CEN/CENELEC Focus Group BDLT
White Paper Subgroup
N 001

Date: 13th June 2018

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
White Paper Subgroup

Document Title	**Recommendations for Successful Adoption in Europe of Emerging Technical Standards on Distributed Ledger/Blockchain Technologies**
Last modification	**12th July 2018**
Document Version	**0.9**

SECRETARIAT UNI/UNINFO

Subgroup Convenor: Pietro Marchionni

Via Sanfront, 1/C • 10138 TORINO ITALY
Tel: +39 011 501027 email: sirocchi@uninfo.it
Convenor: pietro.marchionni@agid.gov.it

Contents

Via Sanfront, 1/C • 10138 TORINO ITALY
Tel: +39 011 501027 email: sirocchi@uninfo.it
Convenor: pietro.marchionni@agid.gov.it

1 Introduction

CEN and CENELEC created a new Focus Group on Blockchain and Distributed Ledger Technologies (FG-Blockchain-DLT), with the 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. They commonly agreed that CEN-CLC FG-Blockchain-DLT would take ownership of this white paper project, to assign it to a dedicated sub-group, and to organize regular stakeholder engagement meetings to support the work of the Focus Group.

The objective of this white paper is to identify potential specific European needs to be addressed by standardization.

2 Executive Summary

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 digitalization of industry and modernization of public services,

The strategy of the Digital Society requires building blocks on which such 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 on which the Digital Society can be built.

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-CENELEC Focus Group on Blockchain and Distributed Ledger Technologies was established and will maintain a white paper collecting identified specific European needs on these technologies, in the context of the particular European normative and technological context. The Focus Group aim then to support standardization bodies at international level and ISO/TC 307 is the preferred route for standardization together with other standardization bodies as indicated in the References section. This will be achieved also by raising awareness on ISO's activities and encouraging a broader European participation in ISO/TC 307.

3 European Commission Initiatives Highlights

Blockchain and distributed ledger technology (DLT) can change the way citizens and organisations collaborate, share information, execute transactions and deliver services.

It is a technology that promotes user "trust" making it possible to share on-line information, agree on and record transactions in a verifiable, secure and permanent way. The technology is being used mainly in financial services and 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 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 should be further invested until the end of the EU funding programme Horizon 2020[4].

In its Communication on ICT standardisation 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

[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
[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

being locked in proprietary solutions, It increases competition, and when adopted in (public) procurement, it offers SMEs better opportunities to compete with major vendors. Through its liaison A with ISO Technical Committee 307 on blockchain and Distributed Ledger Technologies, the Commission is contributing to international standardisation in important areas such as smart contracts, identity, security and privacy, governance, use cases… But there is also a need to identify potential specificities related to the European market, wether they related 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.

This White Paper will contribute to this standardisation effort.

4 The FG DLT Recommendations

1.1 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 every business in Europe can draw the full benefits from digital innovation.

On this basis, this section collects specific elements identified that could make emerging technical standards to effectively contribute to improve the adoption by industrial companies to the Single Digital Market and its integration within the global digital market.

Such adoption would help improving the European and global job market, contribution to (i) new jobs creation, replacing those that would become unnecessary by DL/Blockchain technologies adoption; (ii) new training and professional qualifications opportunities

Digitising European Industry initiative's actions are structured around five main pillars:

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].

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, 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 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 319	Maintenance
CLC/TC 13	Electrical energy measurement and control

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

CLC/TC 205	Home and Building Electronic Systems (HBES)
CLC/TC 215	Electrotechnical aspects of telecommunication equipment
CLC/TC 8X	System aspects of electrical energy supply
CEN/CLC/ETSI SEG-CG	Coordination Group on Smart Energy Grids
CEN/CLC/ETSI SM-CG	Smart Meter Coordination Group

The following IEC Committees are also evaluated as relevant:

IEC SysC "Smart Energy	System Committee "Smart Energy"
IEC/TC 57	Power systems management and associated information exchange
IEC/TC 8	Systems aspects of electrical energy supply

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's also vital that he standardization framework encompasses a set of information security

requirements for demonstrably secure Blockchain implementations, enabling their adoption on the market.

ICT standards have 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 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.

To respond to this task, the 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-CLC Focus Group on Blockchain and DLT monitors 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-CLC Focus Group on Blockchain and DLT could act as a reference point for exchange between the CEN and CLC technical committees, having a potential Blockchain/DLT dimensions, and the other standardization actors, in order to develop coherent set of standards and technical specifications.

Recommendations:

- 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-CLC 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

The FG DLT recommends that

FG DLT Recommendation #:
To focus on DLT characteristics oriented at Enterprise transormation models….

.

1.2 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 EC FinTech Action Plan has been announced last 8th of March 2018 and DL/Blockchain technologies are described as a key success factor for many of 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 favorable 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 programs 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 globalization 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.

As a matter of 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 influence 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 recent 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 fix the lack of mutual trust.

Regarding Tax compliance, DLT/Blockchain technologies can be used to manage simple business process 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 authorization (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 a communication of 10 January 2017 (Building a European Data Economy, 10 January 2017, COM (2017) 9 final) 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 rights;
- 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.

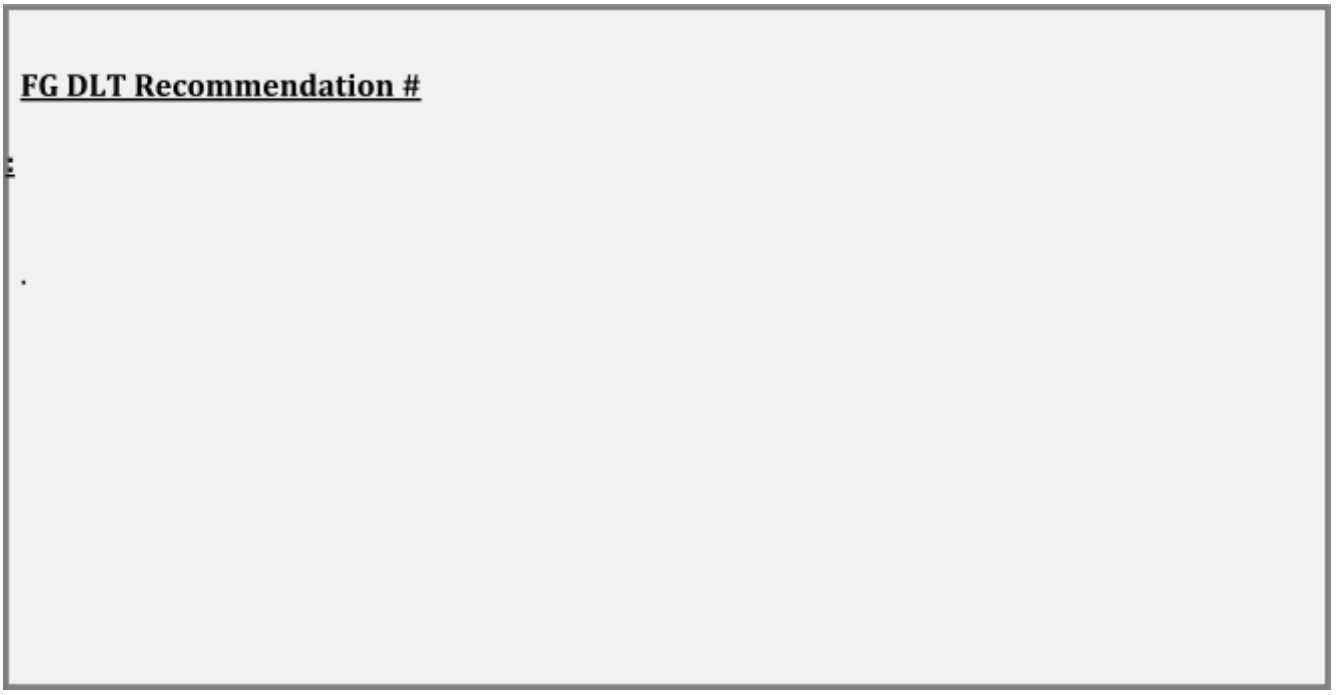
The ability to manage transactions across all bank accounts with a single interface generates advantages such as:

- 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.



1.3 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 program.

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.

Following a list of relevant Horizon 2020 projects is provided, highlighting the business case for the use of blockchain.

Highlighted Projects

KONFIDO (http://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 component logs after being appropriately filtered, transformed and encrypted, they 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 an H2020 project (https://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 behavioural 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.

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 (https://decodeproject.eu/) is a 3 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, startups, 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.

Blockchain integration

1) A blockchain (developed by one of the partners) 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.

Barriers of adopting Blockchain.

The project is investigating the legal status of smart contracts, especially as a binding for

PRIViLEDGE (https://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 decentralized transactions.

Blockchain integration

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 decentralized 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 decentralized software update system to be used in the Cardano stake-based ledger.

FG DLT Recommendation # :

1.4 Support for the Sustainable Development Strategies

Rationale

The EU Sustainable Development Strategy 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, able to tap the ecological and social innovation potential of the economy and in the end able 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 with blockchain application. 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 decentralization 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 digitalization, 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).

A blockchain technology is based on data banks that can manage and process data without a centralized control structure, such as a bank. Everyone can see the transactions between Participant A and Participant B, but each participant in the transaction remains anonymous. Famous example: cryptocurrencies like bitcoins. Blockchain technology is used in the financial sector, but also in many other areas. Especially the energy sector in the framework of decentralization and transition to large share of renewables could benefit from such process.

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. And 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 the year. 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 a decision makers, allowing them to see, to understand, to analyze and, after, to take the best decision for sustainability with a sustainable business model.

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

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

Standards being based on best practices, the work of CEN/CENELEC/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 programs, 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).

FG DLT Recommendation # :

.

1.5 Digital Identity and Signature Management

Rationale

Identification is a key element in any kind of system; and 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 ensures 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.

Three 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 White Paper aims to provision 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**
  - **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.
  - **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 decentralized PKI.

- **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 of blockchain records has to be considered in view of determining a solution to i.e. the 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 decentralized 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 sensitive 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**
  - 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, some functions in eIDAS framework are subject to GDPR requirements such as 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/TC224 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 5: Emerging standards in the decentralized 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.) recognized 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 decentralized 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[7].

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 them 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 decentralized secure cross-border transactions which 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.

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

FG DLT Recommendation # :

.1)Blockchain deployment in eIDAS regulatory context needs to consider enrolment, credential management and authentication domains with their respective privacy facet.

2) 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.

3) 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

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

5) the variety of form-factor hosting eID involved in eIDAS operations and interacting with the blockchain is worth being examined and described

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

7) TC307 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.

1.6 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 and 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[8] on this topic and the EU Blockchain Observatory and Forum started to produce in-depth analysis around the GDPR[9].

According to the GDPR it is mandatory to "implement appropriate technical and organizational measures to comply with the regulation whenever personal data is handled. Ensuring privacy and data protection has therefore to be addressed "by design", not leaving any possibility to compromise personal data and/or personal information.

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".

[8] 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

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

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. But 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. 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 hash function is presented as a solution to comply with the GDPR. The emergence of a standardized approach for hashing personal data and storing these hashes on-chain, exploring opportunities such as salted and peppered hashes or the "hasing-out" method[10], 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. But at the blockchain infrastructure level this is more complicated, particularly in public, permissionless blockchains where all the full nodes

[10] "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.

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**. GDPR stipulates that you can only transfer third-party data to a third country if that country's data protection laws offer equivalent levels of protection. 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 does not get talked about much is the right that GDPR gives data subjects to be protected from automated processing of information. 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 on 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 standardisation bodies is crucial in bringing the answers needed to reconcile Blockchain/DLT and the GDPR.

FG DLT Recommendation # :

.1)It is fundamental that standardisation efforts include the implications of GDPR within their related groups.

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

3) Blockchain technology in relation to governance must address the data controller requirements of GDPR

1.7 Governance

Rationale

Governing networks using DL/Blockchain technologies is a complex process due to its characteristic of decentralized control and operation. The establishment of policies to

guarantee proper governance should include mechanisms to balance the powers of the members (with the associated accountability), and their primary duty of guaranteeing the resilience of the network..

The EU has a longstanding experience in governance of complex distributed legal and economic systems based mainly on consensus among peers. This section will collect the standardization elements for effective governance of networks based on DL/Blockchain technologies aiming to be legally binding within the EU Single Digital Market, based on existing experience of multiple levels and models of governance within the EU

FG DLT Recommendation # :

.

1.8 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, 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.

FG DLT Recommendation # :

- **ISO/TC 307 to works jointly with ISO/JTC 1/SC27 for Blockchain information security aspects**

1.9 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 modernisation of public administrations.

The EU **eGovernment Action Plan 2016-2020**[11] aims:

- to modernise public administration,
- 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[12] is part of the EU eGovernment Action Plan 2016-2020 and 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)[13] supports multiple digital infrastructure projects which 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[14]. The building blocks[15] 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

[11] https://ec.europa.eu/digital-single-market/en/european-egovernment-action-plan-2016-2020
[12] https://ec.europa.eu/digital-single-market/en/news/once-only-principle-toop-project-launched-january-2017
[13] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/CEF+Digital+Home
[14] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Digital+Infrastructures
[15] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Building+Blocks

Market and EU plans to support participation of European experts in international standardisation 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 5 essential building blocks of the digital Single Market: 5G, Cloud Computing, Cybersecurity, Big Data and IoT.

The Digital Single Market has its main enabler in the Connecting Europe Facility (CEF) Programme, the foundation of which comprises of CEF Building Blocks :

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

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

Introduction

Administrative decentralization, accordingly 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"[16].

Similarly, it defines political decentralization 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

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

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 centralized or federated, or more simply from where institutions that constitute the government are located, every government is inherently decentralized 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
- and 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 centralized 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[17] has also been published by Pietro 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…)

[17] 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

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 accomodate (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) in case accommodate flexible consensus models as different member states could require/implement different solutions based on their country-defined governance models related to government processes

FG DLT Recommendation # :

1) Interoperability in data and interfaces must be evaluated as key requirement for any blockchain/DLT running government processes/services
2) Consensus models need to be evaluated when dealing with government processes
3) Cross-border government services would require open standards in data exchange/discovery models

1.10 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 (eg. 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 1 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 multisectorial 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 summarized as a semipublic, 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 European Union.

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 the 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, alpha-numeric 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 harmonized 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 organizations 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 needed 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, the LEI should 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 centers 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 centers to become first-class citizen in the Cloud provisioning landscape for Public Administrations. FaaS crucially relies on blockchain to realize a first-time democratic and decentralized governance model. Blockchain is exploited as an innovative underlying infrastructure underpinning trustless 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 anonymisation history record which is used to dynamically tune anonymisation 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 carried 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*
5	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 evaliuation 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 utilize the power of blockchain technology to digitalize 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 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 revolutionize 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*
7	n/a	*Capital Gains Taxation*

A recent problem for tax authorities is represented by the taxation of capital gains realized 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 realized (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.

For the tax issues related to the taxation of capital gains realized by individuals, we must state the circumstance of how on the issue, to date, there is only an official reference issued by the Italian Revenue Agency, in Resolution no. 72 / E of September 2, 2016, in response to a call made by a company with the objective of starting a Bitcoin exchange business ("exchange").

In the answer to the questions put by the interpellant, the Financial Administration correctly

takes its cue from certain principles contained in a ruling by the European Court of Justice, number C-264/14 (Hedqvist case), which is still a beacon for any discussion in the tax area that interests virtual currencies.

The Inland Revenue in its own document of practice traces the reflections of the EU justice body, which equates virtual currencies by means of voluntarily accepted payment, whose function is therefore exhausted in itself. However, the Administration, even without ever mentioning the term "foreign" in its text, clearly refers to it in the content of its resolution, thus going beyond the conclusions of the EU Court of Justice, which, as mentioned, called Bitcoin as mere "means of payment", never money or currency.

The quotation contained in the resolution, however, which caused a stir, is that with regard to the taxation for the purposes of income tax on customers who are natural persons who hold bitcoins outside the company's activity, "foreign currency spot transactions do not generate taxable income, lacking the speculative purpose".

This analysis of the taxation of capital gains generated by the private sale of cryptocurrencies could therefore be concluded here: with an explicit reference to Circular no. 72/E (Agenzia delle Entrate) to traditional currencies and the lack of speculative purpose of a spot sale of currency (No taxation, No fulfillment).

This indication cannot be accepted for various reasons. The first reason concerns the equation of cryptocurrencies with traditional currencies. In fact, there are evidences that allow us to exclude the equation of Bitcoin and virtual currencies to traditional currencies. The most obvious is contained in the article 1, paragraph 4 Legislative Decree No. 58/98 (TUF) where it is clearly indicated that "means of payment" are not financial instruments.

The confirmation is then represented by the choice, made by the legislator, to place the "exchange" of virtual currencies among the subjects who carry out "other non-financial transactions", article 3 paragraph 5, within the text of the recently integrated anti-money laundering legislation, Legislative Decree No. 231/2007.

Beyond the above criticisms, a prudential and "pragmatic" approach to the determination of the best tax qualification related to the realization of capital gains realized on cryptocurrency exchange rates could continue to be based on the cryptocurrency of the traditional currencies

in the sense suggested by the Agency, but nevertheless using the whole legislation applicable to them.

In fact, it should be taken in consideration the fact that the speculative purpose underlying the sale and purchase transactions is one of the taxed cases, article 67 Decree 917/1972 (TUIR), but not the only one.

In particular, the speculative intent is presumable, as confirmed by the Revenue Agency, in forward transactions, always generate tax matters, and the reflections that can be made are essentially two:

- transactions on virtual currencies can be assimilated to operations carried out on deposits or current accounts, provided that all the aforementioned transactions are recorded on the Blockchain (not counting that the wallets are normally deposited at the exchange or the wallet provider)

- the activity of mere investment can be deduced, beyond the absolute presumptions contained in the article 67 Decree 917/1972 (TUIR), also by other elements that represent signs of the "animus" of the investor.

All in all, given the somewhat cryptic statement contained in the Resolution n. 72/E (Agenzia delle Entrate), the conclusion reached can be a practical solution defensible even in the face of disputes raised in the future by the Administration itself.

The hypothesis of the taxation of virtual currencies according to the typical pattern of foreign currencies held for mere investment, thus brings with it the verification of the quantitative limits contained in paragraph 1-ter of the same article 67 of the Consolidated Income Tax Act introduced to avoid "to attract non-significant cases to taxation" (C.M. No. 165/1998). The limits are those, known, of 100 million lire for over 7 consecutive days.

Also on this aspect, however, the practice referred to here reserves a surprise, contained in the aforementioned C.M. No. 165/1998. Meanwhile, the limit of 100 million lire (or 51,645.69 euro) must be verified, having regard to all the "deposits in foreign currency in deposits and current accounts maintained by the taxpayer" (therefore, for consistency of setting, currencies to legal tender) and virtual currencies); but the truly relevant aspect is that the valuation of the stock limit should be made with regard to the exchange rate at 1 January of

the year in which the condition for taxation occurs.

Given that many investors have approached the world of virtual coins as attracted by the "rally" at the end of the year, in which the value of bitcoin has touched the 20k dollars, it is possible to exclude from taxation anyone who has never owned, simultaneously and for more than 7 days, the remarkable number of about 56 Bitcoins.

The adherence to the classification of virtual currencies as a mere means of payment, adhering to the conclusions of the EU Court of Justice, would necessarily lead to a departure from the above-described taxation method, towards a first alternative, which could see the bitcoin categorised as "non-representative securities" with consequent (e.g. in Italy at 26%) full taxation through declarative regime, or, as opposed, the total exclusion from taxation not being the sale of such innovative instruments that can be framed in any of the cases that the Decree 917/1972 (TUIR) subject to taxation. This second choice is, in all evidence, as well as highly risky, certainly inadvisable.

For the taxation of companies the considerations expressed above are still valid and the rules for the taxation of "global" companies must be valid as well.

5 Conclusions

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" (https://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 (https://uncefact.unece.org/display/uncefactpublic/Blockchain+White+Paper)
- W3C Blockchain Community Group (https://www.w3.org/community/blockchain/)
- IEEE blockchain adoption initiative (https://blockchain.ieee.org/)
- Decentralized Internet Infrastructure Research Group of IETF (https://trac.ietf.org/trac/irtf/wiki/blockchain-federation)

- IETFdraft ALTO for the blockchain (https://tools.ietf.org/html/draft-hommes-alto-blockchain-01)
- W3C Verifiable Claims Working Group (https://www.w3.org/2017/vc/WG)
- W3C Decentralized Identifiers (DID) Community Group (https://w3c-ccg.github.io/did-spec)
- DIF - Decentralized Identity Foundation (https://identity.foundation)

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

(This page intentionally left blank.)

SECRETARIAT UNI/UNINFO

Subgroup Convenor: Pietro Marchionni

Via Sanfront, 1/C • 10138 TORINO ITALY
Tel: +39 011 501027 email: sirocchi@uninfo.it
Convenor: pietro.marchionni@agid.gov.it

Annex A The FG DLT Member Bodies

The FG DLT Member Bodies (MBs), i.e. ….

In 2018 there were fourteen EU Member States participating actively in the work of the FG DLT, as indicated below.

No.	Abbreviation	Description of the Institution of the respective CSCG Member Body	MB[1]
1.	AENOR	Asociación Española de Normalización y Certificación	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.	CCMC	CEN-CENELEC Management Centre	
7.	CYS	Cyprus Organization for Standardization	CY
8.	DIN	Deutsches Institut für Normung e.V.	DE
9.	DKE	DKE German Commission for Electrical, Electronic & Information Technologies	DE
10.	ENISA	European Union Agency for Network and Information Security	EU
11.	ETSI	European Telecommunications Standards Institute	EU
12.	JRC	Joint Research Centre of the European Commission	EU
13.	NEN	Netherlands Standardization Institute	NL
14.	PKN	Polish Committee for Standardization	PL
15.	SIS	Swedish Standards Institute	SE
16.	SN	Standards Norway	NO
17.	SUTN	Slovak Standards Institute	SK
18.	UNI	Ente Nazionale Italiano di Unificazione	IT
19.	UNMZ	Czech Office for Standards, Metrology and Testing	CZ

9.

The FG DLT Secretariat is located at UNI in Italy.

[1] The EU Member States are indicated by the appropriate ISO 3166 two-letter country code. Please note the above list is ordered sequentially by abbreviation of the nominating institutions only, thus the Member Bodies and/or EU Member States are presented without any sequential priorities.

Annex B 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 decentralized 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 synchronized 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 makeings 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.

Annex C Abbreviations

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

Abbreviation[2]	Description of the abbreviated term (and URL where applicable)
AENOR	Spanish Association for Standardisation and Certification *Asociación Española de Normalización y Certificación* http://www.aenor.es
AFNOR	Association française de normalisation http://www.afnor.org
ASI	Austrian Standards Institute *Österreichisches Normungsinstitut* https://www.austrian-standards.at
ASRO	Asociatia de Standardizare din România http://www.asro.ro
AT	Austria
BSI	British Standards Institution http://www.bsigroup.com
CCMC	CEN-CENELEC Management Centre http://www.cencenelec.eu/aboutus/MgtCentre
CEN	European Committee for Standardisation http://www.cen.eu
CENELEC	European Committee for Electrotechnical Standardisation http://www.cenelec.eu
EC	European Commission http://ec.europa.eu

[2] Annex A uses the appropriate ISO 3166 two-letter country code (listed here in *italics* as abbreviation) for these FG DLT members which represent EU Member States. Please refer to the list of FG DLT Member Bodies

Abbreviation[2]	Description of the abbreviated term (and URL where applicable)
ESO	European Standards Organisation
ESRIF	European Security Research and Innovation Forum http://ec.europa.eu/enterprise/policies/security/files/esrif_final_report_en.pdf
ETSI	European Telecommunications Standards Institute http://www.etsi.org
EU	European Union http://europa.eu
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission http://www.iec.ch
ISO	International Organization for Standardization http://www.iso.org
ISO/IEC	ISO and IEC joint activities and joint international standards http://www.standardsinfo.net
IT	Information Technology
JRC	Joint Research Centre of the European Commission http://ec.europa.eu/dgs/jrc/
JTC 1	ISO/IEC Joint Technical Committee No. 1 – Information Technology http://www.iso.org/iso/home/standards_development/ list_of_iso_technical_committees/jtc1_home.htm
MB	Member Body
NSO	National Standards Organisation
SDO	Standards Developing Organisation
SSO	Standards Setting Organization
SME	Small and Medium-sized Enterprise
URL	Uniform Resource Locator a.k.a. web address
WG	Working Group

Contact and Copyright

Point of Contact: UNI

CEN/CENELEC FG DLT 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