

# Joining Forces for Blockchain Standardisation

A Joint Report from INATBA  
and the European Commission

9 December, 2021  
9:00–17:00 CET



International Association for  
Trusted Blockchain Applications



## Table of contents

<b>Introduction</b>	<b>2</b>
Welcome – Goals of the Event and Agenda	3
INATBA Presentation	4
<b>Initiatives by Standardisation and Technical Specification Bodies</b>	<b>5</b>
ISO TC307 Presentation and Liaison Overview	5
ISO/TC 307/JWG 4: Security privacy and identity for Blockchain and DLT	6
ITU-T Presentation	7
CEN CENELEC JTC19	8
ETSI ISG PDL	9
IEEE Blockchain Standardisation	11
W3C Activities	12
OASIS Activities	14
IRTF/IETF Activities	14
<b>National &amp; Regional Initiatives</b>	<b>16</b>
Australian National Strategy	16
Japan	16
Korea	17
India	19
UAE	19
Canada	20
Brazil	22
EUOS/STAND-ICT	23
GBBC	25
AIOTI	26
LACChain	27
EBP/EBSI	28
<b>Panel discussion on possible gaps/overlaps, encouraging collaboration, best practices, recommendations</b>	<b>30</b>
Panellists	30
Moderators	30
<b>Event Takeaways</b>	<b>34</b>
The Organising Team at INATBA	35
The Conference Rapporteur	35
European Commission	35



## Introduction

In 2018, European Union Member States launched the European Blockchain Partnership (EBP), an initiative which is currently developing a European Blockchain Services Infrastructure. Today, all EU Member States, Norway and Lichtenstein are part of the EBP. Thanks to mainly grass-roots initiatives, more than 80 million euros within the Horizon 2020 framework have been allocated toward research and innovation projects where blockchain has been chosen as the major or one of the main technologies. More than 200 H2020 projects are actively undertaking research and innovation activities linked to blockchain. In addition, 300 million euros have been dedicated to a designated AI/Blockchain fund and successfully distributed to stimulate European start-ups.

The global standardisation community is actively working to develop standards for blockchain technology. A majority of internet standardisation bodies have working groups focused on blockchain. For example:

- ISO has established technical committee TC307 where more than 20 EU Member States are full members.
- IEC has set up a joint working group within ISO TC307.
- ITU-T is working on standardisation of blockchain as part of a broader SG16 Multimedia and e-services.
- ETSI has an industry specification group dedicated to Permissioned Distributed Ledgers.
- CEN/CENELEC has set up JTC19 on Blockchain and Distributed Ledger Technologies.
- IEEE has a number of working groups standardising blockchain applications in verticals such as Energy, IoT, e-Health or Agriculture.
- W3C, IETF, OASIS, UNECE are undertaking similar activities related to blockchain.

Given the diversity and vast array of standardisation activities worldwide, the European Commission organised a webinar “Joining Forces for Blockchain Standardisation” which took place in June 2020 and held 10 dedicated thematic roundtables “ICT Verticals and Horizontals for blockchain standardisation” which brought together more than 70 H2020 projects, standardisation communities and EBP members to represent European values and prevent duplicating standardisation efforts.

INATBA, the International Association for Trusted Blockchain Applications, is committed to serving as a convener of critical conversations on global standards for blockchain and other DLT. Its Standardisation Committee works closely with global standards-setting bodies to educate INATBA members about the important role of standards and how they can be involved in international efforts. The Standardisation Committee has hosted numerous roundtables on this topic, including a virtual event on the role of linguistic and cultural barriers in developing global blockchain infrastructure.

To continue these activities, INATBA and the European Commission hosted an online webinar, “Joining Forces for Blockchain Standardisation 2021” on 9 December 2021. The event convened standards-setting and technical specification bodies such as ISO, IEC, ITU-T, CEN/CENELEC, ETSI, IEEE as well as regional bodies like EBP/EBSI, LACChain and national authorities from countries

including Japan, India, Korea, USA, Brazil for a day-long workshop. The event consisted of presentations and panels to discuss progress made as well as ongoing challenges and collaboration opportunities. The workshop will serve as a starting point for 2022 thematic discussions related to Smart Contracts, Identity, Governance, Interoperability and CBDC/Crypto Assets.

## Welcome – Goals of the Event and Agenda

	<p><i>Helen Köpman, Acting Head of Unit, Digital Innovation &amp; Blockchain at the European Commission</i></p>
	<p><i>Rapolas Lakavičius, Policy Officer, Digital Innovation &amp; Blockchain at the European Commission</i></p>

In her opening speech, **Helen Köpman** thanked INATBA for hosting the event and welcomed the participants and speakers on behalf of the European Commission. She explained that the workshop was part of the European Commission strategy on blockchain and a follow up of the webinar “Joining Forces for Blockchain Standardisation”, which took place in June 2020 with dedicated thematic roundtables on ICT verticals and horizontals for blockchain standardisation. This year’s workshop was, then, a chance to build on the results of last year’s event and to take stock of the different initiatives on blockchain standardisation. She, thus, highlighted that the goal was to identify activities and gaps and to encourage cooperation among the various initiatives and standardisation bodies and to overcome challenges.

### Joining Forces for Blockchain Standardisation

17 June 2020

Which areas of blockchain standardisation would benefit the most from collaboration and cohesion?



**Rapolas Lakavičius** reminded the participants that the Blockchain standardisation event by the European Commission of 17 June 2020, with more than 400 participants from all over the world, took stock of various ongoing activities. Areas, such as Identity, Interoperability, Governance, Smart Contracts were considered as most in need for further collaboration and cohesion. Also, a concluding panel discussed cooperation among the different initiatives in order to maximise synergies and resources and minimise fragmentation risks.

Since then, the European Commission has continued working to support blockchain standardisation. In particular, ten roundtables took place covering different thematic areas with the participation of more than 70 H2020 blockchain-related projects. The thematic areas included fintech, digital society,



digital economy and SMEs, cybersecurity, IoT, e-health and future internet, media and big data, as well as SDGs, smart contracts and AI.

Mr Lakavičius presented the 2021 conference program, which was structured in three main sessions: first an overview of the initiatives by Standardisation and Technical Specification Bodies, then of the National and Regional initiatives, and finally a Concluding panel to discuss overlaps and collaboration opportunities.

## INATBA Presentation



*Marc Taverner, INATBA Executive Director. Former Global Ambassador & Markets Development, Bitfury. U.K.*

Mark Taverner welcomes the speakers and participants on behalf of INATBA. He introduces his organisation, INATBA, as a trade association representing the blockchain industry. It was founded with support of the European Commission and also recently partnered with ADGM, the Abu Dhabi Global Market. Despite the continuous support by the Commission, INATBA is not funded or controlled by the Commission, but it remains an independent body.

The association's objectives are to create and maintain permanent dialogue with public authorities and regulators to promote members' interests and to deliver unique networking and ecosystem collaborations, such as this conference. INATBA's publications and reports, such as on data privacy regulation, on policies for encryption and on identity, are available on [inatba.org](http://inatba.org).

As the most impactful and accessible industry body, INATBA has a wide membership base with almost 170 members across 36 countries. Besides private sector's memberships, INATBA has partnerships with Standards Bodies that liaise with the Standardisation Committee. Also, the association has a Government Advisory Body, with a rotating presidency currently held by the European Commission, and an Academic Advisory Body. The latter is involved in the development of many deliverables, such as a strategy to help Europe accelerate the skills for blockchain within a H2020 funded project and a consortium of 25 partners. INATBA has 15 working groups covering vertical sectors and horizontal activities, including standards, governance and interoperability.

Mark Taverner concludes his intervention by inviting industry and all other stakeholders to join INATBA's platform for collaboration to help drive the blockchain industry forward.

## Initiatives by Standardisation and Technical Specification Bodies

### ISO TC307 Presentation and Liaison Overview



*Craig Dunn, Chair, ISO Technical Committee Blockchain and Distributed Ledger Technologies*

As presented by chair Craig Dunn, the aim of ISO TC 307 is to meet the growing need for standardisation in the blockchain area by providing internationally agreed ways of working to improve security, privacy, scalability and interoperability and so encourage the technology's widespread adoption through greater innovation, enhanced governance and sustainable development.

The Technical Committee first met in Sydney in April 2017, with further meetings held in London, Tokyo, Moscow, Dublin and Hyderabad – with virtual meetings since May 2020 owing to COVID-19. It is organised in Working/Study Groups covering aspects such as Foundations, Security-Privacy and Identity, Smart Contracts, Use Cases, Governance, Interoperability and Records Management.

The body works closely with other ISO technical committees and has formal liaisons with other relevant organisations. It has participation from delegations of 60 countries from all continents.

Published or very advanced deliverables include international standards on Vocabulary and Reference architecture, a technical specification on taxonomy and ontology and a technical report on Security management of digital asset custodians. Other technical reports are "Privacy and personally identifiable information protection considerations", an "Overview of existing DLT systems for identity management" and an "Overview of and interactions between Smart Contracts in blockchain and distributed ledger technology systems" as well as "Use cases". The TC also published a technical specification called "Guidelines for governance".

Less mature projects under current development include an "Overview of smart contract security good practice and issues", an "Overview of trust anchors for DLT-based identity management", both technical reports, and an International Standard on "Decentralised identity: for the identification of subjects and objects".

Additional work is ongoing for either technical specification or technical reports on "Legally binding smart contracts", "Identifiers of subjects & objects for the design of blockchain systems", "Data flow model for blockchain & DLT use cases", "Interoperability framework", "Guidance for Auditing DLT systems", "Digital currencies", "Representation of physical asset as non-fungible tokens" and "Application of blockchain technology to records management – issues and considerations". Use cases will soon be published. They use standards templates and cover different industries, so it will be easier to compare them. Governance is also an interesting area, expected to provide helpful guidelines for many stakeholders. Interoperability is also on the radar and work is ongoing.



ISO TC307 values its liaisons with external organisations as key to development of relevant, highest quality and widely accepted standards. These include the Enterprise Ethereum Alliance, the European Commission, Global Standards One, IEEE, the International Federation of Surveyors, the International Telecommunication Union, INATBA, the OECD, the Open Geospatial Consortium, Small Business Standards, SWIFT and UNECE.

Answering one question about participation by local communities and startups, Craig Dunn explains that participation is open via the national standards bodies and via liaison organisations.

## ISO/TC 307/JWG 4: Security privacy and identity for Blockchain and DLT



*Julien Bringer, Convener of the Security, Privacy and Identity Working Groups of ISO Standardization Committee TC307 on Blockchain and Distributed Ledger Technologies*

Julien Bringer firstly introduced JWG 4, the group chairs. This is a Joint Working Group between ISO/TC 307 Blockchain and distributed ledger technologies and ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection. TC 307 aims to meet the growing need for standardisation in blockchain and DLT area by providing internationally agreed ways of working to improve security, privacy, scalability and interoperability and so encourage the technology's widespread adoption through greater innovation, enhanced governance and sustainable development. On the other hand, ISO/IEC JTC 1/SC 27 is responsible for the development of standards for the protection of information and ICT. This includes generic methods, techniques and guidelines to address both security and privacy aspects. SC 27 engages in active liaison and collaboration with appropriate bodies to ensure the proper development and application of SC 27 standards and technical reports in relevant areas, e.g., 2700x series, 15408, 29100, 29115, crypto standards.

So, the joint WG of ISO/TC 307 and ISO/IEC JTC 1/SC 27 focuses on security, privacy and identity for blockchain and DLT with almost 300 experts coming from either group.

The most relevant publications by the JWG include a technical report on privacy and PII (ISO/TR 23244:2020) "Blockchain and distributed ledger technologies – Privacy and personally identifiable information protection considerations", with an overview of privacy and personally identifiable information protection as applied to blockchain and distributed ledger technologies system. Another recent publication was the Technical Report on "Security management of digital asset custodians" (ISO/TR 23576:2020) about threats, risks, and controls related to digital asset custodian services and management of security, asset information (including the signature key of the digital asset) that a custodian of digital assets manages. This document is addressed to digital asset custodians that manage



signature keys associated with digital asset accounts. In such a case, certain specific recommendations apply.

Due in late 2021 or early 2022, there is a Technical Report on “Overview of existing DLT systems for identity management” (ISO/PRF TR 23249), which will provide an overview of existing DLT systems for identity management, i.e., the mechanisms by which one or more entities can create, receive, modify, use and revoke a set of identity attributes.

Besides, on-going works include Technical Report 23642 “Overview of Smart Contract Security good practice and issues”, Technical Report 23644 “Overview of trust anchors for DLT-based identity management” and Preliminary work item (PWI) 12833 on Re-identification and privacy vulnerabilities and mitigation methods in blockchain and DLT.

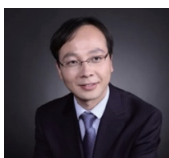
Since mid-November 2021, a new project for an international standard (IS) was launched, i.e., ISO/AWI 7603 on “Decentralized Identity standard for the identification of subjects and objects”. Such a new standard will be for the design and use of decentralised and self-sovereign identification of subjects (legal entities and natural persons) and objects, assets within the design of Blockchain and DLT Systems, in conjunction with verifiable credentials.

Institutional collaboration exists between JWG4 and other groups, such as ISO/IEC JTC 1/SC27 and ITU-T SG17, ISO/TC 68/SC 2. Interest for collaboration also exists with CEN/CLC/JTC 19, and other groups at ETSI and W3C.

Topics of potential interest for JWG4 are also: What are the specific security controls to implement when deploying a blockchain or DLT system? Assessment of security levels? How to preserve privacy of personal information when using a blockchain or DLT system? Mechanisms for privacy? What are the specificities of smart contracts / dApps vs Security, Privacy & ID? Relationships between ID management and blockchain/DLT, SSID/DID concepts. Security assurance processes. In particular, JWG4 is available to produce deliverables in fields where guidelines or requirements are beneficial to industry and other stakeholders.

A question for Bringer points out that W3C is also active in working on standards for decentralised identity and asks if there is collaboration with JWG4. The answer is that there is no mechanism in place for this collaboration, but experts' input is welcome and the JWG4 is open to contributions.

## ITU-T Presentation



*Wei Kai, ITU-T Study Group 16 Q22 Rapporteur Secretary/General of TBI, CAICT*

As presented by Wei Kai, since 2017 ITU-T has created a group on DLT, the ITU-T Focus Group on DLT pre-standardisation. This is followed by ITU-T Study Groups Standardization planned from 2020 onward.



Two technical papers have been published in 2019 by ITU-T: on DLT use cases and on the DLT regulatory framework. In 2020, there are three published recommendations related to DLT: 1. Requirements, 2. Assessment criteria and 3. Reference framework.

The ITU-T work program has a two-layer approach: firstly, Standards for DLT technical aspects, such as interoperability and testing, and, secondly, Standards for DLT enabled e-services. The latter concern applications that include finance, energy, digital media, e-health, public services and others.

The ITU-T DLT meet-ups are scheduled to take place on the first Wednesday of every month. Due to the COVID pandemic and other factors, meet-ups have temporarily been interrupted but they will be resumed as soon as possible.

## CEN CENELEC JTC19



*Andrea Caccia, Chair, CEN/CENELEC Joint Technical Committee on Blockchain and Distributed Ledger Technologies (CEN/CLC/JTC 19)*

CEN-CLC/JTC 19 “Blockchain and Distributed Ledger Technologies”, as presented by its chair Andrea Caccia, was established further to the CEN-CENELEC “Recommendations for Successful Adoption in Europe of Emerging Technical Standards on Distributed Ledger/Blockchain Technologies” (White Paper).

CEN-CLC/JTC 19 focuses on specific standardisation needs to support European legislative and policy requirements in support of the development of the EU Digital Single Market. It gives primacy to international standards setting and develops standards for specific European standardisation needs and/or priorities. Moreover, it identifies and adopts international standards already available or under development, with special attention paid to ISO/TC 307 standards guaranteeing automatic adoption in Europe by all CEN/CENELEC members.

CEN-CLC/JTC 19’s priority relates to Decentralised Identity Management in relation to the proposed revision of the eIDAS Regulation (“eIDAS2”). Other priorities already identified relate to Privacy and alignment with specific European legislation such as GDPR, ePrivacy, KYC, etc. Currently, it is undertaking the adoption procedure for ISO 22739:2020 – Blockchain and distributed ledger technologies – Vocabulary.

In general, the work is expected to be in line with ISO reference architecture and vocabulary. Liaisons exist with ISO/TC 307, ITU-T, CEN-CLC/JTC 13, CEN/TC 224, CEN/TC 445, CEN/TC 468, ETSI/ESI, ETSI ISG PDL.

JTC 19 established WG 1 “Decentralized Identity Management” with the following scope: “Processes, roles and practices for decentralised identity management and its support functions provided by DLTs. This includes management of identifiers, keys, evidential registries and trust anchors.”

WG 1 has prepared a proposal to develop a Technical Specification now under approval: Decentralised Identity Management Model based on Blockchain and



other Distributed Ledgers Technologies. – Part 1: Generic Reference Framework. The objective is to develop a reference architecture for Decentralised Identity Management, aligned with the EU regulatory frameworks that support the Digital Single Market, including the proposed eIDAS2 Regulation, the Single Digital Gateway Regulation and the General Data Protection Regulation. At a later stage the document can become a European Standard or – if there is interest – find its way in ISO/TC 307.

The proposed revision of the eIDAS Regulation (“eIDAS2”) introduces the “European Digital Identity Wallet”, a harmonised identification means for EU natural and legal persons, based on Self Sovereign Identity principles expected to be fully specified and ready for adoption by Q4 2022.

The Rolling Plan for ICT Standardisation published yearly by the European Commission is a bridge between EU policies and standardisation activities in the field of information and communication technologies. Blockchain & DLT, Circular Economy and indeed sections of interest for JTC 19 and other SDOs.

While the new updated version of the Rolling Plan is expected during Q1 2022, the establishment of an ad hoc group is now under approval in JTC 19 to advise on possible activities and actions considering the Rolling Plan with a specific focus to support Circular Economy. The latter is in fact the main priority of the European Green Deal, the new growth strategy of the EU. The recent report by the EU Multi-Stakeholder Platform for ICT Standardisation on “ICT Standardisation supporting Circular Economy” recognized that blockchain technologies are expected to play a major role in support of the circular economy.

## ETSI ISG PDL



*Diego Lopez, ETSI ISG PDL*

According to Mr Lopez, blockchain industrial applicability needs to go beyond the unconstrained environments that built the distributed ledger case, such as manageability, scalability, time and energy efficiency, fairness and legal implications. A permissioned approach is seeking for multi-sector environments, not just Telco but also beyond. First industrial implementations are mostly in one-headed solutions, as many other cloud services, with some advantages, but not real distributed environments.

The ETSI Industry Specification Group (ISG) PDL aims to provide the foundations for the operation of permissioned distributed ledgers. It creates an open ecosystem of industrial solutions deployable by different sectors. It fosters the application of the technology from already available experiences and coordinating with existing initiatives. It defines a set of open operational mechanisms, supports their demonstration and facilitates interoperability assessment. It is now composed of more than thirty members from industry (telco and not telco), public sector and academia.



The scope is on open and well-established operational mechanisms that are capable to validate participant nodes, decide consensus among the participant nodes, publish and execute operations regarding the recorded transactions, facilitate the automation of node management and operation, communicate events relative to node operation, assure ledger data flows for different scenarios, verify the execution of smart contracts and, finally, establish trusted links among different ledgers using these mechanisms.

The focus of the ETS ISG PDL is on data conduits and flows. Essential data processing requirements in terms of trust and security of the data conduits connecting to ledgers need effective conformity assessment, allow an open environment for tracking industrial certified IoT devices, with sensors-to-edge, edge-to-cloud and cloud-to-cloud connectivity. They need to be combined with a certification process to provide trust to the end user while ensuring openness to inter-connect other equipment. On the other hand, distributed and federated data management underpins data collection and data sharing, federated learning, privacy and sovereignty in data pipelines.

Thus, the ETS ISG PDL approach provides architecture, smart contracts and operational modes.

The main deliverables published so far are:

- PDL-001 – Landscape of Standards and Technologies
- PDL-002 – Applicability and Compliance to Data Processing Requirements
- PDL-003 – Application Scenarios
- PDL-004 – Smart Contracts PDL System Architecture and Functional Specification
- PDL-005 – Proof of Concepts Framework
- PDL-008 – Research and Innovation Landscape
- PDL-009 – Federated Data Management
- PDL-010 – Operations in Offline Mode

Ongoing work covers:

- PDL-006 – Inter-Ledger Interoperability
- Key elements for the exchange and use of the information available across DLs
- PDL-007 – Research Landscape
- Facilitate exchange of information on PDL related research projects
- PDL-011 – Specification of Requirements for Smart Contracts' architecture and security
- Normative work for smart contract support in PDL
- PDL-012 – Reference Architecture Framework Specifically based on the scenarios analysed by PDL-003
- PDL-013 – Supporting Distributed Data Management Normative work on data sharing and management

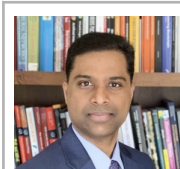


Besides, Proof of Concept (“PoC”) projects are also ongoing. They build awareness and confidence and encourage development of an open ecosystem, by demonstrative deliverables, in addition to informative and normative ones. PoCs are also a key tool for collaboration with research and industrial initiatives.

In conclusion, the ISG PDL intent is to address a gap in the luxuriant landscape of DLT, Blockchain, Cryptocurrency and more. The challenges are to avoid the temptation of reinventing wheels (or levers). The essential concepts are permissioned distributed ledgers, operational aspects focused on minimal requirements and best practices, matching physical assets within the digital world, smart contracts and data processing features as main applications.

The results are intended for any service, thus not limited to telco or network services. Therefore, PDL is intended as-a-service, as a network service and as a network service enabler.

## IEEE Blockchain Standardisation



*Ramesh Ramadoss, Co-chair, IEEE Blockchain Initiative*



*Claudio Lima, IEEE Blockchain Transactive Energy, BCTE, Chair*

Mr Ramadoss firstly introduced the IEEE Standards Association (SA), a global standardisation body composed of more than 34,000 participants from 175 countries and with more than 2,000 standards and projects. IEEE SA’s services include a broad range beyond standards drafting, such as conformity assessment and open-source platform for common projects.

IEEE standards on blockchain are under a common framework, the IEEE Blockchain initiative. The work is organised around horizontal and vertical working groups. The first cover Data, Interoperability, Governance, Identity and Smart Contracts. The second groups are thematic: Energy, IoT, Healthcare, FinTech, Cryptocurrency and Digital Asset.

On horizontal topics, standard 2418.2-2020 – IEEE Standard Data Format for Blockchain Systems has been published, whereas on vertical topics, the most relevant publications are: 2140.1-2020 – IEEE Standard for General Requirements for Cryptocurrency Exchanges; 2140.5-2020 – IEEE Standard for a Custodian Framework of Cryptocurrency; 2143.1-2020 – IEEE Standard for General Process of Cryptocurrency Payment; 2142.1-2021 – IEEE Recommended Practice for E-Invoice Business Using Blockchain Technology; 2144.1-2020 – IEEE Standard for Framework of Blockchain-based Internet of Things (IoT) Data Management.



Mr Lima continued the IEEE contribution focusing on Blockchain in Power & Energy Systems. IEEE P2418.5 provides a Framework and Charter goals.

He notes that IEEE P2418.5 is not just about blockchain, but rather on DLTs more in general. Moreover, it is an energy standard and, as such it covers all power and energy grid definitions by providing interoperability among all the relevant components. Energy blockchain is analysed by segmented in its main use cases, for the energy domains and with DER integration. IEEE P2418.5 also provides Renewable Energy Certificates. The case of EV Charging is considered, as well as DLT Energy Cybersecurity and DLT Energy Smart Contract.

Further, IEEE published a position paper on blockchain transactive energy focusing on the intersection among DLT, Power Energy Systems and Transactive Energy.

A Call for Proposal Submission for the 2022 IEEE Blockchain Transactive Energy Demonstration Project is also available.

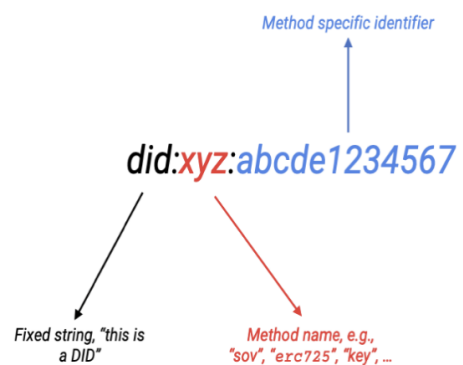
### W3C Activities



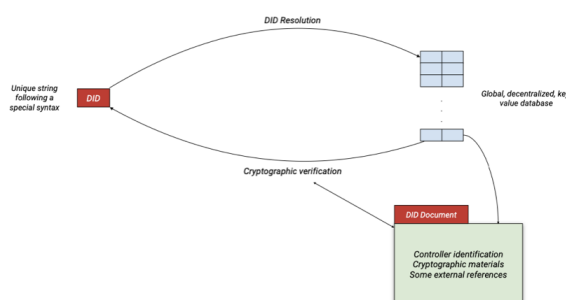
*Ivan Herman, Publishing@W3C Technical Lead*

Mr Herman clarifies that W3C does not currently have groups active on blockchain standardisation or groups that would normatively depend on blockchain technologies. However, he presents two relevant examples where blockchains are an implementation tool.

Firstly, on the importance of identifiers in a digital world, Ivan Herman notes that it is increasingly important to identify persons, concepts or things; that any reasoning, control, associations, etc., of resources rely on this ability; and that the digital economy relies on proper identification to combine information from different sources. So, it is vital that identifiers are unique.



### High level views of DIDs and DID Documents



The different goals of Decentralised Identifiers (DIDs) cover their ease of creation, thus it should be quick, easy, and “cheap” to create possibly thousands of DIDs. Also, they are decentralised, so they do not depend on centralised registries, identity providers, authorities. DIDs are persistent, thus, once created, it

is permanently assigned to the subject. Besides, they are resolvable, i.e., it is possible to find out a basic set of information on the subject. DIDs are cryptographically verifiable, thus, there is a mechanism to cryptographically prove identity and ownership.

However, none of the identifier schemes in use today (email, numerical schemes, web sites, etc.) fulfil all these requirements.

In summary, a DID is a self-sovereign identity, i.e., lifetime, portable, and verifiable digital identity that does not depend on any centralised authority.

DID documents include cryptographic data related to the DID subject, such as RSA, various elliptical curve keys, etc. They can be expressed using JWK or with DID specific terms and can be used for authentication, assertions of credentials, key agreement (e.g., to establish secure communication), capability invocation (e.g., authorization to access an API), capability delegation (e.g., delegate an API access to another authority), etc. DID documents may or may not physically “exist” somewhere in a database, e.g., some methods generate them on-the-fly.

Another important element is “Global, distributed, key-value database”. In fact, there may be several of those. In the DID world, the term method is used for the different approaches and/or implementations. Different methods can have different approaches and characteristics, e.g., may be based on distributed ledgers (generic, like Ethereum, or custom built); DID documents may be stored in a database or on the Web, may be ephemeral DIDs with lighter requirements. The choice depends on the relative importance of the requirements for a specific usage.

DIDs and DID documents are tightly coupled: DIDs have the right features via its DID document; a DID Document is tightly bound to the DID it “describes”; The cryptographic data in the DID Document is a major feature of DIDs.

**DIDs and VCs**

W3C



```

"did:method_a:12345":
  license: 11234562
  hair: BLK
  name: "ALEXANDER JOSEPH"
  address: "2570 24th STREET ..."
  date of birth: 08/31/1977
  issued by: "California DMV"
  issuer ID: "did:method_b:abcdef"
  digital signature: M11B7z0eKq...
  ...
    
```

A DID is also a URI, thus DIDs are within the IETF/W3C world. So, tools, libraries may be used to manage them and existing specifications automatically apply to DIDs: e.g., "[" is valid HTML. Therefore, DIDs are part of the Web.](did:erc725:2F2BC89...1E)

A concrete implementation of DIDs are Verifiable Credentials.

To describe a simple view of a Verifiable Credential, it is a data structure to represent a credential in general and it can be stored on a database, private wallet... or on a distributed ledger.

Ideally, to fit the model of Verifiable Credentials, an identifier should be protected by cryptography and provide information about the holder’s cryptographic keys. Also, it should not depend on a centralised authority to allow for a smooth data portability. So, DIDs are an ideal fit for identifiers in Verifiable Credentials.

## OASIS Activities



*Chaals Nevile, OASIS, Technical Program Director, Enterprise Ethereum Alliance*

Mr Nevile presents OASIS, a global, non-profit, member-driven organisation, built on openness, inclusivity, and innovation, a federation of autonomous communities, member of European Multi-Stakeholder Platform on ICT Standardization.

OASIS's standardisation approach is based on Open Projects, which support shared community development of code, standards, APIs, reference implementations, etc in one place, under open-source licences with a path to recognition in international policy and procurement.

Among the OASIS open projects on blockchain, OriginBX is a global alliance of organisations that are defining digital tax and trade attribute attestations that will enable data to be transmitted across borders via legacy and blockchain platforms.

Another OASIS open project on blockchain is called EEA Community Projects. This is a collaboration between EEA, the Ethereum Foundation, and OASIS. An open community supported to build high quality standards, documentation, and shared test suites that facilitate new features and enhancements to the Ethereum protocol.

Baseline is about Advancing a standard method for universal verified state synchronisation with zero knowledge using the public Ethereum Mainnet. Baseline Protocol is a set of tools and libraries that helps enterprises coordinate complex, multi-party business processes, asset transfers and payments with privacy and without putting any sensitive enterprise information on shared databases or any kind of blockchain. Zero Knowledge circuits employ a common frame of reference that enables all parties in a networked business process to maintain their own systems-of-record in a verified state of consistency.

The Ethereum JSON RPC API, also part of EEA Community Projects, are standardised method calls to Ethereum clients.

## IRTF/IETF Activities



*Thomas Hardjono, CTO of Connection Science and Technical Director of the MIT Trust-Data Consortium*

Mr Hardjono firstly defines the problem IETF intends to solve. This is made of poor or no interoperability of DLT networks today, desirable "interoperability" features, such as digital assets free movement across DLT networks, satisfying atomicity



and consistency properties, satisfying security & integrity properties, foundation for the legal & economic layers.

IETF positions itself in view of its neutrality & openness as a global standards body, with a long history of Internet Architecture development, a history of gateway protocols (e.g., BGP4, IPsec/IKE) a strong expertise in security protocols (e.g., IPsec, IKE, Kerberos, TLS, JWT, JWE, CoAP, RATS, etc.) and a set of existing liaisons (e.g., ITU, W3C, 3GPP, etc.).

The DLT Gateways Model consists of one or more Gateways in each DLT network; it implements Secure Asset Transfer protocol (ODAP). The gateway also hides interior DLT-specific characteristics and is itself owned or operated by legal entities.

The IETF Scope of Work focuses only on the communication between gateways, not on the way each of them works. Thus, the scope is about elements such as gateway API-endpoint definitions, resource identifiers/addresses, payload definition, message flows, secure channel establishment (e.g., TLS1.3) and terminology (extending NIST & ISO).

The current IETF draft technical specifications are the following: DLT gateway architecture, Asset transfer protocol, Gateway crash recovery, Gateway discovery and Data sharing.

Participation is free, voluntary and welcome. The group has been meeting bi-weekly since Sept 2020, operating under IETF IPR Rules (IETF Note Well), on Zoom.

A question to Mr Hardjono is whether it is likely that in the future there will be a network of networks of blockchain, where gateways will be managed and be able to talk to each other to make sure assets can be transferred from one network to another one and what are the risks.

Mr Hardjono answers that it is possible and likely that gateways will be attacked, because they are more vulnerable than the blockchain networks themselves. Thus, there is a growing need for gateways network management and indeed, they could become themselves a blockchain network.





## National & Regional Initiatives

### Australian National Strategy



In his intervention, Mr Benedict provides an update on the Australian blockchain standardisation landscape.

There is significant start-up, fintech and broader DLT commercial activity in the sector. Australia’s largest bank, the Commonwealth Bank of Australia, has announced a plan to allow holding of cryptocurrencies in its market leading mobile banking app (partnering with Gemini). There is significant research sector progression in Australia, with interesting industry/research sector tie-ups. The Australian government conducted and released a key select senate report on cryptocurrency and digital assets – including a recommendation for the recognition and treatment of DAOs by Australian law. This has now been put forward as government policy with a view to implement after the upcoming Australian federal govt election early next year.

The Australian Stock Exchange (ASX) is launching its DLT-as-a-service offering “Synfini”. The Australian government sponsored Digital Finance Co-operative Research Centre is shortly establishing operations and includes participation from the major Australian banks, the ASX and the Reserve Bank of Australia (RBA). The RBA recently released the outcomes of its industry experimentation on a wholesale central bank digital currency – noting the efficiency benefits a Wholesale CBDC provides.

In summary, Mr Benedict believes that a convergence of industry, research, regulatory and government policy interventions is creating a fertile space for DLT activity in Australia.

### Japan



In her intervention, Ms Hiiragi presents the role of JIPDEC. Established as a non-profit organisation in 1967, JIPDEC has been working to advance computer technologies and ensure the security of information systems.

With the progress of the IT industry, JIPDEC continues to tackle various issues and leads in building platforms for safe and secure IT usage. These activities ensure



information security and have led to the development of an infrastructure for personal information protection.

Development and spread of solutions using accurate time and position information from Satellite PNT system have started all around the world. Blockchain is especially expected to be useful in applications that require time series historical data. The information stored in blockchain is extremely difficult to be tampered with, assuming that the information itself is authentic in the first place. Therefore, the methods of sending electronic authentication from navigation satellites to guarantee the authenticity of the information are being developed in many countries. Japan is studying how to utilise accurate time and location information which are verified by electronic authentication sent from navigation satellites in blockchain.

However, while the use of Global Navigation Satellite System (GNSS) such as GPS has become widespread, there are growing concerns about jamming and spoofing technologies that interfere with navigation signals.

As a countermeasure against spoofing, she said that they plan to develop and maintain a "signal authentication system" by 2023 in Japan. It certifies that the navigation messages contained in the navigation signals are genuine by electronic signature technology. In addition to quasi-zenith satellites, it will be able to certify signals of GPS and Galileo.

Various use cases are expected because the "reliability" of the position and time information acquired will be increased. Improved features in navigation and tracking are expected to be exploited in Automobile/Logistics, LBS/Consumer services, Drone, Agriculture, Ship and Infrastructure.

For example, by using blockchain and signal authentication, it is possible to prove that the products (e.g., pharmaceuticals) are shipped from the authentic factory and whether or not there is deterioration in quality (e.g., inappropriate temperature) during the processes of storages and transportations more reliably.

The use of blockchain also comes with challenges. When considering applications, there are several issues such as cooperation with an external system and confirmation of the authenticity of newly written information. For example, it may be necessary to have a mechanism to manage authentication keys on the blockchain. In addition, considering the global use of PNT information, standardisation works might be necessary. Also, a security perspective might be considered.

## Korea



*Kyeong Hee Oh, Representative of TCA Services, Co-Rapporteur of Q14 Security aspects for DLT in SG-17 at ISO South Korea*

Ms Kyeong Hee Oh firstly introduces the policy background for blockchain in South Korea. From 2016, to 2018. Blocking technology has remained at the peak of



hype in the Gartner hype cycle. So, in 2018, the Korean government announced its blockchain development strategy. In 2019, according to the Gartner hype cycle, blockchain was at the bottom of disillusionment, but the strict social distancing goes by, the covid-19, pandemic has accelerated, the digitalisation and non-contact trends in the entire economy and society in Korea. So, there is a strong need to build trust between economic players who cannot meet face-to-face. So as blockchain technology is once again in the spotlight and many countries are having the advantage in competition. So, the Korean government said its blockchain becomes its leading strategy: thus, many pilot projects have been carried out based on it. So, in this year new projects for selected areas will launch.

The Ministry of Science announced the blockchain technology development strategy. A strategic framework has been formed to gain initial momentum implementing technology development. The creation of the blockchain market, the development of blocking technology and industrialization support was set as tasks to support the strategy. The presidential committee on the fourth Industrial Revolution submitted five policy recommendations to the government to answer the questions of the future uncertainty. Like how will we grow or how will it create jobs through growth? Blockchain is a recognised key technology that supports innovations. So, in 2020 blockchain technology was chosen to realise the hyper-connected and contactless trusted society.

The five strategies are like this: first focusing on seven application areas. Second promoting the ID Services, third establishing the integrated supporting system for companies for developing key next-generation technologies and vivid reading, the Innovation ecosystem. So, the first major areas are online, voting donation, social welfare, renewable energy, financial services, real estate trade and postal services. These are vertical applications. Besides, ID service is horizontal.

From 2018 the Korean government has promoted many pilot projects based on the policy. The object of pilot projects is to spread the blockchain Technologies, to Innovative public and public and private services. From 2013 to 2020, 34 pilots were developed in the nation. Net budget of 29,2 billion Korean Won.

This year 2021, 19 pilot projects on the development, including the digital vaccinations.

The first item in the 2020 strategy is to select areas with significant potential for blockchain technology and provide intensive support. Areas include social welfare, customer management, renewable energy and donations.

There are two projects that the Korean government is focusing on. The first one, is the government of your card, by the ministry of interior in safety. And second one is the vaccination certificate by the Korean Center of Disease, Control and prevention. Another project is to provide the central government officers with the digital form of an ID card on their smartphones.

## India



*Ashish Tiwari, Scientist-D, "Electronics and IT" standardization Department (LITD) of BIS. Committee Manager Support of ISO/IEC/JTC1/SC7 Software and Systems Engineering subcommittee.*

Ashish Tiwari represented BIS, the National Standards Body of India (by an Act of Parliament). Established in 1947, it has more than 300 Committees that have formulated more than 20,000 Indian Standards. Members of the committees include Industry and its associations, Government, Technologists and Laboratories, Academia, Users/Consumer Organization. Other activities of BIS are Conformity Assessment and Testing.

Since 2016 with a panel on Blockchain at BIS, the national activities have evolved till the publication of the National Strategy on Blockchain in January 2021.

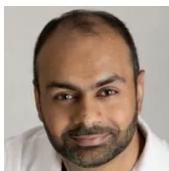
India's standardisation group for blockchain and distributed ledger technologies is LITD 29. It formulates National Standards in the field of Blockchain and distributed ledger technologies and it is the National Mirror Committee for ISO/TC 307.

So far, LITD 29 published one national standard and is working on two more. At the same time the group has contributed to ISO/TC 307, in the Study Group on NFR on Blockchain and in the development Guidelines for Auditing Blockchain/DLT based Systems. It also contributed with five Use Cases from India part of ISO/TR 3242 Use Cases.

As part of the national blockchain framework, several projects or pilots are ongoing. The main technological challenges are about performance and scalability, skillset and awareness, security, privacy and regulation, standardisation and interoperability, ecosystem and supporting framework. There are also legal challenges in the adoption in India.

The Indian strategy and way forward revolve around regulatory and policy considerations, the IndiaChain initiative, India as blockchain hub, procurement process for government agencies to adopt blockchain solutions, and last, but not least, developing and implementing standards.

## UAE



*Waqar Chaudry, Senior Manager, Markets Financial Services Regulatory Authority (FSRA)*

As presented by Waqar Chaudry, UAE has a federal strategy to capitalise on blockchain technology to transform 50 % of government transactions into blockchain based infrastructure. The pillars of the strategy are government efficiency, industry creation and international leadership.



Dubai stands to invest 5.5 billion dirham annually to support document processing via blockchain.

The standardisation efforts of UAE converge into ISO/TC 307.

The main cornerstones and next step of the UAE's blockchain strategy started in 2018 with ADGM FSRA Virtual Asset Business Rules and Guidance issued. Currently in 2021 several VA businesses have gone live. Also, INATBA and ADGM signed an MOU. In 2022 a comprehensive national level review of standards will be completed. Later in 2023 work with various authorities in the UAE to harmonise the blockchain standards approach. So that in 2024, the government intends to make available to organisations a self-certification platform for smart contracts and plan to enable integration using ADGM digital lab. After 2024 authorities will therefore actively encourage local and international standards setting bodies to collaborate with the ADGM through INATBA.

## Canada



*Paul Jackson, Senior Director, Innovation, Science and Economic Development Canada*

The Canadian experience presented by Paul Jackson starts from the considerations on the importance of trust in the digital economy. Many transactions in the economy and society rely upon trust, where each transacting party needs assurance that the other is who they claim to be and that the information they provide is true. Governments and other organisations are trust anchors, enabling trust by issuing documents needed for transactions across the economy and society, such as individual and organisation identities (e.g., birth certificate, article of federal incorporation), licences and permits (e.g., driver's licence, natural gas export licence, electrician licence) and educational qualifications (e.g., college diploma, accounting certificate).

Challenges are in making these documents easy to use in digital transactions across the economy and society, while preventing fraud, preserving privacy and avoiding costly and time-consuming processes.

This is where digital credentials can help. A digital credential is a portable digital record about a business or individual that can be held and shared by them through a digital wallet. It covers digital representation of traditionally physical certificates or information such as personal identification, licences and permits, certificate of incorporation, university degree, etc.

Therefore, a digital credential is a tamper-evident credential that relies upon cryptography to detect fraud and verify the authenticity and the issuer. Digital Credentials can enable quicker, easier and more trusted transactions across the digital economy and society, such as obtaining services, trading across borders and proving claims about a product.



Innovation, Science and Economic Development Canada's interest in digital credentials and blockchain is currently focused on three areas. Firstly, modernising regulatory approaches, supporting the Government's efforts on targeted regulatory reviews to support economic growth and innovation. Secondly, enabling individuals and businesses to participate in and benefit from the digital economy, including supporting trade and commerce in Canada, in accordance with Canada's Digital Charter. And finally, supporting delivery of government services to business by making it quicker and easier for businesses to obtain such services, while ensuring integrity and trust.

There is a recognition in Canada that the future of digital credentials will be driven by a diverse ecosystem of public and private sector digital services within countries and across borders. For instance, it is expected that digital credentials will be held in various digital wallets, with individuals using the certified wallet of their choice. Moreover, those digital credentials will be issued and verified by various public and private sector issuing and verifying services, with sectors and jurisdictions using the services of their choice. And, also, those services will rely upon various public and private sector blockchains and other approaches to issue and verify digital credentials.

There are three key areas that should be considered when implementing digital credentials within your jurisdiction:

1. Digital credential issuing and verifying capabilities
2. Mutual support and interoperability for digital credentials and supporting technologies across the economy
3. Concrete digital credential use cases that enable individuals and businesses to engage in digital transactions (e.g., open a bank account)

Canada is undertaking several initiatives to address these key areas. Firstly, Canada is pilot testing a centralised service for issuing and verifying digital credentials, that would make it easy for individuals and businesses to participate in the digital economy. Secondly, Canada is working to enable mutual support and interoperability for digital credentials and supporting technologies across the economy by establishing national standards and certification bodies, in alignment with international standards and requirements. Moreover, Canada is developing and implementing recommendations for addressing mutual support and interoperability with international partners (e.g., European Commission, INATBA Governmental Advisory Body, Agile Nations). Finally, Canada is undertaking concrete digital credential use cases that enable individuals and businesses to engage in digital transactions (e.g., open a bank account). Canada is working with partners to identify and implement high impact use cases (e.g., business banking with the provinces and banks, cross-border recognition of academic credentials with the European Commission).

Through these initiatives, the following challenges and lessons have been learned:

1. Interoperability is key. We cannot assume digital wallets and digital credentials are interoperable.
2. Standards are still evolving and have gaps. There is a need to work together to address those gaps.



3. Existing business processes may need to be revisited to get all the possible benefits from digital credentials.
4. Help partners and stakeholders to better understand the digital credentials approach up front, to ensure buy-in and avoid bigger delays later on.
5. User experience needs to be improved for digital wallets and the issuing/verifying of digital credentials.

To help address some of these challenges, Canada and the EU organised a Joint Workshop Series to discuss how to enable mutual support and interoperability across jurisdictions. The resulting report, jointly published by Canada and the EU, included the following recommendations

1. Cooperate on the development of digital credential standards and certifications
2. Increase focus on joint proofs of concept and pilots for end-to-end digital credential use cases
3. Establish mutual recognition for digital credentials and digital trust services through formal agreement(s)
4. Build adoption, awareness and support through concrete digital credential demonstrations
5. Create shared repositories for digital credential technologies
6. Foster continued engagement on digital credentials

As next steps, Canada intends to continue the work to implement the recommendations from the Canada-EU Joint Workshop Series. In particular, it will expand work on mutual support and interoperability through the INATBA Governmental Advisory Body and Agile Nations. It will also continue to work on (1) digital credential issuing and verifying capabilities, on (2) mutual support and interoperability for digital credentials and supporting technologies across the economy and on (3) concrete digital credential use cases that enable individuals and businesses to engage in digital transactions.

## Brazil



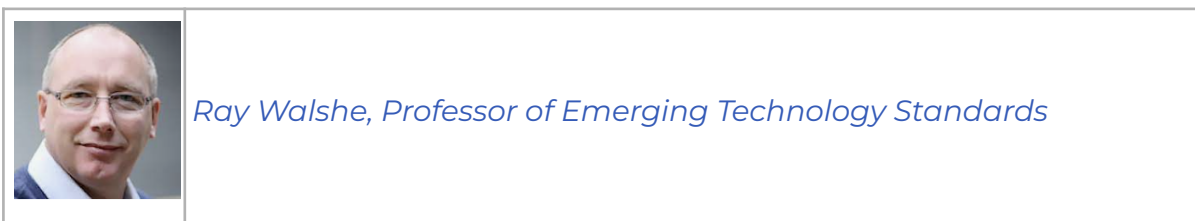
*Suzana Maranhao Moreno, Digital innovation Analyst at BNDES, Associate Rapporteur at ITU/UN, Blockchain Software Engineer, Brazil*

Suzana Maranhao Moreno highlighted Brazil's two approaches for blockchain development: (1) a generic-first with digital infrastructure and decentralisation first and (2) a domain-focused, value-first and more decentralisation later.

The first approach is based on the Brazilian Blockchain Network ("RBB"), made by several levels of Brazil's public entities such as the executive federal level, the state levels, the academic sector, the legislative level, etc.

The second approach is instead demonstrated by the National Health Data Network, a domain focused application with 7.2 million transactions/day. Interoperability for health event timeline blockchain with federated clinic documents based on standards (FHIR) for E-patient. Another example is Digital Payments and Digital Real. Instant payment powered by the Central Bank allowed 40M people to do their first digital money transfer in 2020. Digital Real is about fostering new business models together with open finance: it offers a smart payment system to the digital economy (for example based on Smart contracts, DvP, PVP, IoT etc).

## EUOS/STAND-ICT



Ray Walshe introduces StandICT, a European Commission’s H2020 funded project awarded four million euros, out of which three million euros has been given back to the community of standards experts.

StandICT.eu 2023 counts among its achievements 5 out of 10 open calls for experts already launched. The 5<sup>th</sup> is currently open. Experts who submitted functional grants applications were evaluated and,

so far, 58 received a contract. 8 Webinars were organised on topical subjects such as AI, Cybersecurity, EU ICT Policies, Trusted Information and Education in Standardisation. 12 Memorandum of Understanding signed with relevant players Synergies with 45 Stakeholders. StandICT so far released a promotional video to launch EUOS – European Observatory for ICT Standardisation, 9 Newsletters and 15 Press Releases.

Further to its release, the EUOS Release (March '21) published an AI Landscape Report (June '21) and 2 Technical WGs Reports. Further, 9 Technical WGs on key ICT domains work on dedicated landscapes & gap analysis. 3 new TWGs have been established to cover Ontology, Robotics and Edge & IoT.

The StandICT community now includes 1331 registered users, 2557 LinkedIn followers and 706 Twitter followers. There is also an Active Expert Advisory Group (EAG) with 20 members from SDOs, European Commission & Industry.

As a result of the StandICT.eu received financial grant 57 applicants stated to have contributed to the development/draft of brand-new Standards and 44 are currently working (or contributed) to setting-up new TCs, WGs, sub-committees





or Focus Groups in renowned SDOs. “Following the Fellows Impact Reports”, highlights a variety of evidence-based outcomes gained through the project’s second open call. The report puts the fellows themselves, all of whom are rightly experts within their own respective fields of ICT standardisation – under the spotlight and offers them the opportunity to speak about their work and the added-value they are contributing to standards efforts as awardees from their own perspectives.

The analysis of the first 4 open calls indicate a consistent number of proposals coming from applicants coming from SMEs and/or IT fields as well as from Academia/Research. Cybersecurity, 5G, AI, and Blockchain proved to be yet the most popular topics. A wide range of different topics tackled: e-Health; Semantics; Smart Grids; Smart Cities and more.

EUOS showcases a Repository of Standards & Discussion Groups leveraging an interactive map with 1287 standards to date.

The “Landscape of Artificial Intelligence Standards”, published in June 2021, was the fruit of the dedicated Technical Working Group (TWG AI). The Report provides an encompassing compilation of standardisation efforts underway in the framework of European SDOs, such as CEN and ETSI, Government, Public Bodies and Agencies, Global SDOs, and initiatives. Two new reports are expected to be published soon: TWG Smart Cities Report in December 2021 and TWG Trusted Information Report, Early 2022. Upcoming reports are due on Digital twin, ontologies and blockchain. Upcoming events feature the launch of the EUOS Smart Cities Report at a special session at the UCLG Africa FAMI Convention 2021 on the 8th of December 2021.

A stand-alone initiative is the EUOS Standards Academy, whose key-objectives are the creation of education modules for students (particularly on non-technical aspects & benefits of Standardisation), to set-up a repository of teaching material for newcomers in Standardisation, and to showcase the strategic importance of Standardisation for business and Europe’s competitiveness. Group members are Brian McAuliffe (Chair) – Director of Technology Standards at HP & EUOS TWG Academy, Ray Walshe – University Lecturer at Dublin City University & StandICT.eu EAG Chair, Carol Cosgrove-Sacks – Senior Advisor on International Standards Policy at OASIS OPEN, Henk de Vries – Endowed Professor of Standardisation Management at RSCM, Paul Killeen – Standards Development, Research & Innovation at NSAI, David Filip – NSAI delegate and Expert of ISO/IEC JTC 1/SC 42, Sebastiano Toffaletti – Secretary General of the European DIGITAL SME Alliance, Chiara Giovannini – Senior Manager Policy & Innovation, Cyrill Dirscherl – European Commission Standardization Policy Coordinator, (AAstaRT Network), Ivana Mijatović – Full Professor Department of Quality Management and Standardization, Martin Chapman – Senior Director, Standards Strategy and Policy EMEA (ORACLE), Maria Ines Robles (IETF & Tampere University).

Educational content browsable by category include three default Starter Packs for beginners to intermediate users and advanced users following specific competence requirements for standards professional’s matrix. The academy is a helpful hub to better explore key factors of the standardisation ecosystem, the functioning of the standards process, and its economic and societal benefits.

StandICT has also joined forces with OntoCommons, an H2020 CSA project dedicated to the standardisation of data documentation across all domains related to materials and manufacturing. Both OntoCommons and StandICT.eu hope to provide support to the Data Economy chapter of the ICT Rolling Plan 2022. A new TWG was established on Ontologies with Ontocommons reps from ETSI SAREF, ISO, IIRDS, OMG and the Digital Twin Consortium.

In response to the challenge to reinforce the participation of women experts in the Fellowship Programme, 17% of the funded experts are female among all experts funded until the 3rd Open Call. StandICT actively raises the awareness of the Programme among women engaged in ICT standardisation. The team has been scouting and contacting over 20 EU structures promoting women in standards, in ICT and scientific research. It also established collaboration with ETSI and CEN-CENELEC, ITU-T to reach out to the active female experts. A dedicated webinar #WomenInICTStandards will be organised during Q1 2022.

The “Walk & Talk” StandICT.eu 2023 webinar series features its most recent virtual event on the 27th of October hosted by Joel Myers, Chair of the IEEE IoT Initiative on Smart Cities, with panellists from across Europe and Africa, including Eddy Hartog of the European Commission and Deniz Susar of the United Nations. The event was promoted in advance and live on Twitter and the recording is now available to watch via the StandICT.eu website.

Currently, promotion for the 5th StandICT.eu 2023 Open Call continues across all communication channels, driving traffic to the call’s dedicated website page. Deadline to submit applications: 29th November 2021. Upcoming virtual events organised by StandICT.eu 2023 include Digital Twins: Evolving Global Standards and Walk&Talk: #WomenInICTStandards – to be held via Zoom in December 2021 and January 2022 respectively.

## GBBC



*Sandra Ro, CEO at Global Blockchain Business Council*

Representing the Global Blockchain Business Council, Sandra Ro presents the Global Standards Mapping Initiative (GSMI) as the most comprehensive effort to map and analyse the blockchain and digital asset landscape across key areas, namely legislation and regulatory guidance, technical standards, industry standards and recommendations, university courses and, last but not least, industry consortia.

Nine GSMI Working Groups cover Taxonomy, Digital and Crypto Asset Regulation, Policy, Digital ID, Technical, Green Economy, Global Taxation, Derivatives, and South Korea. They produced a mapping update of 187 Jurisdictions for Crypto and Digital Asset Regulations, with updates on 38 Technical Standards, and a taxonomy with over 180 defined and categorised terms. GSMI includes 12 fellows from seven academic Institutions that joined for an 8-month fellowship to



contribute to GSMI research. Additionally, the Blockchain Education Network (BEN) contributed to GSMI by assisting with the mapping of accredited universities offering blockchain courses.

The global team of GSMI includes over 200 contributors representing 131 organisations worldwide.

The GBBC stated aim is to build the next multi trillion-dollar industry, and advance adoption of blockchain to create more secure, equitable, and functional societies through education, advocacy, and partnership.

## AIOTI



*Tom De Block, Solution architect – Data ecosystems – IT Quality & Governance, SWIFT, National Bank of Belgium, SCHENGEN SIS*

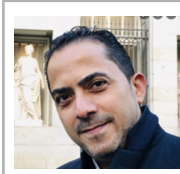
Mr De Block explains that AIOTI serves its members not developing standards but rather mapping them and creating testbed methodologies to demonstrate what the different blockchain platforms are, actually, used and not used for.

His experience comes from the AIOTI WG on Distributed Ledger Technologies, active on matchmaking, convergence and testbeds, but also from the EU Observatory for Standardisation (EUOS) with its TWG “Data interoperability” of the StandICT.eu initiative and Market Operating System (OS).

Published on 7 December 2021, the TESTBEDS Catalogue & Methodology displays 13 out of 42 testbeds being DLT enabled. It includes testbeds dedicated to protocol benchmarking for performance & energy efficiency, where demonstrators provide transparency on the technical stack. Testbed methodology is based on ISTQB, EU Living Labs initiative, IEEE Future Networks Testbeds WG, EU Fed4Fire initiative, Industrial Internet Consortium (IIC).

However, DLT and Blockchain have no standard Testing methodology yet. Therefore, AIOTI published its DLT testbeds: DLT 2.xx PROTOCOL PERFORMANCE and DLT 3.xx ENERGY EFFICIENCY. The technologies considered are Hyperledger, Ethereum, IOTA, Ripple and Cardano with hardware On-Premise, Low-power devices and Edge & Cloud. The outcome DLT 2.xx is a comparison between the different DLT protocols, whereas, DLT 2.xx is about XBRL reporting.

## LACChain



*Albi Rodriguez Jaramillo, LACChain, The Innovation Lab of Inter-American Development Bank (IDB-LAB)*

Mr Rodriguez Jaramillo presents the experience of LACChain, part of IDB-LAB, the Innovation Lab of the Inter-American Development Bank (IDB).

The IDB Lab launched the Global Alliance for development of the blockchain ecosystem in Latin American and Caribbean two years ago with a value proposition to provide an infrastructure technology with the capability to solve DLT problems. For governments, this infrastructure is an approach in the form of a public permission network. So, this is firstly a partnership of public and private stakeholders that provides a technological infrastructure for generating data analytics and impacts with a marketplace of applications.

LACChain has currently more than 650 entities with interest and 80 entities running more than 130 nodes. There are currently 60 projects on top of the network and 37 projects with impact on inclusion. The program is developing an ecosystem in 10 countries.

The program is fully aligned with standards, especially ITU and ISO. Since 2019 we have worked in ITU with all our partners. The technological proposal follows the ISO/TC 307 approach being public like EBSI.

The offer is multi-level: first public-permissioned networks, then, self-sovereign identity according to W3C standards and, third, the ambition is to provide tokenized fiat money. Network statistics show more than 35 million blocks, 130 nodes deployed by 80 entities. The latter have different profiles: governments, enterprises, start-ups, chambers, banks. The most relevant recent publication was on self-sovereign identity, covering not only self-sovereignty but also digital wallets and blockchains.

In order to address the multinational level of the initiative that is active in at least 15 countries and consider the different legislations, legal working groups (LWG) were established in six of the 9 countries. The legal fields that the LWG are considering are privacy, antitrust and consumer protection.

## EBP/EBSI



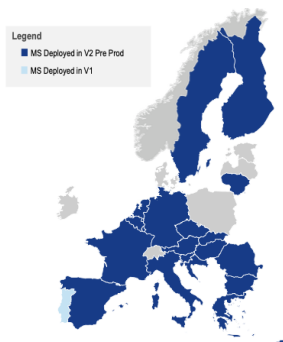
*Pierre Marro, Policy Officer at the Directorate General Communication Networks, Content and Technology (DG CONNECT) of the European Commission*



*Robert Czarny, EBSI Technical Office*

### A solid node network

A solid network of 41 nodes across Europe



**From 38 to 41 nodes in 22 countries**  
of which 33 on V2

#### Nodes per country:

- Austria (1)
- Belgium (1)(1)
- Bulgaria (2)
- Croatia (1)
- Cyprus (1)
- Czechia (2)
- Finland (1)(1)
- France (1)(1)
- Germany (2)(2)
- Greece (2)
- Hungary (3)
- Italy (2)(1)
- Lithuania (1)
- Luxembourg (1)
- Netherlands (2)
- Norway (1)
- Portugal (1)
- Romania (3)
- Slovakia (1)
- Slovenia (1)
- Spain (3)
- Sweden (1)
- EC Nodes

*(Blue are nodes on V1)*

Pierre Marro provides an overview of the EU policy initiatives. These are based on a joint political declaration on the establishment of the European Blockchain (EPB) Partnership and the development of the European Blockchain Service Infrastructure (EBSI) for cross border digital services of public interest connecting global and European expertise.

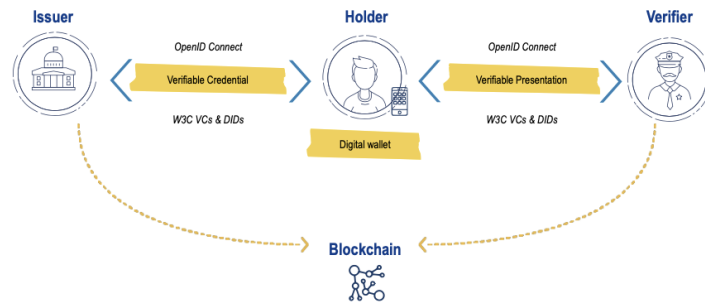
Observatory and Forum brings together the leading global experts to identify obstacles, incentives and practical solutions to promote blockchain uptake. The policy landscape includes INATBA as a public private partnership, which is supported by the European Commission. Further, the EU is investing on research, innovation and deployment, as well as supporting startups and skills development through Digital Europe and Horizon Europe programs. The EC is co-investing through specific support programs for AI and blockchain.

The European Commission is also promoting an enabling legal framework and standardisation.

The European Blockchain Partnership includes 27 EU Member States, plus Norway and LICH cooperating with the EC. The EU ambition is building a Pan-European Blockchain Services Infrastructure (EBSI) supporting cross border public services (at first) as well as private applications and using blockchain for more trustworthy services. A Cross-border Public Services Infrastructure would serve the public sector as a trailblazer, by avoiding fragmentation with many national initiatives. It aims to be a secure, interoperable, GDPR compliant, sustainable infrastructure, also strengthening EU leadership in blockchain.



The first use cases of EBSI are document traceability, exchange of accredited diplomas, the EU self-sovereign identity framework, trusted data sharing, as well as SME financing, EU social security pass and asylum demand management.



EBSI is composed of a node network so far in 22 countries.

According to its plan, EBSI will achieve v2 capabilities deployed to the pre-production environment in 2021. Early Adopters on EBSI will also be in v2 pre-production.

In 2022, EBSI production will begin, also with new capabilities to be deployed to the production environment.

Focusing on EBSI Verifiable Credentials use cases, three components benefit from the Web3 evolution: Verifiable Credentials, i.e., a new way of expressing information; Blockchain, as a new decentralised infrastructure: and, Digital Wallet as a new way to interact for/with citizens.






Some resources are already available. The EBSI's Verifiable Credentials lifecycle for early adopters allows navigating EBSI's Verifiable Credentials profile. The playbook contains all the EBSI specifications. An EBSI Wallet Conformance Testing is also available for early adopters to verify the conformance with EBSI specifications and standards.

About standardisation, EBSI has been already inspired by ISO 307 works on reference models using W3C works on Verifiable Credentials. Further interest includes enhancing privacy, exchange of data and services between different blockchain networks and ensuring interoperability for services. The EC aims to reinforce the cooperation between EBSI and standardisation activities. A new call will be published in early 2022 through the Digital Europe Programme.





## Panel discussion on possible gaps/overlaps, encouraging collaboration, best practices, recommendations

### Panellists

	<i>Pietro Marchionni, European Blockchain Service Infrastructure Agenzia per l'Italia Digitale</i>
	<i>Ramesh Ramadoss, Co-chair, IEEE Blockchain Initiative</i>
	<i>Roman Beck, Head of European Blockchain Center</i>
	<i>Suzana Maranhao Moreno, Digital innovation Analyst at BNDES, Associate Rapporteur at ITU/UN, Blockchain Software Engineer, Brazil</i>
	<i>Waqar Chaudry, Senior Manager, Markets Financial Services Regulatory Authority (FSRA)</i>

### Moderators

	<i>Monique Bachner, Co-Chair of the INATBA Interoperability Working Group and the Standards Committee</i>
	<i>Ismael Arribas, Co-Chair of the INATBA Interoperability Working Group and the Standards Committee</i>



**Monique Bachner kicks off the discussion by asking the panellists how to balance the slowness of standardisation with the pace of innovation.**

Ramesh Ramadoss elaborates that this is a common issue that happens with all new technologies. For instance, now it is happening with the metaverse, before it has been happening with many other technologies. Bringing stakeholders together takes time, often even more than two years are necessary to develop a standard. IEEE is nevertheless open to new topics and many innovative companies are interested to standardise, but indeed speed is an issue.

Roman Beck adds that in blockchain there are a lot of dynamics, but safety and guidance are also important. Standardisation allows for compliance. The market, thus in particular companies, startups, investors and users need stability. So, standards are important. They should not start too late because they should accompany the development of the industry and propel innovation.

**The following question relates to the issues associated with crypto currencies. Did such issues hinder the development of regulation and standards for blockchain?**

Waqar Chaudry replies that the issue of financial services regulators is to decide what the different financial instruments are, whether a commodity, a currency, a payment token, a NFT, etc. Regulators are looking at several angles, such as security and stability. We have decided to deem crypto currencies as commodities. That creates a clear framework. That approach is getting momentum among regulators from North America and Europe, although it creates challenges from a technical point of view. Innovation is not ending, and standards struggle to stay on top of fast technological development.

**Monique Bachner points out that, as noted in the event chat, there is a gap between legislation and technology, and this is a never-ending issue. She continues by asking if the blockchain standardisation community is inclusive enough?**

Suzana Maranhao Moreno says that in her experience participating at ITU there was no restriction to participation in the different groups and that helped to be more inclusive. Knowledgeable people are scarce, so you should not create barriers to enter such groups. I find my opinion being listened to in an inclusive manner.

Roman Beck adds that over 400 different experts participated in the development of a governance standard at ISO. Participants came from many countries including African, South American and Asian. Blockchain standardisation and movement is not dominated by bigtech or by powerful countries. It is more diverse and distributed, so more inclusive.

Albi Rodriguez Jaramillo intervenes by bringing LACChain experience. He explains that countries in his region have different maturity levels. Some National Standards Bodies are still amateur and can only follow. Others are very advanced. We must consider the different levels. Privacy, antitrust or consumer protection are serious issues with different gaps. It is challenging to be inclusive. UNE from Spain is providing good support to other countries in our region.





**Ismael Arribas concludes that emerging markets will benefit a lot from DLT and therefore they need to participate in setting standards. Regarding the permission-less community, what are the solutions to distress public services with private sector innovative solutions? So, how to harmonise this gap also with education and training?**

Suzana Maranhao Moreno noticed that many startups have good and mature solutions. However, the legal framework does not recognise that these new approaches are possible for a public service. The legal entitlement to support the tech solutions is therefore important.

**What are the solutions to address the differences among the national administrations. How do you tackle blockchain regulation?**

Pietro Marchionni elaborates on the lack of knowledge among public administrations. EBSI is certainly going to help. But we still have a problem of vision: what network will EBSI be and what it will be for? Many MSs reps in EBSI are struggling to understand how the vision could be achieved. There is often a culture in public administrations that is not open to innovation. Even cloud computing is difficult to accept. So, the problem is culture.

Roman Beck says that in Denmark, the experts group mirroring ISO is also the advisor to the government on EBSI. This helps. Dansk Standard and the Ministry of Economics are working very closely. This is crucial to create a decentralised mindset.

**The following question by Monique Bachner concerns the green energy transition: are blockchain standards enough considering eco-design and green aspects?**

Waqar Chaudry highlights that, as noted in a recent report by the Global Digital Finance group, sustainability of blockchain depends on energy mix sources. You cannot compare countries that have different dependence on fossil fuels. So, regulators should consider this, and you cannot have the same approach for all countries.

**Ismael Arribas asks the panellists to intervene on a last round by picking any question they had not received so far.**

Ramesh Ramadoss takes the chance to note that, on the question of innovation versus regulation, every emerging technology, like blockchain, there is a risk to regulate too soon. Otherwise, you risk killing it. On the other hand, at the other extreme, not regulating at all is not a good solution either. The startups need clear rules. So, a good balanced approach is needed, and this kind of event is useful in educating regulators.

Pietro Marchionni asks why we should decentralise. Many organisations, both governments and private companies, are losing grip on users or customers. But they don't see the benefit for them to give back control to users. The issue hidden behind many talks is this.



**Monique Bachner concludes that the event was a good way to put together standards organisations in a collaborative effort and move ahead together addressing the different legal barriers and technical issues.**

**Rapolas Lakavičius** thanks all participants and speakers for their contributions. A report is being prepared by **Sebastiano Toffaletti**.

He also shows the results of the online survey that was carried out during the event. Ten votes highlighted interoperability, convergence and governance as main areas.



## Event Takeaways

As a conclusion of the event, one of the main take-aways is broad consensus on the need to ensure interoperability, as to enable a stronger take up of the technology. Blockchain is an open ecosystem, where industry, public administrations and all stakeholders benefit from having the interoperable framework that is provided by standards.





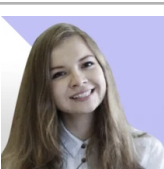
Also, in order for the market to progress, safety and stability are much needed. Thus, the economic operators benefit from tools that enable compliance. Therefore, the availability of international standards is considered important for a mature and coherent use of blockchain technologies.

While coordination and harmonisation at global level are essential drivers for standardisation, the use cases of blockchain are very heterogeneous and legal requirements may vary in the different geographies. Thus, there is still a need to ensure localisation of conformity in the different regions.

Another important element for the success of blockchain standardisation is inclusivity. While the technology is rather democratic with low entry barriers, thus allowing many companies and stakeholders to contribute to it, standardisation seems to follow the same approach by attracting participants and inspiring different initiatives in a wide range of countries. Yet, knowledge about complex novel technologies and about the connected legal requirements is still a scarce resource. So, incentives and public support for the participation of relevant experts and under-represented stakeholders might be needed.

With a more mature development of the market in sight, governance remains an important element. In the struggle between the anarchy of a very dynamic ecosystem and the top-down attempts to regulate, the market driven and voluntary nature of standards makes them a good tool of mediation. Thus many participants agree that governance is a key priority for standardisation initiatives.


## The Organising Team at INATBA

	<b>Marc Taverner</b> , INATBA Executive Director
	<b>Monique Bachner</b> , Co-Chair of the INATBA Interoperability Working Group and the Standards Committee
	<b>Ismael Arribas</b> , Co-Chair of the INATBA Interoperability Working Group and the Standards Committee
	<b>Morgane Stein</b> , INATBA Membership Recruitment & Business Development
	<b>Anna Ivanova</b> , INATBA Marketing and Events Assistant

## The Conference Rapporteur

	<b>Sebastiano Toffaletti</b>
---	------------------------------

## European Commission

	<i>Rapolas Lakavičius, Policy Officer, Digital Innovation &amp; Blockchain, DG CONNECT</i>
---	--



Contact details:

**Website**

[inatba.org](https://inatba.org)

**Contact**

[contact@inatba.org](mailto:contact@inatba.org)

**Join INATBA**

[membership@inatba.org](mailto:membership@inatba.org)