BOJ Reports & Research Papers

Payment and Settlement Systems Report Annex Series

Payment and Settlement Systems Report – Annex

Standardization in Information Technology related to Digital Currencies

Payment and Settlement Systems Department
Bank of Japan
June 2021

(Payment and Settlement Systems Report Annex Series)

The Bank of Japan regularly publishes the Payment and Settlement Systems Report with the aim to provide an overview and evaluate the development of its payment and settlement systems. The report also introduces the engagement of the Bank of Japan and relevant organizations to improve the safety and efficiency of the payment and settlement systems.

The Payment and Settlement Systems Report Annex Series provide in-depth analyses about specific themes concerning those systems. This report focuses on standardization in information technology related to digital currencies. This paper is a part of the study on "standardization of IT relating to digital currency," which was identified as one of the items to be considered in exploring the possible design of CBDC in the "The Bank of Japan's Approach to Central Bank Digital Currency," released by the Bank in October 2020.

This document is an English translation of the Japanese original published on May 25, 2021.

Standardization in Information Technology related to Digital Currencies

Executive Summary

Various standardization efforts have been made to support the smooth processing of financial services such as deposit-taking, loans, and credit transfers by banks as well as brokerage of securities transactions by securities companies. Standards have been developed in the area of message formats for transmitting transaction information, structures for numbering and coding transaction data, and security measures such as encryption methods.

Standardization has contributed to enhancing operational efficiency at financial institutions and the safety and convenience of the services provided to customers by (i) ensuring interoperability among systems that process financial transactions and (ii) ensuring the reliability of the systems. As modern financial services are supported by highly advanced technologies, the standard-setting process also has the benefit of (iii) bringing together and utilizing expertise, and it is becoming increasingly important for a wide range of parties, including businesses and experts, to participate in these international standardization activities.

In recent years, various services by payment service providers have emerged, in addition to the traditional funds transfer and remittance services typically provided by banks. There have also been moves to explore the possibility of new digital currencies issued by private entities, such as stablecoins based on blockchain and/or distributed ledger technology (DLT).

The benefits of standardization in financial services (i.e., ensuring interoperability, ensuring reliability, and bringing together and utilizing expertise) are applicable to digital currencies, and existing international standards in the field of financial services can serve as a useful reference.

These benefits are also applicable to central bank digital currency (CBDC) in many ways. The Bank recognizes the need for cooperation and collaboration with a wide range of stakeholders, including private-sector businesses and experts, as well as for leveraging the cooperative efforts among central banks, in its ongoing consideration of CBDC. The Bank will also closely coordinate with stakeholders in Japan in the area of international standardization related to CBDC.

Table of Contents

I. Introduction

In October 2020, the Bank published the "The Bank of Japan's Approach to Central Bank Digital Currency."[1] Central bank digital currency (CBDC) is a new form of digital central bank money that is different from current account deposits held by banks at a central bank.[2] While the Bank currently has no plan to issue CBDC, the Bank considers it important to prepare thoroughly to respond appropriately to changes in circumstances in order to ensure the stability and efficiency of the overall payment and settlement systems.

The Approach paper outlines the functions and roles expected of "general-purpose CBDC," which is intended to be used by a wide range of end users including individuals and firms, and sets out the core features required for CBDC. It further lists the following points to be considered when exploring the possibility of issuing CBDC: (i) relationship with price stability and financial system stability; (ii) promoting innovation; (iii) ensuring privacy and handling of end-user information; and (iv) relationship with cross-border payments.

In terms of cross-border payments, the Approach paper points out that active discussion among jurisdictions on international standardization of data formats is essential considering the importance of ensuring the interoperability of CBDC issued by each jurisdiction. This paper examines standardization in information technology related to digital currencies as part of the Bank's work on exploring the possible design of CBDC.

The Payment and Settlement Systems Department of the Bank serves as the secretariat of the ISO/TC 68 National Member Body, commissioned by the Japanese Industrial Standards Committee (JISC) established by the Ministry of Economy, Trade and Industry. ISO/TC 68 is a technical committee (TC) of the International Organization for Standardization (ISO) that is responsible for creating international standards in the field of financial services. This paper discusses the benefits of standardization for digital currencies and possible areas of standardization based on the insights accumulated by the Bank through these activities.

The structure of this paper is as follows. Section II considers the benefits of standardization

---

[1] Bank of Japan, "The Bank of Japan's Approach to Central Bank Digital Currency," October 2020. https://www.boj.or.jp/en/announcements/release_2020/rel201009e.htm/

[2] Committee on Payment and Market Infrastructures (CPMI) and Markets Committee, "Central Bank Digital Currencies," March 2018.

for digital currencies, with reference to the benefits of standardization in the financial services field. Section III describes standard-setting activities in the field of financial services and examines specific areas of standardization that are relevant to digital currencies. Section IV concludes with a discussion on the possible application of standardization to CBDC.

II. Benefits of Standardization for Digital Currencies

A. What is Standardization?

Standardization may not be a topic that is familiar to the general public. The Japan Industrial Standards Committee (JISC), which develops domestic standards known as Japan Industrial Standards (JIS), defines "standardization" as "the reduction, simplification, and rationalization of matters that, if left unsorted, would become divergent, complex, or disorderly."[3] Familiar examples are the size of paper, such as A3 and A4, and the specifications of dry cell batteries, such as AA and AAA batteries. By standardizing these sizes and specifications, consumers can easily obtain products from different manufacturers and use them in the same way.

In addition to enhancing convenience for consumers, standardization has various benefits and implications for businesses.[4] For example, standardizing the sizes and specifications of industrial products enables mass production, making it easier for businesses to lower product prices and possibly expand the market. Standardization of quality labeling methods for products and services also contributes to the reduction of transaction costs. In addition, the publication of standards on new technology supports adoption of the technology and development of industries.

Furthermore, as digitalization progresses in various business fields with advances in information and communication technology, standardization is expected to improve the interoperability[5] of products and services, leading to enhanced network effects (an effect in

---

[3] JISC, "About Industrial Standardization," https://www.jisc.go.jp/jis-act/ (available only in Japanese).

[4] See Tanaka Masami, *Kokusai hyōjun no kangaekata: gurōbaru jidai heno atarashii shishin* [International Standardization: A New Guideline for the Global Era], University of Tokyo Press, March 2017 (available only in Japanese).

[5] Interoperability can be generally defined as a characteristic of a product or a system to work with other products or systems. Interoperability can be achieved at different levels. See Section III for details.

which an increase in the number of users leads to an increase in the benefits they gain from a product or a service). An increasing number of standards have also been developed that help ensure the credibility of business operators by providing a mechanism to objectively evaluate their processes in areas such as quality management, environmental responsiveness, and information security.

B. Standardization in Financial Services

Financial institutions provide a wide range of financial services, including deposits, loans, and funds transfers by banks, and brokerage of securities transactions by securities companies. Various standardization efforts have been made to facilitate smooth processing of these services.

Looking back in history, when financial transactions were conducted on a paper basis, the main focus of standardization was on the format of bills, checks, and other paper forms. As processing of financial transactions became automated, message formats for transmitting transaction information and numbering and coding systems became the subject of standardization, thereby improving interoperability among systems that process financial transactions. Furthermore, as financial transactions became highly electronic, information security technologies such as encryption methods, IC cards, and biometrics were added to the scope of standardization. The development of these standards assured that the safety of financial transactions was maintained above a certain level and ensured the reliability of the systems that processed the transactions.

In this way, standardization in the field of financial services in the modern era has brought about the benefits of "ensuring interoperability" between systems that process financial transactions and "ensuring reliability" of the systems, which in turn has contributed to improving the operational efficiency of financial institutions and the safety and convenience of services provided to customers.

In recent years, the benefit of bringing together and utilizing expertise, including knowledge on innovative technologies, in the standard setting process has also been recognized. Standardization efforts are becoming more active on an international level as globalization of financial services progresses. The digitalization of society and the shift to a service-based economy have also raised the importance of incorporating innovative technology into

financial services. As a result, it has become increasingly important to have participation in international standardization activities from not only the financial industry but also from businesses and experts with expertise in technologies applicable to financial services.

C. Standardization of Digital Currencies

In recent years, various services by payment service providers have emerged, in addition to the traditional funds transfer and remittance services typically provided by banks. There have also been moves to explore the possibility of new digital currencies issued by private entities, such as stablecoins based on blockchain and/or distributed ledger technology (DLT). In many of these services, "digital currency" is interpreted widely to include a range of payment services using digital technology.

The following explains in some detail how the benefits of standardization in financial services (i.e., ensuring interoperability, ensuring reliability, and bringing together and utilizing expertise) are also applicable to digital currencies.

1. Ensuring interoperability

Ensuring interoperability is particularly important for payments platforms. Interoperability facilitates the exchange of data between multiple platforms and provides users with network effects that cannot be achieved by a single platform.

Digital currencies provide a versatile payment and remittance service for a wide range of users, including individuals and businesses. If interoperability between different platforms is ensured and digital currencies can be exchanged with each other, it will bring added value to users, such as the expansion of trading partners and the resulting expansion and diversification of trading opportunities, ultimately leading to greater convenience for the public and enhanced efficiency of payment systems.

To ensure interoperability, it is effective to establish a "common language system" that links multiple digital currency platforms, that is, to promote standardization of message formats and data elements for transmitting payment information.

For example, in the area of bank credit transfers, the improvement of cross-border payments has been promoted by the Financial Stability Board (FSB) and the Bank for International

Settlements (BIS) through its Committee on Payments and Market Infrastructures (CPMI).[6] International harmonization among systems through the use of international standards for message formats has been proposed as one of the effective means to solve the problem.

Similarly, for domestic payment services, when private entities consider issuing a new digital currency in the future, working to ensure interoperability with other payment platforms will contribute to improving convenience for the public and efficiency of the payment system. Particularly in Japan, where the demand for cash is strong, ensuring interoperability through standardization will be important in order for private-sector digital currencies to achieve a network effect similar to that of cash and achieve widespread adoption.

2. Ensuring reliability

Reliability is one of the most important factors for digital currencies. If payment information is stolen or rewritten by a third party when holding and using digital currency, users will not be able to use digital currency in their daily lives with confidence. Given that many of the digital currency services are intended to be used by a wide range of users, including individuals and businesses, the social impact of a loss of confidence would be enormous.

Systems for digital currency services are developed by combining a wide range of underlying technologies. Therefore, in order to ensure the reliability of digital currency, it is necessary to select security measures suitable for each underlying technology, and to take steps to ensure safety in terms of both implementation and procedure for the integrated operation of the adopted security measures.

In terms of implementation of security measures, robust information security technologies such as encryption and digital signatures need to be adopted. One way to achieve this may be to use security standards developed by organizations that have gained international credibility in evaluating the security of cryptographic technologies. In particular, in recent years, as research and development of quantum computers has become more active, efforts to standardize quantum-resistant cryptography have begun overseas. For example, the National

---

[6] FSB, "Enhancing Cross-Border Payments: Stage 3 Roadmap," October 2020.
CPMI, "Enhancing Cross-Border Payments: Building Blocks of a Global Roadmap; Stage 2 Report to the G20," July 2020.

Institute of Standards and Technology (NIST) in the U.S. is in the process of selecting a standard for post-quantum cryptography. It started a technical evaluation of fifteen candidate algorithms in July 2020, and plans to narrow down the candidates in 2022.[7] In designing a system for digital currency, adopting recognized standards, as well as having the scalability to update the encryption method in accordance with future developments in cryptography, will help to ensure the continued credibility of the service.

In terms of procedure, a framework for objective evaluation and certification by a third-party organization may be adopted for aspects such as information security management, procurement of related equipment, and privacy protection. Widely adopted international standards in this area include the ISO/IEC 27000 series (Information security management systems), ISO/IEC 15408 (Evaluation criteria for IT security), and ISO/IEC 27701 (Privacy information management system). In designing a system for digital currency, it is important to take into account established procedures that comply with these international standards.

3. Bringing together and utilizing expertise

Digital currencies are expected to meet various safety and compliance requirements such as information security, privacy protection, and anti-money laundering and counter-terrorist financing (AML/CFT), while at the same time providing advanced functionality and convenience by incorporating innovative technologies. The development and provision of digital currency services therefore require expertise from various areas.

In this context, the benefit of the standardization process as a means to deepen discussions among experts and to share a wide range of knowledge has become increasingly important in recent years. For digital currencies, standardization efforts at ISO/TC 307, which deals with blockchain and DLT, and ISO/IEC JTC 1,[8] which deals with information technology, are relevant in addition to those at ISO/TC 68. Participating in discussions on standards that are developed or under consideration in these groups may be useful as a means to efficiently

[7] NIST, "Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process," July 2020.

[8] The Joint Technical Committee (JTC) was jointly established by the ISO and International Electrotechnical Commission (IEC) in 1987 in response to the increasing need to promote standardization in the field of information technology, which spans both computer and network technologies. Subcommittees (SCs) under the JTC include SC 17 (Cards and personal identification), SC 27 (IT security techniques), and SC 37 (Biometrics).

collect knowledge on innovative technologies that can be applied to digital currency services.

It is also important to work to incorporate superior technologies developed domestically into international standards at ISO/TC 68 and other groups in order to facilitate the application of such technologies to digital currencies and other financial services. There may be cases where businesses with promising technologies do not have a strong worldwide presence. If such companies actively participate in international standardization activities, they would be able to take the lead in international discussions and expand their own business opportunities, while also gaining exposure to the latest technological trends. Such efforts may also lead to the development of new technology by bringing together domestic expertise.

III. Possible Areas of Standardization for Digital Currencies

The previous section looked at the benefits of standardization of digital currencies from three perspectives. This section examines specific aspects of digital currency that could be subject to standardization taking into account existing international standards in the field of financial services, with a focus on interoperability and reliability.

A. International Standard-Setting Activities in the Field of Financial Services

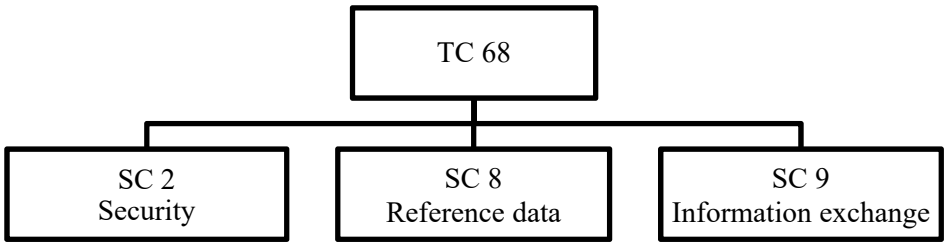
Before looking at specific standards in the field of financial services, this sub-section provides a brief overview of the organizational aspects of international standard-setting bodies.

International standards are created by a variety of organizations and groups, including the ISO, the IEC, and the International Telecommunication Union (ITU) (see box at the end of this paper).[9] International standards in the field of financial services are mainly developed by ISO/TC 68.

[9] Standards that are established by public international standardization organizations based on predetermined procedures are called "de jure standards." Other types of standards include "de facto standards," which become widely accepted through market competition among companies, and "forum standards," which are created by consensus among multiple companies in an industry.

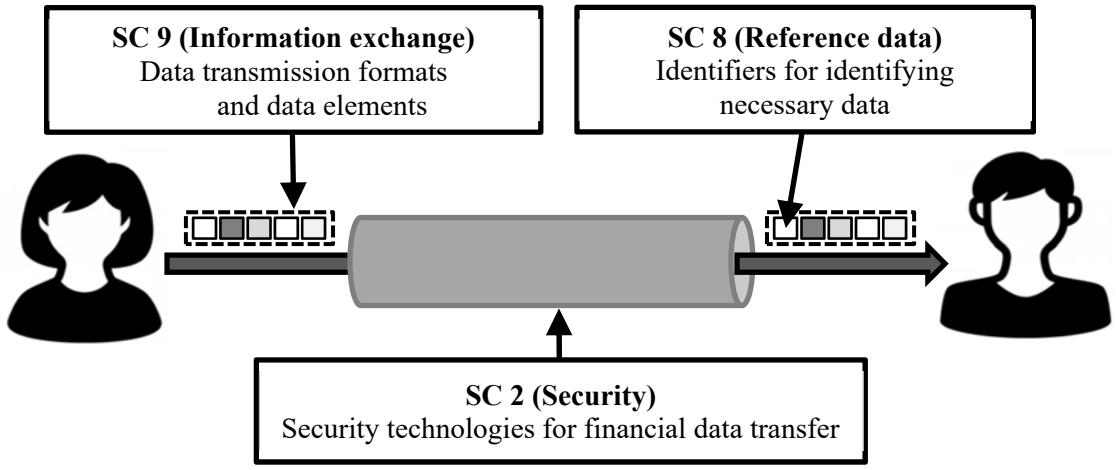
The Bank's Payment and Settlement Systems Department serves as the secretariat of the National Member Body of ISO/TC 68 in Japan. TC 68 has three subcommittees (SC) that consider and develop standards in their respective fields (Figure 1).

Figure 1: Organizational structure of ISO/TC 68



The areas of responsibility of the subcommittees are assigned to reflect the basic elements that are necessary for ensuring the safe and secure exchange of financial services data (Figure 2).

Figure 2. Basic elements of exchange of financial services data



SC 2 (Security) mainly deals with security technologies for financial data transfer, such as PIN management, biometrics, and encryption methods. SC 8 (Reference data) mainly deals with the identifier of financial data. SC 9 (Information exchange) mainly deals with message schemes of financial data transfer.

B. Possible Areas of Standardization for Digital Currencies

Possible areas of standardization that contribute to ensuring interoperability and reliability of digital currencies include: (i) message schemes (data elements and message formats); (ii) identifiers; and (iii) security technologies for financial data transfer. Each of these corresponds to the areas covered by the three ISO/TC 68 subcommittees.

1. Message schemes

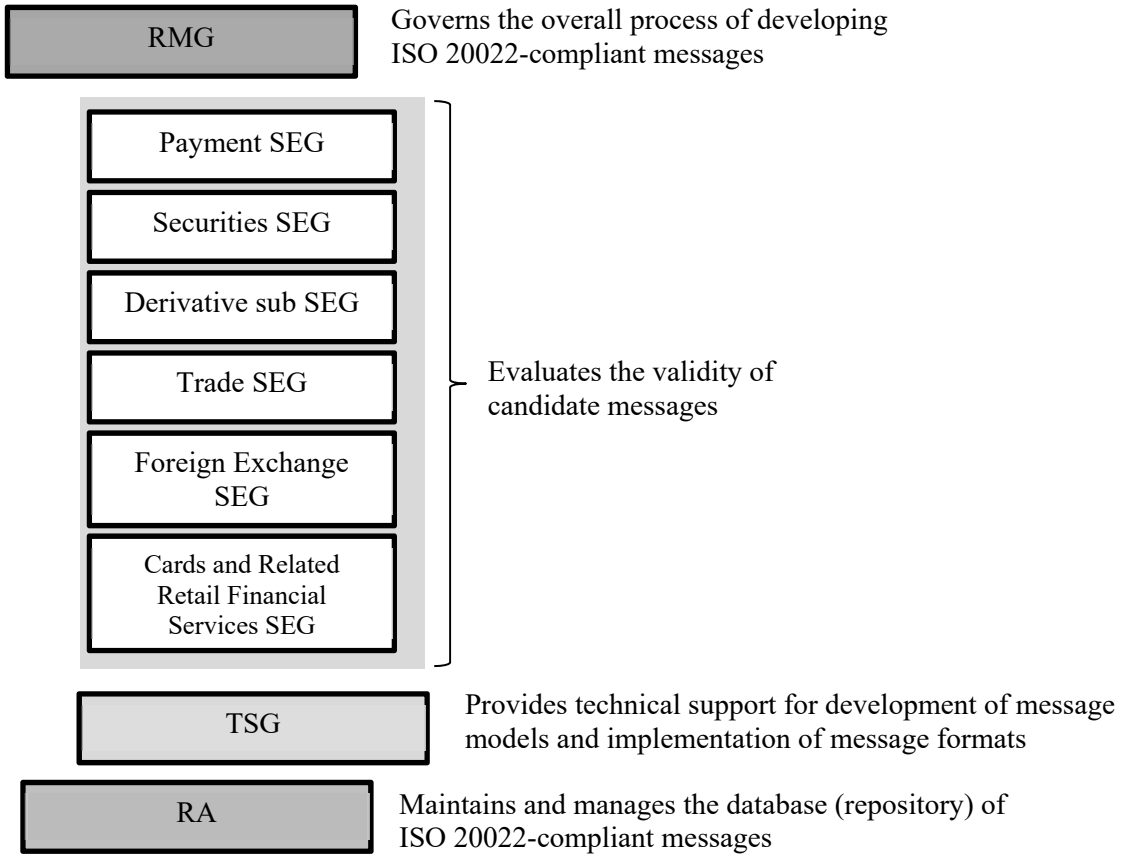
Modern financial transactions are based on the exchange of data between counterparties, including "when" to deliver "which asset" between "which counterparties" and "in what amount." Smooth data transfer requires counterparties to define a message scheme, which is a set of data elements with a message format. Therefore, the standardization of message schemes has been promoted in various fields along with the progress of online processing of financial services.

In the past, international standards for message schemes were developed separately for different areas of financial services, such as ISO 8583 for credit card transactions and ISO 15022 for securities delivery. In 2004, ISO 20022 was developed as an integrated international standard for message schemes covering the entire financial services sector, and has become widely used for the development of message schemes for financial services.

Under ISO 20022, the Standards Evaluation Group (SEG) verifies the validity of the candidate messages proposed by financial industry participants.[10] SEGs have been established in six financial services business domains in order to address the needs of each business area. The completed message format is registered in a repository maintained by the Registration Authority (RA). This entire process is managed by the Registration Management Group (RMG) (Figure 3).

[10] There is also a Technical Support Group (TSG) that provides technical support for implementing message formats and developing business models and message models.

Figure 3: ISO 20022 RMG organization



ISO 20022 is a standard for not only specific message formats, but also the message models, which describe all the information that is needed to perform a specific business activity, as well as the business models, which define the business processes and business concepts. These are all defined and registered in RA (Figure 4).

Figure 4: Information registered in ISO 20022 repository

Registered item	Overview	Description language
Message format	Message format derived from a message model	XML[11] schema ASN.1[12]
Message model	Message components with defined data elements organized in a hierarchical structure	UML[13]
Business model	Business process, roles and actors involved, and information needed	UML

Standardization at three levels, i.e., message format, message model, and business model, has the benefit of being able to address various levels of interoperability. Interoperability can be achieved by: (i) aligning formats so that messages can be exchanged directly between systems; (ii) aligning data elements and requirements so that data can be exchanged between systems accepting different formats through format conversion; and (iii) aligning business flows so as to enhance coordination between systems. ISO 20022 has the advantage that it can be used flexibly to address these various levels of interoperability.

As described above, ISO 20022 is an international standard for developing message formats that can be applied to a wide range of financial transactions including payments. For payments, message formats such as Financial Institution (FI) to FI Customer Credit Transfer (pacs.008) and FI to FI Institution Credit Transfer (pacs.009) have already been registered, and international adoption of ISO 20022-compliant messages is growing.**[14]**

[11] An XML schema describes the structure of an XML document. XML (Extensible Markup Language) is a language for representing structured data that was released by W3C, the standards organization for the World Wide Web, in 1998. Its advantages include high flexibility and extensibility, and low dependence on platforms.

[12] ASN.1 (Abstract Syntax Notation One) is an international standard for data description developed jointly by the Joint Technical Committee of ISO and IEC (ISO/IEC JTC 1) and the International Telecommunication Standardization Sector of the International Telecommunication Union (ITU-T). One of the features of ASN.1 is that it defines data structures by enumerating objects defined by name and type.

[13] UML (Unified Modeling Language) is a language that specifies a notation for modeling the behavior of a system, primarily in object-oriented analysis and design.

[14] As shown in this example, a notation number is assigned to each set of standardized message formats for a specific application, such as payment instructions for customer credit transfers and payment instructions for interbank credit transfers.

As stated in the previous section, the development of a "common language system" for coordinating multiple digital currency platforms, i.e., the standardization of message formats and data elements for transmitting payment information, would be effective for ensuring the interoperability of digital currency services. In doing so, the use of the ISO 20022 framework may be one option. In the aforementioned reports by the FSB and BIS/CPMI, adoption of common message formats such as ISO 20022 is also listed as one of the building blocks for enhancing cross-border payments by banks and other institutions.

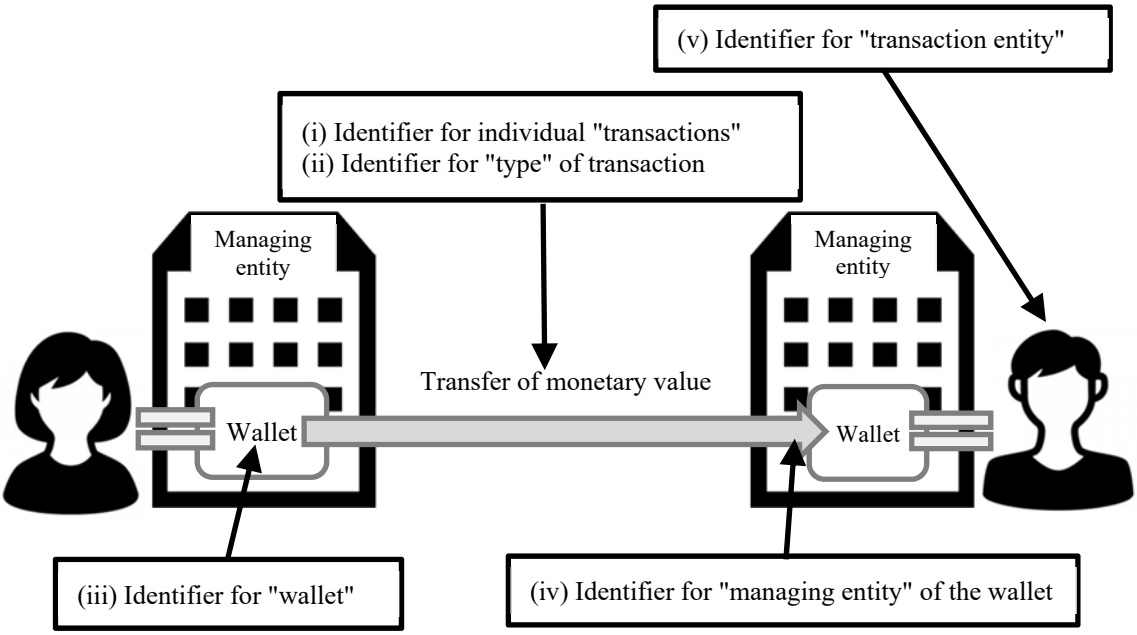
2. Identifiers

In order to enhance interoperability, it is also important to ensure that financial data to be transmitted can be clearly distinguished from among the streams of information. For this purpose, numbers or codes of several to dozens of digits are usually assigned to specific types of transactions or entities based on predetermined rules. Such numbering and coding systems are called "identifiers," and various international standards for identifiers have long been established for international financial transactions.

The following five types of identifiers may be relevant to digital currencies when focusing on the functions of transfer and storage of monetary value (Figure 5):

(i) identifier for individual "transactions" related to the transfer of monetary value;
(ii) identifier for the "type" of transaction related to the transfer of monetary value;
(iii) identifier for the "wallet" in which the monetary value is stored;
(iv) identifier for the "managing entity" of the wallet in which the monetary value is stored;
(v) identifier for the "transaction entity" of the transfer of monetary value.

Figure 5: Identifiers relevant for transfer and storage of monetary value

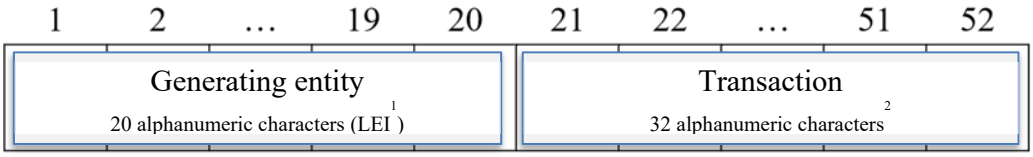


a. Identifier for individual "transactions" related to the transfer of monetary value

In financial transactions, an identifier is usually assigned to each transaction in order to identify individual transactions. For example, for interbank cross-border payments, a unique number called a Unique End-to-end Transaction Reference (UETR) is assigned to each payment for payments tracked on the SWIFT gpi (global payments innovations).

Identifiers for payment instruction messages, including UETR, have not yet become an international standard under the ISO framework. In another area of financial services, an identifier called a Unique Transaction Identifier (UTI) has been developed as ISO 23897 and is currently used for over-the-counter (OTC) derivatives transactions (Figure 6).

Figure 6: Structure of ISO 23897 Unique Transaction Identifier



Notes: 1. See Figure 11 for the structure of LEI.
2. Only uppercase letters may be used for alphabetic characters.

When considering identifiers for individual transactions in the transfer of monetary value in digital currencies, it may be useful to refer to these existing international standards as well as ongoing discussions on payment identifiers.

b. Identifier for the "type" of transaction related to the transfer of monetary value

International standards have been developed to identify and specify a type of transaction, such as the type of currency and the trade exchange where the transaction took place. For example, the international standard for currency codes, ISO 4217, has a numbering system that represents currencies both alphabetically and numerically in three digits, such as JPY and 392 for the Japanese yen and USD and 840 for the U.S. dollar (Figure 7).[15] This standard may also be a useful reference when considering how to represent the denominations of digital currencies.

Figure 7: Examples of ISO 4217 currency codes

Currency	Alphabetic code	Numeric code	Currency	Alphabetic code	Numeric code
Euro	EUR	978	Japanese yen	JPY	392
Swiss franc	CHF	756	U.S. dollar	USD	840
British pound	GBP	826	Australian dollar	AUD	036

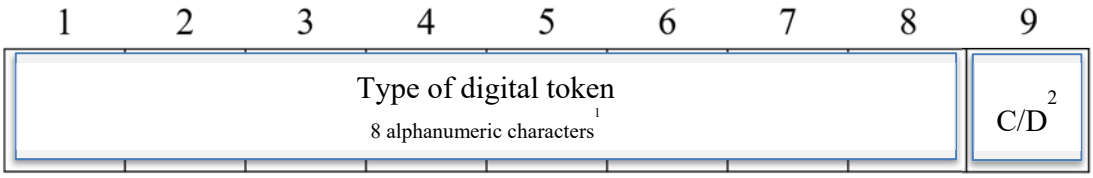
In addition, there may be a need to identify multiple types of digital currencies (e.g., digital currency A and digital currency B), for example, when multiple private entities issue digital currencies denominated in the same currency. This is necessary at least in situations where exchange between these digital currencies takes place. While there is currently no international standard for this purpose in the standards for bank transfers, for digital tokens[16] that utilize DLT, such as crypto-assets and security tokens, an international standard on Digital Token Identifier (DTI) is being considered (ISO/DIS 24165, Figure 8). Such

[15] ISO 4217 defines "currency" as "medium of exchange of value, defined by reference to the geographical location of the monetary authorities responsible for it."

[16] ISO/DIS 24165 defines a digital token as a "fungible digital asset which uses distributed ledger technology for its issuance, storage, exchange, record of ownership, or transaction validation and is not a currency."

identifiers may be relevant in considering identifiers for digital currencies.

Figure 8: Structure of ISO/DIS 24165 Digital Token Identifier



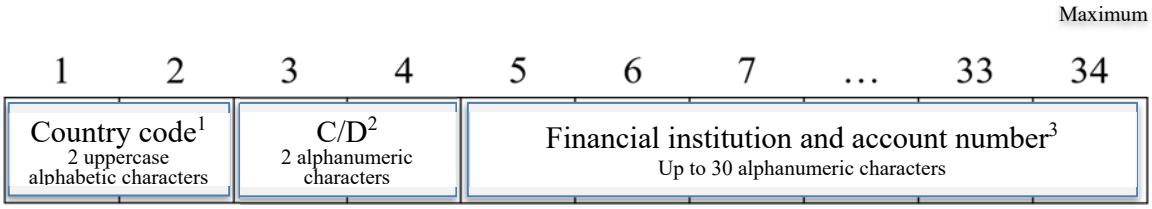
Notes: 1. Only uppercase letters other than A, E, O, I, U, and Y may be used for alphabetic characters. The number 0 may not be used for the first digit.
2. One alphanumeric character. A check digit (C/D) is added to detect any errors made while typing the number into the system.

c. Identifier for the "wallet" in which the monetary value is stored

In digital currency services, the monetary value would not only be transferred between users but also stored in a "wallet" that belongs to each user. This would raise the need to identify individual "wallets."

In the case of bank transfers, deposit accounts function as "wallets," and are identified using account numbers. The international standard for bank account numbers is ISO 13616, which defines the International Bank Account Number (IBAN) that is widely used by banks overseas (Figure 9).[17]

Figure 9: Structure of ISO 13616 International Bank Account Number



Notes: 1. Country code specified in ISO 3166-1.
2. A check digit is added to detect any errors made while typing the number into the system.
3. Country-specific combination of financial institution code and account number.

[17] Banks in Japan use a unique Japanese numbering system for deposit accounts, consisting of a three-digit branch number and a seven-digit account number.

Digital currency services are sometimes categorized as either "account-based" or "token-based," with distinctions made, for example, based on the structure in which the information on monetary value is linked to the owner of the value. While there are a range of different interpretations of these terms, one categorization may be to define "account-based" as a structure that records the total amount of monetary value (balance) owned by each user, and "token-based" as a structure that records the owner of each token with specific monetary value.[18] In either structure, the existing international standard for account numbers may be relevant when considering the numbering system for "wallet" identifiers.

d. Identifier for the "managing entity" of the wallet in which the monetary value is stored

In addition to identifying the "wallet" that stores monetary value, digital currency services may also need to identify the "managing entity" of the wallet, such as a bank or a payment services provider. As an existing identifier that may be used for this purpose, ISO has international standards for codes to identify legal entities.

For example, ISO 9362 is a standard for the Business Identifier Code (BIC) that is used to identify financial institutions in cross-border payments (Figure 10). ISO 17442 is a standard for the Legal Entity Identifier (LEI), which was developed mainly for the purpose of OTC derivatives trade reporting to identify businesses and funds involved in a financial transaction (Figure 11).[19]

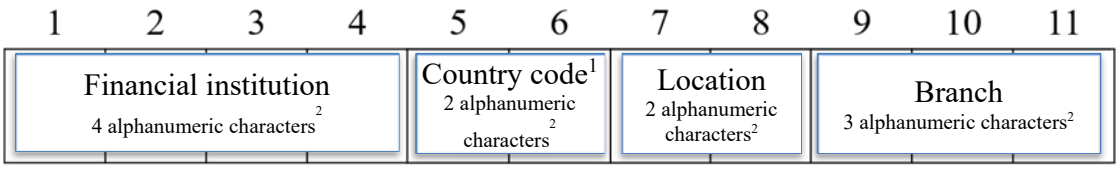
These existing international standards may be utilized in identifying the "managing entity" of a wallet that stores digital currency.

---

[18] This categorization is in line with the Bank of Japan Payment and Settlement Systems Department's, "Chūgin dejitaru tsūka ga genkin dōtō no kinō o motsu tame no gijutsu-teki kadai" [Technical challenges of enabling cash-equivalent functions in central bank digital currency], Payment and Settlement Systems Report Annex Series, July 2020 (available only in Japanese). For discussion on the dichotomy of accounts and tokens, see also Lee, Alexander, Brendan Malone, and Paul Wong, "Tokens and Accounts in the Context of Digital Currencies," FEDS Notes, Board of Governors of the Federal Reserve System, December 2020.

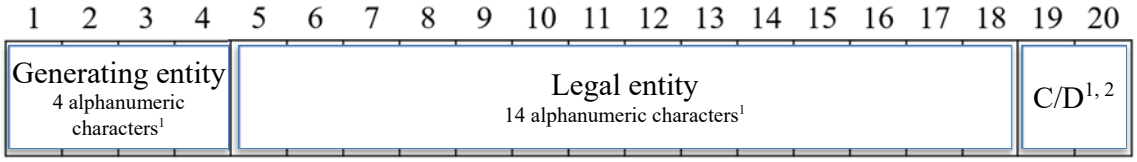
[19] Recently, there have been an increasing number of examples of the use of LEIs in addition to OTC derivatives trade reporting.

Figure 10: Structure of ISO 9362 Business Identifier Code



Notes: 1. Country code specified in ISO 3166-1.
2. Only uppercase letters may be used for alphabetic characters.

Figure 11: Structure of ISO 17442 Legal Entity Identifier



Notes: 1. Only uppercase letters may be used for alphabetic characters.
2. Two alphanumeric characters. A check digit is added to detect any errors made while typing the number into the system.

e. Identifier for the "transaction entity" of the transfer of monetary value

In digital currency services, transfer of value is recorded by linking individual transactions with "transaction entities," or the users of the service.

As mentioned above, for legal entities, ISO 17442 (LEI) and ISO 9362 (BIC) have been developed as standards for identifiers of "transacting entities." While there is currently no existing ISO standard for identifiers of natural persons, a coding system for natural persons is currently under consideration in TC 68 (ISO/DIS 24366 Natural Person Identifier (NPI)).

These standards may be relevant when considering identifiers for "transaction entities" related to digital currencies.

3. Technology for secure data transmission

In financial transactions, ensuring an adequate level of security using up-to-date technologies is essential for the safe transmission of data related to monetary value. The financial services industry has a long history of developing information security-related standards from multiple aspects, including those on technologies, methods, and procedures.

For example, international standards developed by ISO/TC 68 include those for the management of personal identification numbers (PIN), biometrics, and data encryption methods (Figure 12). Recently, in response to the developments in underlying technologies and the widespread use of various electronic devices, standards related to customer identification guidelines (ISO/WD 5158, online customer verification by smartphones, so-called "e-KYC"), code-scanning payment security (ISO/WD 5201, including QR code payment), and security techniques for blockchain and DLT (ISO/WD 24374) are also under consideration.

Figure 12: Security standards developed by ISO/TC 68

Standard	Overview
ISO 9564 Personal Identification Number (PIN) management and security	Specifies basic principles on the issuance, storage, and usage of PINs in card-based systems for financial transactions.
ISO 11568 Key management in retail financial services	Specifies the principles for the management of keys used in cryptosystems implemented within the retail-banking environment, including secure exchange of keys between central systems and end-point systems such as point-of-sale (POS) debit and credit authorizations, and automated dispensing machine and automated teller machine (ATM) transactions.
ISO 13491 Secure cryptographic devices for retail financial services	Specifies the security characteristics for secure cryptographic devices (SCDs) based on the cryptographic processes.
ISO 13492 Key management – application and usage of ISO 8583-1 data elements for encryption	Specifies the requirements for the use of the data element related to key management within ISO 8583-1 (financial transaction card-originated messages), using security related control information and key management data for the Data Encryption Algorithm (DEA) and Triple Data Encryption Algorithm (TDEA).
ISO 16609 Requirements for message authentication using symmetric techniques	Specifies procedures, independent of the transmission process, for protecting the integrity of transmitted messages and for verifying that a message has originated from an authorized source.
ISO 19092 Biometrics security framework	Describes the security framework for using biometrics for authentication of individuals in financial services.

ISO 20038 Key wrap using AES	Specifies a method for packaging Advanced Encryption Standard (AES) cryptographic keys for transport.
ISO 21188 Public key infrastructure for financial services – practices and policy framework	Describes a framework for using Public Key Infrastructure (PKI) in financial services including management of PKI through certificate policies and certification practice statements.
ISO 22307 Privacy impact assessment	Describes a privacy impact assessment (PIA) structure for risk assessment in order to identify and mitigate privacy issues associated with systems processing consumer data.

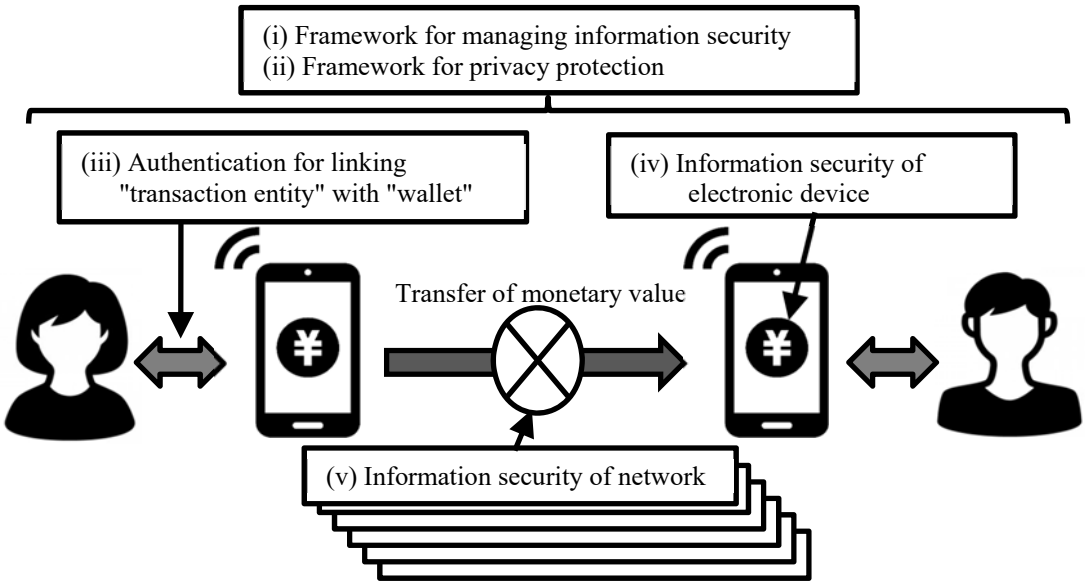
In addition to standards developed by TC 68, there are a wide range of ISO standards that may be relevant to information security in the financial services sector. These include the ISO/IEC 27000 series (Information security management systems), ISO/IEC 15408 (Evaluation criteria for IT security), ISO/IEC 27701 (Privacy information management system), ISO/IEC 29100 (Privacy framework), and ISO/IEC 29134 (Guidelines for privacy impact assessment).

Based on these international standards, potential areas of standardization related to the information security of digital currencies can be identified as follows (Figure 13):

(i) Framework for managing information security;
(ii) Framework for privacy protection;
(iii) Authentication for linking "transaction entity" with "wallet";
(iv) Information security of electronic devices used for digital currency;
(v) Information security of the network transmitting information on monetary value.

As mentioned above, the system for digital currency services will be developed as a combination of a number of underlying technologies, with a range of relevant security areas. Many of the underlying technologies are general-purpose technologies with proven track records. Therefore, in order to ensure an adequate level of security for the system, service providers would not likely apply a single international standard for the entire system but would select and flexibly apply a number of international standards that are relevant to the mixture of underlying technologies adopted by the system.

Figure 13: Potential areas for standardization of security of digital currency services



IV. Possible Application to CBDC

This paper has discussed the benefits of international standards for digital currencies and the possible areas of standardization, taking into account the existing standards in the field of financial services. This section concludes with a discussion on standardization for digital currencies issued by central banks.

The two main benefits of standardization for digital currencies hold true for CBDCs. Standardization of message formats, data elements, and numbering and coding systems will enhance interoperability between CBDCs and other digital currencies. Adopting international standards related to secure data transmission will help ensure the reliability of CBDC.

Interoperability and reliability are particularly important when CBDCs are designed to be used for cross-border payments. In recent years, with developments such as the globalization of the economy and the emergence of global stablecoin initiatives, there has been a growing need for more convenient and cheaper cross-border payments. FSB, CPMI, and G20 have engaged in various works to enhance cross-border payments. These works include exploring the potential role of CBDC to enhance cross-border payments, for example, with arrangements that enable the exchange of CBDCs issued by multiple jurisdictions.

The priority for central banks in considering CBDC will be to ensure and enhance the safety and efficiency of the domestic payment system. Many of the issues faced in cross-border payments would therefore be first addressed through improvements in existing payment systems. At the same time, as it is not always easy to overhaul the existing systems, there may be situations where arrangements using CBDC may emerge as a viable solution. In preparation for such a situation, it would be useful to consider how standardization may enhance interoperability and reliability to support safe and efficient cross-currency CBDC arrangements.

In promoting standardization, cooperation among private-sector entities that are inherently in a competitive relationship may be challenging. In the case of cooperation among central banks, such problems are rare. Seven major central banks including the Bank of Japan and the BIS have worked collaboratively and released a joint report in October 2020.[20] The joint report sets out some foundational principles for a central bank's consideration of CBDC issuance and identifies core features required of a CBDC to fulfill these principles. The joint report also suggests that the potential for cross-border interoperability should be considered by central banks from the outset of research on CBDC. The Bank takes such an approach in its ongoing research on understanding the practical issues and challenges related to CBDC, in cooperation with other central banks.

As an increasing number of countries explore CBDC, it is important that major central banks take the lead in global discussions on CBDC, both on the technological and theoretical fronts. Presenting ideas on the appropriate design of CBDC and possible areas of standardization related to CBDC may be one such step. Moreover, as each of the major central banks takes steps to ensure interoperability in CBDC design based on the common understanding gained through the discussions, any future plan by the Bank to issue CBDC will benefit from added value through enhanced network effects that would not be achieved by a closed arrangement.

Going forward, the outcome of central bank discussions on cross-border interoperability of CBDC may be incorporated into international standards developed by the ISO or other

[20] The Bank of Canada, European Central Bank, Bank of Japan, Sveriges Riksbank, Swiss National Bank, Bank of England, Board of Governors of the Federal Reserve System, and Bank for International Settlements, "Central Bank Digital Currencies: Foundational Principles and Core Features," October 2020.

organizations. ISO/TC 68 has recently formed a new group (ISO/TC 68/AG 5) to conduct research on digital currencies including CBDC. The Bank will continue to actively participate in the work of ISO/TC 68, including participation in ISO/TC 68/AG 5, with a view to ensuring that efforts to develop international standards related to CBDCs proceed in a way that appropriately addresses issues relevant to Japan. The Bank will also continue to be attentive to the efforts by other central banks related to standardization.

As mentioned earlier, CBDC design will also need to support interoperability with domestic payment systems. In a world where private-sector entities provide a variety of payment services to the general public by using CBDC as a payment instrument, CBDC would function as a means of payment that addresses the needs of the digital society and is distinct from cash and central bank deposits. If such services were to include a seamless cross-border payment functionality, interaction mechanisms with domestic systems would also need to take into account international standards. The Bank therefore believes that international harmonization should also be addressed when discussing interoperability between CBDC and domestic payment arrangements.

Section II described that the international standard-setting process for digital currencies would have the benefit of bringing together expertise, both domestically and internationally, and facilitating widespread adoption of superior technologies. Understanding existing international standards and developments in standard-setting activities is one efficient way to collect information and insights that contribute to the selection of underlying technology and system design related to digital currencies. It is also important that stakeholders involved in research and development of digital currencies actively participate in the international standard-setting efforts so that promising domestic technology may be applied to digital currencies around the world.

This approach is applicable to CBDC as well. In July 2020, the Bank moved the secretariat function of the ISO/TC 68 National Member Body from its Institute for Monetary and Economic Studies to its Payment and Settlement Systems Department. This is a reflection of the Bank's commitment to enhancing Japan's payment and settlement systems, potentially including CBDC, by creating synergies between research and analysis related to international standards and policy planning related to payment and settlement systems. Needless to say, the development of payment and settlement systems is not something that can be pursued by

the central bank alone; cooperation and collaboration with a wide range of stakeholders is essential. The Bank will provide the necessary support through ISO/TC 68 and other activities to encourage private-sector entities and experts to actively participate in standardization efforts related to CBDC and take part in cutting-edge discussions. The Bank believes that these efforts will lead to Japan's excellent technologies becoming an important part of international standards and being broadly adopted overseas.

BOX: International standardization process at ISO/TC 68

Organizations that develop international standards, including those for the financial services sector, include the International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), and International Telecommunication Union (ITU) (Figure 14). These organizations maintain a continuous collaborative relationship, for example by sending liaison members to each other's meetings, in order to avoid duplication and ensure consistency in international standards.

Figure 14: Major international standardization organizations

Organization	Overview
International Organization for Standardization (ISO)	Non-profit organization founded in 1947 that develops international standards on various areas including machinery, chemicals, materials, construction, and services. The ISO Central Secretariat is located in Geneva, Switzerland.
International Electrotechnical Commission (IEC)	Non-profit organization founded in 1906 that develops international standards for infrastructure and international trade in electrical and electronic goods. The IEC Central Office is located in Geneva, Switzerland.
International Telecommunication Union (ITU)	Non-profit organization that develops international standards related to information and communication technologies. Other functions of the ITU include developing international agreements, improving access to telecommunication technologies, and managing the radio-frequency spectrum. The ITU is one of the United Nations specialized agencies, and was established in 1932 with the merger of the International Telegraph Union, founded in 1865, and the International Radiotelegraph Union, founded in 1906. The ITU General Secretariat is located in Geneva, Switzerland.

This box provides an overview of the procedures for developing international standards at the ISO, with a focus on ISO/TC 68, for which the Bank's Payment and Settlement Systems Department serves as the secretariat of the National Member Body.

The ISO's standard-setting procedures are defined in ISO Directives, which consist of the

following six stages leading to the finalization (publication) of an international standard.[21] Documents that are at draft stages (1) to (5) are indicated with a stage abbreviation such as "ISO/WD" or "ISO/CD." This notation is also used throughout this paper when referring to standards at a draft stage.

(1) Proposal stage: new work item proposal (NP)

A NP is made for a new standard or a new part of an existing standard. Proposals may be made, for example, by a National Member Body, or the secretariat of that technical committee (TC) or a subcommittee (SC).

(2) Working stage: preparation of a working draft (WD)

After approval of the proposal, the secretariat of the TC/SC sets up a working group (WG) for preparing a WD, and appoints experts to work on the WD in consultation with P-members (P-members are expected to participate actively in the work, with an obligation to vote on all questions formally submitted for voting within the TC/SC, and to contribute to meetings).

(3) Committee stage: preparation and voting on the committee draft (CD)

Once the WD is registered as a CD, it is sent to the P-members of the TC/SC for comments. The CD is accepted for the following enquiry stage when a consensus is reached in a TC/SC, or when it is approved by a two-thirds majority of the P-members.

(4) Enquiry stage: enquiry and voting on draft international standard (DIS)

The registered DIS is sent to all member countries for enquiry and voting. An enquiry draft is approved if a two-thirds majority of the votes cast by the P-members of the TC/SC are in favor, and not more than one-quarter of the total number of votes cast are negative. When the approval criteria are met but technical changes are to be included, the modified draft is registered as a final draft international standard (FDIS). When no technical changes are to be included, the chair of TC/SC may proceed directly to publication, which is the case for many of the standards developed at TC 68.

[21] In addition to the International Standards (IS) finalized based on these procedures, the ISO also publishes "technical specifications (TS)," which summarize items that may be agreed to as IS in the future but cannot be published immediately as the technology to be standardized is still under development, and "technical reports (TR)," which contain collected data and other information but are not normative in nature.

(5) Approval stage: voting on final draft international standard (FDIS)

The registered FDIS is distributed by the ISO Central Secretariat to all member countries for voting. A FDIS is approved if a two-thirds majority of the votes cast by the P-members of the TC/SC are in favor, and not more than one-quarter of the total number of votes cast are negative.

(6) Publication Stage: publication of the international standard (IS)

The approved draft is officially published as an international standard.

The ISO Directives state that an International Standard shall be published within 36 months of the approval of a NP. Especially in the case of new standards, it is rare that the period from NP submission to IS publication is substantially less than 36 months. Furthermore, in many cases, an Ad Hoc Group (AHG) or a Study Group (SG) is set up and substantial consideration of the draft standard takes place over a period of years before a NP is submitted. Therefore, in practice, it takes several years at the earliest to develop a new international standard, usually longer than five years.[22]

[22] The ISO has introduced a Fast-Track Procedure, which allows for the publication of IS in 18 months, in order to respond to the growing speed of technological innovation. This procedure, however, can be applied only under certain conditions such as existing standards developed by other organizations.