ITU – NBTC Training
On

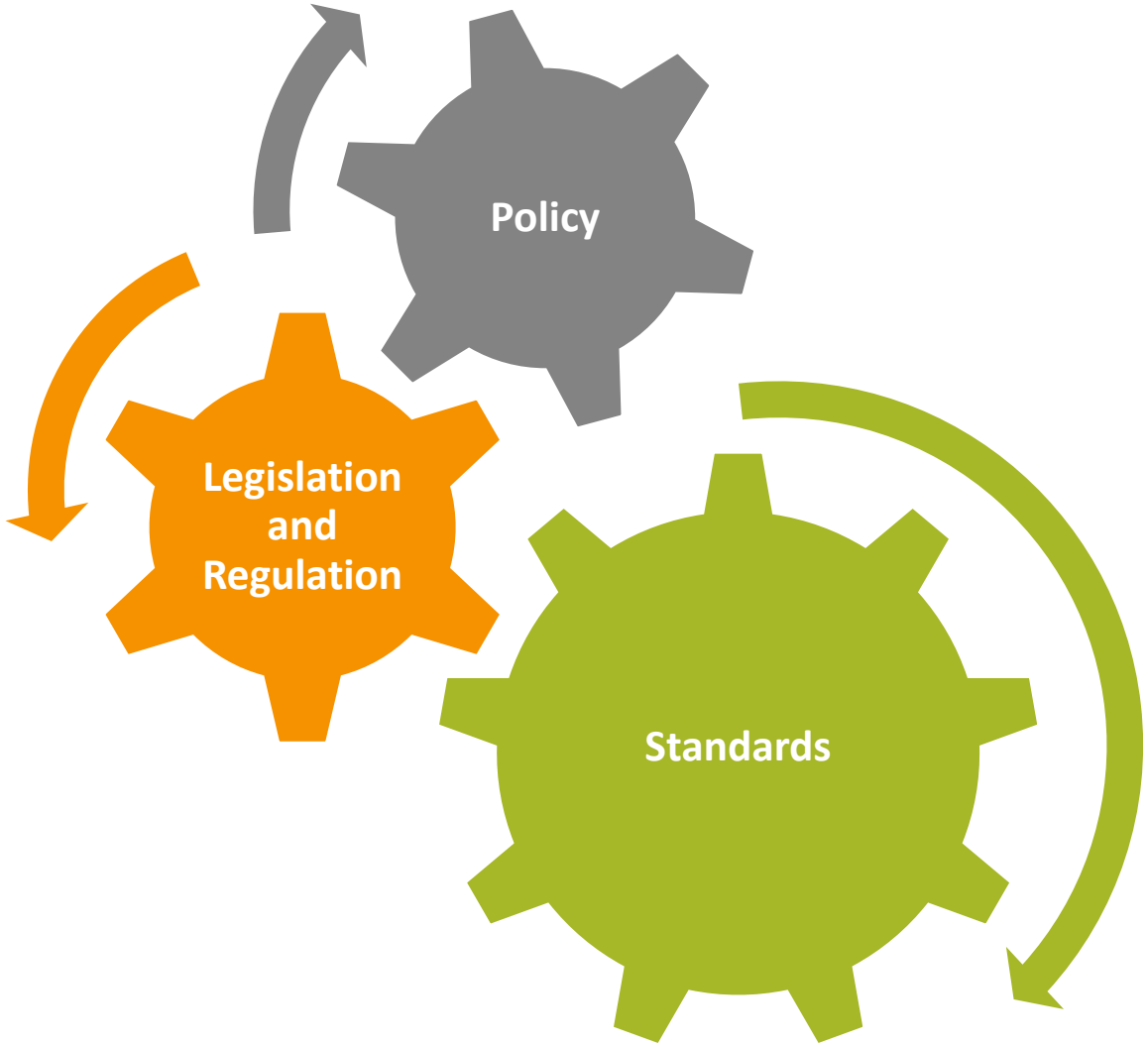
“Building Distributed Ledger Technologies (Blockchain) Projects”

Regulation and Standards

5 – 8 November 2019,
Bangkok, Thailand

Ashish Narayan and Martin Adolph

Linkages between policy, strategy legislation and standards



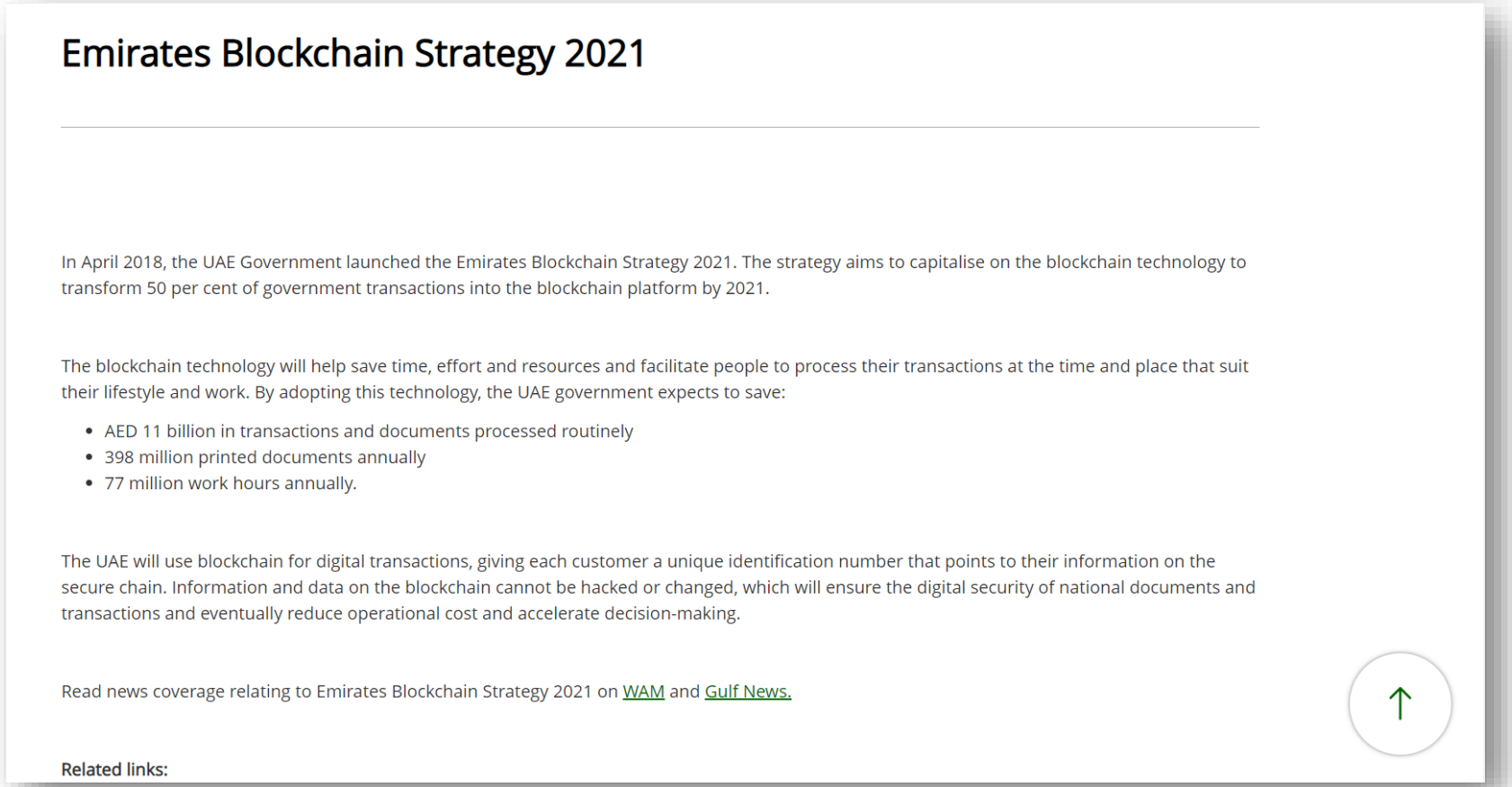
Licenses, Registrations, Regulations, Notifications, Guidelines, Agreements, Industry practices

G20: Finance Ministers and Central Bank Governor's meeting – Communique, June 8-9, 2019

"Technological innovations, including those underlying crypto-assets, can deliver significant benefits to the financial system and the broader economy. While crypto-assets do not pose a threat to global financial stability at this point, we remain vigilant to risks, including those related to consumer and investor protection, anti-money laundering (AML) and countering the financing of terrorism (CFT). We reaffirm our commitment to applying the recently amended FATF Standards to virtual assets and related providers for AML and CFT. We look forward to the adoption of the FATF Interpretive Note and Guidance by the FATF at its plenary later this month. We welcome IOSCO's work on crypto-asset trading platforms related to consumer and investor protection and market integrity. We welcome the FSB's directory of crypto-asset regulators, and its report on work underway, regulatory approaches and potential gaps relating to crypto-assets. We ask the FSB and standard setting bodies to monitor risks and consider work on additional multilateral responses as needed. We also welcome the FSB report on decentralized financial technologies, and the possible implications for financial stability, regulation and governance, and how regulators can enhance the dialogue with a wider group of stakeholders. We also continue to step up efforts to enhance cyber resilience, and welcome progress on the FSB's initiative to identify effective practices for response to and recovery from cyber incidents."

Source: https://www.g20fukuoka2019.mof.go.jp/en/outline/pdf/20190610.pdf

Blockchain Strategy: Example UAE



Emirates Blockchain Strategy 2021

In April 2018, the UAE Government launched the Emirates Blockchain Strategy 2021. The strategy aims to capitalise on the blockchain technology to transform 50 per cent of government transactions into the blockchain platform by 2021.

The blockchain technology will help save time, effort and resources and facilitate people to process their transactions at the time and place that suit their lifestyle and work. By adopting this technology, the UAE government expects to save:

- AED 11 billion in transactions and documents processed routinely
- 398 million printed documents annually
- 77 million work hours annually.

The UAE will use blockchain for digital transactions, giving each customer a unique identification number that points to their information on the secure chain. Information and data on the blockchain cannot be hacked or changed, which will ensure the digital security of national documents and transactions and eventually reduce operational cost and accelerate decision-making.

Read news coverage relating to Emirates Blockchain Strategy 2021 on WAM and Gulf News.

Related links:

Source: https://government.ae/en/about-the-uae/strategies-initiatives-and-awards/federal-governments-strategies-and-plans/emirates-blockchain-strategy-2021

Blockchain Strategy: Example Germany

"Using this strategy, we are pursuing a regulatory policy that creates incentives to make investments, releases forces of innovation, secures stability and thus contributes to inclusive growth that is compatible with the Federal Government's sustainability goals."

Advancing innovations
Giving an impetus to investments
Guaranteeing stability
Strengthening sustainability
Making fair competition possible
Deepening the digital single market
Expanding international collaboration
Integrating the stakeholders
Guaranteeing IT security and data protection
Making provision for adaptations

Source: https://www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/blockchain-strategy.html

Blockchain Strategy: Example Germany

"By the end of 2021, the Federal Government will launch measures in the following five areas of action, to use blockchain technology's opportunities and to mobilise its potential. These are the priority measures in the respective activity areas:

1. Securing stability and stimulating innovations: blockchain in the finance sector

- *The Federal Government aims to open up German law for electronic securities.*
- *The Federal Government will publish a draft legislation to regulate the public offering of certain crypto-tokens.*

2. Bringing innovations to maturity: advancing projects and regulatory sandboxes

- *The Federal Government is piloting a blockchain-based link-up of energy facilities to a public database.*
- *The Federal Government is funding the testing-out of blockchain-based verification of higher education certificates.*
- *The Federal Government will introduce sustainability-oriented requirements as an important decision making criterion in implementing state-funded or state-initiated blockchain projects .*

3. Making investments possible: clear, reliable framework conditions

- *The Federal Government will conduct a round-table discussion on blockchain and data protection issues.*

4. Applying technology: digitised public-administration services

- *The Federal Government is piloting blockchain-based digital identities and evaluating other suitable applications."*

Source: https://www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/blockchain-strategy.html

Regulatory landscape varies: Example cryptocurrency

Government-issued notices about the pitfalls of investing in the cryptocurrency markets. Such warnings, mostly issued by central banks, are largely designed to educate the citizenry about the difference between actual currencies, which are issued and guaranteed by the state, and cryptocurrencies, which are not

Many of the warnings issued by various countries also note the opportunities that cryptocurrencies create for illegal activities, such as money laundering and terrorism. Some of the countries surveyed go beyond simply warning the public and have expanded their laws on money laundering, counterterrorism, and organized crimes to include cryptocurrency markets, and require banks and other financial institutions that facilitate such markets to conduct all the due diligence requirements imposed under such laws.

Some jurisdictions have gone even further and imposed restrictions on investments in cryptocurrencies, the extent of which varies from one jurisdiction to another.

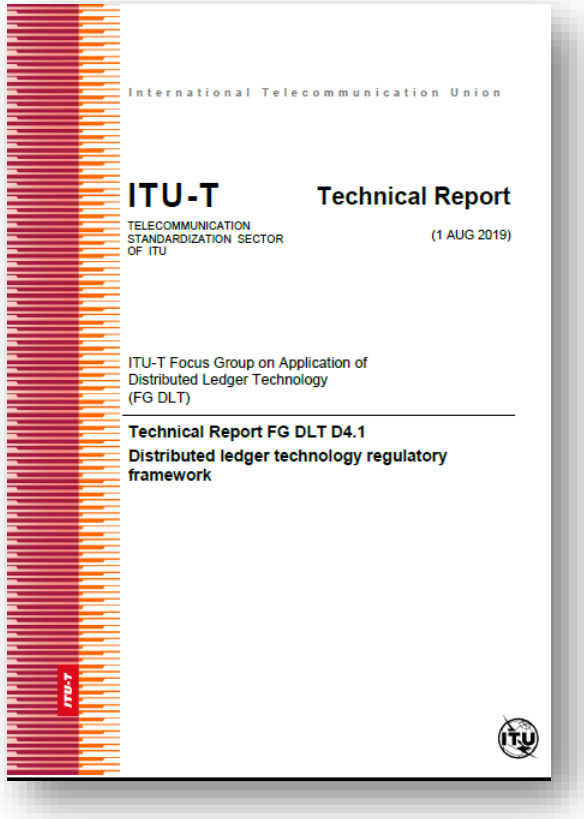
Regulate initial coin offerings (ICOs), which use cryptocurrencies as a mechanism to raise funds

Not recognizing cryptocurrencies as legal tender, see a potential in the technology behind it and are developing a cryptocurrency-friendly regulatory regime as a means to attract investment in technology companies that excel in this sector

Some jurisdictions are seeking to go even further and develop their own system of cryptocurrencies

Source: Report on **Regulation of Cryptocurrency Around the World,** https://www.loc.gov/law/help/cryptocurrency/world-survey.php#compsum

ITU-T Focus Group on DLT – Regulatory Framework



Deliverables

1. DLT terms and definitions
2. DLT overview, concepts, ecosystem
3. DLT standardization landscape
4. DLT use cases
5. DLT reference architecture
6. Assessment criteria for DLT platforms
7. DLT regulatory framework
8. Outlook on DLTs

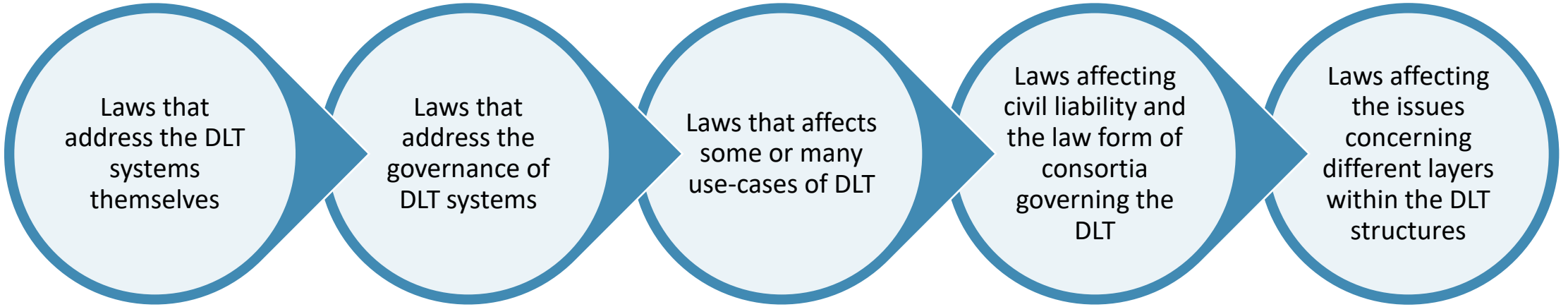
Detailed reports are at https://www.itu.int/en/ITU-T/focusgroups/dlt/Pages/default.aspx

DLT properties and regulatory issues

Feature	Examples of regulatory challenges
Distribution, shared ledger (no central repository) [b-Yaga]	1) Applicable law with respect to nodes established in different states; 2) Legal subjects in multiple jurisdictions; 3) Distributed storage solutions to meet the requirements of production environments; 4) Interoperability requirements; 5) New civil or commercial-law forms, organizations and contracting; 6) Protection of secrecy in open environments.
Autonomy and responsibility	1) Legal smart contract definition and enforceability (valid source code execution); 2) Boundaries of anonymity; 3) Applicable law; 4) Liability of smart contract managers (SC layer governance); 5) Intellectual property of code.
Tamper evidence and resistance	Regulation that requires the correction or removal of data in the ledger, for example: 1) data protection laws / right to be forgotten; 2) content that infringes on third parties' rights (e.g. copyright, trademark etc.); 3) illegal content.
Incentive mechanism and digital assets [b-FINRA, b-Yaga]	1) Coin, token, tokenization legal common (UNCITRAL) definition; 2) ICO definition and minimal requirements for investor protection; 3) Crypto asset/token financial system: legal concept and boundaries; 4) Supervisory policies and procedures in accordance with applicable rules [b-FINRA].
Openness and transparency/ anonymity	1) AML issues, secrecy leaks, personal security [b-FINRA]; 2) Anonymization (no name/encrypted users vs KYC) and pseudonymization [b-EU-a].

Source: ITU-T Focus Group on Application of Distributed Ledger Technology: **Technical Report FG DLT D4.1 Distributed ledger technology regulatory framework**

DLT properties and regulatory issues



e.g. Intellectual property (IP) (patent, copyright) of software code, communications laws and laws that regulate the mining for a DLT system

e.g. recognition of DLT governance, conflict of laws, liability and enforcement of decisions on a DLT system

e.g. crypto regulation and token-economy laws, anti-money-laundering and privacy laws, consumer law protection regimes, and anti-fraud laws as well as laws allowing law enforcement to carry out certain measures or use certain tools in a digital environment

essential for the optimal governance of permissioned systems

e.g. EU eIDAS Regulation and similar currently enforceable laws on electronic signatures worldwide; laws on software IP; laws on DLT-components technical specifications

Source: ITU-T Focus Group on Application of Distributed Ledger Technology: **Technical Report FG DLT D4.1 Distributed ledger technology regulatory framework**

Challenges

- Civil and criminal liability in the blockchain network control, and other sources of responsibility from a public-law perspective (e.g. administrative compliance taxation and even constitutional-law related issues)
- The control management supervision of the network participants s (human or not), including developers administrators, consortia/community managers and legal persons involved within.
- Authoritative sources of records and data;
- DLT-record legal proof;
- Personal data protection compatible with existing regulations.

Source: ITU-T Focus Group on Application of Distributed Ledger Technology: **Technical Report FG DLT D4.1 Distributed ledger technology regulatory framework**

Distribution and ledger sharing

- Applicability of existing law with respect to nodes established in different states;
- Legal responsible subjects in multiple jurisdictions, competition and failure-handling issues are relevant within a DLT governance context.
- Distributed storage solutions to accomplish legal requirements of production environments;
- Legal accomplishment of interoperability requirements. The heterogeneity of DLT devices, operating systems, programming languages, node managers and networks pose a huge challenge within different legal areas;
- New digital civil or commercial-law forms such as multilateral consortia agreements, organizations such as DAOs and decentralized e-contracting including financial system contracts for banking, stock markets and insurance purposes;

Source: ITU-T Focus Group on Application of Distributed Ledger Technology: **Technical Report FG DLT D4.1 Distributed ledger technology regulatory framework**

Distribution and ledger sharing

Protection of secrecy in open environments in accordance with existing data protection regimes in force in different jurisdictions.

Cross-border transfer and data localization: collecting data, retaining data, analyzing data, deleting data and sharing data.

Legal challenge associated with DLT addresses the identification of responsibility in distributed systems. Present legal systems often assume hierarchical control of systems in order to attribute responsibility accordingly.

Multi-jurisdiction and arbitration: Conflicts to be resolved automatically, or autonomously, while maintaining the persistence of the framework and deciding which conflicts are destined for off-chain resolution or off-ledger resolution.

Market Competition: Antitrust and anti-competition law

Source: ITU-T Focus Group on Application of Distributed Ledger Technology: **Technical Report FG DLT D4.1 Distributed ledger technology regulatory framework**

Distribution and ledger sharing

- Protection of secrecy in open environments in accordance with existing data protection regimes in force in different jurisdictions.
- Cross-border transfer and data localization: collecting data, retaining data, analyzing data, deleting data and sharing data.
- Legal challenge associated with DLT addresses the identification of responsibility in distributed systems. Present legal systems often assume hierarchical control of systems in order to attribute responsibility accordingly.
- Multi-jurisdiction and arbitration: Conflicts to be resolved automatically, or autonomously, while maintaining the persistence of the framework and deciding which conflicts are destined for off-chain resolution or off-ledger resolution.
- Market Competition: Antitrust and anti-competition law

Source: ITU-T Focus Group on Application of Distributed Ledger Technology: **Technical Report FG DLT D4.1 Distributed ledger technology regulatory framework**

ITU-T FG DLT recommendations - Distribution and ledger sharing

"We recommend to efficiently combine the aforementioned approaches within the scope of future international working group legal prospection with regard to significant findings by specialized doctrine and jurisprudence and in accordance with governmental national or regional forthcoming sectorial approaches, in particular within these fields:

Civil and criminal liability for blockchain distributed control;
Decentralized controllers/managers (human or not);
Authoritative sources of records and data;
DLT-record and other related digital sources of legal proof."

Source: ITU-T Focus Group on Application of Distributed Ledger Technology: **Technical Report FG DLT D4.1 Distributed ledger technology regulatory framework**

Autonomy and responsibility

Regulatory issues

- **Legal smart contract definition and enforceability, and valid source code execution**
- **Automatic decision-making**
- **Limitations of legal liability for actors who play the key role in information system operation**

Approaches and / or recommendations

Optimal third-party protection requires policies setting on-chain dispute resolution tools on a case-by-case basis prior to an off-chain solution. Associative initiatives within the scope of International Consumer Protection and similar regimes are recommended to complement the aforementioned policies.

Companies using SCs have to comply with the existing regulation. Consumers might be able to benefit from an increased level of trust that does not depend on the trust in the company

Source: ITU-T Focus Group on Application of Distributed Ledger Technology: **Technical Report FG DLT D4.1 Distributed ledger technology regulatory framework**

Autonomy and responsibility

Approaches and / or recommendations (continued)

DLT & corruption

"… Blockchain/DLT is promising in the context of inherently distributed business and governance activities where traditional means are not working.
Anti-corruption and pro-transparency measures should be considered early at the design stage taking into account the intended application of the solution. At present, however, the focus of governmental actors is mostly on privacy (including transaction privacy) protection, which is quite beneficial for corruption-supporting applications of blockchain.
The lack of a designated owner or responsible person in permissionless blockchains combined with trans-jurisdictional operations hinders public oversight and law enforcement.
Properly designed SCs may ensure fair access to goods or services with no interaction with potential criminals. But, they could also be used for collecting bribes. Then, authorized SC removal and vetting systems are needed in public permissioned chains."

Source: ITU-T Focus Group on Application of Distributed Ledger Technology: **Technical Report FG DLT D4.1 Distributed ledger technology regulatory framework**

Tamper evidence and resistance

GDPR – Data protection : Challenges

The GDPR requires a justification for processing of personal data and provides the data subjects with the right to be forgotten (Art. 17), the right to rectification (Art. 16) and the right to restrict processing (Art. 18)

The GDPR requires controllers and processors to have a processing agreement. Controllers are limited to select processors that are providing sufficient guarantees to comply with the GDPR (Art. 28).

The GDPR limits the transfer to third countries. Having nodes in third countries might transfer personal data to those third countries. However, publication is not considered a transfer to a third country, even when the data can be freely accessed from a third country [b-EU-c]. What does this mean for a blockchain with nodes in third countries? Does this privilege a public blockchain over a non-public blockchain?

Source: ITU-T Focus Group on Application of Distributed Ledger Technology: **Technical Report FG DLT D4.1 Distributed ledger technology regulatory framework**

Tamper evidence and resistance

GDPR – Personal Data

The GDPR does not apply to DLT when no personal data is processed. However, the definition of personal data goes far beyond what is considered Personally Identifying Information (PII). In other jurisdictions like the U.S., data that could be attributed to a natural person by the use of additional available information is already considered personal data.

A common way forward is to store the main data outside of a blockchain or on a sidechain and use the blockchain for verification, ordering and time-stamping. This is done by hashing the personal data. However, hashes of personal data may represent personal data themselves.

Typical pseudonymization scenarios, where only names or other identifiers are replaced by hashes (or even random numbers), are usually still considered personal data [b-Art. 29 WP]. When there is a certain context or some metadata stored with the hash on a blockchain, this can also be used to derive personal data. People who have knowledge of the hashed information will be able to connect the metadata with the data they have. Therefore, no metadata should be stored along with the hash that is not included in the information hashed [b-Erbguth-b].

Source: ITU-T Focus Group on Application of Distributed Ledger Technology: **Technical Report FG DLT D4.1 Distributed ledger technology regulatory framework**

Tamper evidence and resistance

GDPR – Personal Data

Zero-knowledge proofs (ZKPs) can be used to make sure that only non-personal data can be derived from an entry on a blockchain.

Encryption can be used to make it impossible to derive any personal data from a blockchain after the key has been deleted. However, storing encrypted personal data on a blockchain is like securing access to data by a non-changeable password which should be avoided [b-Grassi].

Although data protection authorities agree that these techniques substantially reduce the risks for data subjects, the French CNIL still regards them as being personal data with the exception of certain zero-knowledge proofs [b-CNIL]. The Austrian Datenschutzbehörde [b-Austria], however, while considering a case not related to blockchain, held that an effective protection against identifying a person can render the data anonymous, and that this is equivalent to deletion.

Source: ITU-T Focus Group on Application of Distributed Ledger Technology: **Technical Report FG DLT D4.1 Distributed ledger technology regulatory framework**

GDPR – Personal Data

Tamper evidence and resistance

Zero-knowledge proofs (ZKPs) can be used to make sure that only non-personal data can be derived from an entry on a blockchain.

Encryption can be used to make it impossible to derive any personal data from a blockchain after the key has been deleted. However, storing encrypted personal data on a blockchain is like securing access to data by a non-changeable password which should be avoided [b-Grassi].

Although data protection authorities agree that these techniques substantially reduce the risks for data subjects, the French CNIL still regards them as being personal data with the exception of certain zero-knowledge proofs [b-CNIL]. The Austrian Datenschutzbehörde [b-Austria], however, while considering a case not related to blockchain, held that an effective protection against identifying a person can render the data anonymous, and that this is equivalent to deletion.

The GDPR puts obligations on parties in control of data processing. The French CNIL holds that users signing a transaction with their private key for a public blockchain are in control. When users are effectively in control and companies solely provide tools for writing on a public blockchain, the companies might not be responsible for data processing [b-Erbguth-a].

When information on a ledger infringes on personal or commercial rights or violates criminal laws, there may be laws that require the removal of personal and non-personal data from a ledger.

Source: ITU-T Focus Group on Application of Distributed Ledger Technology: **Technical Report FG DLT D4.1 Distributed ledger technology regulatory framework**

Tamper evidence and resistance : Approaches and/or recommendations

Technical recommendations regarding standardization

There are two specific areas of standardization needed to support interoperability and growth in DLT applications that use PKI. One area is the development of an X.509 certificate profile for DLT, a profile that specifies required cryptographic algorithms, choice alternatives for strings and time types and useful certificate extensions. A second area is the development of DLT-specific path validation processing that recognizes the proper role of expired certificates in long-lived signed and timestamped ledgers, and that result in tool behaviors that do not obstruct ledger processing.

A framework standardization approach (for use of symmetric cryptography in DLT systems)

Source: ITU-T Focus Group on Application of Distributed Ledger Technology: **Technical Report FG DLT D4.1 Distributed ledger technology regulatory framework**

Tamper evidence and resistance: Approaches and/or recommendations

Organizational and design recommendations

- *Avoid storing clear-text personal data on a blockchain, unless you have a justification for permanence;*
- *Use sidechains or other private storage options for sensitive data;*
- *Use Zero-knowledge proofs where possible. However, ZKPs are still under development, some demonstrate slow performance. Standards for ZKPs are being developed [b-ZKP];*
- *When storing hashes of personal data:*
  - *Make sure there is enough entropy in the data hashed;*
  - *Avoid combining hashed data with other data on the blockchain;*
  - *Avoid using hash-values as identifiers;*
  - *Add secret passwords to the hashed data as an additional security measure, when this seems suitable for the application. As a sole measure, this is not sufficient, since passwords that cannot be changed do not offer advanced-level security.*
- *Avoid solely relying on consent in the context of personal data and blockchains;*
- *Perform a data protection impact analysis (DPIA) and a risk analysis.*

Source: ITU-T Focus Group on Application of Distributed Ledger Technology: **Technical Report FG DLT D4.1 Distributed ledger technology regulatory framework**

Incentive mechanism and digital assets

For the financing of blockchain projects, in addition to the conventional equity financing methods, currently, there are ICOs for utility tokens and STOs for asset and security tokens. Different countries have different policies for token-based financing methods:

- A complete ban;
- Regulation as done with securities (viewing digital objects as digital assets);
- Specialized simplified regulation;
- No regulation for pure utility tokens.

The regulators should efficiently combine different self-organizing, public-administrative and private national and international law approaches to regulate:

- The basic blockchain, including consensus processing;
- The smart contract validity, effects and definitions for legal purposes within the context of contract laws in different jurisdictions;
- The optimal regimes to regulate the action of intermediaries such as the exchanges used for the fulfilment of transactions;
- The private-law asset or security market and related public-law regimes connected to the tokens including ICOs and similar regimes.

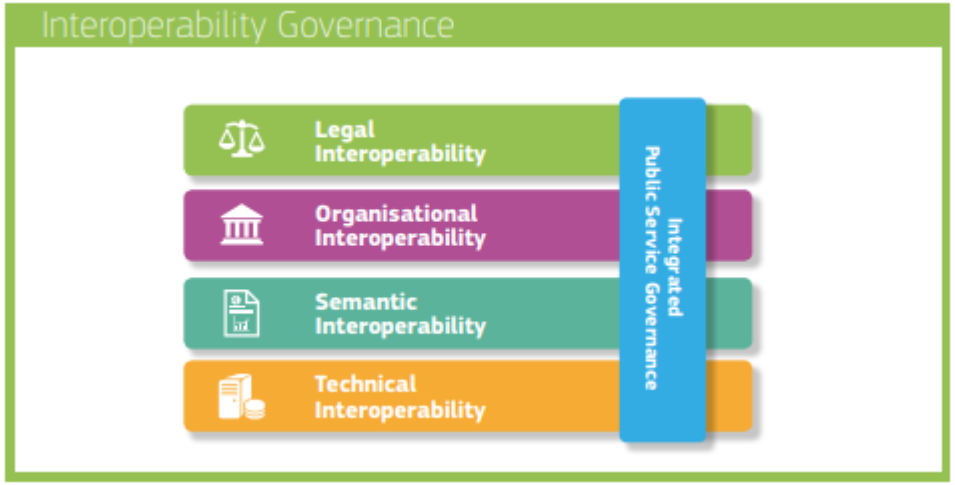
Source: ITU-T Focus Group on Application of Distributed Ledger Technology: **Technical Report FG DLT D4.1 Distributed ledger technology regulatory framework**

Incentive mechanism and digital assets: recommendations

Interoperability

Interoperability can happen at different levels.

For instance, the European Interoperability Framework (EIF) [b-EIF], a commonly agreed approach to the delivery of European public services in an interoperable manner, defines a model with four layers of interoperability: legal, organizational, semantic and technical; a cross-cutting component of the four layers, 'integrated public service governance' and a background layer, 'interoperability governance'.



Implementations of DLT now comprise a new representation of value known as tokens or digital currency. There is a uniform approach to cross-chain interoperability described in clause 7.2 of Recommendation ITU-T X.1255 [b-ITU-T X.1255].

Source: ITU-T Focus Group on Application of Distributed Ledger Technology: **Technical Report FG DLT D4.1 Distributed ledger technology regulatory framework**

Openness, transparency and anonymity

Distributed ledger platforms generally work on an alleged “paradox”, in which, while the information on the ledger is transparent for everyone to see or read, it is also private, thus ensuring the anonymity of the players involved in a given transaction.

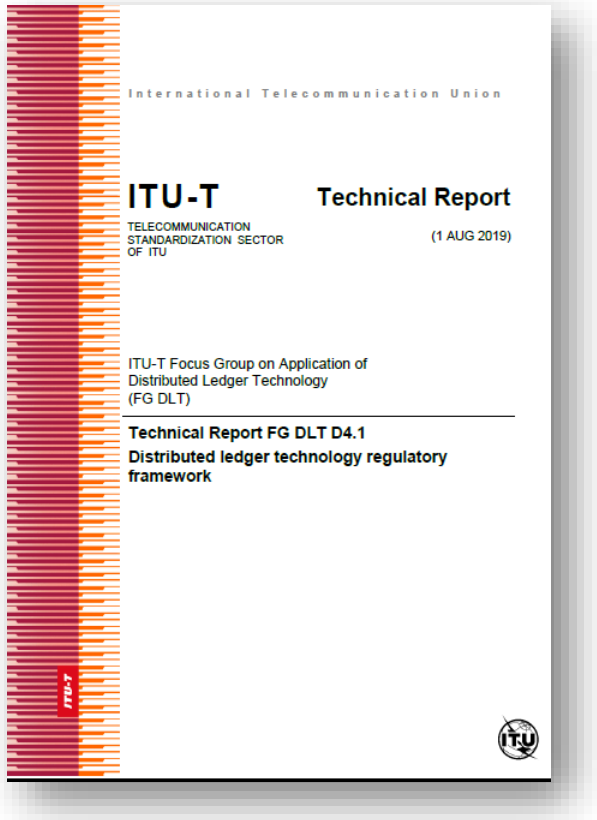
Approaches and / or recommendations

Despite the general agreement on the positive impact that openness and transparency often offer, as seen before, they might also pose some challenges for certain sectors. In this sense, it is recommended that each DLT protocol and governance adjust its level of openness and transparency in accordance with two major factors:

- *Regulation: Currently, many countries are reorganizing or developing their legislations to create codes to govern issues such as privacy, data management and other areas related to the internet but also new applications like cryptocurrencies. DLT platforms take into account such regulations to be able to comply with their directives;*
- *Sector: Each sector has its particularities. The financial sector has different demands and requirements as compared to the education or the health sectors. An efficient solution requires an appropriate DLT platform and a well-designed application.*

Source: ITU-T Focus Group on Application of Distributed Ledger Technology: **Technical Report FG DLT D4.1 Distributed ledger technology regulatory framework**

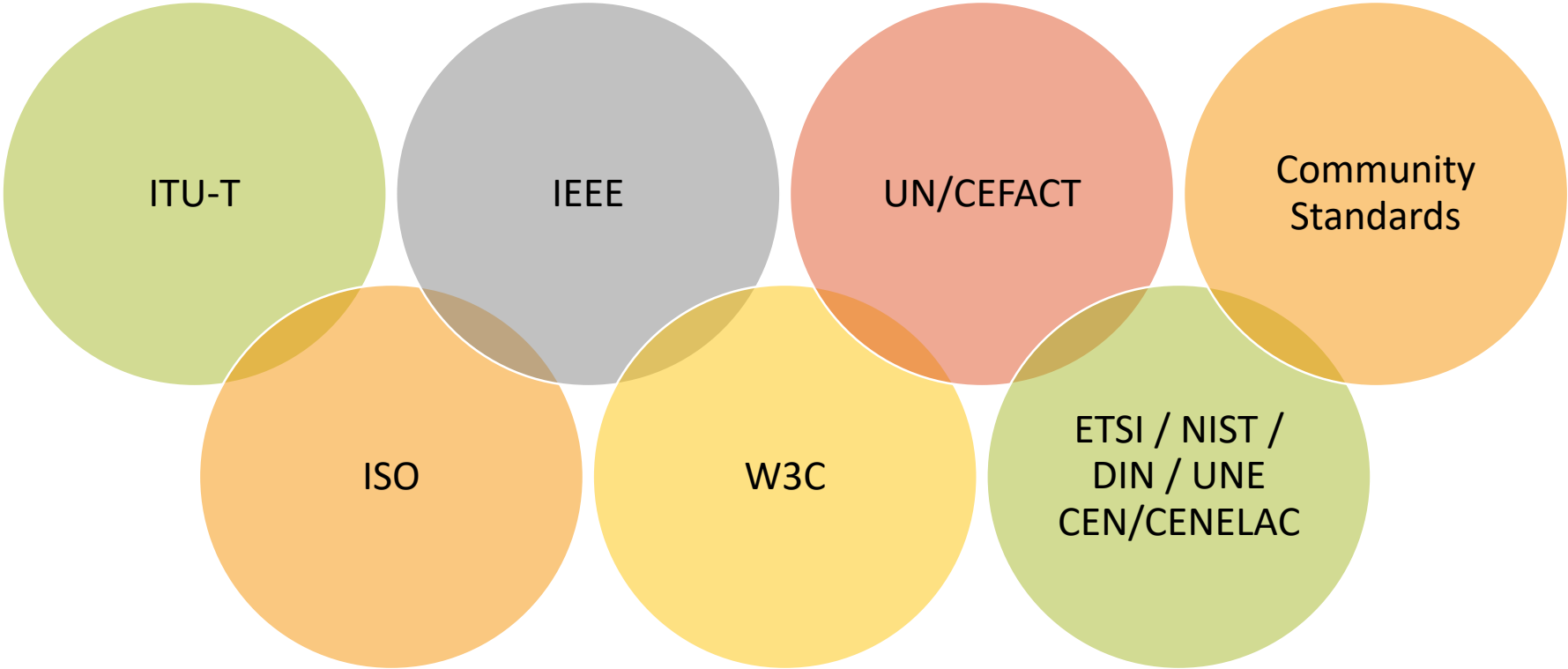
ITU-T Focus Group on DLT - Standardization



Deliverables

1. DLT terms and definitions
2. DLT overview, concepts, ecosystem
3. DLT standardization landscape
4. DLT use cases
5. DLT reference architecture
6. Assessment criteria for DLT platforms
7. DLT regulatory framework
8. Outlook on DLTs

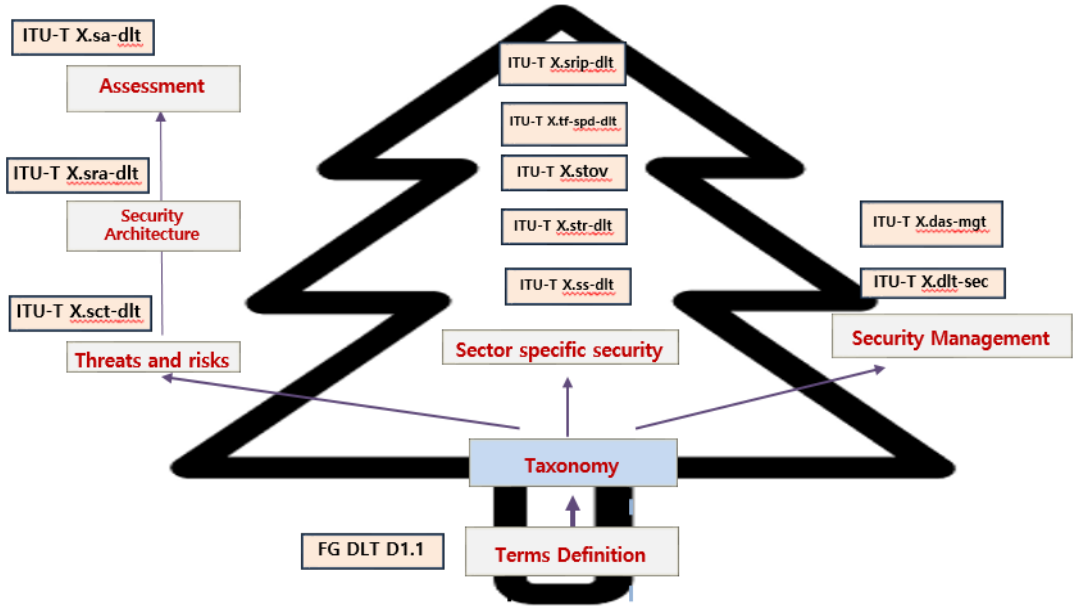
Detailed reports are at https://www.itu.int/en/ITU-T/focusgroups/dlt/Pages/default.aspx



For details, please see **Technical Report FG DLT D1.3 Distributed ledger technology standardization landscape**

Source: ITU-T Focus Group on Application of Distributed Ledger Technology: **Technical Report FG DLT D1.3 Distributed ledger technology standardization landscape**

ITU-T Study Groups and Focus Group



1. **ITU-T Study Group 17: Security**
2. **ITU-T Study Group 16: Multimedia coding, systems and applications**
3. **ITU-T Study Group 13: Future networks, with focus on IMT-2020, cloud computing and trusted network infrastructures**
4. **ITU-T Study Group 20: Internet of things (IoT) and smart cities and communities (SC&C)**
5. **ITU-T Focus Group on Application of Distributed Ledger Technology (FG DLT)**
6. **ITU-T Focus Group on Digital Currency including Digital Fiat Currency (FG DFC)**
7. **ITU-T Focus Group on Data Processing and Management to support IoT and Smart Cities & Communities (FG-DPM)**
8. **ITU-T Focus Group on Environmental Efficiency for Artificial Intelligence and other Emerging Technologies (FG-AI4EE)**
9. **ITU-T Focus Group on Digital Financial Services (FG DFS)**

Source: ITU-T Focus Group on Application of Distributed Ledger Technology: **Technical Report FG DLT D1.3 Distributed ledger technology standardization landscape**

ISO Working Groups

ISO Technical Committee 307: Blockchain and distributed ledger technologies

Group	Title
WG1	Foundations
WG2	Security, privacy and identity
WG3	Smart contracts and their applications
JWG4	Joint ISO/TC 307 - ISO/IEC JTC 1/SC 27 WG: Blockchain and distributed ledger technologies and IT Security techniques
WG5	Governance
WG6	Use cases
SG7	Interoperability of blockchain and distributed ledger technology systems

Source: ITU-T Focus Group on Application of Distributed Ledger Technology: **Technical Report FG DLT D1.3 Distributed ledger technology standardization landscape**

Thank You