Regulatory guidelines for implementation

CHAPTER 05

A

Regulatory considerations: compliance and meeting international standards

Blockchain technology is relatively new, but its reach has already become global. Governments have already attempted in several ways to build legal, regulatory and compliance systems aimed at ensuring that the technology works for the good of society. However, many Governments have not yet established robust legal systems within which the technology could function and thrive. Furthermore, blockchain for trade facilitation purposes has not yet reached mass use, and while many Governments are looking into this potential, many still struggle with the regulation and compliance components of the implementation process.

The present section outlines the foundational steps for building the regulatory environment and implementing blockchain technology in a compliant manner that incorporates such legal and compliance processes into the core design process of the technology. The implementation of blockchain solutions must consider compliance as an integral part of the development and adoption process. Hence, the present section focuses on processes that meet international legal frameworks and standards as well as the approach Governments should take to incorporate these standards into the blockchain implementation process. This section also considers the necessary steps to help stakeholders and user groups understand the nature, procedures and requirements of compliance mechanisms that can ensure safe use of the technology in cross-border trade.

B

Key steps to support regulation and compliance

The technical features of blockchain make compliance, quality assurance and controls particularly enforceable. For example, the use of digital signatures, which is a default feature of the technology, can easily guarantee the safety of the user, security of the systems and auditability of the user activities. This, together with other digital and technical features, can help assure the smooth implementation of compliance mechanisms, improved risk management and regulatory oversight. While blockchain solutions could help Governments meet trade compliance needs in risk management and the prevention of fraud, the technology also needs critical compliance measures for its proper use by stakeholders. Below are the key steps for ensuring a holistic regulatory environment and a compliant implementation process for blockchain for trade facilitation.

1. **Defining the regulatory domain and legal gaps:** Before implementing any digital technology, blockchain included, it is imperative to define areas of regulatory weakness, legal gaps and compliance needs. This allows for the proper setting up of compliance systems to fill the regulatory gaps. As a relatively new technology, blockchain can usually work within existing compliance systems that regulate the broader digital economy, but it sometimes requires more than the existing regulations, especially for certain use-cases. For example, as a decentralized digital infrastructure, blockchain data is usually hosted in multiple systems with servers that are constantly synchronizing in real-time. This introduces new complexities on issues around data governance, privacy and user protection. This could sometimes require new legal structures that are different from the existing centralized data hosting systems. Furthermore, it could also require a new definition of data protection, data liability, user privacy and broader data governance issues around smart contracts and digital signatures before implementing the actual infrastructure.

2. **Identifying the regulatory requirements of expected use-cases:** Once the broader regulatory gaps have been identified, the next step is to determine sector-specific regulatory and compliance needs. While blockchain can be general-purpose technology, the use-case largely determines the compliance processes needed for the technology to function as intended. Thus, while a Government may have broader regulatory gaps for a new technology like blockchain, there can also be sector-specific regulatory ambiguities and discrepancies. Within trade facilitation, there are several trade-facilitation-specific regulatory and compliance processes to respect. Important trade regulations that would have to be considered at this stage could range from the data requirements of trade declarations to quality concerns about the declared goods. Defining sector-specific regulatory gaps would thus determine the specific regulatory processes that will be implemented at the technical level. Compliance with these sector-specific regulatory components can usually be implemented and achieved at the application level of the blockchain infrastructure. Furthermore, international standards on the specific sector could support the regulatory design process. For example, in trade facilitation, technical and legal standards such as the WCO SAFE Framework of Standards to Secure and Facilitate Global Trade, the International Convention on the Simplification and Harmonization of Customs Procedures, and the WCO Data Model are key guidance instruments that could assist the process. At this stage, it is important to involve industry stakeholders and private sector experts to undertake a broad review of existing regulations within the specific expected use-case area(s) and ascertain legal and compliance gaps, discrepancies and risks that could be mitigated by ensuring compliance.

3. **Designing a legal framework:** Once the regulatory gaps have been established at the national, sectorial and use-case levels, the next step is to build a relevant regulatory framework that fits the use-case, while adhering to the broader regulatory system. The regulatory framework must outline the compliance procedures and processes for both users and non-user stakeholders who engage with the blockchain system for all trade procedures. The rules and guidelines of engagement may include standards for data privacy, data governance, security and transparency, as well as guidelines for applications and smart contract development, as well as other aspects of the blockchain application layer. This level of the regulatory design is more specific and will necessarily involve the implementing stakeholder groups.

The design of regulatory frameworks would take place at more than one level:

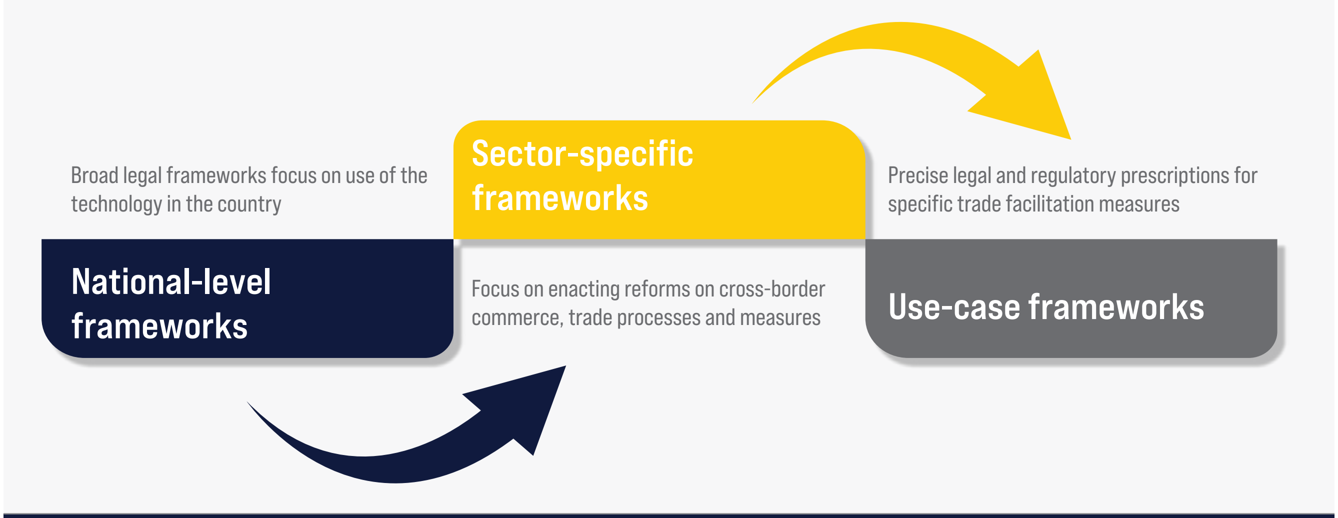
a. *National level frameworks.* This broad legal framework on use of the technology in the country can focus on a sector such as trade and commerce, or it can be a broad legal document on the use of the technology in general within the country. This framework will usually lack implementation precision but will convey strategic policy and regulatory directions that may take into consideration regional and international contexts of the use of the technology;

b. *Sector-specific frameworks.* These focus on exacting reforms on cross-border commerce, trade measures and driving trade facilitation efforts. Sector-specific frameworks focus on broader implementation guidelines that prescribe sector-wide reform strategies and will usually involve multiple stakeholders within the trade ecosystem;

c. *Use-case frameworks.* These regulatory frameworks give more targeted and precise legal and regulatory prescriptions on improving efficiency and driving value in relation to the precise trade facilitation needs of the Government. Such frameworks focus on the use-case of the blockchain solutions, such as in trade auditing, trade risk management, payment of duties, track and trace or fraud detection. The three levels of regulatory framework design are demonstrated in figure 12.

4. **Establishing compliance procedures:** Building a regulatory framework is important but establishing a compliance protocol is particularly relevant for important technologies like blockchain and for critical sectors like trade. Once a framework is in place, the next step will be to develop compliance procedures that help stakeholders meet regulatory requirements in the use of the blockchain solutions. Stakeholders need compliance mechanisms to ensure they successfully use the tools of the new technology and for general proper digital hygiene that reduces risks to users. Compliance procedures must also support system-wide digital health through regular inspections, audits and quality assurance of the systems. These compliance mechanisms should limit the regulatory burden on the user while ensuring that necessary standards are met. Preparing and documenting a protocol on compliance as a simple and understandable user guide can help stakeholders significantly.

Figure 12. The three levels of regulatory framework design


Broad legal frameworks focus on use of the technology in the country
National-level frameworks
Sector-specific frameworks
Focus on enacting reforms on cross-border commerce, trade processes and measures
Precise legal and regulatory prescriptions for specific trade facilitation measures
Use-case frameworks

Source: Compiled by ESCWA.

5. **Informing and supporting user groups:** Educating stakeholder groups such as customs, clearing agents, revenue authorities, traders and ministries about the regulatory framework and compliance mechanisms is a key component of building the regulatory environment for any new technology. Once regulatory frameworks and the technical infrastructure are in place, stakeholder engagement that results in full familiarity with the technical and regulatory procedures is key to ensuring a successful and sustainable use of the blockchain environment. This can be done through stakeholder training, education and information and can take the form of training workshops, seminars, outreaches, flyers and booklets as well as user guides that communicate the user benefits, obligations and key dimensions of compliance.

6. **Enforcement:** While regulatory frameworks may give a particularly useful setting for the successful implementation of blockchain for trade facilitation, compliance is not guaranteed without proper systems of enforcement. Once training and education of the stakeholders is complete, the next step is enforcement that ensures compliance. Enforcement of the regulatory frameworks could take place through appropriate mechanisms such as fines or penalties for non-compliance, or revocation of licenses or certifications for breach of authority or abuse. Enforcement must be conducted fairly and transparently, with appropriate due process of protections for other stakeholders while deterring future non-compliance.

7. **Monitoring and improving the legal systems:** The legal, regulatory and compliance mechanisms should undergo continuous improvement. User feedback must be incorporated into further adjusting and refining the legal frameworks to meet emerging trade facilitation needs of stakeholders. The implementing agency must therefore continuously monitor and collect user feedback and improve the legal frameworks that govern the use of the technology. This allows for out-of-date laws to be changed or replaced as the technology evolves and helps ensure that the regulatory framework remains effective and relevant over time. The process may involve conducting regular legal reviews and assessments of the regulatory frameworks, regular legal updates that reflect changes in the technology, as well as other emerging trade facilitation issues that may impact or be impacted by the regulatory landscape over time.

A summary of these key steps is presented in table 12.

Table 12. Key steps in the legal and regulatory process

Key regulatory step	Description
Defining the regulatory domain and identifying legal gaps	This involves defining areas of regulatory weakness, legal gaps and compliance needs so that compliance systems can be set up to fill the identified regulatory gaps.
Identifying the regulatory requirements of expected use-cases	This step aims to address sector-specific regulatory ambiguities and discrepancies with regards to trade facilitation and compliance with trade measures.
Designing a legal framework	This involves outlining the compliance procedures and processes for both users and non-user stakeholders at the national, sectorial and use-case levels of the technology. The rules and guidelines of engagement may include standards for data privacy, data governance, security, transparency and smart contracts.
Establishing compliance procedures	A compliance protocol outlines measures for system-wide digital health through regular inspections, audits and quality assurance of all digital systems accompanying the blockchain.
Informing and supporting user groups	This involves building stakeholder familiarity with the technical and regulatory procedures for successful and sustainable use of the technology through training workshops, seminars, outreaches, flyers, booklets and guides that communicate user benefits, obligations and key dimensions of compliance.
Enforcement	This involves measures such as fines or penalties for non-compliance, or the revocation of licenses or certifications for breach of authority or abuse. Enforcement should be conducted fairly and transparently, with due process for protections and deterrence.
Monitoring and improving the legal systems	Stakeholder feedback is incorporated into further adjusting and refining the legal frameworks to meet emerging trade facilitation needs. This step involves conducting regular legal reviews and assessments of the regulatory frameworks to undertake regular legal updates that reflect changes in the technology.

Source: Compiled by ESCWA.

C

A work breakdown structure for the regulatory framework

A WBS is useful for breaking down complex legal and compliance processes into smaller, more manageable tasks. Table 13 shows a WBS for the regulatory, legal and compliance process when designing a blockchain ecosystem for trade facilitation purposes.

A work breakdown structure is useful for breaking down complex legal and compliance processes into smaller tasks.

Table 13. A work breakdown structure for the legal and regulatory framework

Steps	Implementation components
Initiation	■ Define regulatory and compliance objectives. ■ Identify implementing partners, experts and stakeholders. ■ Design a national, sector-specific and use-case-specific framework guidelines.
Planning	■ Define regulatory scope. ■ Identify compliance requirements. ■ Undertake legal reviews to establish legal and regulatory gaps. ■ Develop a compliance plan. ■ Create implementation schedules for compliance schemes. ■ Develop implementation budget. ■ Define core regulatory team for domain-specific regulations.
Analysis	■ Conduct a legal and regulatory analysis. ■ Identify compliance risks and enforcement challenges. ■ Develop compliance milestones, penalties and protocols.
Design	■ Design regulatory policies, procedures and protocols. ■ Develop a compliance training and support programme. ■ Design a legal monitoring system and compliance audit processes. ■ Define a process for reporting and investigating breaches. ■ Develop a data governance, privacy policy and information security programmes.
Implementation	■ Implement compliance policies and procedures and protocols. ■ Conduct compliance training for stakeholders. ■ Launch regulatory and compliance audit processes. ■ Implement data governance systems, privacy policies and information security programmes.
Monitoring and reviewing	■ Conduct continuous legal and regulatory audits. ■ Conduct periodic compliance risk assessments. ■ Undertake regular evaluations of regulatory systems to ascertain the effectiveness of compliance. ■ Conduct relevant regulatory reviews and legal updates. ■ Identify areas for improvement and implement changes.

Source: Compiled by ESCWA.

D

Coupling technical standards with regulation and compliance

In the use of blockchain tools, most regulation and compliance issues need a technical component to be reliably enforceable. Thus, Governments may have to establish various technical standards as well as comply with existing standards that will support the implementation of effective blockchain compliance systems. These standards help ensure that the technology is used in a manner that complies with regulations and reduces the risks of fraudulent or illegal activities. Some key compliance areas that will have to be ensured through technical implementation techniques and processes include the following:

1. **Privacy policy, security standards and data governance:** User privacy and security standards are essential for ensuring that personal data is protected from unauthorized access and misuse. Governments that build digital solutions with blockchain for trade facilitation purposes have a legal imperative to design the protocols and processes that appropriately handle the types of user data collected, where that user data is stored, and which users have the rights and authority to access such sensitive data. This may include alignments with already existing data management protocols and processes that are not specific to blockchain. Also, key compliance disclosures around user data handling including credentials such as usernames, contact details and IP addresses, must be clearly communicated. Technical standards around data encryption, secure storage and access control that ensure the protection of sensitive personal data must therefore be implemented both at the user portal level and on the database. Trade data can be sensitive or even proprietary and these kinds of data must be protected, encrypted and guarded by modern data management practices. From declarations to invoices, licences and certificates, data handling through the blockchain that are aimed at ensuring ease of information flow must also meet protection standards for purposes of regulation and compliance. For example, the blockchain-enabled advance cargo information system for the Egyptian Government was designed to be compliant with the provisions of the WCO SAFE Framework as well as the WCO Data Model and many other WCO instruments and items of guidance (Kotb and Igor, 2022).

2. **Interoperability standards:** For compliance, interoperability standards that ensure that critical information can be passed between one blockchain network and another or between a blockchain system and a legacy system must be properly designed, implemented and enforced. Ensuring safety and compliance in data storage is as important as ensuring compliance with the transfer and exchange of that data. Thus, interoperability standards should not only be aimed at the seamless transfer of data, but also the safety of the data while in transit. Governments implementing blockchain for trade facilitation purposes must establish technical standards that specify the protocols, formats and security requirements for data exchange between different digital domains. Technical standards around the encryption of data in transit, secure transfer and access controls must thus be implemented at the user-facing level as well as the back-end when possible.

3. **Smart contract standards:** Smart contract standards specify the technical requirements for developing and deploying smart contracts on blockchain networks. As tools for business logic between the blockchain and the user-facing portals, smart contracts play key roles such as defining user credentials, rights and privileges, as well as being used for automation purposes. Compliance standards on smart contracts should focus on data protection, safety, privacy and security. As digital vehicles that allow users to interact with the blockchain based on the use-case, smart contracts must meet minimum standards around data transfer, automation and communication. This compliance can be achieved by extensive design testing and auditing of the smart contracts.

4. **Consensus mechanism standards:** Consensus mechanism standards specify the rules and procedures for validating records and adding new information to the blockchain. This aspect of the technical design process forms the core of the blockchain infrastructure. Standards of regulation and compliance can be ensured by the technical specifications that are baked into the core of the consensus mechanism. Data requirements around the security, speed and resilience of the network influence the user experience and the compliance thereof. Specifications around the type of consensus, block size—the amount of data that can be stored in a single block of records— as well as the adopted cryptographic primitives, all

influence performance and user experience. But they also impact compliance. For example, a proof of authority consensus blockchain will naturally require that a hierarchy of authority be allocated to the network participants, which will grant some network participants higher compliance privileges compared to others. Governments must therefore establish technical standards that specify the requirements for consensus mechanisms, including performance, security, the degree of decentralization of the blockchain network and the dynamics of authority to ensure compliance.

5. **Identity standards for users:** Digital identities and user identifiers are default features of blockchain. The use of blockchain for a multi-user, multi-agency ecosystem like trade facilitation requires a distinct set of policy, regulatory and technical standards on user identity management and user identifiers. This will influence many aspects of the use of the blockchain solution, including the auditability of user activities, risk management, access controls and quality assurance. The standards and protocols on user identity management will also determine the level of user protection, user accountability and user privileges. Digital identity standards thus specify the technical requirements for verifying and managing digital identities on the blockchain network. To ensure compliance, bodies implementing blockchain for trade facilitation must create technical standards for digital identity verification, authentication and authorization that are in line with the established regulatory and policy environment.

6. **Auditing and quality control standards:** While ensuring compliance is an ongoing activity, the implementation procedures that ensure continuous compliance must be designed at the beginning. Auditability of user activities, data processes and security protocols must be at the centre of the design process. Audits and reporting standards specify the requirements for quality assurance of activities on the blockchain to ensure compliance with regulations. Technical standards that specify data elements, frequency and format for reporting blockchain records and activities will be necessary for ensuring compliance for most trade facilitation use-cases and for efficient and safe use of the technology in general.

A summary of technical standards for regulatory compliance is provided in table 14.

Table 14. Summary of technical standards for regulatory compliance

Standard	Description
Privacy policy, security standards and data governance	These are technical standards around data encryption, secure storage and access controls to protect sensitive personal data implemented both at the user interface levels and at the database levels.
Interoperability standards	These are technical standards that specify the protocols, formats and security requirements for data exchange between different digital domains comprising blockchain and non-blockchain legacy systems.
Smart contract standards	Standards on smart contracts focus on data protection, safety, privacy and security for compliance around data transfer, automation, communication and storage.
Consensus mechanism standards	These standards specify the requirements for consensus mechanisms, including performance, security and the degree of decentralization of the blockchain network, with compliance as a key consideration.
Identity standards for users	User identity management standards determine user protection, user accountability and user privileges. They specify technical requirements for verifying and managing digital identities on the blockchain network and grant rights around approvals, authentication and authorization.
Auditing and quality control standards	Auditing and reporting standards specify the requirements for quality assurance of data, the auditability of user activities and security protocols. The standards also specify data elements, as well as the frequency and format for reporting blockchain records and activities.

Source: Compiled by ESCWA.