

A Field Guide to Extending Settlement Capabilities

November 2026

Disclaimer

This publication provides general information on industry implementation approaches for digital money arrangements. It is descriptive in nature and does not constitute legislation, regulation, regulatory guidance, supervisory expectations, legal or financial advice, or other professional advice.

The framework, archetypes and examples presented in this publication are based on observed industry arrangements and implementation experience. They are intended to provide practical reference points, are not exhaustive, and do not constitute endorsement by the Monetary Authority of Singapore of any form of money, settlement asset, issuer model, infrastructure, technology provider, interoperability mechanism, control architecture or commercial arrangement.

References to organisations, projects, products and implementations are included for illustrative purposes and do not imply approval, recommendation or assurance by the Monetary Authority of Singapore or BLOOM. Legal and regulatory characterisations, implementation arrangements and participant roles should be understood in the context of the specific examples described.

Institutions remain responsible for determining and complying with the laws, regulations, supervisory requirements, contractual arrangements, institutional policies, and risk management requirements applicable to their activities, and should obtain independent legal or other professional advice where appropriate. Participating institutions remain responsible for the decisions, controls, exceptions, escalation, records and remediation associated with their respective roles.

Document Version

Version	Date	Rationale
1.0	19 November 2026	First publication

Contents

1 Introduction 5
2 The BLOOM Framework 7
3 Settlement Structures 13
4 Connectivity 19
5 Controls 26
6 Implementation 33
7 Industry Case Studies 37
8 Priorities and Next Steps 43
Acknowledgements 46
BLOOM Implementation Profile 47
Glossary 54
Sources and Further Reading 57

1 Introduction

Digital money arrangements increasingly span multiple issuers, infrastructures, forms of value and jurisdictions. As these arrangements become more interconnected, institutions will need to address recurring implementation questions around acceptance, conversion, redemption, liquidity, settlement, information exchange, controls and responsibility. A consistent way of describing and analysing these arrangements can help institutions identify how these elements come together across an end-to-end transaction.

1.1 Background and Motivation

As participation and use cases expand, similar implementation questions arise across different combinations of institutions, infrastructures and forms of digital money[1]. Where arrangements are developed through separate bilateral connections and institution-specific arrangements, integration requirements can accumulate and common problems may need to be addressed repeatedly.

A common framework provides a consistent way to describe these arrangements, identify the functions and connections required across an end-to-end transaction, and organise implementation considerations that recur across different use cases.

In this Field Guide, a "**digital money arrangement**" refers to the combination of participants, functions, infrastructure, forms of value, settlement mechanisms, information flows and controls involved in completing an end-to-end transaction. The arrangement is distinct from the particular form of digital money used within it. The same form of digital money may be used across different arrangements, while a single arrangement may involve multiple forms of digital money.

BLOOM, which stands for Borderless, Liquid, Open, Online, Multi-currency, is a public-private sector collaborative initiative established by the Monetary Authority of Singapore[2] to advance the use of digital money and extend the settlement capabilities offered by financial institutions. It covers domestic and cross-border arrangements involving different forms of digital money and multiple currencies, including arrangements designed to use tokenised deposits and regulated stablecoins. Its use cases include treasury management, trade finance and agent-initiated transactions.

Practical implementations through BLOOM provide a basis for identifying recurring features across these arrangements. These features form the basis of the BLOOM Framework, which provides a common structure for describing and analysing how digital money arrangements operate across different institutional, technical and jurisdictional settings.

1.2 Purpose and Scope

The Field Guide sets out the BLOOM Framework as a common framework and vocabulary for understanding and implementing digital money arrangements. It maps the functions required across an end-to-end transaction, describes recurring settlement structures, examines how institutions and infrastructures connect, and sets out the controls that operate across an arrangement. Together,

[1] Monetary Authority of Singapore, *Orchid Blueprint*, November 2023. The Orchid Blueprint identifies regulated stablecoins, tokenised deposits and central bank digital currencies as forms of digital money.
[2] Monetary Authority of Singapore, *MAS Launches BLOOM Initiative to Extend Settlement Capabilities*, October 2025.

these dimensions provide a structured way to understand how different elements of a digital money arrangement interact in practice.

The BLOOM Framework focuses on functional and implementation features rather than determining the legal or regulatory characterisation of the instruments used. Examples drawn from industry implementations illustrate how these elements can be combined in practice.

The Field Guide is intended for practitioners across banking, payments, treasury, market infrastructure, digital assets, risk, compliance and public policy.

The Field Guide describes approaches observed through industry implementation. It accommodates different settlement assets, infrastructures, use cases and stages of implementation. References to particular forms of digital money describe their intended design or role in the relevant arrangement and do not, by themselves, indicate that an instrument has been assessed as meeting all applicable legal or regulatory characteristics of that form of money. Each implementation remains subject to applicable jurisdictional requirements, institutional policies, contractual arrangements and risk appetite.

CHAPTER 2

2 The BLOOM Framework

Digital money arrangements can combine different institutions, forms of digital money, infrastructures and jurisdictions within a single transaction[3]. Understanding such an arrangement therefore requires more than identifying the technology or settlement asset being used. It requires an end-to-end view of what happens, how value and obligations are structured, how participating environments connect, and what information, rules and decisions govern the transaction.

The BLOOM Framework describes the digital money arrangement through four related aspects: Functions, Structure, Connectivity and Controls.

- **Functions** describe the activities performed across the transaction.
- **Structure** describes the forms of value and obligations involved, how they are transferred or discharged, and where settlement and finality occur.
- **Connectivity** describes how institutions, infrastructures, forms of digital money and jurisdictions interact across the arrangement.
- **Controls** describe the information, rules and decisions that determine whether and how the transaction progresses.

These aspects are analytically distinct but operate together when implementing a digital money arrangement. A connectivity mechanism, for example, may coordinate a transaction without itself providing settlement; an infrastructure may record a transfer without determining the legal nature of the underlying claim; and technical completion may occur separately from discharge of an obligation or legal finality.

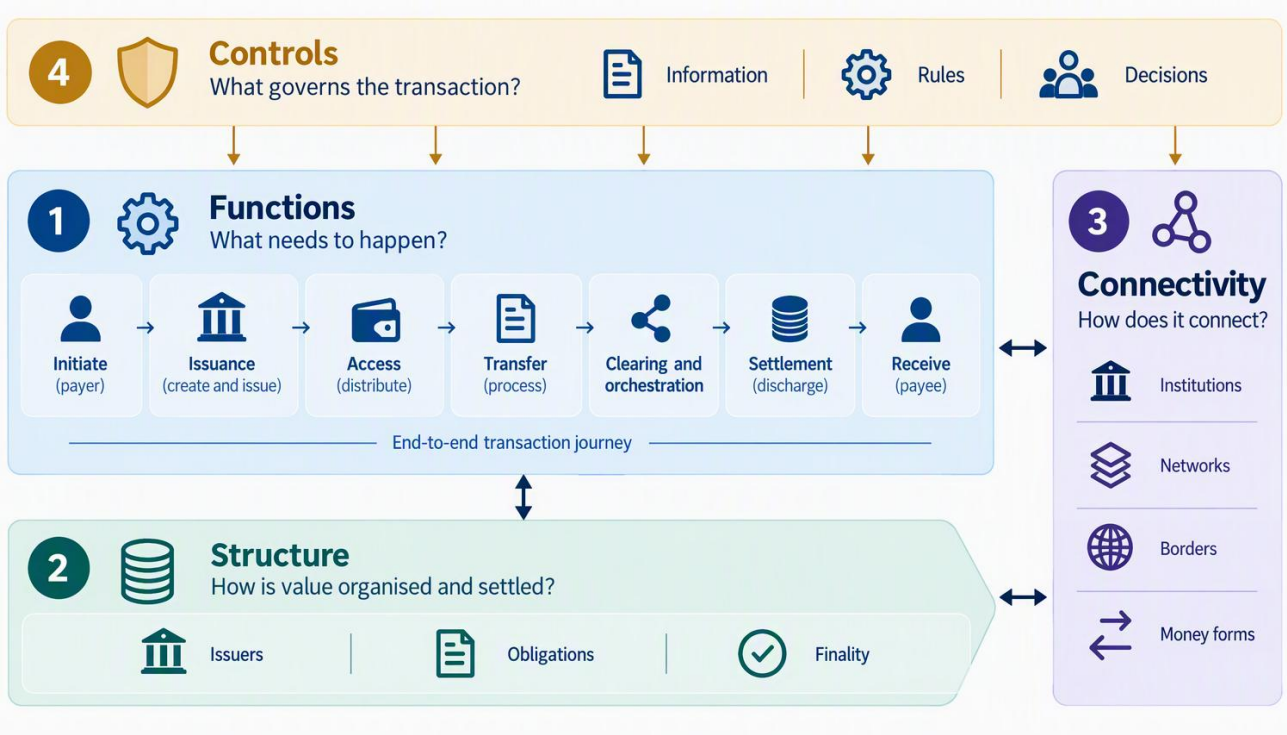


Figure 1: The BLOOM Framework: Functions, Structure, Connectivity and Controls.

[3] Adapted from Bank for International Settlements and Committee on Payments and Market Infrastructures, *Tokenisation in the Context of Money and Other Assets: Concepts and Implications for Central Banks*, October 2024.

The framework begins with the end-to-end transaction journey. Across that journey, the analysis traces the movement of value and information, the creation and discharge of obligations, and the decisions that govern transaction progression. It also identifies the participant responsible for each function, the relevant authoritative records, and the events that establish completion.

The following chapters apply the other aspects of the framework to the end-to-end transaction journey. Chapters 3, 4 and 5 examine Structure, Connectivity and Controls respectively. Chapter 6 brings the four aspects together with the operating arrangements and design considerations as an implementation profile.

2.1 Define the Transaction Context and Participants

The functional analysis begins with the transaction being supported and its intended outcome. Defining this context establishes the boundary within which functions, dependencies and responsibilities can subsequently be mapped.

- **Transaction context.** Record the intended transaction, transacting parties, use case, currencies, jurisdictions, forms of digital money or assets involved, operating window and relevant boundaries of the arrangement. This provides the scope for mapping the functions across the end-to-end transaction.
- **Participants.** Identify the legal entities and service providers involved and the functions they perform. These may include issuers, distributors, account or wallet providers, originating and receiving institutions, settlement institutions, custodians, liquidity and conversion providers, infrastructure operators, orchestrators, and information or credential providers.

Participants and functions are recorded separately. One participant may perform several functions, while one function may involve several participants or shared services. The nature of an entity does not therefore determine its function within the transaction.

2.2 Map Functions Across the End-to-End Transaction

The functional view identifies what must occur for the transaction to progress from initiation to completion. Depending on the arrangement, this may include initiation, issuance, distribution and access, transfer, clearing, orchestration, settlement and recipient access or redemption.



Figure 2: Functional roles across an end-to-end digital money arrangement

For each relevant function, the arrangement accounts for:

- the participant performing the transaction;
- the form of digital money, asset or obligation involved;
- the information required and produced;
- the authoritative record;
- relevant decision or control points;
- dependencies on other functions or participants; and
- the event that establishes completion of the function.

Mapping out the functional journey allows different institutional and technical arrangements to be compared without assuming that the same function must be performed by the same type of participant or infrastructure.

2.2.1 Issuance

Issuance creates the digital money and records the corresponding liability, reserve or backing arrangement. The arrangement identifies the issuer, legal claim, denomination, holder eligibility, authoritative record, issuance and redemption terms, custody where relevant, and controls governing creation and extinguishment.

2.2.2 Distribution and Access

Distribution and access establish how institutional or end users obtain, hold and use the money through accounts, wallets, custody, on-ramps and off-ramps, onboarding, permissions and servicing. Distribution may be performed by the issuer or by service providers (which can include regulated financial service providers and technology providers).

2.2.3 Transfer

Transfer records or effects a movement of value or an instruction to move value between participants or environments. The arrangement identifies the asset or liability involved, originating and receiving parties, relevant records, transaction information and the event establishing the completion of the transfer.

2.2.4 Clearing and Orchestration

Clearing and orchestration coordinates transaction progression across participants or transaction legs. Functions include routing transactions, matching or calculating obligations where applicable, coordinating transaction state, sequencing transaction legs, validating conditions such as funding status, managing timeouts and exceptions, triggering settlement and supporting reconciliation. The arrangement takes into account the coordinating service (or logic) and the authority attached to it.

The coordinating function is distinguished from the settlement mechanism. An orchestrator may coordinate or initiate settlement without itself providing the asset or infrastructure through which the resulting obligation is discharged.

2.2.5 Settlement

Settlement effects or records the authoritative transfer through which the relevant financial obligation is discharged. The arrangement identifies the settlement instruction, settlement asset, settlement institution or venue, and the relevant completion and finality events.

Technical completion, participant confirmation, discharge of a financial obligation and legal finality may occur at different points in an arrangement. These events should therefore be identified separately where relevant rather than treated as a single settlement event.

2.3 Trace Value, Information, Obligations and Decisions

The functional journey features four related, but distinct flows:

- **Value** identifies the money or assets created, held, transferred, converted, redeemed or used for settlement.
- **Information** identifies the instructions, identity or credential information, transaction data, confirmations and other information required across the transaction.
- **Obligations** identify financial claims arising between participants, and how and where those obligations are discharged.
- **Decisions** identify the rules, evaluations, approvals, restrictions or interventions that determine whether and how the transaction progresses.

Tracing these flows helps distinguish functions and activities that may occur together technically, but perform different roles within the arrangement. Movement of information does not itself establish movement of value; coordination of transaction state does not itself establish settlement; and technical execution does not by itself establish legal finality.

2.4 Identify Authoritative Records and Completion Events

Different stages of a digital money arrangement may rely on different records to determine the authoritative state of a transaction, asset or obligation. Hence, it is necessary to identify the **authoritative record** associated with each function.

This may include records of issuance and outstanding liabilities, customer holdings, transaction state, cross-institution obligations, settlement, redemption or legal ownership.

The arrangement should also identify the relevant **completion events**. Where applicable, these should distinguish technical execution, confirmation to participants, discharge of the financial obligation, and legal finality.

In doing so, arrangements that span across several infrastructures can be analysed without assuming that the infrastructure on which a transaction is technically executed necessarily determines settlement or legal completion.

2.5 Information and Controls Across the Functions

Information and controls operate across the functional journey. They include identity and credentials, transaction information and messaging, screening, policy evaluation, decision states, restrictions, administrative actions, exception handling and evidence.

For each relevant control point, the arrangement identifies the information required, its source, the applicable rule or policy, the party performing the evaluation, the institution responsible for the decision, the resulting transaction state and the evidence retained.

Chapter 5 examines Controls in greater depth, including the application of programmable compliance concepts to digital money arrangements.

2.6 Supporting Infrastructure and Connectivity

Functions may be performed across institutional systems, payment and market infrastructures, blockchains or distributed ledgers, gateways, bridges and shared services.

Infrastructure is recorded according to the function it performs and the authoritative record it maintains for that function, rather than treating a particular technology as determining the nature of the arrangement. A blockchain or DLT network is therefore an infrastructure choice[4] within the arrangement; the underlying legal claim, institutional responsibility and settlement structure are identified separately.

Where a transaction crosses environments, the framework identifies the interfaces through which information, instructions or value is transferred, and the mechanism through which the relevant activities are coordinated. Chapter 4 examines Connectivity in greater depth.

2.7 Operating the Arrangement

Functions, Structure, Connectivity and Controls describe how the transaction operates. Operating arrangements identify what is required to sustain those functions across participating institutions. These arrangements support the operation of the framework. They remain relevant where several functions are provided through a common infrastructure or service.

Operating area	What the arrangement records
Participation and rulebooks	Eligibility, onboarding, rights, obligations, transaction scope, finality, operating hours, service levels, sanctions, suspension and exit.
Governance and decision rights	Ownership, participant representation, policy ownership, technical and rule changes, emergency action, escalation and disputes.
Risk, liability and assurance	Allocation of loss, recourse, indemnities, assurance, evidence, audit rights and remediation.
Resilience and recovery	Redundancy, fallback, substitution, recovery, incident communication and post-recovery reconciliation.
Commercial operation	Service ownership, customer proposition, pricing, fees, cost allocation, liquidity and integration costs, support and expansion.

2.8 Apply Design Considerations

The appropriate design of an arrangement depends on its intended transaction and operating context. The BLOOM Framework therefore applies a set of design considerations across the four aspects.

Relevant design considerations include:

Design consideration	What the framework records
Finality and certainty	Technical completion, legal finality, discharge of obligations, authoritative records and evidence of completion.
Acceptance, reach and convertibility	Eligible users, participating institutions, jurisdictional reach, receiver acceptance, conversion and redemption.
Liquidity and efficiency	Funding availability, prefunding, rebalancing, conversion

[4] Bank for International Settlements, *Blueprint for the Future Monetary System: Improving the Old, Enabling the New*, Annual Economic Report 2023.

	capacity, working-capital implications, fees and operating costs.
Speed and availability	Processing time, operating windows, service availability and completion under normal and degraded conditions.
Interoperability and coordination	Connectivity across institutions and networks, information exchange, state coordination and synchronisation across legs.
Privacy and transparency	Controlled disclosure, confidentiality, traceability, access to information and evidentiary records.
Resilience	Exception handling, fallback, recovery, substitution and continuity during disruption.
Scalability	Ability to add transaction volume, participants, infrastructures, assets, use cases or jurisdictions.

These design considerations help identify dependencies and trade-offs between different design choices, and should be assessed against the intended use case, operating conditions and responsibilities of participating institutions.

2.9 From Framework to Implementation

Applying the BLOOM Framework produces a structured method to implement digital money arrangements, bringing together:

1. the transaction context and participants;
2. the end-to-end functional journey;
3. the forms of digital money, assets and obligations involved;
4. authoritative records and completion events;
5. settlement structure;
6. connections between participating environments;
7. information, controls and decision responsibility;
8. operating arrangements and dependencies; and
9. implementation evidence and unresolved issues.

This provides a consistent method for determining how an arrangement works, where its critical dependencies lie, who is responsible at each point and what evidence demonstrates that the intended transaction can complete under defined operating conditions.

The functional view establishes what happens across an end-to-end transaction. The same functional journey can operate through different settlement structures depending on the liabilities used, the issuers involved, how those liabilities move between participants and how resulting obligations are discharged. Chapter 3 examines three recurring settlement structures and the different ways in which these functions can be organised to achieve settlement.

CHAPTER 3

3 Settlement Structures

Digital money arrangements can involve different issuer liabilities and different mechanisms for discharging the financial obligations arising between participants. Understanding settlement therefore requires more than identifying the digital money or infrastructure used in a transaction. The analysis distinguishes the liabilities through which participants transact, the obligations arising between institutions, the asset and mechanism used to discharge those obligations, and the point at which settlement becomes final.

The BLOOM Framework applies the settlement analysis in two stages.

First, it identifies the **issuer-liability structure** underlying the transaction. Three recurring structures are observed:

1. **Common Issuer**
2. **Multiple Issuers under Common Rules**
3. **Interconnected Issuer Arrangements**

Second, it identifies **how any resulting settlement obligation is discharged**, including the settlement asset, institution or venue, authoritative record and finality event.

Separating these questions distinguishes the money used by participants from the mechanism through which obligations between institutions are ultimately settled[5].

[5] Bank for International Settlements, *Wholesale Central Bank Money in the Context of Technological Innovation*, September 2025; Tobias Adrian, *Tokenized Finance*, IMF Note 2026/001, International Monetary Fund, April 2026.

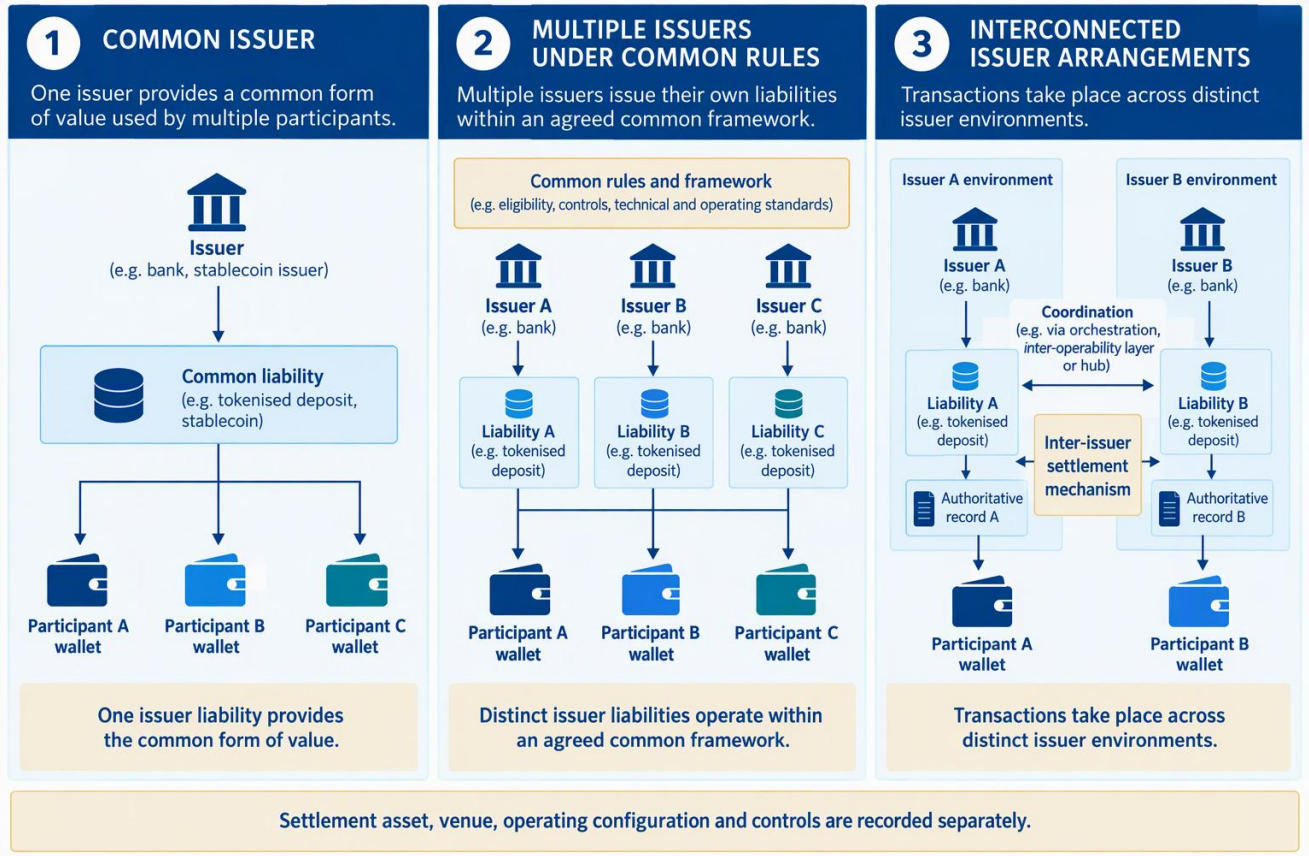


Figure 3: Three recurring issuer-liability structures

3.1 Classify and Compare the Settlement Structures

The classification follows the legal issuer and settlement structure. Ownership, technical standards and shared infrastructure do not by themselves determine the archetype. The inter-issuer settlement mechanism is also recorded separately. A multi-issuer arrangement may use central bank money, commercial bank money, another accepted settlement asset[6] or coordinated settlement through existing infrastructure.

Dimension	Type 1: Common Issuer	Type 2: Multiple Issuers under Common Rules	Type 3: Interconnected Issuer Arrangements
Issuers	One legal issuer	Multiple legal issuers	Multiple legal issuers
Participant-facing liabilities	Common issuer liability	Distinct issuer liabilities	Distinct issuer liabilities
Relationship between issuers	Not applicable	Liabilities operate under an agreed common framework	Issuer arrangements remain independently governed
Basis for interoperability	Common liability	Common rules governing operation of distinct liabilities	Connection between otherwise independent environments

[6] Bank for International Settlements, *Wholesale Central Bank Money in the Context of Technological Innovation*, September 2025; Bank for International Settlements, *The Next-Generation Monetary and Financial System*, Annual Economic Report 2025.

Inter-issuer obligations	Not inherent to use of the common liability	Determined in accordance with the common framework	Arise where transactions cross issuer environments
Settlement mechanism	Recorded separately where applicable	Recorded separately	Recorded separately
Defining pattern	Participants transact using a liability issued by the same legal issuer.	Distinct issuer liabilities operate within an agreed common framework.	Transactions take place across distinct issuer environments, with value, information and settlement obligations handled across them.

These structures classify the relationship between the issuer liabilities involved in the arrangement. They do not prescribe the infrastructure through which transactions occur or the asset and venue through which resulting obligations are settled.

A single arrangement may contain more than one structure across different transaction legs. Where an arrangement does not fit these structures, it should be described on its own terms rather than forced into the nearest category.

3.2 Type 1: Common Issuer

Participants use and accept a form of money issued by the same legal issuer. The issuer liability provides the common form of value across the relevant transaction. Depending on the nature and form of the digital money, transfers may occur across different users, wallets, service providers or distribution channels while the underlying issuer liability remains the same. Particular attention should be given to the nature of the issuer liability, who may hold and use it, where the authoritative record is maintained, the conditions for transfer and acceptance, and how issuance, redemption and completion are effected.

- **Defining feature.** One legal issuer liability provides the common form of value. The issuer may be a bank, bank-group entity, non-bank entity or dedicated issuing entity established by a consortium. Consortium ownership does not make the arrangement multi-issuer since one legal entity issues the liability.
- **Settlement.** Settlement occurs through the transfer, redemption or other discharge of the common issuer liability in accordance with the rules of the arrangement.
- **Arrangement record.** Record the issuer and nature of the liability, eligible holders and participants, issuance and redemption arrangements, acceptance conditions, authoritative record, transfer mechanism, custody or wallet arrangements, conversion and settlement and completion events.

3.3 Type 2: Multiple Issuers under Common Rules

Different institutions issue their own liabilities within an agreed framework enabling those liabilities to operate within the same arrangement. The liabilities remain attributable to their respective issuers. Particular attention should be given to the common rules governing participating issuers and liabilities, the degree of standardisation between them, acceptance and conversion between issuer liabilities, and the mechanism for creating and discharging inter-issuer obligations.

- **Defining feature.** Distinct issuer liabilities operate under common rules or shared arrangements rather than being replaced by a single issuer liability. Common elements may cover participation, instrument characteristics, technical interfaces, messaging, acceptance, controls, conversion, redemption and inter-issuer settlement.
- **Settlement.** The common arrangement establishes how obligations between participating issuers are determined and discharged when their respective liabilities are used within the arrangement. The settlement asset, venue and process form part of, or operate in accordance with, the agreed common framework.
- **Arrangement record.** Record participating issuers and liabilities, eligibility, instrument characteristics, issuance and redemption, acceptance, standards, transfer and conversion processes, information requirements, operating responsibilities and the mechanism for settling obligations between issuers.

3.4 Type 3: Interconnected Issuer Arrangement

Different institutions maintain separate issuer arrangements, including their own liabilities, rules, customer relationships and authoritative environments. A separate interoperability or settlement arrangement enables transactions to occur across those environments without bringing the underlying liabilities under common issuance and operating rules.

- **Difference from Type 2.** Type 2 applies where distinct issuer liabilities operate within an agreed common framework. Type 3 applies more broadly where distinct issuer environments are connected without requiring that level of common issuance and operating rules.
- **Defining feature.** The issuer arrangements remain independently governed. A Type 3 arrangement establishes how transactions crossing from one issuer environment to another are recognised, processed and settled.
- **Settlement.** Each issuer environment remains independently governed. Where a transaction crosses issuer environments, the interconnection must determine the resulting obligations between institutions and how those obligations are discharged. The settlement mechanism may operate separately from the issuer environments and use central bank money, commercial bank money, another accepted settlement asset or existing settlement infrastructure.
- **Arrangement record.** Record each issuer, liability and authoritative environment; customer and institutional relationships; acceptance, transfer, conversion and redemption; information exchanged; creation and discharge of settlement obligations; settlement asset, venue and finality mechanism; liquidity and funding; confirmation; reconciliation; exceptions and recovery.

3.5 Identify the Settlement Mechanism

The issuer-liability structure does not by itself determine how resulting financial obligations are settled. For each material settlement obligation, the arrangement records:

Component	Description
Obligation	The financial obligation being discharged
Settlement asset	The money or asset used to discharge it
Settlement institution / venue	Where the settlement asset is held and transferred

Settlement mechanism	How settlement is initiated and effected
Authoritative record	The record evidencing the transfer or discharge
Coordination mechanism	Where a separate service coordinates transaction activity with settlement
Liquidity arrangements	Including funding, prefunding and rebalancing where applicable
Finality event	The event at which settlement becomes final

Settlement may occur on infrastructure different from that on which the underlying transaction is executed. A bridge, orchestrator or other coordination mechanism may relay instructions or coordinate transaction states without itself providing the settlement asset or establishing legal finality.

The settlement mechanism should therefore be identified according to the function it performs rather than the technology through which it operates.

3.6 Completion, Discharge and Finality

A digital money arrangement may involve several distinct completion events.

Technical execution identifies when the relevant technical process or ledger update has completed.

Participant confirmation identifies when the transaction is communicated to a participant as completed.

Discharge identifies when the relevant financial obligation between participants has been satisfied.

Legal finality identifies the point at which settlement becomes irrevocable and unconditional under the applicable legal and contractual framework[7].

These events may occur at different times and may rely on different authoritative records. They should therefore be identified separately where relevant.

This distinction is particularly important where a transaction spans multiple infrastructures or where the participant-facing transfer, inter-institution settlement and legal record of ownership occur in different environments.

3.7 Applying the Settlement Structures in Practice

Identifying the settlement structure provides a starting point for determining how and when a transaction becomes final. Different arrangements may establish technical completion, participant confirmation, discharge of the relevant financial obligation and legal finality at different points, potentially across different infrastructures and authoritative records. Participating institutions should therefore identify the finality arrangements appropriate to the intended use case, including the conditions under which a transaction may remain subject to reversal, cancellation or unwind after it appears to have completed.

The relevant completion and finality events should also be communicated clearly to participants and users. In particular, the arrangement should establish when value can be treated as irrevocably

[7] Committee on Payments and Settlement Systems and Technical Committee of IOSCO, *Principles for Financial Market Infrastructures*, April 2012, in particular Principle 8 on settlement finality.

received, which record evidences that outcome, and the risks and responsibilities that apply before legal finality is achieved[8].

The settlement structure does not, by itself, determine the arrangement's acceptance, conversion, redemption, information-exchange or connectivity features. These may affect whether and how the transaction can be completed, but should be analysed separately under the relevant aspects of the BLOOM Framework.

Taken together, the analysis establishes what value participants transact in, whose liabilities are involved, what obligations arise between institutions, how those obligations are discharged, and when the resulting settlement becomes final.

[8] See also Bank for International Settlements, *"The Sovereign Money Question: CBDCs, Stablecoins, and the Fight for the Settlement Layer"*, September 2026, discussing final settlement as the irrevocable and unconditional discharge of an obligation and the importance of distinguishing final settlement from preceding transaction events.

CHAPTER 4

4 Connectivity

The settlement structures in Chapter 3 describe the issuer liabilities involved in a transaction, the obligations arising between institutions, how those obligations are discharged and when settlement becomes final. This chapter addresses a separate question: **how the participating environments connect and interact so that the end-to-end transaction can be executed**.

Connectivity covers the interfaces, information flows, instructions, coordination mechanisms and operating arrangements that enable activity across institutional, infrastructural or jurisdictional boundaries[9]. It identifies what passes across each connection, which functions are performed at or through that connection, which records establish transaction state, and which participants are responsible for operating and managing it.

For this purpose, an **environment** may comprise an institution's systems, an issuer arrangement, a payment or market infrastructure, a blockchain or distributed ledger, a wallet or custody platform, or another service through which a transaction function is performed or an authoritative record is maintained.

The unit of analysis is the **connection between environments**. A single digital money arrangement may contain several connections, and different connectivity configurations may apply at different points in the transaction journey.

Connectivity and settlement are related but analytically distinct:

- **Connectivity** addresses how participating environments exchange information or instructions, coordinate transaction state(s) and, where applicable, transmit or make value available across the transaction journey.
- **Settlement** addresses what financial obligations arise, the asset and mechanism through which they are discharged, which record evidences settlement, and when settlement becomes final.

A connectivity mechanism may initiate, route or coordinate settlement without itself providing the settlement asset, maintaining the authoritative settlement record or establishing legal finality. The applicable settlement structure and finality events remain determined under Chapter 3.

4.1 Mapping Connections across the Transaction Journey

The connectivity analysis begins with the transaction journey defined in Chapter 2. It identifies each point at which the transaction crosses between participating environments.

For each material connection, the arrangement takes into account:

- the environments being connected;
- the participants responsible for those environments;
- the functions performed at or through the connection;
- the information, instructions or value passing across it;
- the interface, protocol, messaging arrangement or other connection mechanism used;

[9] Bank for International Settlements and Committee on Payments and Market Infrastructures, *Tokenisation in the Context of Money and Other Assets: Concepts and Implications for Central Banks*, October 2024; Committee on Payments and Market Infrastructures, *Linking Fast Payment Systems Across Borders: Governance and Oversight*, October 2024

- any service coordinating activity across the environments;
- the transaction states, acknowledgements and confirmations exchanged;
- the authoritative records maintained on either side of the connection;
- dependencies on participants, infrastructure, operating windows or external services;
- responsibility for operating, monitoring and changing the connection; and
- exception, reconciliation, fallback and recovery arrangements.

This analysis distinguishes the ability of environments to communicate or coordinate from the financial and legal effects of the underlying transaction. An instruction may be transmitted successfully even where settlement subsequently fails. Similarly, two environments may maintain consistent transaction states without either environment maintaining the record that establishes discharge or legal finality.

4.2 Cross-Institution Connectivity

Cross-institution connectivity enables institutions operating separate environments to transact with one another. Connections may support transaction initiation, validation and routing, information exchange, transaction state coordination, movement or conversion of value, confirmation and reconciliation.

The analysis identifies which functions remain within each institution's environment and which are performed through the connection or by another service. It also identifies the information and authority made available across the connection, including whether a receiving institution obtains an instruction, a transaction status, an attestation, a representation of value or access to an authoritative record.

Where the transaction creates obligations between institutions, the connectivity map identifies where settlement instructions are generated and transmitted. The nature and discharge of those obligations remain part of the settlement analysis in Chapter 3.

For a Type 3 *Interconnected Issuer Arrangement* under Chapter 3, connectivity describes how the independently governed issuer environments interact. It does not itself determine the settlement asset, venue or finality mechanism used to discharge obligations between the issuers.

4.3 Additional Considerations for Cross-Border Arrangements

Cross-border arrangements apply connectivity across jurisdictions and may involve multiple institutions, currencies, networks, legal frameworks and settlement infrastructures. The same connectivity analysis applies, but additional dependencies may arise from differences in operating hours, information requirements, currency arrangements, participant access and applicable controls[10].

The connectivity map should trace the relevant connections across the complete transaction journey. Depending on the use case, this may include:

Transaction leg	Involved parties	Connectivity considerations
Originating leg	Payer and originating institution	Initiation channel, source of funds, required information and originating record

[10] Committee on Payments and Market Infrastructures, *Moving on Up: Results of the 2024 Cross-Border Payments Monitoring Survey*, CPMI Brief No. 10, December 2025.

Funding and FX	Funding and conversion providers	Pricing, liquidity, instructions, confirmation and operating windows
Cross-border leg	Institutions, networks or partners across jurisdictions	Routing, information exchange, coordination, transaction state and dependencies
Receiving leg	Receiving institution and any conversion or redemption provider	Receipt, conversion, local processing and reconciliation
Beneficiary credit	Receiving institution and beneficiary	Credit, confirmation, availability and access to funds

For each leg, the analysis identifies the responsible participant, relevant environment, information and instructions exchanged, transaction state and completion event. It also identifies dependencies between the legs, including operating windows, funding and rebalancing, data and screening requirements, delayed or partial completion, returns, refunds, reconciliation and recovery.

The completion of one leg does not establish end-to-end completion where another leg remains outstanding. Where obligations arise between institutions, their discharge and legal finality are analysed separately under Chapter 3.

4.4 Observed Connectivity Configurations

Connectivity between participating environments can take a range of connectivity configurations. Four frequently observed configurations are **Direct**, **Orchestrated**, **Shared** and **Layered**.

These configurations describe how connectivity functions are allocated. They do not correspond to the settlement structures in Chapter 3 and do not determine the form of digital money, settlement asset, settlement venue or legal finality. An arrangement may combine more than one configuration, and the relevant configuration should be identified at the level of each material connection.

The configurations are not intended as mutually exclusive technical architectures. Rather, they provide a common vocabulary for describing observed operating patterns and the location of relevant connectivity functions.

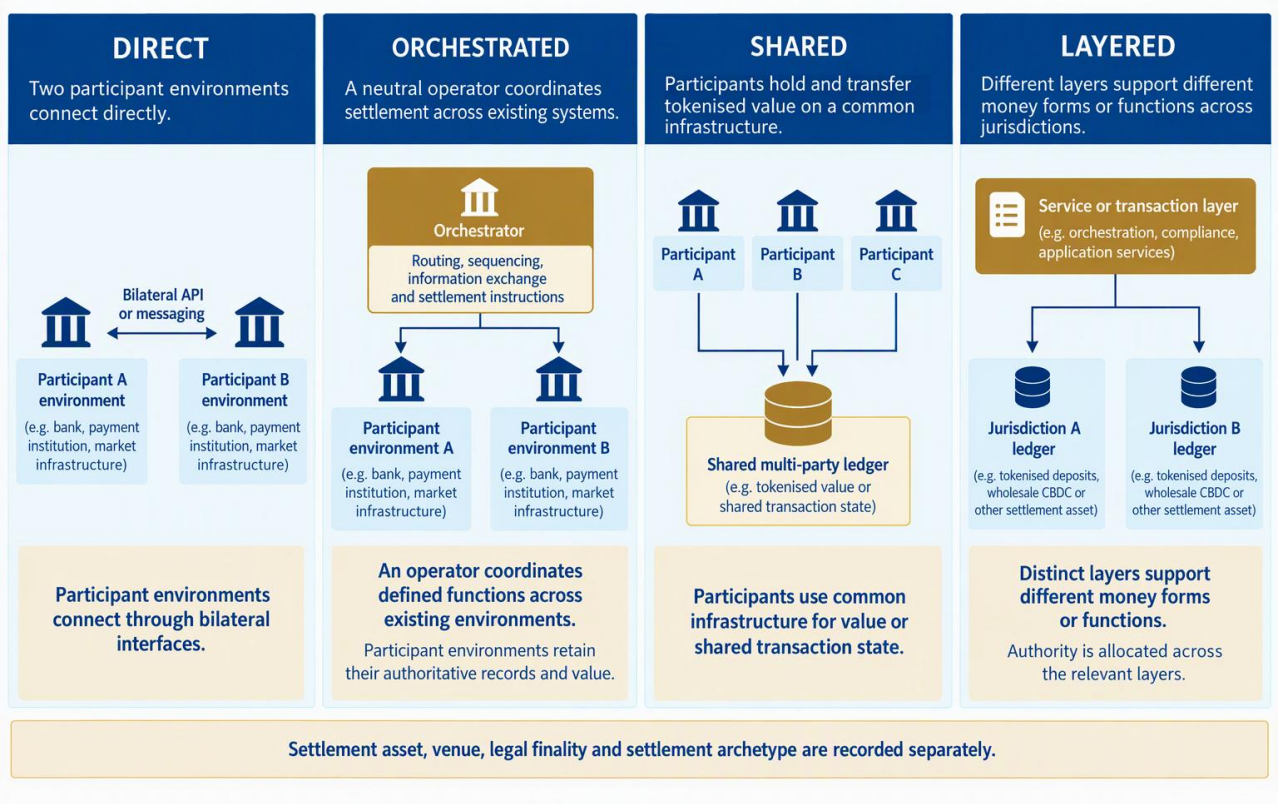


Figure 4: Four observed cross-institution and cross-border connectivity configurations

4.4.1 Direct

Under a direct configuration, participating environments connect through interfaces established between them. Each participant maintains its own environment and exchanges the required information, instructions or transaction states directly with another participating environment.

The connectivity map identifies:

- the environments connected;
- the interfaces and standards used;
- the information and instructions exchanged;
- any value represented or transmitted across the connection;
- the records maintained by each participant;
- the allocation of validation, confirmation and reconciliation functions; and
- responsibility for maintaining the bilateral connection and resolving failures.

Direct connectivity can preserve institutional control over each environment, but the number and complexity of interfaces may increase as additional participants, assets or networks are added.

4.4.2 Orchestrated

Under an orchestrated configuration, an operator, service or common coordinating layer manages specified activities across participating environments. These activities may include routing, sequencing, validation, matching, transaction-state coordination, information exchange, generation of settlement instructions, timeout management or confirmation.

The participating environments may continue to maintain the underlying customer relationships, liabilities, value and authoritative records. The orchestrator's role should therefore be identified according to the functions and authority assigned to it.

The connectivity map records:

- the functions performed by the orchestrator;
- the information and authority available to it;
- the transaction state that it maintains or communicates;
- how it interacts with participating environments;
- whether it initiates or coordinates settlement;
- which records remain authoritative for the underlying value and obligations; and
- arrangements for delay, inconsistency, unavailability, substitution and recovery.

An orchestrator may coordinate settlement without itself providing the settlement asset or maintaining the authoritative settlement record.

4.4.3 Shared

Under a shared configuration, participating institutions use shared infrastructure to perform one or more transaction functions or maintain shared transaction state. The infrastructure may receive and process instructions, coordinate transfers, facilitate an exchange of value, calculate obligations or support settlement between participants.

For this Field Guide, **shared infrastructure** means infrastructure used by more than one participating institution to perform specified functions. It does not necessarily imply a common issuer, common liability, common customer relationship or a single authoritative record for the complete arrangement.

The connectivity map identifies:

- the participants using the shared infrastructure;
- the functions performed through it;
- the assets, liabilities or transaction states represented;
- the records maintained on the shared infrastructure and those retained by participants;
- the authority of the infrastructure operator;
- connections to external institutional or settlement environments; and
- arrangements for access, change, suspension, recovery and exit.

Use of shared infrastructure does not itself determine whether the arrangement involves a common issuer, multiple issuers operating under common rules, or interconnected issuer arrangements. That classification is determined under Chapter 3.

4.4.4 Layered

Under a layered configuration, different environments or infrastructures perform distinct functions within the transaction journey. One layer may support customer access or transaction initiation, another may perform coordination or processing, while another provides the money, asset or infrastructure used for settlement.

The connectivity analysis identifies:

- the function performed by each layer;
- the participant responsible for it;
- the value, information and instructions exchanged between layers;
- the authoritative record maintained at each layer;
- the event that triggers progression to the next layer;
- the dependencies between layers; and
- the treatment of inconsistent states, delay or failure.

A layered configuration should not be taken to mean that every layer has equal legal or operational significance. The analysis should distinguish, for example, an interface that transmits an instruction from an infrastructure that maintains the authoritative record of value or establishes settlement completion.

4.5 Combining Connectivity Configurations

An end-to-end arrangement may combine several configurations. This may arise where digital money operates across separate networks with different operating rules, messaging arrangements and authoritative records. Shared infrastructure may perform functions within one part of the arrangement, while an orchestrated or direct connection links it to another institutional or settlement environment. A layered arrangement may similarly contain direct interfaces or a coordinating service between individual layers.

Where multiple networks or infrastructures are involved, common connectivity services may provide participant or network discovery, routing, information exchange, transaction initiation, validation, sequencing or confirmation. Such services may reduce the need for separate bilateral integrations while allowing the connected environments to retain their respective functions and authoritative records.

The relevant configuration is therefore identified at the level of the connection. The arrangement as a whole should not be assigned a single configuration where doing so obscures material differences between its constituent connections.

4.6 Information, State and Completion across Connections

Connectivity requires participating environments to exchange sufficient information[11] to initiate, evaluate, process and confirm the transaction. Depending on the arrangement, this may include:

- participant and account or wallet identifiers;
- transaction instructions and references;
- currency, amount and payment-purpose information;
- identity attributes or attestations;
- screening or policy-evaluation outcomes;
- funding, conversion or settlement status;
- timestamps and transaction states;
- confirmations, rejections and exception messages; and
- reconciliation and recovery information.

The arrangement identifies the source, recipient, timing and permitted use of information exchanged across each connection. It should also distinguish the communication of information from the authority associated with that information. Receipt of an instruction, status or attestation does not by itself determine the recipient's legal, regulatory or risk responsibilities.

Where environments maintain related transaction states, the connectivity map identifies how those states are aligned and which record is authoritative for each function. It also specifies how the arrangement responds where one environment records completion while another records a pending, failed or inconsistent state.

[11] Committee on Payments and Market Infrastructures, *Harmonised ISO 20022 Data Requirements for Enhancing Cross-Border Payments*, updated February 2026.

Participant-facing confirmation should be distinguished from completion of an individual technical process, discharge of a financial obligation and legal finality. These events may occur at different points and may be evidenced by different records.

4.7 Responsibility, Resilience and Operation

The operating model assigns responsibility for functions performed across connected environments. Relevant roles may include issuers, originating and receiving institutions, settlement institutions, FX and liquidity providers, orchestrators, infrastructure operators, information providers, policy owners and assurance providers.

For each connection, the operating model identifies responsibility for:

- maintaining and securing the interface;
- supplying and validating information;
- routing and coordinating transactions;
- maintaining transaction state;
- generating and transmitting settlement instructions;
- monitoring availability and performance;
- confirming completion;
- reconciling records;
- resolving inconsistent or incomplete states; and
- managing exceptions, fallback and recovery.

Where connectivity depends on an orchestrator, shared service or network, the operating model should address the scope of the operator's authority, service levels, change control, access, liability, loss allocation, incident handling, suspension, substitution and exit.

Resilience should be assessed across the end-to-end transaction rather than only at the level of each component. The arrangement should account for unavailable connections, delayed messages, duplicate or out-of-sequence instructions, inconsistent transaction states, failed downstream legs and unavailable shared services.

Fallback arrangements should identify whether the transaction is held, rejected, rerouted, processed manually or returned, and which participant is authorised to make that decision. Recovery should include reconciliation of the relevant records and confirmation of the eventual transaction and settlement status.

4.8 From Connectivity to Controls

Applying the connectivity analysis produces a map of the environments involved, the connections between them, the functions performed at each connection, the information and instructions exchanged, the records maintained and the participants responsible for operating them.

This map provides the basis for identifying control points across the transaction journey. Each connection may introduce requirements relating to information quality, identity, access, screening, confidentiality, policy evaluation, transaction-state management, intervention, evidence and accountability.

Chapter 5 examines how these requirements are translated into controls, how the relevant capabilities are allocated across participating institutions and services, and how responsibility for each decision is retained and evidenced.

5 Controls

Controls begin with the legal, regulatory, contractual and institutional requirements applicable to the institution, activity, customer, asset, corridor and transaction. The implementation translates these requirements into controls applied at defined points in the transaction journey.

The approach to embedding controls in this chapter takes reference from the Global Layer One ("GL1")[12] Programmable Compliance model ("PC model")[13]. BLOOM applies this model across a defined end-to-end transaction journey, identifying where each capability operates, which participant is responsible for the relevant decision and what evidence is retained.

Participating institutions remain responsible for the legal, regulatory, risk and transaction obligations attached to their respective roles. The architecture supports the implementation of controls and the production of evidence demonstrating their operation; it does not determine the requirements applicable to an institution or transfer responsibility for meeting them.

5.1 Applicable Requirements

The legal, regulatory, supervisory, contractual and institutional requirements applicable to each participant and transaction leg are identified at the outset. The applicable requirements depend on the legal entity, regulated activity, service provided, customer relationship, form of digital money and jurisdictions involved. The Field Guide does not replace that assessment.

For Singapore-linked digital token activity, relevant starting points may include the Payment Services Act 2019 ("PS Act"), Financial Services and Markets Act 2022 ("FSMA") and requirements issued under both Acts. MAS Notice PSN-02 and FSM-N27 apply to licensees regulated under the PS Act and FSMA respectively and set out anti-money laundering and countering the financing of terrorism ("AML/CFT") requirements for those licensees. Banks and other regulated institutions should identify the requirements that apply under their respective regulatory frameworks.

Financial crime risk is an important area addressed through transaction controls. AML/CFT requirements form a central part of this framework and may cover customer and beneficial-owner identification, sanctions screening, originator and beneficiary information, transaction monitoring, escalation of unusual or suspicious activity and record keeping.

Other requirements beyond AML/CFT may also apply depending on the jurisdiction and transaction. These may include capital flow management or exchange-control measures, payment or value-transfer requirements, customer or investor eligibility, consumer protection, data protection and localisation, tax and regulatory reporting, and restrictions relating to payment purpose, amount, currency, corridor or recipient.

The **regulatory requirements register** provides the starting point for control design. It records the requirements relevant to each institution, activity, customer, asset, corridor and transaction type. For each requirement, the register identifies the source, scope, responsible institution, required

[12] GL1 is a multilateral industry initiative involving global financial institutions and policymakers and develops shared approaches intended to support interoperable digital financial activity.
[13] Global Layer One, *Programmable Compliance: Compliance Architecture for Regulated Tokenised Assets*, June 2026 ("GL1 PC paper").

information, decision or action, timing and evidencing requirement[14]. Relevant requirements captured in the register inform the policies, control parameters and evidencing arrangements applied across the transaction journey.

5.2 GL1 Programmable Compliance Model Architecture

Digital money transactions may cross institutions, wallets, infrastructures and jurisdictions while remaining subject to different legal, regulatory and institutional requirements. The information required for a decision may be held by different parties, and controls may operate at different points in the transaction journey. If policy, data and execution logic are tightly coupled, similar controls may need to be rebuilt for different assets, networks, corridors or use cases.

The GL1 PC model addresses this by separating the principal compliance capabilities. Policy rules and parameters can therefore be governed and updated without necessarily redesigning the underlying asset or transaction infrastructure. Individual capabilities may be operated by participating institutions, shared services or distributed components, while responsibility for the relevant decision remains with the institution to which that responsibility applies.

Figure 5 presents the GL1 PC reference architecture used in this chapter.

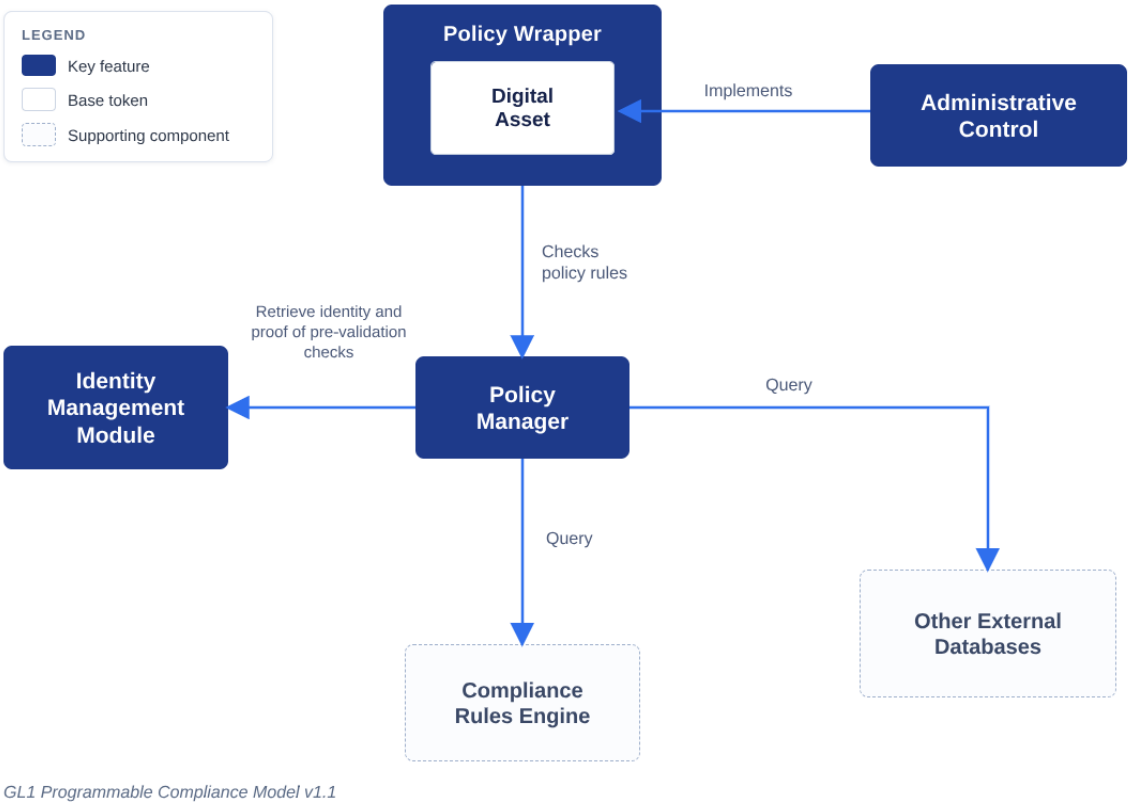


Figure 5: GL1 Programmable Compliance Model[15]

[14] The GL1 PC model uses the Status, Transaction, Asset and Reporting ("STAR") framework to classify compliance requirements relating respectively to participant eligibility, transaction conditions, asset-level controls, and reporting and auditability. This classification may be used to organise requirements in the regulatory requirements register where useful.

[15] Global Layer One, *Programmable Compliance: Compliance Architecture for Regulated Tokenised Assets,* June 2026, Figure 1. Reproduced with permission.

The GL1 PC model provides a reference architecture for translating regulatory and institutional requirements into controls that can operate across digital financial infrastructure. BLOOM uses this architecture as a reference for organising the control capabilities described in this chapter.

The model comprises the following principal capabilities.

- **Identity Management Module,** which links parties and relevant identifiers and makes the required identity attributes and attestations available for evaluation.
- **Policy Manager,** which identifies the policies applicable to a transaction and coordinates their evaluation.
- **Compliance Rules Engine,** which performs the computation required by the applicable policies.
- **Policy Wrapper,** which applies the resulting outcome at the transaction-execution boundary.
- **Administrative Control,** which provides a separate path for authorised asset-level intervention.
- **Compliance Attestation,** which records the outcome of the compliance evaluation for a particular transaction against the policy version and dependencies active at that time. It is distinct from identity credentials or attestations used as inputs and does not replace suspicious transaction reports, transaction reports or other statutory reporting obligations.

These capabilities need not operate on a single platform. Their allocation depends on the transaction, participating institutions and operating arrangement. The implementation should nevertheless identify the operator of each capability, the institution responsible for the relevant decision and the evidence retained.

5.3 Applying Controls across the Transaction Journey

BLOOM applies the GL1 PC model to a defined transaction journey. The journey identifies the parties, participating institutions, accounts or wallets, form of digital money, jurisdictions, transaction information, movement of value and settlement steps.

The regulatory requirements register is mapped to the points in the journey at which information is supplied, an evaluation is performed, a decision is applied, value moves or evidence is produced. Relevant requirements inform the policies and parameters managed through the Policy Manager and allocated to the appropriate control capabilities.

The resulting **control-capability map** identifies:

- the applicable requirement and policy;
- the relevant control capability;
- the operator of that capability;
- the institution responsible for the decision;
- the required inputs and outputs;
- the point in the transaction journey at which the capability operates; and
- the evidence retained.

Figure 6 places the capabilities described in the preceding section within the wider BLOOM transaction context, showing the relationship between applicable requirements, the transaction journey, control capabilities, decisions and evidence.

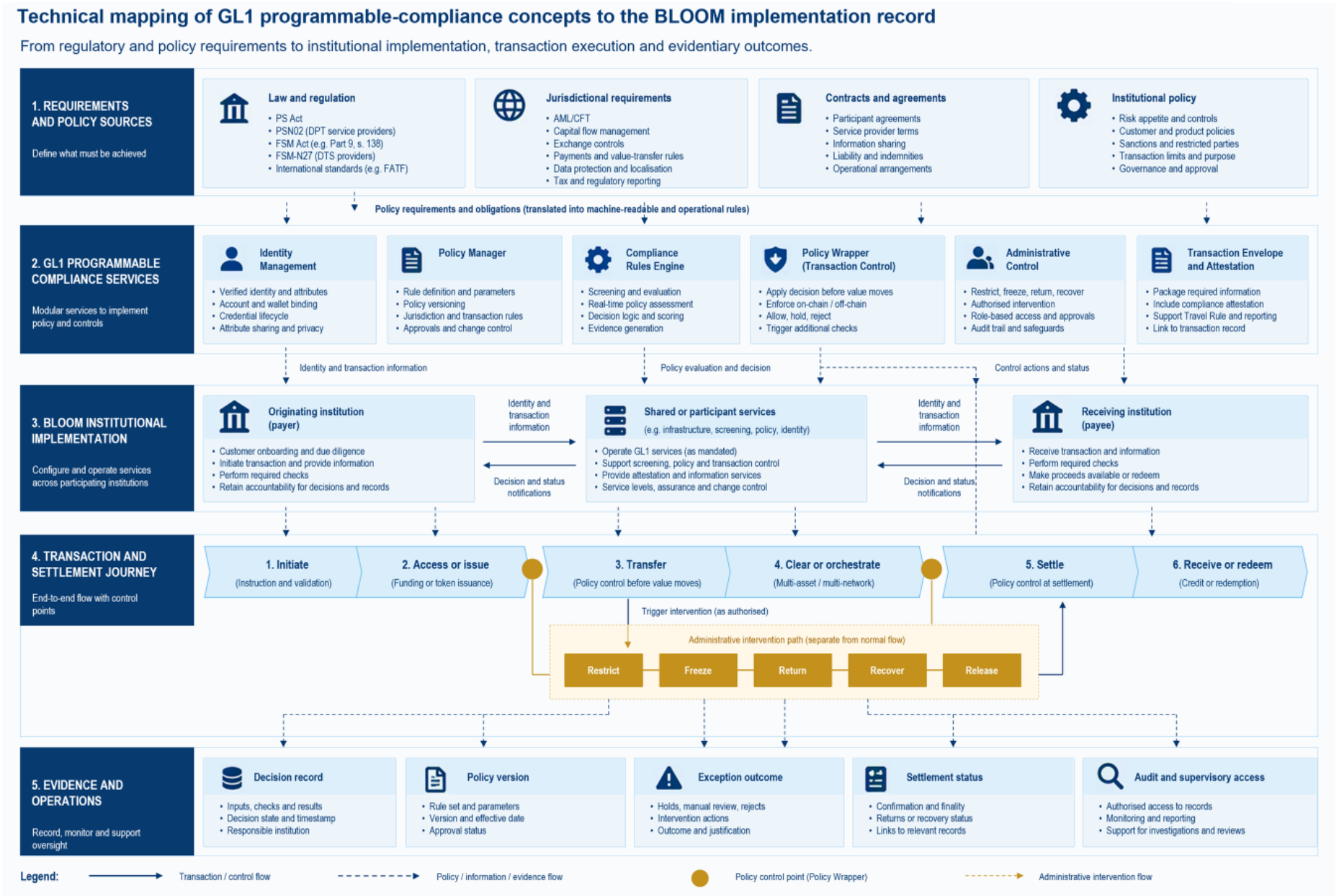


Figure 6: Application of the GL1 PC Model across a BLOOM transaction journey

The allocation shown is illustrative. An implementation may allocate the capabilities differently across participating institutions and services. The control-capability map should identify where each capability operates and distinguish operation of the capability from responsibility for the resulting decision.

5.3.1 Identity, Accounts and Wallets

This subsection applies the Identity Management Module in the GL1 PC model to the parties, accounts, wallets and identifiers involved in the transaction journey.

Each party to a transaction is linked, where applicable, to the account, wallet or other identifier through which that party transacts. The control-capability map records the customer or institution represented, the party performing verification, the attributes available for the transaction and the source of supporting evidence.

A reusable identity credential is one means of making selected verified attributes available across institutions. It may bind an account or wallet to defined attributes, identify the issuing institution and include relevant attestations. Each receiving institution establishes the basis on which the information is used and the checks it continues to perform. The credential does not transfer responsibility for the receiving institution's decision.

5.3.2 Payment and Transfer Information

The information required to initiate, evaluate and complete a transfer may include the originator, beneficiary, ordering institution, beneficiary institution, amount, currency, payment purpose, corridor, account or wallet identifiers and transaction reference. Under the GL1 PC model, relevant transaction and party information may be assembled into a Transaction Envelope[16] and enriched with the attributes, attestations and evaluation results required as the transaction progresses.

For transactions subject to payment transparency or Travel Rule[17] requirements, record the required fields, the party supplying each field, the recipient, when the information becomes available and the action taken where information is missing or inconsistent.

Information may travel with the payment instruction, be retrieved through an authenticated reference or use a hybrid model. The control-capability map also records relevant requirements for confidentiality, authorised access, data minimisation, correction, retention, data location, availability and fallback.

Where a transaction includes digital-asset and fiat legs under different regulatory perimeters, information concerning checks performed upstream may accompany the payment instruction. This information may inform the downstream institution's assessment but does not replace checks that the downstream institution is required to perform.

5.3.3 Screening and Compliance Evidence

Screening services and evidence provide inputs that may be used in policy evaluation under the GL1 PC model. They should be distinguished from the Compliance Rules Engine, which performs the computation required by the applicable policies, and from the institution responsible for the resulting decision.

[16] The GL1 PC paper describes the Transaction Envelope as a structured transaction record that accumulates relevant transaction and party information through construction, enrichment, evaluation and enforcement. Its precise form is implementation-dependent.
[17] Financial Action Task Force, *The FATF Recommendations*, as amended June 2026, Recommendation 16 and its Interpretive Note.

The screening allocation identifies which checks are performed by each institution, which use a shared service and how evidence created earlier in the transaction is made available to subsequent participants.

For each screening step, the screening record identifies the party screened, data used, relevant lists or regimes, screening time, matching method, treatment of possible matches, decision owner and evidence produced. Where prior evidence is available, the evidence record identifies its issuer, scope, time of issue, validity, revocation method and supporting information. The receiving institution separately identifies the checks it performs under its own applicable requirements and responsibilities.

5.3.4 Policy Management, Configuration, and Transaction Decision

The Policy Manager identifies the approved policies applicable to a transaction. Policies may vary according to jurisdiction, participant type, customer or wallet category, payment purpose, amount, currency, transaction velocity, sanctions regime, required information, permitted recipient and applicable capital flow management or exchange-control measures.

Each policy identifies its owner, legal or institutional source, scope, rule logic, required inputs, effective date, version, approval status and review cycle. Policy-governance arrangements establish precedence where multiple policies apply and address missing, stale or conflicting inputs.

The Compliance Rules Engine performs the computation required by the applicable policies. The Policy Manager consolidates the evaluation results and determines the applicable outcome.

5.3.5 Transaction Enforcement

The Policy Wrapper or other transaction-control mechanism[18] applies the transaction outcome before value moves. The implementation should identify which outcomes permit execution, which prevent execution and which place the transaction into a defined exception or review path.

The enforcement record should identify the policy version applied, evaluation result, resulting transaction state and any subsequent release, rejection or exception handling. Where the implementation does not use a technical Policy Wrapper, the control-capability map should identify the mechanism that performs the equivalent enforcement function.

5.3.6 Administrative Control

Administrative Control provides an authorised path for actions such as restricting an account or wallet, pausing a transfer, freezing value, returning funds, releasing a restriction or recovering assets.

Each action is linked to the applicable legal, regulatory or contractual authority. The procedure identifies the initiating, approving and executing roles; access and key controls; segregation of duties; affected value; supporting evidence; notification requirements; and audit trail. It also addresses release or reversal, failed execution, unavailable shared services, reconciliation and recovery. These paths are tested separately from successful transaction execution.

[18] The GL1 PC paper illustrates the Policy Wrapper through a wrapped-asset implementation. References to a “Policy Wrapper or other transaction-control mechanism” recognise that the equivalent enforcement function may be implemented differently depending on the technical arrangement.

5.4 Accountability and Evidence

5.4.1 Roles and Accountability

Each control capability has an operating party and a responsible institution. The operating model records this allocation and distinguishes operation of a technical component from ownership of the regulatory, risk or transaction decision. Relevant roles may include participating institutions, credential issuers, information services, screening providers, policy operators, technical infrastructure providers, manual reviewers, and enforcement operators.

A shared service performs only the functions within its mandate. Participating institutions retain the responsibilities attached to their customers, payment instructions, screening decisions, settlement actions and interventions. The operating model also records relevant service levels, change control, assurance, incident handling, business continuity, data-access rules, exit arrangements, escalation paths and decision rights.

5.4.2 Evidence and Transaction Record

The evidence created at each control point forms part of the **transaction record**. The transaction record links the transaction context, information used, policy version, checks performed, evaluation result, Compliance Attestation where used, decision state, responsible institution, manual action, exception outcome and settlement, return or recovery status.

The transaction record establishes what was evaluated, when it was evaluated, which policies and dependencies were active and who made or approved the relevant decision. The transaction-record specification identifies the authoritative record, retention period, access rights, correction process and relationship to supporting evidence held elsewhere.

A Compliance Attestation may record the evaluation outcome for a particular transaction at a particular point in time. It forms part of, but is not equivalent to, the wider transaction record. It does not replace applicable reporting obligations or the human-readable records and supporting evidence required for investigation, audit or supervisory review.

5.5 End-to-End Application and Testing

The end-to-end control flow brings together the preceding elements. It shows how transaction information is assembled; how the transaction context is enriched through identity and other information services; how the Policy Manager identifies the applicable policies; how the Compliance Rules Engine performs the required evaluations; how the Policy Wrapper or other transaction-control mechanism applies the outcome; when value is permitted to move; and how completion and supporting evidence are recorded.

The control flow also covers non-success paths. Missing or stale information, possible screening matches, policy failures and service outages move the transaction into the applicable hold, information-request, manual-review, rejection or fallback state. Restrictions, freezes, release, return and recovery follow the separate Administrative Control path. Testing should cover successful transactions, missing or stale information, screening matches, conflicting policy outcomes, unavailable services, failed settlement, return and recovery scenarios.

The regulatory requirements register, transaction journey, control-capability map, operating model, transaction record and test results together form the implementation record.

6 Implementation

A digital money arrangement is implementable only when its complete transaction journey can operate across the participating institutions, forms of digital money, infrastructures and controls under the conditions in which it is intended to be used.

The preceding chapters describe how an arrangement can be analysed through its Functions, Structure, Connectivity and Controls. This chapter brings these four aspects together in an **implementation profile** for a defined use case. The implementation profile provides a standardised basis for understanding how the transaction is intended to work, identifying the dependencies required to support it, testing whether it can operate under defined conditions, and recording the evidence produced through implementation.

The implementation profile provides an end-to-end view of the use case, including its scope, participants, transaction journey and relevant framework characteristics. It distinguishes intended design from what has been implemented, tested and observed, and provides the basis for assessing operating readiness and implementation evidence[19].

6.1 Building the Implementation Profile

The implementation profile starts with the transaction being supported, its intended outcome and the scope within which the arrangement is being assessed.

The transaction journey established through the functional analysis in Chapter 2 provides the common reference point. Structure, Connectivity and Controls are then applied at the points in that journey where the relevant characteristics arise.

The implementation profile brings together:

- **Transaction context**: The purpose and intended outcome of the transaction, the users and beneficiaries, and the currencies, jurisdictions, operating conditions, implementation stage and scope.
- **Participants and functions**: The participating legal entities and service providers, the functions they perform, their roles and decision rights, and the principal dependencies between participants.
- **Transaction journey**: The end-to-end movement of value, information and decisions, including the assets involved, authoritative records, settlement events and participant-facing completion points.
- **Framework application**: The settlement structures, connectivity configurations, applicable requirements, control capabilities and transaction decision points relevant to each part of the transaction journey.
- **Operating conditions**: The responsibilities, funding and liquidity, fallback arrangements, economic flows, fees and other dependencies needed to support the transaction under its intended operating conditions.

[19] See, Monetary Authority of Singapore, *GUARDIAN*; Monetary Authority of Singapore, *BLOOM*, for related public-private approaches focused on practical implementation and the progression of industry trials and use cases.

The framework dimensions are applied where the relevant characteristics arise. Settlement structures apply to the transaction legs in which they are observed. Connectivity configurations apply to the connections between environments. Control capabilities apply at the points in the transaction journey where information, evaluation, decisions or intervention are required.

The level of detail reflects the scope and maturity of the use case. Assumptions, proposed design choices and unresolved issues remain distinguishable from features that have been implemented, tested or observed.

6.2 Assessing End-to-End Operation

Successful operation of a digital money arrangement requires all parts of the transaction to execute and complete.

The implementation assessment follows the complete transaction journey across participating institutions and infrastructures. Dependencies between transaction legs remain visible so that the completion of one stage is not treated as evidence of end-to-end completion where subsequent information, value, controls or settlement remain outstanding.

This assessment covers three operating paths:

6.2.1 Normal operation

This determines whether the transaction can progress from initiation to completion under its intended operating conditions. This includes the required information, liquidity, decision states, value movements, settlement and confirmations.

6.2.2 Exception handling

This determines how the arrangement responds when a required condition is not satisfied. Relevant scenarios may include:

- missing or inconsistent information;
- failed control or screening outcomes;
- insufficient liquidity or conversion capacity;
- unavailable participants or shared services;
- delayed or failed transaction legs;
- unavailable settlement infrastructure; and
- incomplete or inconsistent transaction states.

The implementation profile identifies where the transaction is held, rejected, rerouted or escalated, the participant responsible for the decision and the evidence retained.

6.2.3 Recovery

This determines how an interrupted or incomplete transaction is resolved.

This may include alternative routing, fallback settlement, release of held transactions, return or reversal where applicable, participant or service substitution, reconciliation and post-recovery confirmation.

Testing the successful transaction path is therefore necessary but not sufficient to establish operating readiness.

6.3 Assessing Operating Readiness

Operating readiness assesses whether the end-to-end transaction can be supported under the intended operating conditions, including normal operation, exceptions and recovery.

The assessment considers the following areas:

Area	What to assess
Participation and service operation	Eligibility, onboarding, technical integration, participant obligations, operating hours, service levels and support.
Funding, liquidity and conversion	Funding source, prefunding or committed liquidity, limits, FX, conversion capacity, rebalancing and contingency arrangements.
Settlement and completion	Obligations being settled, settlement asset and venue, authoritative record, technical completion, confirmation, discharge, legal finality and reconciliation.
Information and controls	Data sources and recipients, credentials, screening, policy ownership, decision states, evidence and manual review.
Governance and accountability	Decision rights, operator authority, policy ownership, liability, disputes, change and participant exit.
Resilience and recovery	Unavailability scenarios, alternative routing, fallback settlement, recovery and post-recovery reconciliation.
Commercial operation	Service owner, customer proposition, pricing, fees, cost allocation, support and expansion commitments.

Readiness is assessed across the complete transaction journey. Dependencies between participants, infrastructure, liquidity, information and controls remain visible so that successful operation of an individual component is not treated as evidence that the end-to-end transaction can complete.

Dependencies on shared services, infrastructure operators and other critical providers are assessed together with the fallback available where a dependency cannot perform its intended function.

Readiness also considers dependencies between transaction legs. Completion of one leg does not establish end-to-end completion where subsequent movement of information or value remains outstanding.

6.4 Implementation Stage and Evidence

Implementation evidence should support the claims being made about an arrangement.

The implementation profile distinguishes intended design from capabilities that have been built, tested, observed or used, and links evidence to the participants and transaction journey in scope, functions, scenarios and operating conditions in which it was obtained.

Implementation stage describes the context in which that evidence was produced. It is not, by itself, a measure of operating readiness.

Implementation stage	Evidence to record	What the evidence can establish
Concept or design	Scope, assumptions, proposed participants, target flow and unresolved design choices.	Coherence of the intended arrangement and matters requiring further implementation
Prototype or proof of concept	Functions implemented, test environment, scenarios executed and technical observations.	Whether selected functionality operates under the specified test conditions
Pilot or trial	Participating institutions, transaction journeys, operating conditions, controls and exception outcomes.	Whether the tested transaction or functions operate for the defined participants and conditions
Recurring or production use	Operating volumes where cleared for use, service levels, recurring demand, support, liquidity, resilience and extension evidence.	Evidence of continuing operation within the stated production scope

The depth of evidence increases with implementation maturity. A concept or design records intended operation and unresolved choices. A prototype or proof of concept provides evidence of specified functions under defined test conditions. A pilot or trial provides evidence from defined participants, transaction journeys and operating conditions. Recurring or production use provides evidence of continuing operation and the dependencies required to sustain it.

A successful technical test does not by itself establish operating readiness. Evidence remains attributable to the participants, transaction journeys, functions, conditions and scenarios under which it was produced.

The implementation profile, operating-readiness assessment and supporting evidence together provide a consolidated view of the use case and its stage of implementation. An illustrative BLOOM Implementation Profile is provided in the Annex, translating the analysis in Chapters 2 to 6 into a practical template for a defined use case.

7 Industry Case Studies

The preceding chapters set out a common framework for understanding and implementing digital money arrangements through their Functions, Structure, Connectivity and Controls. This chapter draws on implementation experience and inputs contributed by BLOOM industry participants, and applies that framework to selected industry use cases, illustrating how these dimensions come together in practice.

7.1 Interoperability across banks' tokenised deposit environments

DBS and Kinexys by J.P. Morgan have launched a cross-bank interoperability solution supporting transactions involving tokenised deposits issued by the respective banks. The solution connects the banks' permissioned tokenised deposit environments to enable instant, 24/7 USD transfers between the United States and Singapore.

This enables institutional clients to deploy on-chain USD liquidity on demand across entities, banking partners, markets and time zones, including outside traditional banking hours. It supports corporate treasury and liquidity-management needs by providing greater flexibility over when liquidity can be moved and deployed.

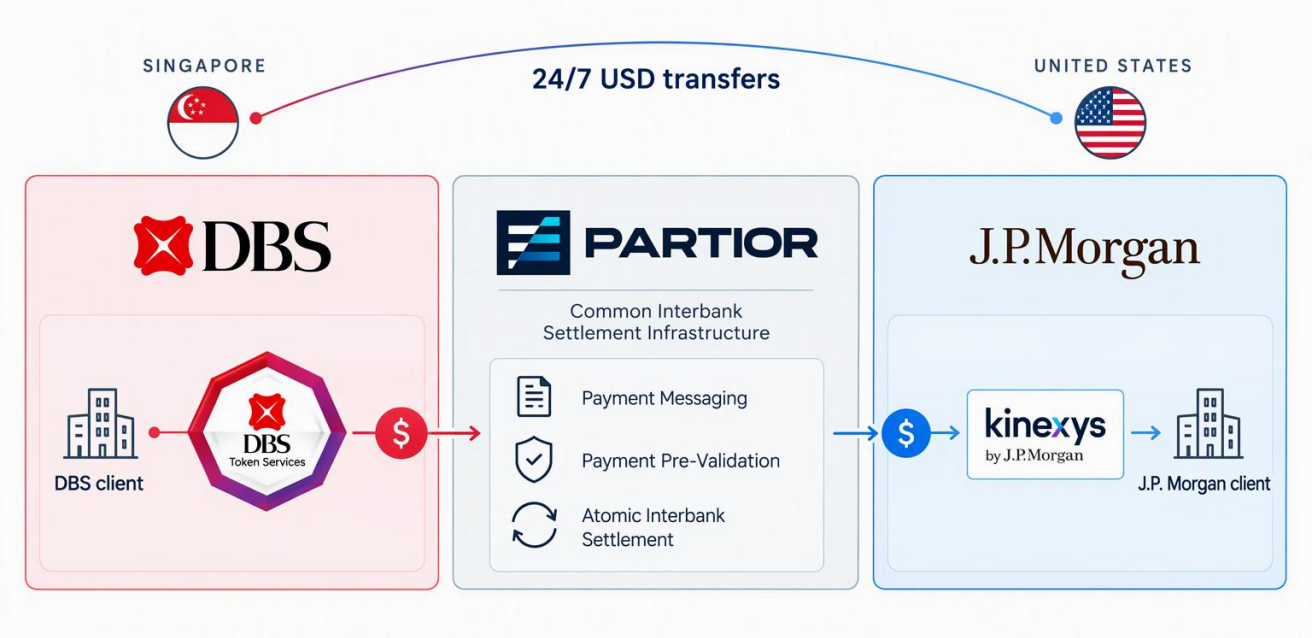


Figure 7: Cross-bank interoperability solution to enable instant, 24/7 USD transfers between the United States and Singapore

7.1.1 Structure

The arrangement involves separately issued tokenised bank deposits, with each bank maintaining its own tokenised deposit environment. Transactions across the two environments therefore require the value transfer and resulting interbank obligations to be coordinated and settled.

While there is no native transfer of tokens between the two banks, the transaction involves a corresponding transformation of the liability from that of the sending bank to that of the beneficiary bank. The arrangement therefore requires the resulting interbank obligation to be coordinated and settled through an agreed settlement mechanism.

7.1.2 Connectivity

Partior provides a common orchestration and settlement layer between the two banks, connecting their respective tokenised deposit ecosystems and coordinating the value transfer and resulting interbank settlement with the underlying correspondent banking arrangements. Payment pre-validation and coordinated settlement provide greater certainty over the completion of the transaction.

7.1.3 Controls

Each bank retains responsibility for the controls applicable within its respective tokenised deposit environment, payment and blockchain systems, and customer relationships. Within the payment and settlement lifecycle on Partior, capabilities like programmability and payment pre-validation provide greater control over value transfers based on pre-defined conditions. These capabilities can reduce payment failures and rejections, thereby reducing the need for manual handling by the banks.

7.2 Digital money settlement on card network

Visa and Nium conducted a pilot under BLOOM to examine the operational feasibility of extending card-payment settlement beyond traditional banking windows using stablecoins. The pilot focused on a defined issuer-to-Visa settlement flow, with Nium as the card issuer, USD as the settlement currency and USDC as the settlement asset.

The pilot was designed to support settlement seven days a week, including weekends and public holidays, while retaining Visa's existing payment processing, risk-management and compliance arrangements. Its scope was deliberately narrow: authorisation, clearing and transaction processing continued through Visa's existing infrastructure, while the mechanism used to settle Nium's resulting USD obligation to Visa was changed.

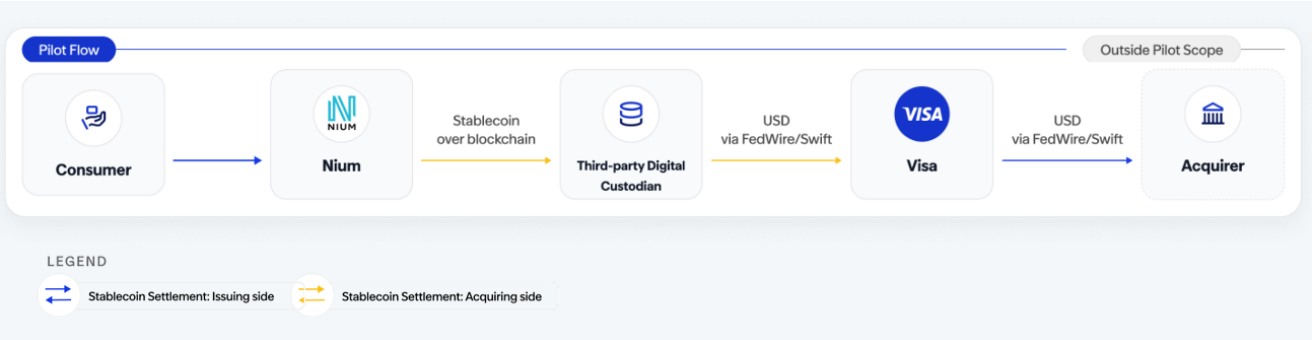


Figure 8: Issuer-to-Visa settlement flow

7.2.1 Structure

VisaNet continued to calculate Nium's net settlement position through the existing clearing process. Once the USD settlement obligation was determined, a stablecoin settlement instruction was generated and Nium transferred USDC from its wallet to Visa's designated digital custodian.

Following receipt, the custodian converted the USDC into USD fiat and transferred the corresponding fiat amount to Visa. The pilot therefore used USDC as an intermediate settlement asset for the issuer-to-Visa leg while Visa ultimately received fiat currency. On-chain confirmation provided a record of the USDC transfer.

The pilot did not extend the stablecoin settlement flow to the acquirer side. Settlement from Visa to the acquirer continued through existing fiat settlement channels.

7.2.2 Connectivity

The arrangement connects Visa's existing card-payment infrastructure with digital-asset infrastructure without changing the underlying authorisation and clearing processes. VisaNet continued to process transactions and calculate settlement positions, while the resulting settlement instruction initiated a separate stablecoin-based settlement flow involving Nium's digital wallet and the designated custodian.

The pilot therefore illustrates a layered connectivity configuration, in which established payment infrastructure performs authorisation, clearing and calculation of settlement obligations, while digital-asset infrastructure provides an additional mechanism for transferring value to meet the resulting settlement obligation. The custodian provides the connection between the stablecoin and fiat environments by receiving USDC, converting it into USD and transferring the fiat proceeds to Visa.

7.2.3 Controls

The pilot was designed to extend settlement availability while preserving Visa's existing payment processing, risk-management and compliance frameworks. As authorisation, clearing and transaction processing remained on Visa's existing infrastructure, the stablecoin component was limited to the settlement leg tested.

The on-chain transfer also produced a verifiable transaction reference that could support reconciliation between the participating parties. Within the pilot, the control implications therefore relate primarily to integrating the stablecoin settlement leg with the existing settlement process while retaining the controls applicable to the underlying payment activity.

The pilot did not test a broader programmable-compliance architecture or changes to the controls applied to the underlying card transaction. Its implementation evidence should therefore be read within the defined scope of the issuer-to-Visa settlement flow.

7.3 Cross-border payments connecting domestic payment environments

StraitsX's Payment Network (XSPN), together with Kasikornbank's (KBank) Q Wallet and Grab, seeks to enable real-time, low-cost cross-border payments for travellers and merchants. Consumers initiate payments through their digital wallets using standard merchant-presented QR codes, while merchants receive settlement in their local fiat currency. Stablecoins facilitate value transfer between participating intermediary institutions, but together with the underlying blockchain-based arrangements, remain abstracted from end users and merchants. Travellers therefore do not need to hold local currency, and merchants do not need to accept a new payment instrument.

The arrangement brings together three principal participant types. First, StraitsX acts as the payment network operator, issuing XSGD and XUSD stablecoins, managing clearing and settlement, and minting and redeeming Purpose Bound Money (PBM) tokens used to intermediate transactions. Second, wallet operators such as KBank’s Q Wallet, provide the payment interface through which end users pay with the operator’s own e-money on blockchain (Q-money), and maintain sufficient digital asset float to clear demand. Third, merchant acquirers such as Grab onboard and verify merchants and receive consolidated settlement from StraitsX.

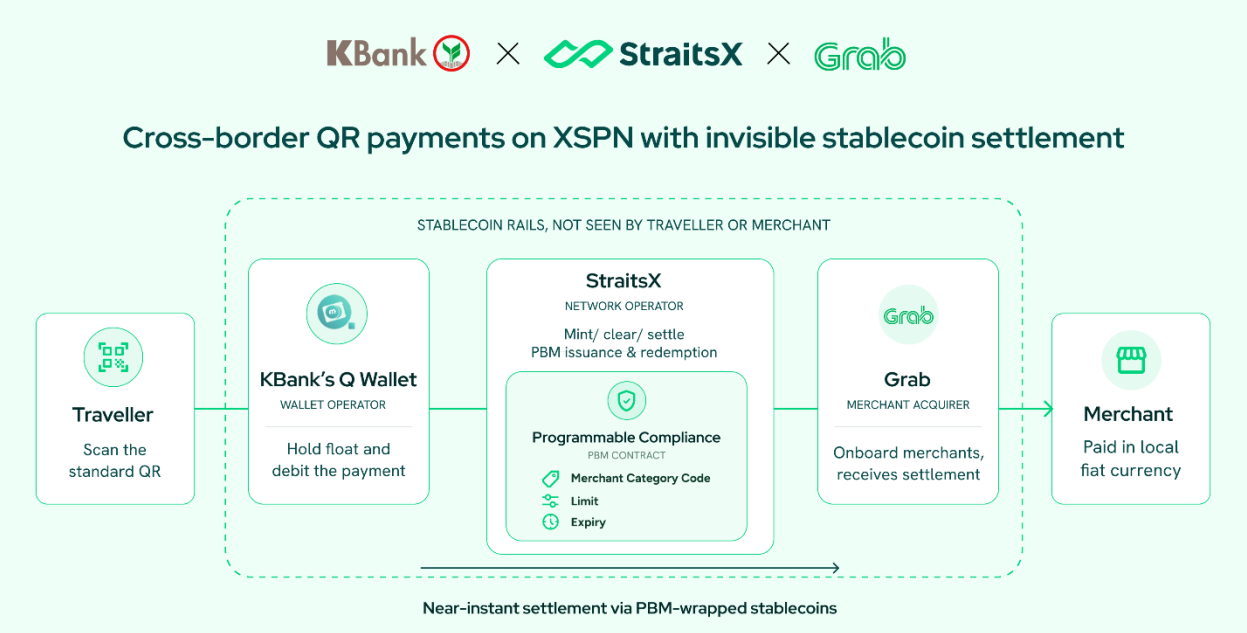


Figure 9: Settlement of Purpose Bound Money tokens via StraitsX

7.3.1 Structure

The arrangement distinguishes the consumer-facing payment instrument from the mechanism used to transfer value between participating institutions and from the local fiat value ultimately received by the merchant. StraitsX manages the clearing and settlement process, with stablecoins used for settlement between institutions on public blockchains and merchant acquirers receiving consolidated settlement from StraitsX.

PBM tokens are used within the transaction flow to apply conditions to the value being transacted. The arrangement therefore distinguishes the instrument used by the consumer to initiate payment, the mechanism through which transaction conditions are applied, and the local fiat settlement ultimately received by the merchant.

7.3.2 Connectivity

XSPN connects the consumer's wallet environment, StraitsX's payment network and the merchant-acquiring environment within an end-to-end transaction journey. Wallet operators provide the consumer-facing access point, while merchant acquirers connect merchants to the arrangement. StraitsX coordinates the network across these participants, including the clearing and settlement activities required to complete the transaction.

This enables the underlying digital-money and blockchain components to operate between participating institutions while remaining abstracted from the consumer and merchant experience. Consumers can initiate payments through participating wallets using the merchant's existing QR payment interface, while merchants receive settlement through their existing acquiring relationship.

7.3.3 Controls

XSPN illustrates how programmable controls can be applied within a defined payment journey. PBM acts as a transaction-control layer through which conditions can be applied before a transaction completes. Merchant category codes can be embedded in the PBM contract logic so that value cannot be redirected outside authorised merchant segments, while transaction limits can similarly be enforced for each transaction.

PBMs can also incorporate programmed expiry conditions, under which unused balances following the specified validity period are revoked and returned to the issuing party. Eligibility, purpose and transaction limits can therefore be evaluated as conditions of the transaction, rather than solely through post-transaction review.

On the wallet operator side, KBank applies programmable controls intended to support compliance with applicable local regulations. The token is implemented as a secure and tamper-resistant credentialing layer to represent KYC-verified customer identities, together with smart contract rules reflecting identity status, transaction thresholds, and screening outcomes. This can reduce reliance on retrospective monitoring and support an audit trail for reconciliation and exception management.

The implementation demonstrates a narrower set of controls than the fuller programmable-compliance model described in the BLOOM Framework. The architecture can accommodate additional control capabilities, including identity management, where required by the use case. This illustrates an incremental approach to implementation, where institutions can begin with the control capabilities relevant to the transaction and extend them as requirements and use cases develop.

7.4 Cross-institutional coordination across bank environments

The Swift Digital Ledger case illustrates how a shared orchestration layer can coordinate payment commitments and transaction states across independently operated bank environments, to eventually support transactions involving tokenised deposits. DBS, OCBC and UOB participated using their respective bank environments for domestic SGD transactions with the Swift Digital Ledger providing a coordination layer across them. The coordination layer linked the banks, aligned transaction state and recorded or calculated the resulting interbank obligations, while final interbank settlement remains separate and is effected through the agreed settlement mechanism.

The arrangement was intended to support future transactions involving tokenised deposits issued by participating banks with a narrow focus to demonstrate the coordination functionality.

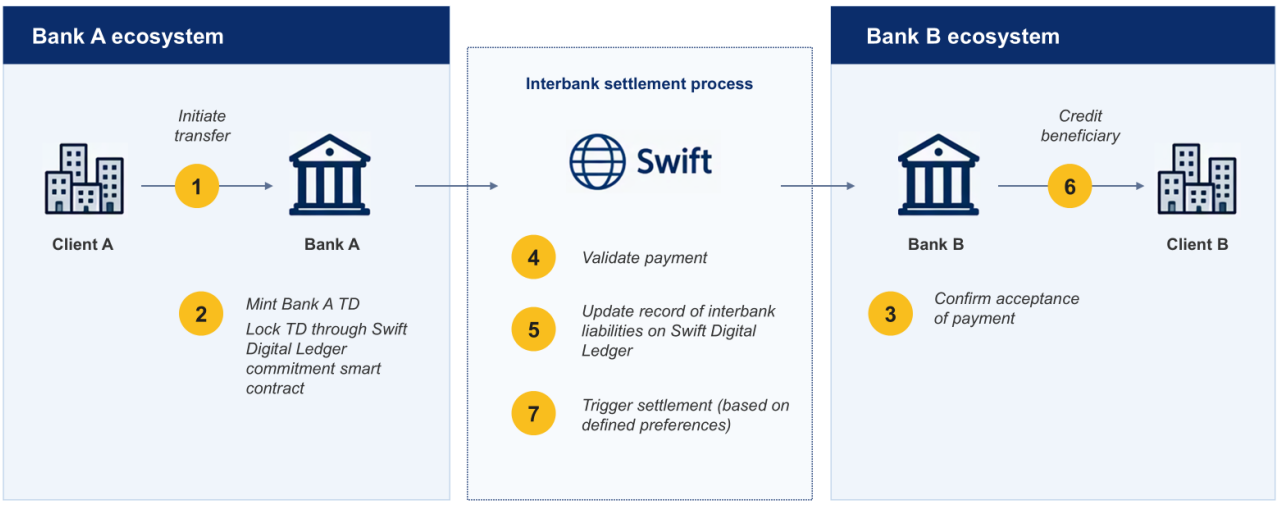


Figure 10: Payment commitments and transaction states across DBS, OCBC and UOB bank environments coordinated through the Swift Digital Ledger

7.4.1 Structure

The participating banks operate within their respective bank environments and records. Within the tested arrangement, the payer bank locks tokens representing a payment commitment, while the beneficiary bank accepts the payment on the basis of that commitment recorded on Swift Digital

Ledger. The Swift Digital Ledger coordinates transaction status and records or calculates the resulting interbank obligations.

The coordination layer does not itself discharge those obligations. Final interbank settlement remains separate and is effected through the applicable settlement mechanism. The case therefore distinguishes the payment commitment and resulting interbank obligation from the mechanism through which that obligation is ultimately discharged.

7.4.2 Connectivity

The Swift Digital Ledger provides an orchestration layer across the independently operated bank environments. It links participating banks, coordinates payment commitments and transaction states, and maintains a common view of the resulting interbank obligations, without requiring the participating banks to operate on a common ledger.

This illustrates an orchestrated connectivity configuration under the BLOOM Framework. The coordination layer enables separately operated environments to interact while their respective customer relationships and records remain with the participating banks.

Importantly, connectivity is distinct from settlement. The Swift Digital Ledger coordinates activity across the participating environments, while a separate settlement mechanism discharges the resulting interbank obligation.

7.4.3 Controls

Control responsibilities remain allocated to the participating banks and relevant services according to the functions they perform. Each bank remains responsible for the controls applicable within its own environment and customer relationships, while the coordination layer manages the transaction states and information required for coordination across participating environments.

8 Priorities and Next Steps

The BLOOM Framework provides a common method for describing digital money arrangements across the end-to-end transaction journey. It brings together Functions, Structure, Connectivity and Controls while preserving the distinct role of each dimension.

The framework can be applied to arrangements at different stages of implementation and across different forms of digital money, institutional structures and technical environments. The purpose is not to prescribe a single architecture. It is to provide a consistent basis for describing how an arrangement works, identifying its dependencies and examining what has been implemented and demonstrated.

The case studies in Chapter 7 illustrate different ways in which these elements can be combined. Continued implementation can build on this experience and provide further evidence on how digital money arrangements operate across institutional and jurisdictional boundaries.

8.1 Applying the Framework Today

The Field Guide can be used to structure both proposed and existing digital money arrangements. Functions provide the common transaction journey. Structure identifies the forms of value and obligations involved, how those obligations are discharged and where settlement and finality occur. Connectivity identifies how participating environments interact. Controls identify how applicable requirements, information and decisions are applied across the journey.

These dimensions can be applied at the level at which the relevant characteristics arise. A single use case may involve different settlement structures across its transaction legs, different connectivity configurations between participating environments and different control capabilities at different transaction stages.

The implementation profile in Chapter 6 brings these elements together for a defined use case. The profile can be used to identify dependencies, assess operating readiness and distinguish intended design from capabilities that have been implemented, tested or observed.

This allows different implementations to be described consistently while preserving differences in their institutional, legal, technical and operating models.

8.2 Priorities for Continued Implementation

Continued implementation can deepen practical experience in areas where end-to-end operation depends on coordination between multiple institutions, infrastructures or jurisdictions.

Priority areas include **cross-institution interoperability**, particularly where separately issued forms of digital money need to be accepted, exchanged or used across different institutional environments[20].

[20] Monetary Authority of Singapore, *BLOOM*, October 2026; Monetary Authority of Singapore, Bank Negara Malaysia and Bank of Thailand, *MAS, Bank Negara Malaysia and Bank of Thailand Partner with Industry to Advance Cross-Border Settlement in Digital Money through BLOOM*, October 2026.

Settlement, finality and liquidity remain important where transactions create obligations between participating institutions[21]. Further implementation can test different settlement assets and venues, funding and rebalancing arrangements, the points at which settlement becomes final, and approaches to managing liquidity across normal and stressed operating conditions.

Information exchange and controls are also important where transaction information, identity attributes, screening evidence and policy decisions need to operate across institutional boundaries. Implementation can provide further evidence on how information can be reused or exchanged while preserving the responsibilities of participating institutions.

Connectivity across networks and infrastructures can provide further practical insight into common integration surfaces, routing, orchestration, transaction-state coordination, authoritative records and the handling of dependencies across connected environments.

Operating resilience requires attention to incomplete transactions, unavailable participants or services, alternative routing, recovery and reconciliation. End-to-end testing should therefore extend beyond successful transaction paths to the conditions under which a transaction is delayed, interrupted or cannot complete.

These areas do not constitute additional dimensions of the BLOOM Framework. They are practical areas in which further implementation evidence can deepen understanding of how the existing dimensions operate together.

8.3 Maintaining the Field Guide

The Field Guide should remain grounded in implementation experience. Evidence from new use cases, pilots and recurring operation can be incorporated where it clarifies how the framework is applied or identifies considerations that are not adequately captured today.

New evidence may refine the description of settlement structures or connectivity configurations, identify additional implementation considerations, strengthen guidance on controls and operating readiness, or provide new illustrative cases.

Changes should preserve the core structure of the BLOOM Framework. A new implementation pattern does not necessarily require a new framework category. The existing dimensions should first be used to determine whether the observed characteristic represents a variation within a settlement structure, connectivity configuration, control capability or operating consideration.

Case studies should also remain explicit about implementation stage and evidence. Conceptual designs, prototypes, pilots and recurring use provide different forms of evidence and should be described accordingly.

Maintaining a consistent framework while incorporating implementation experience allows the Field Guide to remain comparable across use cases and useful as digital money arrangements develop.

8.4 Closing Observation

Digital money arrangements depend on the complete transaction journey working across the institutions, infrastructures, forms of digital money and controls involved. The BLOOM Framework

[21] Committee on Payments and Settlement Systems and Technical Committee of IOSCO, *Principles for Financial Market Infrastructures*, April 2012.

provides a common basis for describing these elements, applying them to implementation and assessing the evidence produced through practical use.

Continued implementation can strengthen that evidence and identify where further guidance is useful. The Field Guide provides a consistent structure for incorporating those lessons while preserving a common basis for understanding and comparing digital money arrangements.

***

Acknowledgements

This report was developed through the collective efforts of the BLOOM working groups:

1. **Token Interoperability working group**, led by DBS and J.P. Morgan
2. **Programmable Controls working group**, led by StraitsX and OCBC

The contributions to the development of this report were provided by the following organisations, listed in alphabetical order:

- Ant International
- Circle
- DBS
- J.P. Morgan
- Kasikornbank (KBank)
- Nium
- OCBC
- Partior
- Standard Chartered
- StraitsX
- Stripe
- UOB
- Visa
- Xweave

ANNEX A

BLOOM Implementation Profile

The BLOOM Implementation Profile provides a practical template for applying the BLOOM Framework to a defined digital money arrangement. It brings together the transaction context, Functions, Structure, Connectivity and Controls with the operating conditions and implementation evidence relevant to the arrangement.

The profile is intended to support a consistent description of how an arrangement is designed and operates, identify key dependencies and responsibilities across the end-to-end transaction journey, and record what has been implemented, tested or observed. It is illustrative and may be adapted according to the scope, complexity and maturity of the relevant implementation. Not every field will be applicable to every arrangement.

A1. Transaction Context and Participants

Define the transaction being supported and establish the scope within which the arrangement is being assessed.

Field	Record
Use case and intended transaction	Transaction or activity being supported
Intended outcome	Intended outcome for participating institutions, users or beneficiaries
Participants	Legal entities and service providers involved in the arrangement
Users and beneficiaries	Relevant institutional or end users and beneficiaries
Money and assets	Forms of digital money and any other assets involved
Currencies	Relevant transaction and settlement currencies
Jurisdictions	Jurisdictions relevant to the transaction and participating institutions
Operating conditions	Operating window, transaction scope, relevant limits and other material boundaries
Implementation stage	Concept/design, prototype/proof of concept, pilot/trial, or recurring/production use
Scope and assumptions	Matters included or excluded from the assessment and material assumptions

The transaction context defines the boundary for the subsequent analysis. Where an implementation covers only part of the end-to-end arrangement, the profile should identify the functions or transaction legs that remain outside scope.

A2. End-to-end Functional Journey

Map the functions required for the transaction to progress from initiation to completion. Functions that are not applicable may be omitted, and additional functions may be recorded where required.

Function	Participant(s)	Value, asset or obligation	Information required or produced	Authoritative record	Completion event
Initiation					
Issuance					
Distribution and access					
Transfer					
Clearing and orchestration					
Settlement					
Recipient access or redemption					
Other relevant function					

Where one participant performs several functions, or a function is distributed across several participants or services, these should be recorded separately where doing so is material to understanding responsibilities and dependencies.

A3. Structure and Settlement

Identify the issuer liabilities involved in the transaction and how any resulting financial obligations are discharged.

A3.1. Issuer-liability structure

Field	Record
Issuer(s)	
Issuer liabilities	
Eligible holders/participants	
Issuance and redemption arrangements	
Applicable settlement structure(s)	Common Issuer / Multiple Issuers under Common Rules / Interconnected Issuer Arrangements
Inter-institution obligations	Obligations arising between participating institutions and how they are determined

Where different settlement structures apply to different transaction legs, these should be recorded separately rather than assigning one structure to the arrangement as a whole.

A3.2. Settlement mechanism and finality

Field	Record
Financial obligation being discharged	
Settlement asset	
Settlement institution or venue	
Settlement mechanism	
Authoritative settlement record	
Coordination mechanism, where applicable	
Liquidity and funding arrangements	
Technical completion	Event establishing completion of the relevant technical process
Participant confirmation	Event at which completion is communicated to the participant
Discharge	Event at which the relevant financial obligation is satisfied
Legal finality	Event at which settlement becomes irrevocable and unconditional under the applicable legal and contractual framework
Reversal, cancellation or unwind	Circumstances, if any, in which the transaction may be reversed, cancelled or unwound before or after relevant completion events

The profile should distinguish technical execution, participant confirmation, discharge and legal finality where these occur at different points or rely on different authoritative records.

A4. Connectivity

Map each material connection between participating environments. The configuration should be recorded at the level of the connection rather than necessarily characterising the arrangement as a whole.

Connection	Connection 1	Connection 2	…	Connection N
Environments connected				
Function(s) supported				
Connectivity configuration	Direct / Orchestrated / Shared / Layered	Direct / Orchestrated / Shared / Layered		Direct / Orchestrated / Shared / Layered
Information, instructions or value exchanged				
Coordination mechanism				
Authoritative record(s)				
Responsible participant/operator				

For each material connection, also record where relevant:

Consideration	Record
Interfaces and standards	
Transaction states and confirmations	
Operating windows and dependencies	
Monitoring and reconciliation	
Exception handling	
Fallback	
Recovery	
Change and access management	

A connection may combine characteristics of more than one connectivity configuration. The profile should record the functions actually performed rather than assign a configuration where doing so obscures the arrangement.

A5. Controls and Decision Responsibility

Identify the controls operating across the transaction journey and distinguish operation of a control capability from responsibility for the resulting decision.

Control point	Control point 1	Control point 2	…	Control point N
Applicable requirement or policy				
Information/input				
Control capability or mechanism				
Capability operator				
Decision owner				
Transaction outcome/state				
Evidence retained				

Relevant control points may include identity and credential checks, transaction information, screening, policy evaluation, transaction enforcement, administrative intervention, manual review and exception handling.

Where information, credentials, screening results or other evidence are received from another participant or service, the profile should record how that information is used and the responsibility retained by the institution making the relevant decision.

A6. Operating Conditions and Readiness

Assess whether the complete transaction journey can operate under its intended conditions, including normal operation, exceptions and recovery.

Area	Key dependencies	Normal operation	Exception or fallback	Responsible participant	Evidence/status
Participation and service operation					
Funding, liquidity and conversion					
Settlement and completion					
Information and controls					
Governance					

and accountability					
Resilience and recovery					
Commercial operation					

Readiness should be assessed across the end-to-end transaction journey. Successful operation of an individual component or transaction leg should not be treated as evidence that the complete arrangement can operate where subsequent information, controls, value movement or settlement remain outstanding.

A7. Scenarios, Evidence and Open Issues

Record the scenarios examined and the evidence supporting claims about the implementation.

Function or scenario	Implementation stage	Activity performed	Evidence or observation	What the evidence establishes	Limitation or open issue
Normal transaction					
Missing/ inconsistent information					
Control or screening exception					
Insufficient liquidity/ conversion capacity					
Participant/ service unavailable					
Settlement failure/delay					
Recovery/ reconciliation					
Other relevant scenario					

Evidence should remain attributable to the participants, functions, transaction journeys, scenarios and operating conditions under which it was produced. Where a capability remains proposed or assumed rather than implemented or tested, this should be identified explicitly.

A8. Implementation Summary

Conclude the profile with a short consolidated assessment.

Field	Summary
Arrangement	What the implementation is intended to enable
Implementation stage	Current stage and scope
Structure	Principal issuer-liability and settlement arrangements
Connectivity	Principal connections and configurations
Controls	Principal control arrangements and decision responsibilities
Key dependencies	Dependencies material to end-to-end operation
Evidence demonstrated	Capabilities or operating conditions supported by implementation evidence
Limitations	Matters not tested, demonstrated or within scope
Open issues / next steps	Further implementation, testing or decisions required

The implementation summary should distinguish **intended design from demonstrated capability** and avoid extrapolating evidence beyond the participants, transaction journeys and operating conditions in which it was obtained.

Glossary

Authoritative record. The record relied upon within an arrangement to establish the state of a transaction, asset, liability or obligation for a particular function. Different functions within the same arrangement may rely on different authoritative records.

Clearing. The process of transmitting, reconciling and, where relevant, confirming transactions before settlement, including the calculation of positions or obligations between participants where applicable.

Compliance Attestation. A record of the outcome of a compliance evaluation for a particular transaction against the policy version and dependencies active at that time. It is distinct from identity credentials or attestations used as inputs and does not replace applicable regulatory reporting or record-keeping obligations.

Connectivity. The interfaces, information flows, instructions, coordination mechanisms and operating arrangements through which participating environments interact across a digital money arrangement. Connectivity is distinct from the mechanism through which financial obligations are ultimately settled.

Connectivity configuration. A pattern describing how connectivity functions are allocated between participating environments. The Field Guide describes Direct, Orchestrated, Shared and Layered configurations. These configurations do not determine the settlement structure, settlement asset or legal finality of an arrangement.

Conversion. The exchange of one form of money or asset for another, including between different currencies, issuer liabilities or forms of digital money.

Digital money. A digital representation of monetary value or a monetary claim used within a digital money arrangement. The term is used generically in this Field Guide and does not, by itself, indicate a particular legal or regulatory characterisation.

Digital money arrangement. The combination of participants, functions, infrastructure, forms of value, settlement mechanisms, information flows and controls involved in completing an end-to-end transaction. An arrangement is distinct from the particular form of digital money used within it.

Discharge. The satisfaction of a financial obligation between participants. Discharge may occur at a different point from technical execution, participant confirmation or legal finality.

Distributed ledger technology (DLT). Technology that enables records to be shared and synchronised across participating nodes or systems. For the purposes of the Field Guide, use of DLT is an infrastructure choice and does not by itself determine the legal nature of an asset, the settlement structure or finality.

End-to-end transaction journey. The complete sequence of functions required for a transaction to progress from initiation to completion, potentially including issuance, distribution and access, transfer, clearing and orchestration, settlement, and recipient access or redemption.

Environment. An institutional system, issuer arrangement, payment or market infrastructure, blockchain or distributed ledger, wallet or custody platform, or other service through which a transaction function is performed or an authoritative record is maintained.

Finality event. The event that establishes that settlement has become final under the applicable arrangement.

Implementation evidence. Evidence obtained through design, prototype, pilot, trial or production activity that supports claims about the operation of specified functions or an arrangement under defined participants, scenarios and operating conditions.

Implementation profile. The consolidated description of a defined use case produced by applying the BLOOM Framework, bringing together the transaction context, participants and functions, transaction journey, settlement structures, connectivity configurations, controls, operating conditions, implementation stage and evidence.

Interoperability. The ability of institutions, systems, infrastructures or arrangements to interact sufficiently to support an intended transaction or function. Interoperability can involve information exchange, transaction coordination or movement of value and does not, by itself, imply common infrastructure or a common settlement mechanism.

Issuer liability. A financial claim or obligation attributable to the legal entity that issues a form of money. The Field Guide uses the relationship between issuer liabilities as the basis for distinguishing its three recurring settlement structures.

Legal finality. The point at which settlement becomes irrevocable and unconditional under the applicable legal and contractual framework. It may occur separately from technical execution or participant confirmation.

Orchestration. The coordination of transaction progression across participants, environments or transaction legs. It may include routing, sequencing, matching, validation, transaction-state coordination, triggering settlement, exception handling and reconciliation. Orchestration does not itself imply settlement.

Orchestrator. A participant, service or coordinating layer that performs one or more orchestration functions. An orchestrator may initiate or coordinate settlement without providing the settlement asset or maintaining the authoritative settlement record.

Participant confirmation. The point at which a transaction is communicated to a participant as completed. Participant confirmation does not necessarily establish discharge or legal finality.

Programmable compliance. An approach under which requirements and policies are translated into control capabilities that can evaluate and apply transaction outcomes within digital financial infrastructure. In this Field Guide, the approach draws on the GL1 Programmable Compliance model.

Purpose Bound Money (PBM). A protocol through which conditions may be applied to the use of an underlying form of digital money. Within the Field Guide, PBM is treated as a transaction-control mechanism rather than, by itself, determining the nature of the underlying money.

Reconciliation. The process of comparing records or transaction states maintained by different participants or environments, identifying inconsistencies and, where necessary, resolving them.

Redemption. The process through which a holder returns or extinguishes a form of digital money in exchange for the corresponding money, asset or claim in accordance with the issuer's applicable terms.

Regulated stablecoin. A stablecoin that is subject to an applicable regulatory framework governing its issuance or operation. References to a stablecoin as regulated should be understood by

reference to the relevant jurisdiction and applicable regulatory requirements rather than as a generic description of all stablecoins.

Settlement. The process through which the relevant financial obligation between participants is discharged by the authoritative transfer of the applicable settlement asset.

Settlement asset. The money or asset used to discharge a financial obligation between participants.

Settlement mechanism. The process through which settlement is initiated and effected, including the relevant settlement asset, institution or venue and authoritative record. A settlement mechanism may operate separately from the infrastructure on which the underlying transaction is executed.

Settlement structure. The relationship between the issuer liabilities involved in a digital money arrangement and the mechanism through which resulting financial obligations are discharged. The Field Guide identifies three recurring issuer-liability structures: Common Issuer, Multiple Issuers under Common Rules and Interconnected Issuer Arrangements.

Shared infrastructure. Infrastructure used by more than one participating institution to perform specified transaction functions or maintain shared transaction state. Shared infrastructure does not necessarily imply a common issuer, common liability, common customer relationship or single authoritative record for the complete arrangement.

Stablecoin. A digital token designed to maintain a stable value relative to a specified fiat currency or other reference asset. References in this Field Guide describe an instrument's intended design or role and do not, by themselves, establish that it satisfies any particular legal or regulatory classification.

Technical execution. Completion of the relevant technical process or ledger update associated with a transaction. Technical execution does not by itself establish discharge or legal finality.

Tokenised deposit. A form of digital money that constitutes or represents a deposit liability of a bank. References in this Field Guide describe the intended form of the instrument and do not substitute for assessment of its applicable legal or regulatory characteristics.

Transaction record. The record linking the transaction context, information used, policies or rules applied, checks performed, evaluation outcomes, decision states, responsible institutions, manual interventions, exceptions and eventual settlement, return or recovery status.

Transaction state. The recorded status of a transaction at a particular point in its journey, such as initiated, pending, validated, held, rejected, settled or completed. Different environments may maintain related transaction states, and these should not automatically be assumed to have the same legal or operational significance.

Sources and Further Reading

Adrian, Tobias. *Tokenized Finance*. IMF Note 2026/001. April 2026.

Bank for International Settlements. *Blueprint for the Future Monetary System: Improving the Old, Enabling the New*. Annual Economic Report 2023. 2023.

Bank for International Settlements, *The Next-Generation Monetary and Financial System*, Annual Economic Report 2025. 2025.

Bank for International Settlements. *The Sovereign Money Question: CBDCs, Stablecoins, and the Fight for the Settlement Layer*. September 2026.

Bank for International Settlements. *Wholesale Central Bank Money in the Context of Technological Innovation*. September 2025.

Bank for International Settlements and Committee on Payments and Market Infrastructures. *Tokenisation in the Context of Money and Other Assets: Concepts and Implications for Central Banks*. October 2024.

Committee on Payments and Market Infrastructures. *Harmonised ISO 20022 Data Requirements for Enhancing Cross-Border Payments*. Updated February 2026.

Committee on Payments and Market Infrastructures. *Linking Fast Payment Systems Across Borders: Governance and Oversight*. October 2024.

Committee on Payments and Market Infrastructures. *Moving on Up: Results of the 2024 Cross-Border Payments Monitoring Survey*. CPMI Brief No. 10. December 2025.

Committee on Payments and Settlement Systems and Technical Committee of IOSCO. *Principles for Financial Market Infrastructures*. April 2012.

Financial Action Task Force. *The FATF Recommendations*. Recommendation 16 and Interpretive Note. As amended June 2026.

Global Layer One. *Programmable Compliance: Compliance Architecture for Regulated Tokenised Assets*. June 2026.

Monetary Authority of Singapore. *BLOOM.*

Monetary Authority of Singapore. *GUARDIAN.*

Monetary Authority of Singapore. *MAS Launches BLOOM Initiative to Extend Settlement Capabilities.* October 2025.

Monetary Authority of Singapore. *Orchid Blueprint*. November 2023.

Monetary Authority of Singapore, Bank Negara Malaysia and Bank of Thailand. *MAS, Bank Negara Malaysia and Bank of Thailand Partner with Industry to Advance Cross-Border Settlement in Digital Money through BLOOM*. October 2026.

