiatives and investments for digitising industry, and to ensure the commitment of Member States, regions and private sector to achieve the DEI goals.

2. Digital innovations for all: Digital Innovation Hubs

Digital Innovation Hubs (DIHs) are one-stop-shops where companies – especially SMEs, start-ups and mid-caps – can get help to improve their business, production processes, products and services by means of digital technology. One of the key DEI priorities is to support a strong network of DIHs to ensure that every company in Europe can take advantage of digital opportunities.

3. Strengthening leadership through partnerships and industrial platforms

To reinforce the EU's competitiveness in digital technologies, the DEI initiative supports both the development of digital industrial platforms and large-scale piloting

and Public-Private Partnerships (PPPs) that provide the digital technology building blocks of the future.

4. A regulatory framework fit for the digital age

A digital-friendly regulatory framework is important for the EU's industry and economy to strive. Within the Digital Single Market strategy, the European Commission has already proposed several measures to update regulations in key fields for industry such as cybersecurity and free flow of data.

5. Preparing Europeans for the digital future

To make the most of the digital transformation we must ensure that all Europeans are ready for these changes. Adapting the workforce and our education and learning systems, together with major investments in reskilling citizens, are needed. European initiatives such as the digital skill and jobs coalition and the digital opportunity scheme can help to bridge the gap.

As Pillars 1, 2 and 5 refer mainly to governmental policy and training initiatives, in this section of the White Paper the FG-BDLT will focus first on defining and understanding what is known as Industry 4.0 and then make recommendations that the European Commission may choose to consider related to Pillar 3 (digital industrial platforms) and Pillar 4 (regulatory frameworks).

The fundamental objective of **4th Industrial Revolution** I4.0 is to improve industrial companies by the best application of existing great improvements available today and expected future breakthroughs in information and communication technologies

While large corporations may have entire departments dedicated to analyse trends and adopt new technical developments in their sectors, a small and medium size business (SME) manager may find it challenging to even understand and predict the effects of the paradigm shift on the business, when and how to respond or who to ask for help.

I4.0 is the industrial initiative that proposes the application of the Internet and the previously defined IoT to the fullest extent, by directly integrating the operational and technical processes of businesses with their commercial and customer service facets.

Examples of this new breed of novel, integrated and highly disruptive businesses are Amazon, AirBnB and Uber. They have leveraged current communications and data

processing capabilities so that their customers are self-served in automated ways, while reducing capital expenditures by leveraging the assets of others, by drop shipping from manufacturers, promoting empty apartments, or organising a fleet of vehicles, respectively.

Industry 4.0 Key Characteristics

Cyber-Physical Systems (CPS)

Intelligent systems that combine 'hardware' and 'software' of the computers and the devices or physical components. They acts as a unified system and interact to interpret the changes in the real world.

Internet of Things (IoT)

Infrastructures, technologies and applications that create a bridge between the virtual world of computers and the real world.

Additive Manufacturing (AM)

Production of a product directly from a virtual 3D model in a completely automated manner using a 3D printer or similar devices.

Horizontal Integration

Horizontal integration goes beyond the internal operations of a Company, combining all the key contributors of the various stages of the supply chain, from suppliers all the way to customers and consumers.

Vertical Integration

I4.0 digitises and integrates all the processes in a vertical manner throughout the organisation, from product development and purchasing all the way to production, logistics and customer service.

Big Data

IoT and the technologies that are based on remote offsite storage ('Cloud Storage') and remote massive computation ('Cloud Computing'), the main service of Amazon Web Services ('AWS') and Microsoft Azure, greatly foster the proliferation of data generation and the possibility to collect and store them, even when they are

generated in factories and industrial plants. This new capability allow factories to monitor and control the processes with a high degree of sophistication, but they must be stored, retrieved when necessary, and convert them into usable information and analysed to derive knowledge.

Standards

In the business world, standards are considered the sum of rules, laws and directives that determine the essential requirements that a product must follow. Standards are considered obligatory if they are included in certification documents.

The final objective of I4.0 is to horizontally and vertically connect all the phases of the production process. The integration will be successful as long as the necessary technology is supported by standards that are defined by consensus; as an example there are already several initiatives being developed for IoT.

The standards will help improve safety and planning in the factories, and are the foundation for product quality and reliability improvements. They are at the disposal of businesses, industries and governmental bodies to get together, comment and generate the international standards that may be required. Standards ensure that components and systems from different suppliers and with different technologies may interact to create a working whole.

The continuous development of common standards will guarantee that data may automatically flow among different automation system without requiring conversions or interpretation since the logic will be shared among all of them.

A similar situation was endured during the development of standards for the electronic systems for buildings and homes, as mentioned one of the first applications of IoT, and agreement took between five and ten years; it has not been a simple task to arrive at systems such as LON or Konnex.

According to Bas de Vos, director of IFS Labs:

> *"one of the biggest potential use cases for blockchain in aviation [or industry] is to help track parts and assets. Today's assets are often tracked in disparate systems with incomplete records from written or verbal communication and*

large volumes of paperwork (…) This is where Blockchain has inherent value — when there is a large, complex supply chain. It's also useful if there are multiple points of potential failure, a high risk of cyberattacks or if there are high costs involved. By providing trustworthy information across the entire chain of transactions, the technology helps provide a single picture of the truth to all parties involved."

Blockchain helps reduce some of the security concerns of IT Managers that are overwhelmed with the tsunami of data being received from thousands of sensors, and are forced to move storage to cloud-based systems. Without security, the possibility of interception of this data by hackers is a real concern, especially in critical plants where interruptions are very expensive or may even put lives at risk.

Digital industrial platforms are key to place Europe in the lead of digital transformation, as they make the bridge between technology building blocks on the one hand and industrial applications on the other and DLT/Blockchain technologies can represent a key value for such digital platforms.

As an example, BMW, Bosch, Ford, General Motors, Renault, ConsenSys, IBM, Hyperledger, and others launched the Mobility Open Blockchain Initiative in May 2018.

MOBI's first projects develop Blockchain use cases and technology standards for automotive applications. MOBI's first project is to build a vehicle digital identity prototype or car passport that can track and secure a vehicle's odometer and relevant data on distributed ledgers. This can dramatically reduce fraud in used car sales as buyers can finally have an accurate vehicle history.

Furthermore, in this context, the Joint Research Centre (JRC) of the European Commission has issued a Science for Policy report, providing evidence-based scientific support to the European policy making process, which addresses Blockchain for Industrial transformations[6].

[6]https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/blockchain4eu-blockchain-industrial-transformations

In this report, the need to improve the current multi-stakeholder governance processes for the development of standards is described. Fostering interoperability with wider engagement to avoid vendor lock-ins is notably emphasised.

Therefore, the protection of personal data, interoperability, ethical and (data) security standards to be applied to Blockchain and Distributed Ledger Technologies are critical to ensure the successful deployment of Blockchain and DLT throughout Europe.

CEN and CENELEC already have Technical Committees (TC) in place, supporting the digital transformation of Industry, and addressing the above-mentioned aspects:

CEN/TC 114 and CLC/TC 44X	Safety of machinery
CLC/TC 65X	Industrial-process measurement, control and automation
CLC/SR 119	Printed electronics
CEN-CLC/JTC 13	Cybersecurity and data protection
CEN-CLC/JTC 8	Privacy management in products and services
CEN/TC 310	Advanced automation technologies and their applications
CEN/TC 438	Additive Manufacturing
CLC/TC 210	Electromagnetic Compatibility (EMC)
CEN/TC 224	Personal identification and related personal devices with secure element, systems, operations and privacy in a multi sectorial environment
CEN/TC 225	AIDC Technologies

CEN/TC 319	Maintenance
CLC/TC 13	Electrical energy measurement and control
CLC/TC 205	Home and Building Electronic Systems (HBES)
CLC/TC 215	Electrotechnical aspects of telecommunication equipment
CEN/TC 224	Personal identification and related personal devices with secure element, systems, operations and privacy in a multi sectoral environment
CLC/TC 8X	System aspects of electrical energy supply
CLC/TC 57	Power systems management and associated information exchange
CEN/CLC/ETSI SEG-CG	Coordination Group on Smart Energy Grids
CEN/CLC/ETSI SM-CG	Smart Meter Coordination Group

The following IEC Committee is also evaluated as relevant:

IEC SyC 'Smart Energy'	System Committee 'Smart Energy'

In support to the European Industrial priorities and the Digital transformation of European industries, and to ensure the uptake of Blockchain and DLT, the potential

revision of the current scope of the above-mentioned technical committees could be envisaged.

This will also suppose that an appropriate Blockchain and DLT expertise is or will be available within these Technical Committees.

It is also vital that the standardization framework encompasses a set of information security requirements for demonstrably secure Blockchain implementations, enabling their adoption on the market.

ICT standards have also a considerable impact on industrial competitiveness. It is especially important that products and services are mutually compatible and interoperable. Standards help to ensure that products made by different companies are able to work together seamlessly.

The ICT and Industrial standardization landscape is composed of different actors: European Standardization Organizations, international Standards-developing organizations, fora and consortia. These organizations should join forces in order to develop a consistent set of standards and technical specifications to ensure the digital transformation of industry.

European Commission has triggered the establishment of a Joint MSP/DEI Working Group (Joint Multi-Stakeholder Platform on ICT standardization and the Digitising European Industry initiative) to respond to this challenge.

This group will notably focus on the standardization needs for the 'smart' manufacturing sector, create a first overview and analysis of the related market needs, and develop a model for the synchronization of the various activities.

The first outcomes are expected by the end of 2018.

It is therefore recommended that the CEN-CENELEC Focus Group on Blockchain and DLT monitor the activities of the Joint MSP/DEI WG, in order to identify areas of cooperation with SDOs, fora and consortia, and identify the various initiatives related to blockchain for the industrial sectors.

The CEN-CENELEC Focus Group on Blockchain and DLT could act as a reference point for exchange between the CEN and CENELEC technical committees, having a potential

Blockchain/DLT dimension, and the other standardization actors, in order to develop coherent set of standards and technical specifications.

Elements to be taken into consideration:

- Support to ISO and IEC activities;
- Ensure a high-level of convergence between the European and international standards;
- Explore the possibility to extend the scope of the current CEN-CENELEC TCs active in the support to Industry's digital transformation, in order to address the Blockchain/DLT dimensions;
- Assess the conditions for the creation of an European Technical Committee on Blockchain and DLT, in support of ISO/TC 307, in order to adopt European Standards in the field of Blockchain and DLT, supporting the digital transformation of the European Industry;
- Monitor the developments of the Joint MSP/DEI WG.

In this context, the FG-BDLT recommends that:

FG-BDLT Recommendation #1:

R1-1: *Standardization bodies to focus on DLT characteristics oriented at organizations' transformation models.*

R1-2: *European Commission to encourage the definition, use and further improvement of open data and communication standards and protocols, secured with Blockchain technologies to encourage the proliferation of Collaborative Work Environments***.**

R1-3: *The standardization framework to encompass a set of information security requirements for demonstrably secure Blockchain implementations, enabling their adoption in the market.*

4.2 Financial & Tax compliance and cross border economic data exchange

Rationale

With the advent of workforce mobility, globalised economies and new ways of fundraising (e.g. ICOs) the potential of DL/Blockchain technologies for disruption in financial services can drive efficiencies as well as create issues in cross-border settlements and taxation aspects.

As an example, the European Commission's FinTech Action Plan was last announced on the 8th of March 2018 and DL/Blockchain technologies are described as a key success factor for many new FinTech services.

Emerging standards on DL/Blockchain technologies should take on board key elements for effective contributions to reduction of the administrative burden of compliance with the global and European regulations contributing to financial stability and the compliance of Anti Money Laundering/Know Your Customer and Tax Compliance regulations.

Most of these elements are global in nature, so they should be taken in consideration by the standards intending to be globally accepted.

Context

The current international context is particularly favourable to the fight against cross-border tax evasion, primarily through the instrument of the exchange of information between tax administrations.

In the Offshore Voluntary Disclosure - Comparative Analysis, guidance and policy advice of September 2010, the OECD highlighted the effectiveness of voluntary compliance programmes adopted by several countries, which facilitated the collaboration of the taxable subjects involved, while at the same time achieving considerable savings, including in terms of litigation (including criminal litigation). Recently, the creation of a new relationship between tax administrations around the world with the involvement of large companies began.

The spread of globalisation and the growth of transnational and multi-sector companies have made it necessary for the Central Public Administrations to resort to the definition of different mechanisms of cooperative compliance with these companies that have multilingual budgets and revenues dispersed across multiple virtual platforms and not always easy territorial identification.

For this reason, a new alternative tool was needed, no longer based on the mere static contrast between tax authorities and large companies, but on the contrary, on a solution of open, frank and transparent dialogue.

In fact, cooperative compliance is a normative resource that was created to realign the two perspectives on the same ground of comparison: where the point of view of the big business and that of the Financial Administration align themselves, collaborating, with the application of the norm.

Cooperative compliance is a tool that has been present for about ten years in the tax warrant, which has recently had a very strong diffusion because it has become a central regulatory provision for every Central Public Administration.

Here it is not necessary to dwell on the laws, codes and norms that have expanded its initial perimeter well beyond all expectations, getting to involve, in addition to Italy, also the United Kingdom, The Netherlands, Australia, Canada, France, Finland, Germany, Ireland and Russia.

Attention to the development of technology influences the creation of executive legislative policies, which, in the context of fiscal policies, are closely linked in an indissoluble relationship between them (as in the case of the web tax in Italy). Today a non-efficient, non-cooperative and expensive Central Administration is not an option, but a damage for everyone.

In this context, with DLT/ Blockchain technologies transactions can be carried out in complete safety, with more subjects involved and without the need for intermediaries, using mathematics and technology to address the lack of mutual trust.

Regarding Tax compliance, DLT/Blockchain technologies can be used to manage specific business processes such as:

- simple presentment from supplier to customer - invoice can be in any format or standard (e.g. EN 16931:2017, UBL XML, CII XML, cXML, EDI, EDIFACT, CEFACT etc.);
- provision for simple invoice clearance;
- third party authorisation (e.g. a Tax Authority);
- provision for invoice factoring;
- discounted sale of unpaid invoice to third parties for immediate collection of financial resources;
- dispute handling and payments handled out-of-band;
- more initial focus on document information presentment.

Interoperability must be understood as an axiomatic concept for the implementation of a principle of free movement of goods, services in the digital world and a necessary condition for the creation of this new equilibrium. Interoperability is also essential to regulate competition in the digital market.

The lack of interoperability creates technical boundaries that the European Commission has long sought to eliminate in order to achieve the internal market (White Paper on completing the internal market, 14 June 1985, COM (85) 310 final).

Until now, the reference to interoperability has been made mainly with reference to standardization processes, and the Commission intends to encourage this activity and focuses on the governance of interoperability (The New European Interoperability Framework, 23 March 2017) and on the promotion of standards.

Bank Transactions

The recognition in the Treaties of a principle of free circulation of data is indicated by the Presidency of the European Union (Executive Summary of the Vision Paper on the Free Movement of Data, 8 August 2017), that the Commission seems to have anticipated with their communication of 10 January 2017 (Building a European Data Economy, 10 January 2017, COM (2017) 9 final), which should form the basis for arriving and having an interoperability of digital content that also takes into account:

- the temporality of data and the need to ensure that digital content remains accessible over the years;
- the need to introduce a requirement for the publication of interfaces in order to guarantee the portability of digital contents by the user;
- the use of open formats without licenses;
- digital content must remain accessible in space and time;
- a single transnational and trans-sectoral terminology must be guaranteed.

The account that a national bank holds in a foreign bank in the currency of the foreign country, which refers to specific accounts that are used to facilitate and simplify trade and currency transactions through their reconciliation. These specific accounts can become transactions stored on a blockchain to drastically improve transparency and efficiency through automatic reconciliation of accounts and transactions.

The ability to manage transactions across all bank accounts with a single interface generates advantages such as:

- greater visibility of the status of the transaction, of the current account balance;
- monitoring over time;
- timely and accurate legal compliance of all accounts and operations carried out.

Big advantage therefore derives from the registration of the transactions, the accounts involved, and the monitoring of the ownership of the goods that thanks to the use of the blockchain can be made more efficient and transparent.

It is essential to establish a reliable identity, which is the cause of costly background checks, required in the verification phase.

The OECD published a new set of bilateral exchange relationships established under the Common Reporting Standard Multilateral Competent Authority Agreement (CRS MCAA).

The last months have also been marked by a significant increase of jurisdictions participating in the multilateral Convention on Mutual Administrative Assistance in Tax

Matters, which is the prime international instrument for all forms of exchange of information in tax matters, including the exchange upon request, as well as the automatic exchange of CRS information and Country-by-Country Reports.

It is important to see Blockchain and DLT as a future part of these bilateral exchange data by international standard.

The FG-BDLT recommends that:

FG-BDLT Recommendation #2

R2-1: *ESOs and SDOs to liaise with OECD and other international initiatives to foster the uptake of bilateral data exchanges in standardization.*

R2-2: *SDOs to focus on interoperability as essential element to regulate competition in the digital market and to avoid technical boundaries that pose a threat in achieving the long needed interconnected market.*

4.3 Business cases coming from research projects

Rationale

Both at national level and at European level, several research projects are being funded on Blockchain and DLTs. One example can be the DT-Transformations-02-2018-2019-2020 Transformative impact of disruptive technologies in public services topic of Horizon 2020 programme.

All these projects are going to produce a well-documented output that may be of high value for standardization bodies.

On this basis, the Focus Group aims to collect the main outputs of such projects and create a specific report to highlight experiences that may be helpful to regulators.

A list of relevant projects is provided, highlighting the business case for the use of blockchain.

Highlighted Projects

KONFIDO (www.konfido-project.eu/konfido) is a H2020 project that aims to create a scalable and holistic paradigm for secure inner- and cross-border exchange, storage and overall handling of healthcare data in a legal and ethical way both at national and European levels. KONFIDO will enable secure exchange, processing and storage of health related data, using privacy by design principles. The federation architecture will enable cross-border interoperation of eHealth services provided by individual countries while each participating entity (private and public actors, empowered citizens) will be able to implement specific policies for the protection and control of personal and health related data. The KONFIDO project aims to advance the state-of-the-art of eHealth technology with respect to the four key dimensions of digital security: data preservation, data access and modification, data exchange and interoperability and compliance.

Blockchain Integration with KONFIDO:

In the frame of KONFIDO, blockchain technology is integrated as a main component so as to:

1. Develop effective logging and auditing mechanisms that will provide traceability and liability support within the KONFIDO infrastructure. In particular, openNCP [7] component logs after being appropriately filtered, transformed and encrypted, will be stored as immutable transactions within a dedicated blockchain federated network to ensure auditability and accountability for any security critical data exchange between openNCP federated nodes;
2. Ensure that Patient Informed Consent is logged in the Blockchain in an immutable way. When an OpenNCP User (Doctor, Pharmacist, Nurse) requests to access the Patient Data then, a Blockchain Smart Contract is updated logging the specific Consent Data; blockchain purpose logging is deemed as even more necessary for auditability and traceability in emergency cases for which the Patient cannot give an explicit Consent.

GHOST is a H2020 project (www.ghost-iot.eu) aiming to respond to security challenges involved in smart-homes.

This is driven by the sudden rise in the use of IoT devices as building blocks for smart-homes and smart-cities. Such devices are vulnerable to attacks giving rise to security issues related to personal privacy and security.

The project will apply behavioral design principles for the elaboration of a novel reference architecture for user-centric cyber security in smart home environments. This architecture will stimulate security-friendly user behaviour enforced by an unobtrusive and user-comprehensible solution.

At the core of the GHOST solution lies a smart home network gateway, supporting a wide range of wired and wireless protocols, that will host the security toolset and the Blockchain defence infrastructure.

[7] https://ec.europa.eu/cefdigital/wiki/display/EHNCP/OpenNCP+Community+Home

Blockchain integration with GHOST:

1. Informed consent use case: GDPR requires to gather the informed consent of a user before start collecting data from any system. GHOST developed a use case in which, previously to the configuration of the system, a screen will be shown to accept the data disclosing. This acceptance is stored in the blockchain and the system checks periodically the blockchain to ensure that the informed consent is signed. The business model here is that service providers can reduce and leverage the processes for guaranteeing this process;
2. Blacklisting sharing use case: in this case, GHOST system is able to classify the sources (IP address and other devices identification) according to the privacy risk. For that reason, each gateway at home (the central element of the smart home that gathers all the information) has a list of classified devices that can be blacklisted if a high security risk breach is detected. Each node of the system writes the information in the blockchain, guaranteeing that all the nodes of the network can retrieve this risky information sources with integrity. The business model is related with the information contained in the blockchain and the possible use as risk repository;
3. Software integrity: this case, each node will store in the blockchain a unique hash of the device (computed as a combination of hardware and software features). In each moment, the system will check the hash against the blockchain and if someone has altered the software, it will be detected. The business model is related with the problem of piracy in manufacturers.

DECODE (www.decodeproject.eu/) is a three-year H2020 project started in 2017 that aims at giving people ownership of their personal data.

The project develops tools that people can use to control how their data is shared, inspired by the principles of Privacy by Design.

Based on the increased control afforded by these tools, DECODE explores how to build a data-centric digital economy where data that is generated and gathered by citizens, the Internet of Things (IoT), and sensor networks is available for broader communal use, with appropriate privacy protections.

As a result, innovators, start-ups, NGOs, cooperatives, and local communities can take advantage of that data to build apps and services that respond to their needs and those of the wider community.

In particular, four European pilots will show the wider social value that comes with individuals being given the power to take control of their personal data and given the means to share their data differently.

The pilots are about online voting, community participation, fair home sharing and citizen-driven IoT. Furthermore, DECODE adopts an open-source approach in order to be transparent about the technology used and avoid patent lock-ins for adopters.

Blockchain integration with DECODE:

1. A blockchain (developed by one of the partners, but in an interoperable way with Ethereum) is used to record 'entitlements', i.e. smart contracts that users define to specify how and who has access to their data. The project is developing also a visual interface that can facilitate users in defining the contracts;
2. The consortium is investigating also how the blockchain can store the code of the virtual machine executing the code for the smart contracts;
3. The project is investigating the legal status of smart contracts, to assess whether smart contracts can be used as legally valid contracts and under what conditions, as well as the relation with existing legislations as the GDPR.

Regarding standardization, DECODE is interested in standardizing (parts of) the process with which data subjects can entitle particular entities to use their data, and the enforcement of such entitlements.

This process includes specifying what data is shared and which entities can have access, under what conditions and for how long, as well as the mechanisms that implement what the user has specified. In particular, given that in DECODE the data subject reveals just as much of their personal data as what is needed, e.g. in an online transaction proving to be older than 18 to buy alcohol, DECODE can contribute to the digital identity discussion and standardization.

PRIViLEDGE (www.priviledge-project.eu) is the acronym for Privacy-Enhancing Cryptography in Distributed Ledgers and is a Horizon 2020 project that aims to provide cryptographic protocols enabling privacy, anonymity, and efficient decentralised consensus for distributed ledger technologies.

PRIViLEDGE will show how to use advanced cryptographic tools to allow both confidentiality and integrity of data stored in a blockchain. Moreover PRIViLEDGE will show how to use the blockchain technology for realizing secure decentralised transactions.

Blockchain integration with PRIViLEDGE*:*

1. Verifiable on-line e-voting: this use case, starting from the traditional approach based on bulletin boards, will show how to use the blockchain technology to obtain decentralised e-voting systems;
2. Insurance smart contracts: this use case will show a ledger-based solution for insurance markets to allow all main stakeholder types (e.g., consumers, brokers, validators) to operate on a ledger containing data in encrypted format;
3. Diploma record ledger: this use case consists of realizing a distributed and secure ledger of higher education degrees in Greece. This ledger will be used to store transactions concerning a student that uses his degree obtained from an institution;
4. Cardano stake-based ledger: this use case will focus on developing a secure and decentralised software update system to be used in the Cardano stake-based ledger.

PRIViLEDGE in practice is giving experimental practical implementation on a standard set of crypto primitives needed to provide the blockchain has a shared computing infrastructure.

The FG-BDLT recommends that:

FG-BDLT Recommendation #3:

***R3-1**: Standardization bodies and EC to identify methodologies and software that can be reused in a wide variety of applications leveraging the business case for the use of blockchain in various fields such as medical data processing, software security, IoT, etc.*

***R3-2**: EC to encourage project research consortia related to DLT technologies (or might allow for a DLT approach) to regularly contribute in the form of techniques, methods and applications related to standardization of certain procedures such as cross border sensitive data movement.*

***R3-3**: Notable outputs of EC-funded projects should be considered by standardization bodies and raise awareness in order to pinpoint sectors where DLTs offered significant improvements, leading to new business cases and possibilities for SMEs, the public sector, the academic sector or individuals.*

***R4-4**: EU research projects relevant for standardization should be encouraged to release their results in an open way (open-source license or in any case patent free) to facilitate adoption and uptake into standardization.*

4.4 Support for the Sustainable Development Strategies

Rationale

The EU Sustainable Development Strategy's aim was to identify and develop actions to enable the EU to achieve a continuous long-term improvement of quality of life through the creation of sustainable communities able to manage and use resources efficiently, to tap the ecological and social innovation potential of the economy and to ensure prosperity, environmental protection, inclusiveness and social cohesion/impact.

In order to allow Blockchain related technologies to play a relevant role within long-term strategies they have to be kept at a state-of-the-art information security level.

On this basis, the Focus Group aims to highlight the key sustainability factors that need specific focus from the standardization bodies.

Sustainability in energy market - Smart energy grid - Smart Homes/Cities

Various actors are developing pilot projects in the energy sector utilizing blockchain technology. Several flagship projects have been launched recently in several countries, and all engaged stakeholders consider standardization as a key element for replication and scaling-up, with the aim of developing a new market, fully adapted to our EU energy related challenges in the energy transition framework. Thus, standardization of the processes is particularly necessary at the level of the interactions between the devices connected to the Web (IoT) and the blockchain itself. In addition, reference to standards will help in gaining public acceptance.

With this in mind, several NSBs - National Standardization Bodies - have started to consider these issues, as, for instance the Swiss Standards Association (SNV) that has recently set up a working group called 'Blockchain and Distributed Ledger Technologies'.

Such applications of a blockchain process would benefit to end users, energy suppliers, distributors, policy makers, and would contribute to meeting our ambitions

regarding energy transition to large share of renewables and thus efficient decentralisation strategies.

That's why the Swiss Federal Office of Energy (SFOE) supports lighthouse/pilot projects with blockchain application- such as for the 'Quartierstrom' project in Walenstadt - as a promising process for moving the energy transition strategy to reality.

The SFOE has also launched a panel of experts to look at different issues in the area of digitalisation, including Blockchain, with the aim to gather feedbacks from experiments and identify gaps and needs for further RDI (Research, Development and Innovation) actions, legislative improvement and reference processes (standardization).

Energy sector could clearly benefit from Blockchain technologies in the framework of decentralisation and transition to large share of renewables.

In that spirit, PostFinance – a financial institution - has launched a pilot project in this field in collaboration with the energy supplier and distributor Energie Wasser Bern – ewb. Both partners are looking for concrete applications for Blockchain solutions and found the energy sector particularly well adapted for pilot/demo projects. Several districts with different configurations and characteristics are tested.

Owners of buildings with rooftop photovoltaic installations have the possibility to directly bill the electricity produced to their tenants. It is precisely at this level that the innovative solution applies: the countdown by Blockchain is automatic, from the electricity meter to the account. In addition, the count is simple, transparent and secure.

PostFinance follows the development of this future-oriented technology with great interest, with an established innovation process, where the possibility of implementing Blockchain and cryptocurrencies is studied.

This case of concrete applications in the energy sector should make it possible to gather experiences in payment and settlement solutions by the end of 2018. If they are positive, nothing will stop their launch on the market. Standardization will then play a major role for replication and scaling up.

A few other very promising international demo projects are launched, such as in the Chinese city of Hangzhou, where a blockchain powered internet-of-things (IoT) network, has been proposed. The IoT network would manage air quality, energy storage and various energy and environmental systems within several towers (buildings).

The network created would use Blockchain technology to allow the smart devices in the buildings to interact. A local-based company would be in charge of the on-site deployment of the platform, as another large-scale application of IoT, powered by Blockchain. This approach offers tools for decision makers, allowing them to see, to understand, to analyse and, after, to take the best decision for sustainability with a sustainable business model.

Collaborative development in the framework of the SESEC IV programme could be of interest.

Blockchain technology and processes are foreseen as important contributors to energy transition and decentralisation, by bridging all stakeholders of the energy chain and helping in behaviour change to make final users becoming 'prosumers' instead of traditional consumers.

With standards based on best practices, the work of CEN, CENELEC and ETSI (ESOs) could benefit from these experiences and pilot cases implemented at national or local levels.
Especially in Europe, with a legislative context particularly adapted and existing RDI framework programmes, as well as national pilot/demo projects already launched, European Standardization Organizations (ESOs) would be relevant to launch new standardization developments, moving innovation to market(s).

The European Clean Energy Package and notably the new Electricity Market directive will introduce a new data management format, which will have to be standardized, for easy and secure access to information (meter data, market data, grid data) to any party (consumers, flexibility providers, grid operators):

- important pre-requisite for distributed resources, allowing cross sector data exchange;

- that could be potentially based on blockchain;
- for which standardization solutions are needed.

The FG-BDLT recommends that:

FG DLT Recommendation #4:

R4-1*: For the energy decentralisation and transition, IoT solutions based on Blockchain should be further explored; standardization work should also address the issue of energy consumption during the processes, with the aim to limit interactions between IoT devices to the minimum needed.*

R4-2*: Standardization bodies to address energy management, which is especially important for Europe considering the new European legislative context (Clean energy package).*

4.5 Digital Identity and Signature Management

Rationale

Identification is a key element in any kind of system; the EU has developed a cornerstone for it, the Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation) adopted by the co-legislators on 23 July 2014, to provide a predictable regulatory environment to enable secure and seamless electronic interactions between businesses, citizens and public authorities.

The aim is ensure that people and businesses can use their own national electronic identification schemes (eIDs) in other EU countries accepting eIDs to access online public services.

This section collects specific standardization elements for compatibility of eIDAS regulation of emerging DL/Blockchain identity management, like the so called self-sovereign identities, in order to ensure that automatic execution of exchanges of value are legally binding for those involved in the automatic execution.

The eIDAS mandatory mutual recognition of eIDs across the EU, can be rolled out with practical uses cases for identification, authentication and access to services (refer Chapters II, II, IV of eIDAS Regulation). It mainly targets the public sector since Member States shall permit citizens from other Member States to use their own eIDs to access online services.

The eIDAS Framework could be effectively adopted as an identity framework for permissioned and/or private blockchains, where the safeguards of the current identity management mechanisms implemented in the different Member States could provide for an additional layer of operational security and easiness of use for blockchains and distributed ledger.

Current best practices already available for the lifecycle management of digital identities could be used for these innovative services.

While, in a public/permissionless blockchain, there is no a priori trust between participants, in a private/permissioned system there is some kind of trust, and eIDAS is exactly targeted to provide trust in a cross-border fashion.

The same kind of reasoning cloud be applied to digital signatures. While participants in a blockchain, as stated, agree on the content of some data, the problem of their agreement on the meaning of these data is not solved at this level.

A digital signature, in the form of a qualified digital signature as specifically defined in the eIDAS Regulation, could provide an effective way to have not reputability, in a law-abiding way, between participants.

Tree levels of insurance are defined by the Regulation (low, substantial, high).

To provide the required confidence in a person and the authentication, the implementation should cover requirements for the following domains:

- Enrolment (registration);
- Credential management (attributes and related claims);
- Authentication.

Therefore, the application of Blockchain in eIDAS regulatory context raises at least the following questions:

1. Does a blockchain lends itself to the requirements of the three domains mentioned above?
2. What changes will impact the roles usually sustaining eIDAS framework?
3. Under which form factors would a primary eID support interact with the blockchain?
4. How does a new business case serve as a momentum to leverage blockchain deployment?
5. What are emerging standards in the blockchain identity / Self-Sovereign Identity (SSI) space and how are they related to eIDAS?

This section aims to address those questions with detailed statements out of which recommendations can be derived.

Question 1: in correlation with GDPR, eIDAS deployment shall consider privacy protection. Each domain or phase comprises a set of ID scheme management functions for which privacy principle(s) should be met:

- ❑ **Enrolment phase**

  - o **Application and initiation** touch upon e.g. user consent, purpose legitimacy and specification, collection limitation, openness, transparency and notice, accuracy and data quality, individual participation and access.

  - o **Identity proofing and identity information verification** touch upon e.g. collection limitation, use, retention and disclosure limitation, accuracy and quality, accountability. This function entails a systematic verification and selection of data before its enrolment on board the blockchain; accordingly an IDentity Provider or Attribute Provider (eIDAS roles) will take in charge the checking of data and may act as nodes. Whenever PII data are part of a transaction the fact that they can be mined or anyway stored in all Blockchain nodes, must be taken in consideration.

    This does not mean that the actual data will be hosted on the blockchain, but it could be e.g. their hash, so that later verification of attribute claims could be performed against such hash.

    In some implementations a different approach is used where PII data are not part of the transaction data ad not stored within the blockchain: in this case the blockchain would act as a decentralised PKI.

  - o **Archiving, record-keeping** touch upon e.g. use, retention and disclosure limitation, individual participation and access. While intended for the blockchain, the PII-related data delivered with user consent, may be stored on other supports as well (e.g. as a backup on databases, cloud storage) about which the PII principal should be notified.

    Immutability or temper proofness of blockchain records has to be considered in view of determining a solution to i.e. the right to erasure (right-to-be-forgotten). With regard the storage of (private) personal data, off-chain

option may be considered e.g. data can be stored with peer-to-peer decentralised file system like IPFS whereas the permanent IPFS link to the data (hash) is stored into the blockchain (through a blockchain transaction); whereby ensuring a timestamping and securing the content but without having to store personal data on the blockchain itself.

Note: the enrolment cannot get rid of a centric checking role before data or its hash or reference are recorded onto the blockchain; such important role is undertaken by a trusted third party either checking the data signature or signing it itself or verifying the signature endorsing such data in case they were certified by a third party (public institution, corporate, etc.).

Blockchain Governance guidance should deliver recommendations as to how eIDAS Attribute Provider; and Identity Provider or a public institution can be used as a trust anchor in the Self-Sovereign Identity (SSI) ecosystem.

- ❑ **Credential management phase**

o It comprises functions across the credential lifecycle such as **credential creation, pre-processing**, **issuance**, **activation**, **storage**, **renewal**, **suspension**, **revocation**, and/or **destruction** are be redesigned in blockchain context. In addition to the immutability issue evoked above, other GDPR requirements apply to the eIDAS framework such as in the instance of credential renewal, suspension, revocation and removal/destruction (decommissioning).

The PII principal should be notified whenever their attribute claims or credentials or PII related data are explored or verified by e.g. a service provider or relying party to grant them access to some service.

The LoA (Level of Assurance) may vary and the LoA offered by the blockchain need to be determined clearly. The credential verification out of the blockchain can come along with the user authentication, in which case an eID support (device, mobile, smartcard, connected object, etc.) offering a secure environment hosting eID data can be involved.

- **Authentication phase**
  - This function may resort to a trusted third party (Authentication service) or/and to the Registration Authority. Privacy-enabling protocols for anonymous authentication (e.g. zero-knowledge based, enhanced role authentication, etc.) can be put in place outside blockchain context as part of permissioning control. Then the credential verification relying on blockchain may stand as a means to enhance the LoA (i.e. from substantial to high).

The signature management is worth a specific observation:

As stated in the Draft Technical Report CEN/TC 224 Draft TR 419 211:2017:

> "*eIDAS defines an electronic seal which authenticates the origin of data but created under control, as opposed to "sole control" for electronic signatures, of a legal person (i.e. organisation), as opposed to natural person (i.e. individual). Technically, electronic seals have similar requirements as electronic signatures and both can be based on digital signatures. eIDAS recognises a special level of qualified electronic seal which is created using a qualified seal creation device (QSealCD) and supported by a qualified certificate, in the similar way as a qualified electronic signature is created using qualified signature creation device (QSigCD) supported by a qualified certificate… The requirements for a qualified signature creation device are considered to be met by the equivalent defined in Directive 1999/93 referred to as a secure signature creation device (SSCD)… CEN has issued standards EN 419 211 parts 1 to 6, which were initially aimed at SSCD but have been accepted as applicable to QSigCD and QSealCD (COMMISSION IMPLEMENTING DECISION (EU) 2016/650 of 25 April 2016).*

Generation of qualified seal or digital signature in the context of blockchain is still to be clarified.

Blockchain envisioned as certificates repository can bring out certificate integrity but the binding of a certificate to its genuine owner through the blockchain is still to be investigated. Accordingly, practical use cases against the features of the CEN

standards, which may be used to support electronic seals in accordance to EU Regulation N° 910/2014 are still to be figured out with blockchain.

Other promising uses of blockchains in relation to electronic signatures and seals is to keep certificate revocation information (in place or complementing CRL use) and to keep trusted list information (i.e. the qualified status of trust service providers).

Question 2: eIDAS commonly identified roles comprises the entity (user, person, principal), the trusted third party (i.e. authentication service), the relying party, the attribute provider, the registration authority.

In blockchain context, there is no need for eIDAS framework roles to resort to the Registration Authority or to the Attribute (Credential) Provider since they can access/verify directly the data on the blockchain during operational phase (access to data can be allowed via the blockchain in case such data resides off the blockchain) . Nevertheless, during enrolment phase, an Attribute or Credential provider is needed to validate the data before their referencing on the blockchain.

Question 3: Integrity of data stored on or off-chain does not spare the need to ensure that the source(s) of such data is/are reliable; this concept relates to the Level of Source Credibility. The data owner, provider or generator should be able to claim the ownership of such data. This may seem obvious when it bears on proving e.g. precedence of ownership against blockchain proof of estates, including Intellectual Property; but another significant situation occurs when personal data e.g. digital attributes or credentials are referred to from the blockchain or hosted on it in a privacy-preserving way, and in such case the User should have preferably at hand a personal asset repository e.g. secure token, smartcard, or secure storage device shielding his personal data. This provides as well an explicit disposition for the users to consent on the transfer of all or part of their personal data from their personal token towards the blockchain, whereby fulfilling at least the user consent privacy principle.

Therefore, it is advisable to elaborate on how a variety of secure primary eID form factors could interact with the blockchain.

Question 4: Blockchain deployment opportunities are swarming whereas the recurring question still arises as to how the involved stakeholders participating in the blockchain setting up could raise benefits out of it, and how could they achieve a promising return on investment. It does not suffice to consider that 'the miners are rewarded', all the more when other proofs than the proof of work can be employed. It matters instead to carefully examine the role of each participating party in terms of their respectively incurred expenditures versus tangible benefits.

The description of use cases without bringing out clearly such accountancy ratio would not leverage blockchain deployment effectively. Besides, as often observed, the attractiveness of blockchain use cases foreseeing sustainable development, inclusiveness or any other societal benefit for a new democratically digital society, but without highlighting enough the trivial accountancy aspects, comes up against the economically reality and so turns even detrimental to a blockchain promotional speech.

Attention should be drawn on those aspects and namely on the business model whenever designing new use cases.

Question 5: Emerging standards in the decentralised identity / Self-Sovereign Identity (SSI) space and how the EU could benefit from them.

Decentralized Identity Management is a growing new market with a variety of use cases, which rely on any exchange of attestations (e.g. bank account, university degree) or attributes (e.g. name, over 18) especially between untrusted entities. Depending on the use case, a public or private and permissioned or non-permissioned DLT acts as a neutrality layer between these entities which enables collaboration.

In regards to eIDAS, especially platforms based on public DLTs are interesting. This is because these platforms have the potential of serving as a worldwide Self-Sovereign Identities (SSI) carrier which allows any issuer (public/private) and owner of

identities to participate. While in the last couple of years, these platforms were built on proprietary standards, platform vendors (e.g. Microsoft, uPort, Sovrin etc.) recognised the need for interoperability. As a consequence, they work together in dedicated working groups in the W3C and in the Decentralized Identity Foundation (DIF).

The goal is to achieve a common understanding of the general architecture of decentralised identities and to develop standards that enable interoperability between different implementations even on different DLTs while following privacy and security-by-design principles. The following provides an overview of the standards with the highest potential impact:

- W3C Community Group - Decentralized Identifier (DID);
- W3C Working Group - Verifiable Claims;
- DIF - DID Auth.

As stated in the current working draft of the DID specification (v0.10):

> "*Decentralized Identifiers (DIDs) are a new type of identifier for verifiable, "self-sovereign" digital identity. DIDs are fully under the control of the DID subject, independent from any centralized registry, identity provider, or certificate authority. DIDs are URLs that relate a DID subject to means for trustable interactions with that subject. DIDs resolve to DID Documents. Each DID Document contains at least three things: cryptographic material, authentication suites, and service endpoints. Cryptographic material combined with authentication suites provide a set of mechanisms to authenticate as the DID subject (e.g. public keys, pseudonymous biometric protocols, etc.). Service endpoints enable trusted interactions with the DID subject.*"

DIDs are only the basis of Decentralized Identity Management but do not provide much information about the subject itself. In order to proof to a inspector/verifier that the DID subject has ownership of certain attestations or attributes, Verifiable Claims (VC) are used which are being standardized by the W3C. VCs are cryptographically linked to DIDs (holder) and an issuer. The issuer could be the DID subject (self-claimed), or a trusted entity. Trust is established either by trusting the issuer's DID

(e.g. out-of-band, bilateral relationship, trust lists) or any other means. An inspection system/verifier could then use the presented cryptographically protected selective disclosure proof (e.g. over 18) to verify the ownership and trustworthiness of the claims.

Public Decentralized Identity Management i.e. SSI platforms would greatly benefit from highly trusted identities provided by the public sector. This will speed up their adoption and create new use cases especially in the Fintech space. Technically, it should be possible to leverage the eIDAS network (eIDAS nodes, TSPs) for this purpose by deriving qualified SSIs from existing eIDs and trust services (e.g. QES), or new potential trust services (e.g. TSPs issue DIDs/VCs). The Austrian e-Government Innovations Centre (EGIZ) described the high potential of SSI platforms in their whitepaper[8].

Further evaluation of these concepts is required and adaptations of the aforementioned standards might be necessary as well.

The European Commission should provide input or requirements to W3C and DIF either directly or indirectly (via CEN/CENELEC, ISO/IEC) in order to make room for a bridge between eIDAS and SSIs. This will allow such entities to make use of the existing and trusted eIDAS network. As this is an interesting and global market, this might be a chance for eIDAS to scale beyond European borders in the private and public sector.

European citizens, companies as well as countries would benefit from enabling new use cases based on decentralised secure cross-border transactions that can be conducted worldwide.

This will also guarantee that European companies, the European Union and the eIDAS network will keep its leading role in the future digital identity and related technologies (e.g. Fintech) space and gains more attention worldwide.

Some considerations arise from the actual market situation:

[8] https://www.egiz.gv.at/files/download/Self-Sovereign-Identity-Whitepaper.pdf

1. The impact on eIDAS framework roles that are usually involved needs to be determined clearly, as a consequence of disintermediation and distribution features resulting from blockchain application.
2. As a consequence to 1), raise awareness at TSPs and eIDAS Node providers that SSI ecosystems exist, new standards are being developed in W3C and Decentralized Identity Foundation (DIF) – such as Decentralized Identifier (DID) and Verifiable Claims – which can provide a mutual benefit to citizens, government and public / private sector service provider by enabling new uses cases, new revenue streams and frictionless transactions. Standardization bodies will have to check these requirements against existing standards or implement new standards to facilitate industrial adoption.
3. The variety of form-factor hosting eID involved in operations and interacting with the blockchain is worth being examined and described.
4. With versus without blockchain argumentation is worth being elaborated to increase confidence and trust with regards to blockchain disruptive effect on existing authentication models.

The FG-BDLT recommends that:

FG-FDLT Recommendation # 5:

R5-1*: Blockchain deployment in regulatory context needs to consider enrolment, credential management and authentication with their respective privacy facet. Standardization activities should be aligned with those needs.*

R5-2*: Blockchain contribution to electronic certificate and strong authentication as well as legally binding signature service and signature delegation needs to be described in terms of architecture components, interfaces, roles and factual improvement.*

R5-3*: In regards to 1-2), as there are already standardization activities in W3C and DIF in regards to decentralised identities / decentralised identity management, which are leveraged by European organisations, normalisation activities in TC307 and corresponding subgroups (e.g. WG2) should align with these standards - i.e. Decentralised Identifier, Verifiable Claims - to ensure future compatibility.*

R5-4*: European Commission should provide input or requirements to W3C and DIF either directly or indirectly (via CEN/CENELEC, ISO/IEC) in order to make room for a bridge between eIDAS and SSIs. This will allow them to make use of the existing and trusted eIDAS network*

R5-5*: Blockchain development in regulatory context requires to define digital identities management systems that manage digital identities in their complete lifecycle (i.e. request, enrol, issue, suspension, renewal, revocation…) providing users the same levels of assurance, protection of personal data, peace of mind and ease of use that are already available for traditional digital identity systems*

R5-6*: on electronic seals/signatures, to study blockchain use cases related to the features of the CEN standards in accordance to EU Regulation N° 910/2014*

R5-7*: TC307 and other standardization bodies should establish a liaison peer groups and provide requirements to allow SSI ecosystems to leverage the existing eIDAS network - i.e. TSP, eIDAS Nodes and eID Schemes - to derive, issue and/or authenticate DIDs and Verifiable Claims.*

4.6 Privacy and Data Protection

The interplay between the General Data Protection Regulation (GDPR) and Blockchain/DLT is complex and still under debate. It is clear that the GDPR should be kept in mind when moving toward the definition of standards applied to Blockchain/DLT, as the stakes for firms, institutions are high, and the impact of this regulation is global.

Researchers and institutions are currently trying to identify the main points of tension between the GDPR and Blockchain/DLT, as well as possible ways to resolve these tensions. Most notably, Senior Researcher Michèle Finck published a research paper[9] on this topic and the EU Blockchain Observatory and Forum started to produce in-depth analysis around the GDPR[10].

Furthermore, the EU Blockchain Observatory and Forum will publish a detailed ***thematic report on Blockchain and GDPR*** that will shed light on data privacy and protection in relation to the DLT/Blockchain technologies and will become one of the key references for this section of the whitepaper. As soon as published the document will be available at www.eublockchainforum.eu.

The thematic report was not yet published at time of writing the present document and the CEN-CENELEC Focus Group BDLT will integrate its outcomes in a next release of the White Paper.

So far, the Focus Group has explored the following aspects:

According to the GDPR it is mandatory to implement appropriate technical and organizational measures to comply with the regulation whenever personal data is handled. A key-stone article in the GDPR of particular relevance to Blockchain is the concept of data protection by design and by default. Both at the time of the

[9] Finck, Michèle, Blockchains and Data Protection in the European Union (November 30, 2017). Max Planck Institute for Innovation & Competition Research Paper No. 18-01. Available at SSRN: https://ssrn.com/abstract=3080322 or http://dx.doi.org/10.2139/ssrn.3080322

[10] The EU Blockchain Observatory and Forum produced a research paper in partnership with the University of Southampton, organised a workshop in Brussels on June 8th and a report is under development.

determination of the means for processing and at the time of processing itself, the controller shall implement appropriate technical and organisational measures designed to implement data-protection principles and to integrate the necessary safeguards in order to meet the requirements of the GDPR. The data protection rules and principles have to be integrated already in the design of the blockchain.

According to the article 5, paragraph 1, of the GDPR, there is the need to respect the following principles: 'lawfulness, fairness and transparency', 'purpose limitation', 'data minimisation', 'accuracy', 'storage limitation', 'integrity and confidentiality'. Paragraph 2 of the above mentioned article 5 states: *"The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')".*

In fact, in case of private Blockchains/DLTs it is surely possible to respect the principles as mentioned above, because there will be an entity that could be considered as controller while in public implementations this could be more complex.

Another point is the respect of the first principle (lawfulness, fairness and transparency) regarding the data subject's consent. According to the article 6, paragraph 1, of the GDPR:

> *"Processing shall be lawful only if and to the extent that at least one of the following applies:*
>
> *(a) the Data Subject has given consent to the processing of his or her personal data for one or more specific purposes;*
>
> *(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract".*

In this scenario, there are some relevant elements to evaluate in relation to the subject's consent when data is stored in a public blockchain to correctly address the legal issues related to the compliance with the data protection law (GDPR).

Given the several principles and key concepts provided by the GDPR, some questions and incompatibilities can be identified:

- **Personal data**. The GDPR defines personal data as any information relating to an identified or identifiable natural person. It can be difficult to determine what falls under personal data is in the context of Blockchain/DLT. Clearly transactional data that includes information in messages or any other content traceable to an individual is considered personal data. However, there is open debate about whether or not the public keys that are used in Blockchain/DLT systems as addresses are personal. It is generally accepted that data related to a public key can only be seen as pseudonymised and not anonymised, meaning that it has to follow the GDPR. However, there is currently under development address obfuscation methods such as ring signatures that might allow to consider as nearly impossible to link a public key to an identifiable person. In addition to the GDPR, the European Data Protection Board- EDPB – (previously Article 29 Working Party) and the European Court of Justice (CJEU) have consistently provided a wide definition of what constitutes personal data

  The second debated element is encrypted data, there is a general consensus within the community to see encrypted personal data as personal data, as encryption is a reversible method and considering the high probability that current state of the art encryption algorithms will be broken in the next ten years. Finally, there are conflicting positions on the status of hashes of personal data. Storing personal data off-chain and referring to this data using a direct hash function cannot be presented as a solution to comply with the GDPR as the hash accomplishes only pseudonymisation, not anonymization. The emergence of a standardized approach for hashing personal data and storing these hashes on-chain, exploring opportunities such as salted and peppered hashes together with the 'hazing-out' method [11], would represent a great progress for the industry.;
- **Roles**. In Blockchain/DLT systems it can be difficult to apply the concepts of data controller and data processor. In decentralised application (dApps) the data controller is the legal entity behind the app. However, at the blockchain

[11] "Hashing-out" consists in storing personal data off-chain, having in the chain only a hash that could be used to link to an encrypted database where full data is stored.

infrastructure level this is more complicated, particularly in public, permissionless blockchains where all the full nodes would appear to be data controllers. One question this raises is how to identify what GDPR-recognised roles the different actors are playing on a blockchain network at any given time. For instance there is no unique answer regarding the status of nodes and it should be looked upon case by case. A party can be both a controller for certain data, and a processor for other data (e.g. if data is only routed).;

- **Governance and liability**. Another important question is how to handle governance in a fully decentralised network – not just in terms of technology but also off-chain governance. If roles are fluid so are responsibilities, making liability a major question as well.;
- **Territoriality & third countries**. the GDPR's territoriality scope is wide and captures, for example, instances when a controller not established in the Union processes personal data of data subjects who are in the European Union. Open, permissionless blockchains are global in nature, and it is close to impossible to control where the data goes.;
- **Data minimization and erasure**. Blockchains are append-only databases, which means that information can (in theory) only be added and not deleted, seemingly clash with GDPR's data minimization and right to amendment/erasure principles. Moreover, it is not clearly defined in the GDPR what can be considered as erasure. The commonly accepted work around to address this issue is to avoid putting personal data on the blockchain.;
- **Automated processing**. A final point that is not often discussed is the right that GDPR gives data subjects to be protected from automated processing of personal data. One of blockchain's great innovations, at the heart of many of its most important applications, is the ability to automatically process many transactions via smart contracts. Can these be reconciled with GDPR?

GDPR may appear to be in conflict in many ways, but at closer look the two are not a priori incompatible. As both mature - GDPR in terms of case law and clarifications, Blockchain in terms of the technology and its possibilities - the more common ground they might find.

The role of standardization bodies is crucial in bringing the answers needed to reconcile Blockchain/DLT and the GDPR.

The FG-BDLT recommends that:

FG-BDLT Recommendation #6:

***R6-1**: It is fundamental that standardization efforts include the implications of GDPR within their related groups.*

***R6-2**: Defining and formulating GDPR compliant standards (e.g. in terms of design, architecture, non-reversible data transformation methods or address obfuscation methods) would have to consider impact on entrepreneurs and institutions.*

***R6-3**: Blockchain technology in relation to governance must address the data controller requirements of GDPR.*

4.7 Standards Landscaping

Rationale

There is a large and growing number of standardization initiatives on DL/Blockchain technologies across the world. At the same time, there is a relative shortage of experts with relevant experience.

The combination of both facts requires more coordination and wider participation to deliver sound standards in a timely manner. This risk could also be mitigated reusing as much as possible already existing standards and identifying possibly redundant efforts that should be merged or, at least be aligned.

To this end, this section will collect identified existing and ongoing technical standards that should be reused or referenced in order to increase the efficiency of the process of elaboration of emerging standards on DL/Blockchain technologies, with special

focus on existing European standards, or national standards of European Union member states that could be relatively unknown outside its borders.

Relevant standards are meant to focus on all aspects of DL/Blockchain technologies, including their expected information security level so it is recommended that ISO/TC 307 works jointly with ISO/JTC 1/SC27 on this topic

The reference section of this document will list some of the already identified initiatives, while the white paper will include a more comprehensive list of standardization initiatives, including a few ones that could become 'de facto' standards even though they are not under the scope of official standardization bodies.

The FG-BDLT recommends that:

FG-BDLT Recommendation #7:

***R7-1**: ISO/TC 307 to consider possibility to work jointly with ISO/IEC JTC 1/SC 27 for Blockchain information security aspects*

***R7-2**: CEN-CENELC FG Blockchain/DLT to foster cooperation with CEN-CLC/JTC 13*

4.8 Government transformation

Rationale

The digital transformation of government is a key element to the success of the Single Market; helping to remove existing digital barriers and preventing further fragmentation arising in the context of the modernization of public administrations.

The EU **eGovernment Action Plan 2016-2020**[12] aims:

- to modernise public administration;

[12] https://ec.europa.eu/digital-single-market/en/european-egovernment-action-plan-2016-2020

- to achieve the digital internal market; and
- to engage more with citizens and businesses to deliver high quality services.

The Action Plan will support the coordination and collaboration at European Union level. Through the joint efforts between Member States and the Commission, the availability and take-up of eGovernment services can be increased, resulting in faster, cheaper and more user-oriented digital public services.

The Once Only Principle (TOOP) project[13] is part of the EU eGovernment Action Plan 2016-2020, which will contribute towards increasing the efficiency of the Digital Single Market.

The project will ensure that information is supplied to public administrations only once regardless of the company's country of origin. This step eliminates unnecessary burdens for European, which are asked to present the same data and documents repeatedly.

Thanks to their distributed nature, and to tamper resistance of registered data, Distributed Ledger Technologies are expected to play a key role to implement the once only principle.

The Connecting Europe Facility (CEF DIGITAL) [14] supports multiple digital infrastructure projects that contribute to improvements in the daily lives of Europeans through digital inclusion, the connectivity and interoperability of European digital services, and the development of a Digital Single Market.

Digital services in sectors such as Justice, Health and Taxation have been built with help from the CEF Building Blocks[15]:

- eDelivery – supporting electronic registered delivery of data and documents;
- eID – extending use of online services to the EU citizens;
- eInvoicing – helping public entities adopt the European standard on eInvoicing;

[13] https://ec.europa.eu/digital-single-market/en/news/once-only-principle-toop-project-launched-january-2017

[14] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/CEF+Digital+Home

[15] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Digital+Infrastructures

- eSignature – creating and verifying electronic signatures;
- eTranslation – exchanging information across the EU.

The building blocks[16] are basic capabilities that can be reused in any project to facilitate the delivery of digital public services across borders and sectors.

Both cross border eGovernment services could benefit from blockchain functionalities such as notarization.

The European Commission has set up ICT standardization priorities for the Digital Single Market and EU plans to support participation of European experts in international standardization decisions, in so increasing the European contribution to the emergence of innovative solutions on a global scale.

StandICT.eu is a new initiative funded by the European Commission focused on supporting the participation and contribution of EU Specialists to SDO and SSO activities covering the essential building blocks of the digital Single Market: 5G, Cloud Computing, Cybersecurity, Big Data and IoT.

This section will highlight government transformation processes running within EU to help standardization bodies in producing standards supporting government regulations.

Rationale

Administrative decentralisation, according to the World Bank,:

> *"seeks to redistribute authority, responsibility and financial resources for providing public services among different levels of government. It is the transfer of responsibility for the planning, financing and management of certain public functions from the central government and its agencies to field units of government agencies, subordinate units or levels of government, semi-autonomous public authorities or corporations, or area-wide, regional or functional authorities"[17].*

[16] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Building+Blocks

[17] http://www1.worldbank.org/publicsector/decentralization/admin.htm

Similarly, it defines political decentralisation as:

> *"political decentralization aims to give citizens or their elected representatives more power in public decision-making. It is often associated with pluralistic politics and representative government, but it can also support democratization by giving citizens, or their representatives, more influence in the formulation and implementation of policies".*

Clearly, independently from the form of governance, being it centralised or federated, or more simply from where institutions that constitute the government are located, every government is inherently decentralised or better 'distributed', and this is multiplied even more if we think at EU-level government interoperability and communication.

The EU Commission is looking carefully at Blockchain developments with the objective of setting the right conditions for an open, innovative, trustworthy, transparent, and EU law compliant data and transactional environment.

EC will assess, in the first place, if, when and how Blockchain technologies may help public authorities to deliver European services and implement policies in an optimised way. It will examine opportunity, benefits, and challenges of a range of options, including an enabling framework at EU level or an infrastructure supporting Blockchain-based services.

A wide introduction and use of Blockchain in the public services has the potential to transform the public sector and produce benefits for public organizations, users and citizens both at state and at EU-level.

Transparency, speed, shared & controlled consensus, can affect the relationship and trust between public administration and citizens/corporations and between different states public administrations, potentially reshape interactions in the society.

Such technologies are able to change the way relations are managed among several actors, including firms, and produce large savings and increase accountability.

There are a large number of entities that work to provide key services to citizens within a typical government organization.

A short list of the main services provided by governments would include:

- Health Services;
- Social Services;
- Identity Services;
- Education Services;
- Security and Judiciary Services;
- Currency and Financial Services;
- Environmental Services;
- Transportation and Infrastructure Services; as well as
- many more areas of activity

These are provided, depending on the specific government structure, by central or local authorities and at EU-level must be integrated or be interoperable.

Within each of these areas there are many sub-entities running local and regional services. A typical example is Healthcare where there could be centralised management (for example approval by health regulators of new medicines for the public) and local services (such as hospitals).

This is clearly a distributed ecosystem where thousands of functions (services) are performed by each entity and where many of them are cross-related.

The vision would be that any citizen traveling from any EU state to another would be able, through his own digital identity, to share needed information with any member state public service on need. To give a specific example, a German citizen having vacation in Italy or France, on need should be able to share digitally his health data with the local hospitals or doctors.

European government bodies are already in process of defining specific implementations of government-based Blockchain infrastructures (e.g. in Spain with Alastria or in Italy where a research paper[18] has also been published by Pietro

[18] Pietro Marchionni, Next Generation Government Service Bus - The Blockchain Landscape (March, June, 2018). Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3141749

Marchionni on this topic) and such implementations are also defining new consensus mechanisms that can be in line with government processes governance.

To be able to be part of a real government transformation process, any Blockchain implementation should have key characteristics as the following:

1. Blockchains/DLTs should adopt open and standardized interfaces to interact with external services (semantic e.g. JSON structures to access…);
2. Whenever Blockchains/DLTs should store data within their blocks, storage must be structured in a standardized format in order to guarantee easy portability from blockchain to blockchain or from blockchain to external services;
3. Blockchains/DLTs must be able to accommodate (plug in) eIDAS-compliant identity services in order to identify users interacting with the chain data;
4. Blockchains/DLTs should be able to be run/operate in a dedicated infrastructure (e.g. avoiding 'cloud-only AsAService' blockchains/DLTs) as many government processes cannot be hosted in public cloud services;
5. Blockchains/DLTs should be able to accommodate different types of consensus mechanisms (plug-in consensus or anyway open-source blockchain where consensus mechanism can be modified without making different versions non-interoperable) to accommodate flexible consensus models as different member states could require/implement different solutions based on their country-defined governance models related to government processes.

The FG-BDLT recommends that:

FG-BDLT Recommendation #8 :

***R8-1**: Standardization bodies should focus on interoperability in data and interfaces as key requirement for any blockchain/DLT running government processes/services.*

***R8-2**: EC and Standardization bodies should focus on new and redesigned consensus models when dealing with government processes.*

***R8-3**: Standardization bodies should take in consideration that cross-border government services would require open formats in data exchange/discovery models.*

5. Conclusions

This White Paper was developed by the CEN-CENELEC Focus Group on Blockchain/DLT with the objective to identify specific European needs for Blockchain/DLT standardization. Digital identity, data protection and integrity, security, cross border data-sharing, interoperability, electronic signatures, and process automation have been identified as topics requiring particular attention at European level.

The Focus Group will maintain this white paper and will continue to collect identified European needs, to support the activities being carried out within ISO/TC 307, as well as the European Commission's initiatives. As a final recommendation, the CEN-CENELEC Focus Group on Blockchain/DLT would like to particularly encourage CEN's members' participation within ISO/TC 307.

6. References

We here highlight the major standardization initiatives CEN/CENELEC FG BDLT is willingly to target with the white paper (and in case their related working groups); this list will be further developed within the white paper itself

- ISO/TC 307 "Blockchain and distributed ledger technologies" (www.iso.org/committee/6266604.html)
- ITU-T Focus Group on Application of Distributed Ledger Technology (https://www.itu.int/en/ITU-T/focusgroups/dlt/Pages/default.aspx)
- ITU-T Focus Group on Digital Currency including Digital Fiat Currency (https://www.itu.int/en/ITU-T/focusgroups/dfc/Pages/default.aspx)
- UN/CEFACT Blockchain whitepaper (uncefact.unece.org/display/uncefactpublic/Blockchain+White+Paper)
- W3C Blockchain Community Group (www.w3.org/community/blockchain)
- IEEE blockchain adoption initiative (www.blockchain.ieee.org)
- Decentralized Internet Infrastructure Research Group of IETF (www.trac.ietf.org/trac/irtf/wiki/blockchain-federation)
- IETFdraft ALTO for the blockchain (www.tools.ietf.org/html/draft-hommes-alto-blockchain-01)
- W3C Verifiable Claims Working Group (www.w3.org/2017/vc/WG)
- W3C Decentralized Identifiers (DID) Community Group (www.w3c-ccg.github.io/did-spec)
- DIF - Decentralized Identity Foundation (www.identity.foundation)

Also leading consortia or fora (e.g. Enterprise Ethereum Alliance, Linux Foundation, Sovrin and others) will be taken in consideration.

7. Annex 1 - European Use Cases for blockchain implementation

Rationale

In Europe, there are several DL/Blockchain use cases, either funded at EU or National level, or independently implemented by market stakeholders (e.g. industrial actors).

These use cases can be of interest to the standardization bodies to better understand the wide possible applications in which DL/Blockchain technologies can be used and what have been the roadblocks in such implementations.

Within this topic, this paper will highlight the areas of such use cases extending for each area one example and listing other samples with related URLs.

Considering some basic archetypes of properties, some areas where we can group use cases may be taken into consideration:

- Financial services and asset management (including KYC)
- Registry services/License management
- Asynchronous/distributed automation
- Data protection and information security
- Identity Management (including SSID)
- Fundraising: tokens issuance through blockchain
- Smart energy grid
- Smart homes / cities

This list will be further developed within the white paper itself based on further identification of the actual implementations status within EU.

Use Cases/Case Studies

Use Case #	*Use Case/Case Study Name*	*Use Case Type*
1	ALASTRIA	Infrastructure
URL	https://alastria.io/	

Alastria is the first multi-sectoral consortium promoted by organizations and institutions for the establishment of a semi-public Blockchain/DLT infrastructure, supporting services with legal effectiveness in the Spanish scope and according with European regulation. The consortium is open to any organization that wishes to have available a fundamental tool for the development of its own existent regulation, that enables the associates to experiment this technologies in a Blockchain/DLT strategy with the aim of distributing and organizing products and services for the Spanish market. Alastria can be summarised as a semi-public, independent, permissioned and neutral Blockchain/DLT network, designed to be accordant with the cooperative environment.

Among its founders are also professionals such as notaries and lawyers who will ensure the security and veracity of information through the identification of natural and legal persons. Not in vain, the digital ID will be the main focus of Alastria in its beginnings through the standard of Digital Identity 'ID Alastria', which will allow citizens to have control over their personal information in a transparent way following the guidelines set by the EU. Alastria is an open platform for more companies, startups, SMEs, large corporations, universities and other actors from all sectors in Spain to join.

The Alastria network will provide a shared platform on which the various participants, and in particular large companies, will be able to create digital representations of the assets with which they work in their usual economic activity, also known as 'tokens'. With these 'tokens' it is possible to develop new products and innovative cutting services, in addition to being able to develop current processes faster, safer and more efficiently. In this way, the network accelerates the digital transformation of current

processes and enables a new paradigm of collaborative and multisectoral innovation in a very efficient way.

Use Case #	*Use Case/Case Study Name*	*Use Case Type*
2	GLEIF	Identity
URL	https://www.gleif.org/	

The development of a system to uniquely identify legal entities globally had its beginnings in the 2008 financial crisis. Regulators worldwide acknowledged their inability to identify parties to transactions across markets, products, and regions for regulatory reporting and supervision. This hindered the ability to evaluate systemic and emerging risk, to identify trends, and to take corrective steps. Recognizing this gap, authorities, working with the private sector, have developed the framework of a Global LEI System (GLEIS) that will, through the issuance of unique LEIs, unambiguously identify legal entities engaged in financial transactions. Although the initial introduction of the LEI was for financial regulatory purposes, the usefulness of the LEI can be leveraged for any purpose in identity management for legal entities both by public and private sectors. This includes but is not limited to supply-chain, digital markets, trade finance, and many more.

The LEI initiative is driven by the Financial Stability Board (FSB) and the finance ministers and governors of central banks represented in the Group of Twenty (G20). In 2011, the G20 called on the FSB to take the lead in developing recommendations for a global LEI and a supporting governance structure. The related FSB recommendations endorsed by the G20 in 2012 led to the development of the Global LEI System that provides unique identification of legal entities participating in financial transactions across the globe and the subsequent establishment of the GLEIF by the FSB in 2014. The GLEIF is overseen by a committee of global regulators known as the LEI Regulatory Oversight Committee (LEI ROC), including the Reserve Bank of India represented by Nanda S. Dave, Executive Committee, Vice-Chair.

The LEI itself is a 20-digit, alphanumeric code based on the ISO 17442 standard developed by the International Organization for Standardization. The developer of ISO 17442, ISO/TC 68, also maintains a liaison with ISO/TC 307.

The LEI connects to key reference information that enables clear and unique identification of legal entities participating in financial transactions. Moreover, the LEI provides freely accessible look up (identification) of the parties to transactions. GLEIF has explored the impact of rising digital technologies on entity verification and the potential capabilities and benefits afforded by adopting a standardized method using the LEI.

The LEI offers businesses a one-stop approach to identifying legal entities, which has the potential to take the complexity out of business transactions. Via the Global LEI Index, GLEIF makes available the largest online source that provides open, standardized and high quality legal entity reference data. No other global and open entity identification system has committed to a comparable strict regime of regular data verification.

Integrating the LEI into other entity verification methods, including solutions based on digital certificates and Blockchain technology, therefore will allow anyone to easily connect all records associated with an organization, and identify who owns whom. By becoming the common link, the LEI will provide certainty of identity in any online interaction, making it easier for everyone to participate in the global digital marketplace.

GLEIF believes that digital certificate technology based on strong cryptography is critical to the smooth operation of the evolving digital economy. The proliferation of digital certificates, whether issued by governments or the private sector, has allowed organizations and individuals do business digitally. However, the current manner in which digital certificates are issued is causing identity challenges in today's digital world. These challenges need to be resolved to ensure they can effectively support the smooth operation of the global digital economy.

The major challenge with digital certificates stems from the current practice of obtaining certificates from a host of different issuers and records are kept in multiple silos by a variety of organizations globally. Digital certificates come with a unique

public-private key pair and a fingerprint. When they expire, a new certificate must be obtained with a completely different public/private key pair. Organizations usually hold multiple certificates from different certificate schemes, e.g. eIDAS and CAB/Forum, at the same time and for different use cases.

The reference data, e.g. the name, legal form and address, are embedded as strings. These strings are not harmonised across different certificate issuers. It is not possible to relate one certificate to another or determine the links between different parties without repeating the same manual matching exercise. Digital certificates today are strong in adhoc authentication but lack the ability to view their owners in an unambiguous way.

Furthermore, certificates carry information that was available at the time of issue. During the period during which a certificate is valid, an owner could change its name, address or legal form, which cannot be reflected by changing the certificate content, as this would break the cryptographic checks. As a result, the information held about organisations is not kept up to date in a systematic way, or at all, by the certificate issuers. With no connection between different digital certificates relating to one entity and no way to decide which is out of date and which is current, determining identity in the digital sphere only will become even more complex.

Organizations and individuals need a way to ensure the information they are obtaining through a certificate is correct and up to date. A solution is required to build certainty and trust in the system and the information it provides.

GLEIF wishes to simplify identification for the digital age by combining the LEI with digital certificates, which would result in an easy approach to relate all records associated with an entity, determine which are current and clear up any variances. It will also allow business users easily assess information on who owns whom.

This seemingly minimal addition will significantly reduce the complexity and cost – both people and technology related – associated with due diligence and validation of customers, partners and suppliers. LEI codes would represent the reference data of a legal entity as well as the issuer entirely. Certificate handling would become faster (less payload) and most current information could be obtained on demand from the

Global LEI System (GLEIS) via APIs. The LEI could become an essential building block for the usage of digital certificates in any kind of distributed supply-chain.

Digital certificates are already integral for organizations and individuals interacting and transacting digitally, and their usage is only set to increase with emerging technologies, such as IoT and Blockchain. Today, different digital ID systems are based on varying standards, keys and encryption and the only common link between them is the entity name, which can vary widely and change over time. Without a consistent numerical link between IDs, automated methods will always result in errors and further challenges for organizations. The LEI could provide this consistent link and cement its position as a force for good digital identification.

In case any Blockchain/DLT application is not going to use digital certificates for authentication of individuals acting on behalf of a business. For example, the LEI can be embedded in the ledger directly, linked to the way any use is identified, e.g. biometrics. This applies also for self-sovereign ledger systems.

Use Case #	*Use Case/Case Study Name*	*Use Case Type*
3	SUNFISH	Cloud Federation
URL	http://www.sunfishproject.eu/	

Nowadays, the Public Sector is equipped with a large number of private Cloud systems, whose administration is becoming more expensive and less effective due to brief usage picks, barriers on flexible resource provisioning and limited access to distributed data sources. An impelling need is to provide software infrastructures enabling secured and controlled interaction across multiple Cloud systems. The key driver for creating such cross-Cloud systems stands in the access to data and services otherwise not available and better utilization of computational resources.

The governance aspects of cross-Cloud systems are of paramount importance to encourage wide application and foster systematic integration of private Clouds in the Public Sector. European countries such as Italy and France suffer from a large

proliferation of small/medium data centres concurrently supporting Public Administrations. This causes inefficiency, costly management and low resource utilization.

To tackle this issue, the SUNFISH project conceived, designed and implemented so-called *Federation-as-a-Service* (FaaS) [Ref. 8a], an innovative federation approach for Cloud systems that allows small/medium data centres to become first-class citizen in the Cloud provisioning landscape for Public Administrations. FaaS crucially relies on Blockchain to realise a first-time democratic and decentralised governance model. Blockchain is exploited as an innovative underlying infrastructure underpinning untrustworthy federated Clouds with data computation integrity and availability.

Blockchain offers not just resilient data storage, but a decentralised computation facility at hand that alleviates the need for a trusted-third-party and reduces systemic risks of disputes and frauds in cross-Cloud interactions. The corner stone of the approach is an innovative democratic governance of Cloud federations: none of the federated Cloud rules on the others, but each of them shares the same authorities and duties. The governance is carried out and enforced in a decentralised manner according to Blockchain smart-contracts. Besides representing the governance rules negotiated among the federation participants, smart-contracts support democratic e-voting and strengthen the overall security assurance of data security functionalities and Cloud applications.

To improve security assurance of privacy-preserving services, smart-contracts are used to shield key ingredients from tampering attacks, e.g. the masking key used by data masking services to securely and privately store sensitive data. At the same time, smart-contracts are used to offer a tamperproof anonymization history record, which is used to dynamically tune anonymization techniques in order to ensure continuous privacy protection of already released anonymised datasets.

This smart-contract infrastructure has been exploited, together with FaaS, to put in operation a cross-Cloud payroll application for the Italian Ministry of Economy and Finance. Specifically, smart-contracts are used to carry out certified tax calculation on sensitive data from the Ministry of Interior. The combined used of encryption,

certified smart-contract executions and decentralization ensures that tax calculation for payroll is correct, that no private data is leaked to the Ministry of Economy and Finance and there is no trusted-third-party carrying out any computation.

The outcome of the project, developed using open-approach and reusable technology, constitutes an important asset for the renewal and transformation required by the agenda for Digital Italy and the Digital Single Market. In this regard, the Head of the General Administration, Personnel and Service Department of the Ministry of Economy and Finance, Luigi Ferrara, underlined how *"SUNFISH represents a great opportunity for the rationalisation of public IT infrastructures and, therefore, spending. The technology used in the Italian use case will be used for the renewal of NoiPA and applied to "Cloudify NoiPA""*, which by January 2019 will support more than 3 million public employees.

Use Case #	*Use Case/Case Study Name*	*Use Case Type*
4	CIMEA BCERT	Certification
URL	http://www.cimea.it/	

CIMEA is the official Italian Centre within the NARIC - National Academic Recognition Information Centres – network of the European Union and the ENIC - European National Information Centres – network of the European Council and of UNESCO Since 1984, CIMEA (Information Centre on Academic Mobility and Equivalence) has performed its focused activity of information and advisory on the procedures of qualifications recognition and on themes linked to Italian and international higher education and training. CIMEA supports academic mobility in all its forms and owns an international document centre and specialised databases on foreign higher education systems, on the types of qualifications of every country and on the national legislation in terms of higher education.

CIMEA's Credential Information Service – CIS, a credential evaluation service of certification and comparison of Italian and foreign qualifications, with a view to

rendering qualifications increasingly more comprehensible and recognizable in a national and international context.

CIMEA has decided to utilise the power of blockchain technology to digitalise the process of recognition of qualification (based on Lisbon Recognition Convention principals) and Credential Information Service CIS asking student related documentation temper-resistant erasing any possibility of falsification of given certificates and qualification information.

The chosen approach is to create an interlaced distributed network of information that allows one to precisely identify the credentials and certification of any registered user and provide CIS services, certifying their truthfulness.

This can be achieved with a modern distributed technology and strategic process flow approach that takes success stories from other markets and adapts them successfully to the certification ecosystem utilizing the latest technologies as Blockchain and Artificial Intelligence.
CIMEA has defined use cases, identified key requirements and designed a system that will revolutionise the certification process simplifying the trusted distribution of verified certifications and reducing frauds.

The BCERT Blockchain network is a private permissioned network where every stakeholder participates to building-up the ecosystem based on its role: end user, certifying authority, certificators.

Certification Authorities are further divided in 'Direct Certification Authorities' that are entitled only to certify users belonging to their organization (e.g. Universities) and 'Cross Certification Authorities' that are entitled to certify every user within the BCERT network (e.g. NARICS).

Each of the stakeholders has specific write permissions on the network based on its related entitlement.

In case an organization has already its own network and therefore needs to integrate it to BCERT, an appropriate gateway will guarantee interoperable exchange of information between the organization network and BCERT.

Users, when registered within CIMEA BCERT, are assigned a personal account within the blockchain that will be their repository for every document related to their education.

This account belongs to the user and any interaction with it must be allowed by the user itself utilizing the cryptographic key assigned at time of the creation of the account.

The account is fed by external smart contracts handling different tasks. Whenever the user itself, his organization or a cross certification authority adds a document related to the user education, a dedicated smart contract is activated. The task of this smart contract is to verify that the appropriate permissions (e.g. organization, user information, etc) and data structure (e.g. appropriate organization signatures) are used together with consistent metadata (e.g. this certification is not in conflict with other certifications).

Use Case #	*Use Case/Case Study Name*	*Use Case Type*
5	n/a	Capital Gains Taxation

A recent problem for tax authorities is represented by the taxation of capital gains realised or achievable by the sale of cryptocurrencies.

The widespread growth of cryptocurrencies has placed all financial and tax operators in front of the issue concerning the taxation of capital gains realised (or achievable) from the sale of the same.

To this day there is a great legislative confusion that does not only concern the fiscal discipline of cryptocurrencies, but which concerns their technical and civil definition, the impacts on security, privacy and anti-money laundering and anti-crime regulations.

The crypto coins are very flexible tools and can be used in many ways; anyone can create new ones and launch an Initial Coin Offering (ICO), that is, an initial offer of new virtual tokens.

Alongside the 'classic' crypts, which fall into the category of crypto currencies (so-called currency token), you can have tokens designed to be used as financial instruments (so-called security token), tokens that allow access to digital services provided by issuer (so-called utility token) and tokens of mixed nature (so-called hybrid token).

Establishing the nature of a token can sometimes be difficult, but it is of fundamental importance to identify the applicable tax discipline, which may present significant margins of uncertainty.

Regarding the tax treatment of the currency tokens, there is a clear position of the Court of Justice of the European Union in the judgment of 22 October 2015, case C-264/14 'Hedqvist', concerning bitcoins, in which was stated that they can be qualified, for VAT purposes, as 'currencies', with the consequent application of the exemption provided for the exchange of transactions relating to *"currencies, banknotes and coins with liberating value"*.

In Italy, as an example, in the matter of direct taxes, the Resolution of the Revenue Agency no. 72 / E of September 2, 2016 (relating to bitcoin) follows the ruling of the European Court by ruling that tax rules on foreign currencies are applicable to companies that own these cryptocurrencies.

Such an approach is criticisable because the company that owns bitcoin will be called to determine the value of its portfolio in cryptocurrency according to the exchange rate in force on the closing date of the financial year, with consequent taxation of any still latent capital gains, which will not necessarily be realised in concrete, due to the considerable volatility of virtual currencies.

The aforementioned Resolution can also be criticised specifically on regards to the section in which it states that the ownership of bitcoins by natural persons, acting outside of the business activity, does not generate taxable income, since it is a matter of spot currency transactions in which it lacks the speculative purpose.

It should be remembered that the Italian tax legislation, in art. 67, c. 1-ter of the Consolidated Law on Income Taxes (TUIR), for foreign currency spot transactions with total deposits of all deposits and current accounts in foreign currency (during the year) exceeding € 51,645.69 for at least seven continuous working days, the taxation of capital gains.

The tax regime for security tokens to which the provisions of the Consolidated Law on Income Taxes (TUIR) relating to financial instruments and, in particular, instruments similar to shares or bonds, depending on the specific characteristics of token, with the consequent tax effects deriving from it, both for issuers and for underwriters.

The treatment of token utilities is still different, and they seem to be similar to the documents of legitimation provided for by art. 2002, Civil Code, ie *"documents that serve only to identify the person entitled to the benefit, or allow the transfer of the right without observing the forms of the assignment"*.

The proceeds from the sale of utility tokens should be taxed as revenues and subject to VAT, if received in the exercise of a business, art or profession.

If, on the other hand, they are purchased by an individual outside of the company, they should be irrelevant for the purposes of direct taxes and also VAT.

In Italy for example, actually, the rate applicable for the taxation of capital gains realised for companies is equal to 24%.

While the capital gains realised by natural persons apply the substitute tax of 26%.

The Italian tax payer, according to current legislation, has two possibilities:

1) if its activities do not achieve the conditions for the regulation of the average stock in the tax period and any capital gains that may be earned are not realised for the exercise of business activity, and there is no speculative intent under the legislation, taxable income seems to be generated according to the reconstruction given by the Italian Revenue Agency.

2) if instead these requirements are integrated, the substitute tax of 26% will apply.

Use Case #	*Use Case/Case Study Name*	*Use Case Type*
6	Validata	*Corporate identity*

A self-sovereign identity for businesses and organisations, based on blockchain validated data.

The VALIDATA project was launched in March 2018 at the initiative of Flanders Information Agency and the Agency for Innovation and Business (VLAIO) . In a first phase, contact, information and support is sought with and from Flemish and federal public services, local authorities, professional organisations, financial and administrative players and a large number of other external partners.

The VALIDATA network is an opportunity to create a source of truth.

Entrepreneurs and companies can share validated data from and with various authorities and external partners such as bank-insurers, professional organisations, social secretariats and universities.

Blockchain technology makes it possible to share both validated and authentic data of the entrepreneur or enterprise, with 100% certainty about its correctness and reliability.

Examples of these data are:

- The content of the Crossroads Bank for Enterprises (KBO);
- Insurance certificates;
- Receipts;
- Permits;
- Shareholders;
- Accreditations; and
- Small and medium-sized enterprises (SME) ‘stamp’.

30 years after the digitization of this data, companies are still confronted with a complex search for the correct sources of the data they are obliged to supply. By setting up a sufficiently broad consortium, the validation data network can be the start of the ultimate administrative simplification for entrepreneurs and businesses.

The creation of a widely supported network of players with an interest in receiving data from or supplying data to the entrepreneur or business gives rise to a number of possibilities:

- developing a self-managed identity of the company; and
- returning all data of the entrepreneur to his or her hands, and making them enforceable against third parties.

From an authentic source, it is possible to connect the 'authentic' stamp on the data directly to all participants throughout the VALIDATA network.

The VALIDATA application also makes it possible for entrepreneurs and companies to upload information, preferably in the form of structured data or documents, to a personal data / document store or digital safe.

Recognised validators can then validate this information (e.g. a bank-insurer uploads an insurance certificate, or validates the insurance certificate that the entrepreneur has uploaded), and the combination of information and validation can then be shared.

The sharing of information is always under the control of the entrepreneur/company, unless it concerns public information. If information is shared between mandated authorities, the entrepreneur/enterprise can see who has had access to it.

During the exploration phase, discussions are held with all possible partners for the network.
The first objective is to form a 'coalition of the willing', a limited but diverse group, including those from the above group. In the coming months, we will be able to work together on a minimum viable product for the application. We would like to stress that the above list is not exhaustive. It is only a list of the initial discussion partners.

The exploration phase of the VALIDATA project started at the beginning of 2018. All aspects of the architecture and vision presented in this document are therefore still open to discussion and the concept is subject to improvement.

There is room for extensive consultation with existing initiatives, both public and private. Clear coordination is also planned for possible cross-fertilisation and joint development efforts.

The second objective is to take a first step in setting up this application before the summer of 2018 and to deliver a 'minimum viable product' by the beginning of 2019.

Use Case #	*Use Case/Case Study Name*	*Use Case Type*
7	Tennet	*Energy*
URL	https://www.tennet.eu/news/detail/tennet-unlocks-distributed-flexibility-via-blockchain/	

TenneT is a leading European electricity Transmission System Operator (TSO) with its main activities in the Netherlands and Germany while Vandebron supplies 100% renewable energy produced by local sources. The company does this through its marketplace for renewable energy. The renewable energy company is a pioneer in the field of innovation, customer care and sustainability, and has been named 'Best Energy Supplier of the Netherlands'.

TenneT is responsible for maintaining the balance on the high-voltage grid. To guarantee a continuous supply of electricity, supply and demand have to be balanced 24 hours a day, seven days a week. In the event of imbalance between supply and demand, TenneT makes sure additional electricity is supplied or deploys reserve capacity. In this pilot project, Vandebron (in the Netherlands) will work with customers who own an electric vehicle to make the capacity of their car batteries available to help TenneT balance the grid. Vandebron will provide this service to its customers

without compromising the availability of their car battery. The blockchain enables each car to participate by recording their availability and their action in response to signals from TenneT.

Redispatch measures prevent regional overloads on the grid. This system is necessary, for example in Germany, when wind energy produced in northern Germany cannot be transported to the industrial centres in the south of the country. In this pilot project with sonnen eServices (the energy group of the Sonnen group), a network of residential solar batteries will be made available to help reduce the imposition of limitations on wind energy at times of insufficient transport capacity.

The blockchain presents the operator from TenneT with a view of the available pool of flexibility, ready to activate at the push of the button, after which the blockchain records batteries' contribution. This will enable sonnen and TenneT to support the integration of renewable energy sources into the German electricity supply system.

Market parties will be informed about the pilot projects and relevant developments by means of newsletters and market consultation workshops in the Netherlands and Germany. Once the concept has been proven to work, it will be launched and the TenneT Energy Community will be open for other parties to join.

The digital process of verifying and documenting the performance values of these distributed flexible energy devices is delivered using Hyperledger Fabric, a blockchain framework implementation and one of the Hyperledger projects hosted by The Linux Foundation. Blockchain is suited to connecting multiple parties and large numbers of distributed computed nodes and enabling them to undertake joint action in a scalable, transparent and trusted network. This platform ensures the verifiability and transparency of the transactions of the small-scale batteries and electric cars. The blockchain will enable optimal distribution across all markets and functions. This way, TenneT will be able to gain insight and have the possibility to activate flexibility in the energy system, while consumers are facilitated in making their flexibility available to the balancing market.

Use Case #	*Use Case/Case Study Name*	*Use Case Type*
8	MTK	*Government*
URL	*n/a*	

MTK (The Central Union of Agricultural Producers and Forest Owners) with 317,000 members will become the first organization in Finland to launch a blockchain based e-government solution. MTK's director of business development Marko Mäki-Hakola confirms MTK's interest in new technology if it has the potential to provide tangible cost and other benefits: *"In blockchain, we see a number of features which could lend themselves well to the needs of entrepreneurs and citizens in the countryside as well as in the cities."*

Combining with the ToitaSuomesta.fi employment service developed by CoReorient Oy, Essentia will be used by employment offices, employers and suchlike as a platform for managed employment in the local community.

Within this framework, any worker can save certificates of their performed jobs to the Essentia platform and allow their future employers and employment office to view these.

This way we can ensure easier and safer cooperation. The employer can view and also add a job certificate(s) even if they are not a user of the ToitaSuomesta work mediation service.

This option grants security and is actually a real time-saver both for employers and employees. Last but not least, employment offices can view the progress of the employee across all work mediation services and confirm that he/she fulfils benefits criteria.

From now on it won't be necessary to share an individual's entire job records between services and there will also be no need for a new database at the employment office.

MTK, whose members hail from various regional and local organizations, believe that this is only the start of real life testing for MTK's main interest lies in other areas. One of them is managing and sharing machine-generated data from tractors, dairy, and other equipment. They are also tracking production chains, for example, forest side products from the owner to the refinery, or end-user land registries that will no longer need field sizes regularly updated; the future possibilities for blockchain technology are endless.

Use Case #	*Use Case/Case Study Name*	*Use Case Type*
9	Carrefour	*Food Tracking*
URL	http://www.carrefour.com/current-news/carrefour-launches-europes-first-food-blockchain	

Retailer Carrefour will use blockchain-based technology to improve checks on the standards of its food products. Carrefour is among several leading companies tapping into the growing use of blockchain in order to track where products come from, as consumers increasingly look to ensure that products meet standards regarding ethics and general safety.

The use of blockchain would enable shoppers in France to trace where certain food products are sourced, and added it was extending its use of such technology in this capacity.

Within the same field, Nestle, Unilever, Tyson Foods and other large food and retail companies joined an IBM project to explore how blockchain technology can help track food supply chains and improve safety.

Carrefour will extend the use of blockchain to honey, eggs, cheese, milk, oranges, tomatoes, salmon and hamburgers by end-2018. It currently uses the blockchain programme to trace the production of free-range chicken in the Auvergne region in central France. Consumers can use a smartphone to scan a code on the package to obtain information at each stage of production, including where and how the chickens were raised and what they were fed as well as where the meat was processed, added the French company.

Carrefour is also currently conducting blockchain tests to improve tracing the source of food products in China and could expand it to other countries.

Use Case #	*Use Case/Case Study Name*	*Use Case Type*
10	Provenance	*Food Tracking*
URL	https://www.provenance.org/	

Project Provenance Ltd. operates an online data platform that enables users to gather and share stories of products and their makers.

The company Project Provenance Ltd claims its aim is to empower people to change the way the global economy works. Creating and fostering open and accessible information about products is at their core, inspiring citizens to be active through the things they choose to buy.

Provenance has developed a distributed cryptographic ledger, or blockchain, designed to provide transparency to track fresh produce from origin to grocery store shelf. This follows a successful international pilot tracking tuna through Southeast Asian supply chains and a pilot project with the world's largest consumer cooperative tracking fresh produce.

In the art world, 'provenance' refers to the earliest known source or origin of a piece of artwork and a history of the hands that it has passed through. When it comes to

tracking fresh produce, or any other supply chain, a blockchain can provide a highly detailed provenance for every action that a crate of lettuce, fish or tomatoes go through.

For example, workers fill up a crate of freshly picked tomatoes and a label is added to the side that uniquely identifies it. That identifier and the time of the crates placement in storage awaiting transport is written into the blockchain. When that crate is placed in a truck, that action gets written as a record to the blockchain. This keeps happening with each exchange from truck to distribution centre, centre to refrigerated grocery chain truck, from truck to grocery store.

Since a blockchain provides a secure way to encrypt and sign all of the metadata associated with every transaction — what, who, where, when and whatever else is needed — it makes it difficult to modify or remove transactions after the fact. As a result, if those tomatoes go missing, are delivered damaged or are discovered to be contaminated, their entire route from hand-to-hand can be backtracked. This opens up a lot of opportunities for maintaining food safety and streamlining product transport operations.

By design, every transaction along a supply chain on the blockchain is fully auditable. By inspecting the blockchain, smartphone applications can aggregate and display information to customers in a real-time manner; furthermore, due to the strong integrity properties of the blockchain, this information can be genuinely trusted. A thoughtful user interface that sheds light on the digital journey of a product can empower better purchases by giving users a true choice that they can exercise.

There are substantial broad effects of bringing near-frictionless transparency to consumer purchase decisions and product identity; clearly there is likely to be an additional ‘virtuous’ component in purchase decisions, especially among mid-level purchases where a marginal increase of 20% to the price does not affect the willingness to buy. Additional levels of guarantee over genuine articles is a high-value use case. While an initial introduction of this technology may be in the form of a discrete and removable label, easily verified through a smartphone-readable QR-code, a more progressive possibility would be a conspicuous holographic or RFID tag,

embedded in the brand label, allowing the owner to prove the authenticity of the product at any time by accessing the data on the blockchain through the tag.

Additional features could securely provide crowd-sourced scrutiny as a complement the formal certification process; e.g., workers themselves could report from farms and factories about the operational processes if they obtain a secure identity in the system.

A detailed whitepaper has been published by Provenance at www.provenance.org/whitepaper.

8. Annex B The FG-BDLT contributing Members

In 2018, there has been sixteen CEN or CENELEC members, which have been participating actively in the work of the FG-BDLT, as indicated below.

No.	Abbreviation		
1.	UNE	Asociación Española de Normalización	ES
2.	AFNOR	Association française de normalisation	FR
3.	ASI	Austrian Standards Institute	AT
4.	ASRO	Asociatia de Standardizare din România	RO
5.	BSI	British Standards Institution	UK
6.	ELOT	Hellenic Organization for Standardization	GR
7.	CYS	Cyprus Organization for Standardization	CY
8.	DIN	Deutsches Institut für Normung e.V.	DE
9.	DKE	German Commission for Electrical, Electronic & Information Technologies	DE
10.	NEN	Netherlands Standardization Institute	NL
11.	PKN	Polish Committee for Standardization	PL
12.	SIS	Swedish Standards Institute	SE
13.	SN	Standards Norway	NO
14.	SUTN	Slovak Standards Institute	SK
15.	UNI	Ente Nazionale Italiano di Unificazione	IT
16.	UNMZ	Czech Office for Standards, Metrology and Testing	CZ

ETUC (European Trade Union Confederation) also participated in the work.

The FG-BDLT Secretariat is located at UNI, the Italian member of CEN and ISO.

9. Annex C The Blockchain / DLT ecosystem

Blockchain technology represents an evolution of network communications. The Internet and the world wide web have been transforming lives for decades. Information has never been so accessible and instantaneous. Blockchain is probably the most disruptive technology since the arrival of the Internet and has the potential to transform industries by decentralizing trust, generating an exchange of goods and services without the need for third parties.

A blockchain is a type of decentralised database, in which transactions are verified, validated and aggregated into 'blocks'. The blocks are then linked together in 'chains.' This results in a structure of blocks linked together in a chain that increases in size in a linear direction.

Within certain conditions, the data contained within the blockchain cannot be changed and can no longer be manipulated or deleted. If new data is added, the blockchain will be updated in all connected nodes everywhere.

Their ability to store any kind of data as a consensus of replicated shared and synchronised digital records distributed across multiple sites, without depending on any central administrator, together with their properties regarding temper-proofness (and therefore non-repudiation) and multi-party verifiability opens a wide range of applications, and new interaction models among those entities willing to record the transactions associated to those interactions through these ledgers

This improved data security and ensures that data is kept safe from frauds and makings the sharing of data more secure overall.

In conjunction with Industry 4.0, blockchain is ideally suited for the secure and global sharing of sensitive information, such as design and production parameters.

One function of a blockchain that is of significance for the evolution of the ecosystem is that of 'smart contracts.' These are software applications that can for example represent internet-based contracts where the contractual obligations are permanently programmed and have been saved within the blockchain, and can be executed,

without possibility to be tampered, by the network independently from the actor who saved it there.

In the context of Industry 4.0 services, Blockchain technology can therefore be used as a platform, for example for the generation, autonomous negotiation and automated closure of dynamic value-added chains.

10. Annex D Abbreviations

The FG-BDLT White Paper makes use of several abbreviations as comprised below.

Abbreviation *Description of the abbreviated term*

UNE	*Asociación Española de Normalización*
AFNOR	Association française de normalisation
ASI	Austrian Standards Institute
ASRO	Asociatia de Standardizare din România
AT	Austria
BSI	British Standards Institution
CEN	European Committee for Standardization
CENELEC Standardization	European Committee for Electrotechnical
EC	European Commission
ESO	European Standardization Organization
ESRIF	European Security Research and Innovation Forum
ETSI	European Telecommunications Standards Institute
EU	European Union
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
ISO/IEC standards	ISO and IEC joint activities and joint international

IT	Information Technology
JRC	Joint Research Centre of the European Commission
JTC 1	ISO/IEC Joint Technical Committee No. 1 – Information Technology
MB	Member Body
NSO	National Standards Organization
SDO	Standards Developing Organization
SSO	Standards Setting Organization
SME	Small and Medium-sized Enterprise
URL	Uniform Resource Locator a.k.a. web address
WG	Working Group

11. Contact and Copyright

Point of Contact: UNI

CEN/CENELEC FG-FDLT Secretariat

Via Sanfront, 1/C

10138 TURIN

Italy

Tel.: +39 011 501027

email: sirocchi@uninfo.it

White paper convenor: Pietro Marchionni

<pietro.marchionni@agid.gov.it>

Copyright Notice

SECRETARIAT UNI/UNINFO

Via Sanfront, 1/C • 10138 TORINO ITALY

Tel: +39 011 501027 email: sirocchi@uninfo.it

Subgroup Convenor: Pietro Marchionni

Convenor: pietro.marchionni@agid.gov.it