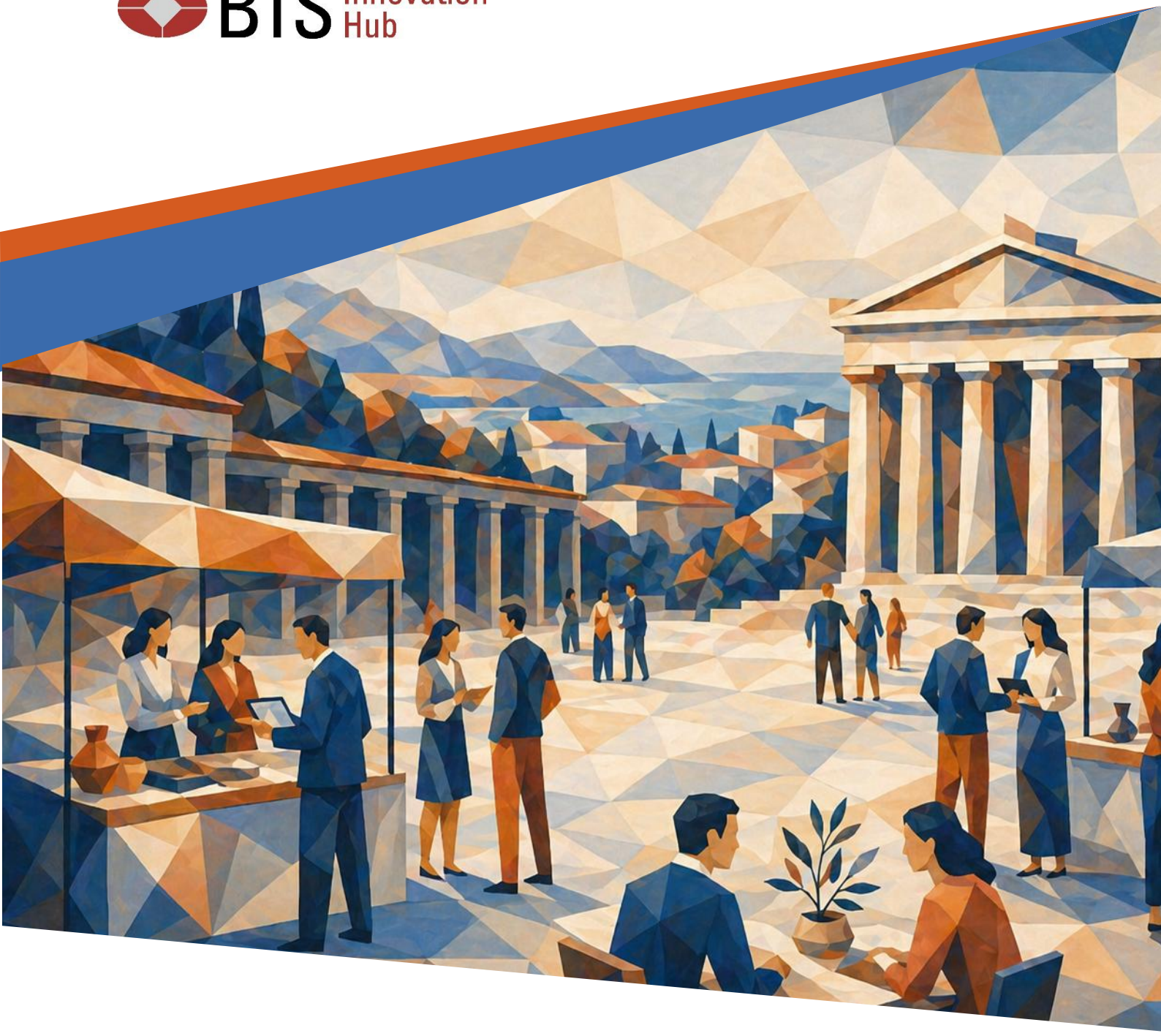
BIS Innovation Hub



Project Agorá

A shared programmable platform for wholesale cross-border payments

Convened by

BIS

IIF Institute of International Finance

Central bank project participants

日本銀行 Bank of Japan

Bank of Korea

European Central Bank Eurosystem

Banque de France Eurosystème

Schweizerische Nationalbank
Banque nationale suisse
Banca nazionale svizzera
Banca naziunala svizra
Swiss National Bank

Bank of England

Federal Reserve Bank of New York

Private sector project participants

Amina Bank
Banco BV
Banco Santander
Banorte
Banque Cantonale Vaudoise
Basler Kantonalbank
BBVA
BNP Paribas
BNY
CaixaBank
Citi
Commerzbank AG
Crédit Agricole CIB
Deutsche Bank AG
Eurex Clearing AG
Euroclear S.A./N.V
FNBO
Groupe BPCE
Hana Bank
HSBC
IBK
JPMorgan Chase Bank N.A.
KB Kookmin Bank
Lloyds Banking Group
Mastercard
Mizuho Bank
Monex
MUFG Bank Ltd.
NatWest Group
NongHyup Bank
PostFinance Ltd.
SBI Shinsei Bank Ltd.
Shinhan Bank
SIX Digital Exchange (SDX)
Standard Chartered
Sumitomo Mitsui Banking Corp
Swift
Sygnum Bank
TD Bank N.A.
UBS
Visa
Woori Bank

Table of contents

The views expressed in this report do not necessarily represent those of the participating institutions. The legal analysis in this report does not represent legal or other advice or a legal opinion. The analysis is limited to a technical review of the content and structure of relevant legislation in the different jurisdictions and an assessment of its applicability to cross-border payment transactions with tokenised reserves and tokenised deposits on a Project Agorá-type platform. The analysis does not express, and should not be construed as expressing, in any way a view or opinion on the suitability, desirability, appropriateness or effectiveness of any law, legislative or policy approach adopted, or to be adopted, in any jurisdiction. It is the result of collective analysis and should not be attributed to any individual contributor or the organisation that they represent, and it may not necessarily reflect the views of an individual contributor or the organisation that they represent.

Executive summary

Project Agorá – Greek for "marketplace" – is a public-private collaboration convened by the Bank for International Settlements (BIS) and the Institute of International Finance (IIF) to explore how tokenisation and programmability can enhance wholesale cross-border payments.

Cross-border payments today are burdened by structural inefficiencies that make them slow, costly and opaque. Complex, sequential processes and networks delay transactions, increase costs, limit end-to-end visibility and silo liquidity – complicating cash and treasury management. Together, these frictions weigh on global trade and financial activity, constraining innovation and growth.

Over the past two years, Project Agorá has tested the hypothesis that a multi-currency settlement mechanism that leverages tokenisation and programmability could mitigate these inefficiencies and frictions, making wholesale cross-border payments safer, faster and more transparent. By tokenising central bank reserves and commercial bank deposits, Project Agorá sought to enable secure, verifiable cross-border transactions while preserving the safety, trust and reliability of the existing banking system. This type of solution could also unlock new capabilities, including conditional and always-on wholesale cross-border payments.

To explore these concepts, the BIS and the IIF established a collaboration unique in scale and design, bringing together seven central banks and more than 40 regulated financial institutions. The resulting prototype preserves correspondent banking as the backbone of global payments while applying new technology to enhance its performance.

Project Agorá has delivered on its objectives. The prototype demonstrates that a shared distributed ledger technology (DLT) platform can support safe settlement in a tokenised environment and address long-standing challenges in wholesale cross-border payments. This prototype and its successful testing lay the groundwork for next-generation solutions.

The Project Agorá prototype

The Project Agorá prototype architecture is based on a unified ledger concept, articulated by the BIS in 2023,[1] which envisioned bringing together tokenised central bank reserves and commercial bank deposits on a shared DLT platform. It enables multi-currency, cross-border settlement and allows participants to execute payments through smart contracts.

The prototype goes beyond a proof of concept: it was developed iteratively across multiple milestones and user-tested with participating institutions. In parallel, the project included an assessment of legal and regulatory considerations associated with implementing the correspondent banking model on a programmable platform for wholesale cross-border payments. The purpose of the legal analysis was to support the development of a platform which meets Project Agorá objectives by making design choices in a legally aware manner, while also identifying legal aspects,

[1] BIS, *Annual Economic Report 2023*, June 2023.

if any, which may warrant future consideration. The design reflects a legally informed approach, aligning with existing frameworks, while also identifying areas for future consideration.

Key features

The prototype is characterised by the following key features:

- **Atomic settlement**: Atomic settlement ensures all balances update or none at all, eliminating settlement risk. The prototype shows that atomic settlement is achievable in tokenised central bank reserves and tokenised commercial bank deposits across all seven participating jurisdictions.
- **Two-layer architecture**: The prototype's architecture consists of two blockchain layers: (i) a unifying layer that is composed of a unifying ledger where tokenised commercial bank deposits are recorded and all participants can have access; and (ii) a jurisdictional layer that is composed of independent jurisdictional ledgers where tokenised central bank reserves are recorded. This design supports jurisdictional autonomy, regulatory control and flexibility for jurisdictions in the design of their respective ledgers, while ensuring sufficient commonality across ledgers.
- **Privacy controls**: The prototype ensures data protection and privacy on two levels: the token level and the transactional level. At the token level, privacy-preserving controls hide sensitive data, including customer information, while enabling the implementation of compliance controls. At the transaction level, privacy groups ensure that information is shared only among relevant participants in a transaction. Any data-sharing remains compliant with applicable legal and regulatory constraints.
- **Financial crime controls**: Each institution implements anti-money laundering (AML) / countering the financing of terrorism (CFT) / anti-fraud controls and sanctions screening independently and confidentially, while the platform ensures that all required validations are completed prior to settlement. The prototype includes functionality that would support enhanced financial crime-related information-sharing in future.
- **Implementation of data standards and best practices**: The prototype incorporates global payments data standards, such as legal entity identifiers (LEIs) and ISO 20022 Cross-Border Payments and Reporting Plus (CBPR+) as well as best practices, like "confirmation of payee" processes, improving data consistency and payment integrity.
- **Settlement finality**: The legal analysis highlighted settlement finality is achievable across all seven participating jurisdictions. Further work is needed, such as defining technical, operational and contractual requirements that are best aligned with the legal frameworks in the applicable jurisdictions.
- **Interoperability by design**: The platform is designed to operate alongside existing payment infrastructures and supports seamless cross-border workflows, ensuring that new jurisdictions and assets can be added without disrupting existing operations.

Key outcomes

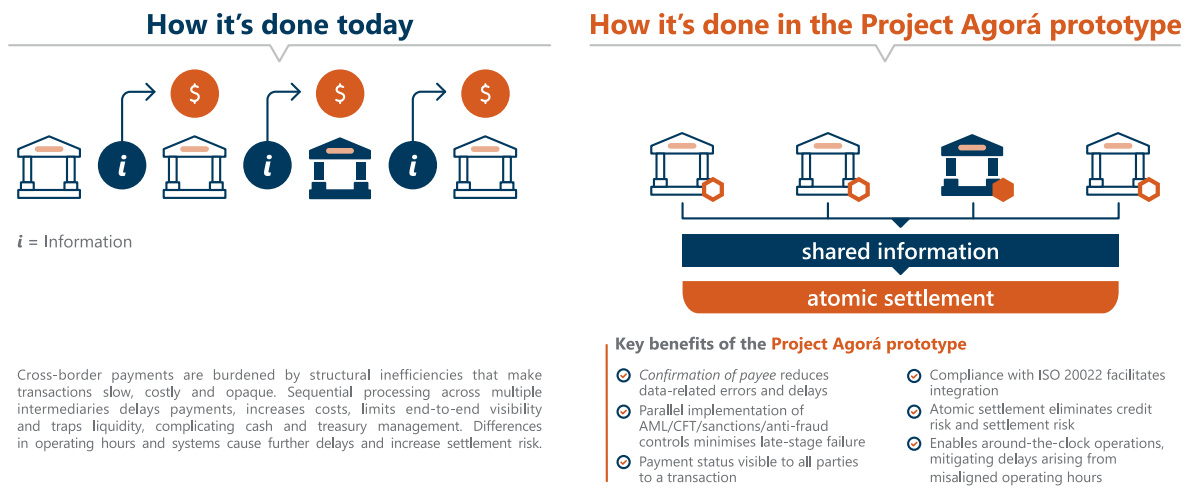
The prototype illustrates how shared infrastructure, interoperable tokens, programmable workflows, atomic settlement and privacy-preserving execution can address many of the well known pain points in cross-border payments (Figure 1). It demonstrates that atomic settlement, which ensures that either all balance updates occur or none at all, eliminates credit and settlement risk.

The need for sequential processing is reduced by combining a path discovery mechanism with the ability to perform certain controls, such as sanctions screening, AML/CFT checks and fraud detection, in parallel. In addition, the prototype brings forward the alignment of payment-related information to take place before liquidity is committed and settlement occurs. This decoupling of information from the movement of funds enables atomic settlement, potentially lowering the incidence of failed payments and reducing the costly need to unwind transactions after liquidity has been committed.

Speed is also improved, with settlement occurring in seconds once funds or liquidity are locked. The platform is designed to operate around the clock, helping to mitigate delays caused by misaligned operating hours across jurisdictions.

The prototype also enhances transparency. All parties to a transaction have access to real-time payment status, while maintaining privacy from non-participating entities. In future, such visibility could be extended to end users, including debtors and creditors.

Wholesale cross-border payments today and in Project Agorá
Benefits of the Project Agorá platform **Figure 1**



Source: Project Agorá.

The prototype design, validated through user testing, achieves its primary objective by demonstrating that a shared ledger can address many of the pain points in wholesale cross-border payments. More broadly, Project Agorá has delivered additional outcomes demonstrating the viability of key legal and operational foundations required for the future development of tokenisation-related initiatives.

- **Tokenisation using blockchain technology can significantly enhance cross-border payment workflows.** The prototype shows how processes that are traditionally fragmented can be integrated, enabling the coordinated crediting and debiting of multiple accounts.
- **Large-scale public-private collaboration is essential to unlock new potential.** The breadth of participation ensured that the prototype accommodates diverse technical, legal and business requirements.
- **A shared ledger can preserve jurisdictional autonomy and flexibility.** The Project Agorá prototype's two-layer design allows central banks to pursue jurisdiction-specific initiatives while ensuring sufficient commonality to enable atomic settlement and integration with payment workflows between tokenised reserves and tokenised deposits on a shared platform.
- **Tokenisation does not fundamentally alter the legal nature of money.** Legal analysis confirms that tokenisation as contemplated in this prototype does not alter the legal characterisation of the underlying balances or the nature of the obligations represented by tokenised reserves and tokenised deposits, allowing for the development of tokenisation projects within existing legal and regulatory frameworks.
- **A shared ledger does not require shared data.** Privacy controls enable data sharing only when necessary and approved by participants, rather than by default.
- **Interoperability of tokenised deposits is key in the development of a tokenised financial ecosystem.** Settlement in tokenised central bank reserves is one way to enable deposits to operate seamlessly, supporting broader applications, including cross-border capital market transactions.

In addition, the Project Agorá prototype identified a number of areas that could be explored to enhance the functionality of the prototype and unlock additional benefits. These enhancements, along with further legal and regulatory analysis, would be needed to strengthen the prototype's feasibility and value proposition. Examples include exploring more coordinated AML/CFT, sanctions and anti-fraud approaches, developing liquidity saving mechanisms, strengthening cybersecurity posture and operational resilience, and advancing interoperability and compatibility requirements. Additional work on governance, rules and oversight – covering participation, settlement finality, data governance and risk management – will be essential to support safe and scalable deployment while preserving jurisdictional autonomy.

Project participants, including central banks, have expressed strong and sustained interest in further exploring the potential benefits of the prototype. Future work is expected to involve an enhanced role for the private sector, supported by continued and active engagement from participating central banks.

Introduction

Project Agorá – Greek for "marketplace" – is a public-private collaboration convened by the Bank for International Settlements (BIS) and the Institute of International Finance (IIF) to explore how tokenisation and programmability can enhance wholesale cross-border payments.

Cross-border payments, representing trillions of dollars in daily flows, underpin global trade and economic activity. Correspondent banking remains the backbone of this system: trusted, resilient and globally connected. Yet its fragmented structure creates persistent inefficiencies, leaving cross-border transactions slower, more costly and less transparent than domestic payments.

At the same time, tokenisation – the recording of assets and claims on a distributed, programmable platform – is a potentially transformative innovation for the international financial system. Public and private institutions are testing how its core features, particularly programmability and composability, may enhance efficiency, mobilise capital, harness liquidity and broaden market access. Tokenisation may have similar benefits for correspondent banking, yet it has not been widely tested in a multi-institution, multi-currency setting.

Over the past two years, Project Agorá has explored how implementing the correspondent banking model on a programmable platform may make wholesale cross-border payments faster, more efficient and safer. It also has explored how this programmable platform may enable additional innovative functionalities in cross-border payments. To test this hypothesis, the BIS and the IIF established a public-private collaboration unique in scale and design. The project brought together seven central banks and more than 40 regulated financial institutions to build a prototype that preserves correspondent banking as the backbone of global payments while applying new technology to enhance its performance. Since Project Agorá launched, significant developments in the tokenisation landscape have elevated the opportunities and urgency for infrastructure to support settlement of tokenised reserves and tokenised deposits.

Project Agorá has delivered a prototype that demonstrates that tokenised commercial bank deposits can be successfully combined with the trust and safety of tokenised central bank reserves on a shared platform. The prototype enables atomic, multi-currency settlement of wholesale cross-border payments, which could occur on an around-the-clock basis if implemented. More broadly, by leveraging smart contracts, the platform allows financial institutions to embed workflow logic, compliance requirements and conditional payment triggers directly into transactions. This promises to reduce reconciliation burdens, manual intervention and other operational frictions – key sources of delay, cost and payment failure in today's cross-border system.

Project Agorá has sought to use innovation to strengthen the existing correspondent banking model while enabling new payment capabilities. At the same time, it has balanced technological advancement with trust, stability and financial integrity. In parallel, the project has examined the legal and regulatory implications of tokenised deposits and tokenised reserves – including settlement finality, anti-money laundering and countering the financing of terrorism (AML/CFT) and data protection and privacy. By identifying cross-jurisdictional challenges and gaps, Project Agorá may help to lay the foundation for a resilient and well regulated next generation of cross-border payments.

This report describes Project Agorá and the prototype it delivered. It includes seven chapters that, taken together, describe the vision, design and functioning of the prototype and

highlight the project's key achievements – including an effective public-private collaboration that balanced the interests of all participants. Chapter 1 provides an overview of the context, vision and objectives for the project. Chapter 2 describes the process by which those objectives were translated into specific business requirements and design choices that guided the development of the prototype. Chapter 3 provides a snapshot of the key components of the prototype and how those components work in practice to facilitate a wholesale cross-border transaction. Chapters 4 and 5 are self-standing chapters that provide in-depth discussion of specialised topics. Chapter 4 details the technical specifications for the prototype, and Chapter 5 details the legal analysis that was undertaken in relation to the prototype. Chapter 6 explains how a Project Agorá-like solution could benefit cross-border payments, including providing examples of how this type of platform could improve specific transactional scenarios experienced today. Chapter 6 also explains the limitations of the prototype. Chapter 7 summarises the key outcomes of the project overall and identifies areas that may be considered for future exploration.

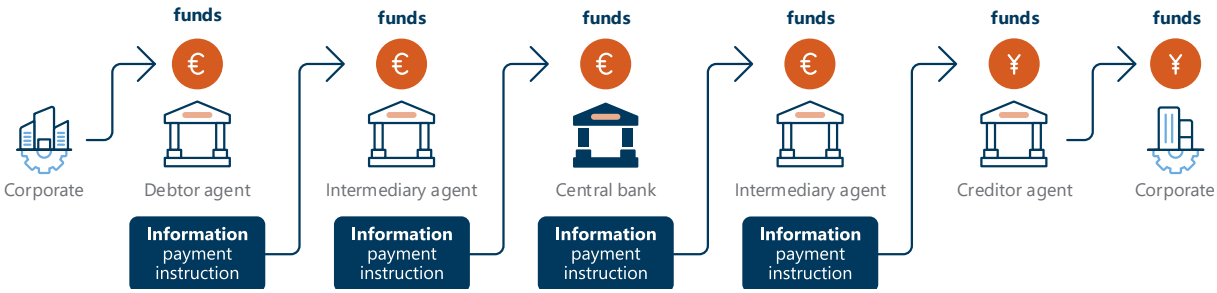
The BIS undertook Project Agorá within the BIS Innovation Hub, which aims to foster international collaboration on innovative financial technology in the central banking community. BIS Innovation Hub projects are experimental in nature, for the purpose of investigating technological and practical feasibility. During this prototype build, the project prioritised foundational architecture over full optimisation, reflecting a deliberate design choice to focus on the essential core elements necessary to inform the technical design and architecture needed for a multi-currency, multi-jurisdiction payments platform. The report therefore identifies areas for further development and distils key lessons for a future tokenised financial ecosystem.

Chapter 1: Context, vision and objectives

Cross-border payments are a critical enabler of global trade and finance. In 2024, they totalled $195 trillion and are projected to reach $320 trillion by 2032.[2]

Correspondent banking, the network of relationships and processes that moves funds across banks, countries and currencies, remains the backbone of cross-border payments. However, it is burdened by structural inefficiencies that make transactions slow, costly and opaque. Sequential processing across multiple intermediaries delays payments, increases costs, limits end-to-end visibility and siloes liquidity, complicating cash and treasury management. Differences in operating hours and systems further delays and increase settlement risk (see Figure 2 for an illustration of cross-border payment flows today).

Cross-border payments done today **Figure 2**



Source: Project Agorá.

These challenges are compounded by high false-positive rates in compliance screening, inconsistent data quality and limited transparency on transaction status, routing and fees. At the same time, rising costs and risks have contributed to a decline in correspondent banking relationships, increasing the risk that some institutions, jurisdictions or regions lose reliable access to cross-border payment services.[3]

Taken together, these frictions weigh on global trade and financial activity, constraining efficiency, innovation and growth. In response, global policymakers have prioritised cross-border payment reform, including through the G20 Roadmap for Enhancing Cross-Border Payments, while private sector institutions continue to invest in improvements in this space.[4]

---

2 FXC Intelligence, "New data: cross-border payments market now worth over $194tn and is forecast to reach $320tn by 2032", 16 January 2025.

3 Financial Stability Board, *FSB Action Plan to Assess and Address the Decline in Correspondent Banking*: Progress Report, May 2019.

4 Financial Stability Board, *G20 Roadmap for Cross-border Payments: Consolidated Progress report for 2025*, May 2025. In 2020, at the request of the G20, the Financial Stability Board, in coordination with the BIS Committee on Payments and Market Infrastructures (CPMI) and other international standard-setting bodies, developed the G20 Roadmap for Enhancing Cross-Border Payments. The G20 Roadmap sets out a comprehensive, high-level plan to address four core challenges: high costs, slow speeds, limited access and insufficient transparency. It has since provided the overarching framework for reforms aimed at reducing structural frictions – including extending central bank and payment system operating hours and promoting the adoption of harmonised data standards.

Vision for the unified ledger and Project Agorá

Efforts to enhance cross-border payments have delivered incremental improvements, yet operational inefficiencies persist.[5] Tokenisation, the recording of assets and claims on a programmable platform, may offer a credible path to overcoming some of these structural frictions.

In its 2023 Annual Economic Report, the BIS argued that the full benefits of tokenisation are best realised if tokenisation is implemented in a way that preserves the two-tier banking system. In this framework, central banks anchor the monetary system by issuing the unit of account and ensuring settlement on their balance sheets, while commercial banks provide financial services and issue deposits to the public.[6]

The BIS emphasised that this structure safeguards the "singleness of money": the principle that payments denominated in the sovereign unit of account settle at par, regardless of whether they are made using public or private forms of money. The BIS report explained that this property is fundamental to financial stability.

To operationalise this vision, the BIS proposed a blueprint for a future entirely tokenised monetary system centred on a *unified ledger* concept that integrates tokenised central bank reserves and tokenised commercial bank deposits. By co-locating these forms of money on a shared platform, transactions could benefit from the settlement finality of central bank reserves, while enabling programmability and innovation, combining trust with technological capability.

Project Agorá builds on this concept in two ways. First, it seeks to enhance the existing correspondent banking model through tokenisation. Tokenised deposits remain claims on commercial banks, but their programmable nature enables faster settlement, automation, and composability of transactions, with interoperability across jurisdictions and infrastructures, strengthening efficiency and reach.

Second, the project explores new payment capabilities. It examines whether such a platform can support innovative use cases, including conditional, instant and always-on cross-border transfers executed safely, efficiently and with integrity embedded. Central bank reserves and commercial bank deposits remain central to the financial system, and the project demonstrates how these instruments can be tokenised on a common platform across multiple currencies and jurisdictions, each with distinct legal and regulatory frameworks.

Project participants

The BIS and the IIF launched Project Agorá in April 2024 as a joint public-private initiative. The BIS convened seven central banks representing the major convertible currencies:[7] the Banque de France (for the Eurosystem), the Bank of Japan, the Bank of Korea, the Bank of Mexico, the Swiss National

---

5 T Lammer, D Rees, T Rice and T Shirakami, "Enhancing cross-border payments: state of play and way forward," *BIS Bulletin*, no 119, December 2025.

6 BIS, *Annual Economic Report 2023*, June 2023.

7 Bank for International Settlements: *Triennial Central Bank Survey of Foreign Exchange and Over-the-counter (OTC) Derivatives Markets in* September 2025.

Bank, the Federal Reserve Bank of New York (via its New York Innovation Center) and the Bank of England. The IIF brought together a group of more than 40 regulated financial institutions.

Participants were selected to ensure diversity in business models, institutional size, expertise and geographic representation. Eligibility to join the project required being a regulated financial entity (eg a commercial bank, payment service provider or financial market infrastructure) with additional jurisdiction-specific requirements such as access to real-time gross settlement systems, or central bank reserve accounts. Priority was given to institutions active in cross-border payments and innovation initiatives.

Public and private sector participants guided and directed all project activities through the Project Agorá Committee, co-chaired by the BIS and the IIF and comprising representatives from participating institutions. Design and development work was organised across three core workstreams: business, technology and legal. A separate communications workstream coordinated all public-facing activities. Each workstream included representatives from across the BIS, the IIF and participating public and private sector institutions.

Project objectives

Project Agorá participants assessed the BIS unified ledger concept against key cross-border payments challenges and focused on wholesale payments, including large corporate transactions, given their systemic importance. Wholesale payments accounted for 91% of cross-border payment value in 2023[8] and offer strong potential for network effects.

In defining the project's scope participants also drew on insights from earlier initiatives exploring tokenisation in financial markets and banking. The objective was to build on established learnings and further develop emerging concepts. For example, BIS Innovation Hub projects, such as Project Helvetia and Project Jura, examined payment settlement using wholesale tokenised central bank reserves, on a national and cross-currency basis, respectively.

Similarly, the Regulated Liability Network project, an industry-led initiative, explored the concept of a blockchain-based financial infrastructure enabling (tokenised) commercial bank deposits, central bank reserves and stablecoins to operate on a shared ledger.[9] In parallel, the Eurosystem's exploratory work highlighted strong interest among market participants in using DLT and tokenisation for wholesale transactions, particularly to improve efficiency through process redesign. The Eurosystem's work also confirmed the importance of central bank reserves as a safe settlement asset for DLT-based transactions.[10]

[8] FXC Intelligence, "Cross-border payments market sizing data", available at https://www.fxcintel.com/cross-border-payments-market-sizing-data (accessed 27 April 2026).

[9] The Regulated Liability Network, *The Regulated Liability Network: digital sovereign currency*, November 2022.

[10] European Central Bank, *Bridging innovation and stability: The Eurosystem's exploratory work on new technologies for wholesale central bank money settlement*, June 2025, https://www.ecb.europa.eu/paym/dlt/exploratory/html/index.en.html.

Based on this analysis, participants pursued four potential benefits:

- **Interoperability of tokenised assets**: A shared ledger could support the interoperability of tokenised reserves and tokenised deposits, unlocking safe settlement of cross-border and cross-currency transactions.
- **Programmability and composability**: Integration of functions and processes traditionally handled separately, such as messaging, clearing and settlement, reducing delays and operational frictions.
- **Atomic settlement**: Joint execution of payment steps (eg debiting accounts, updating nostro balances, settling in central bank reserves and crediting recipients) in a single transaction, eliminating settlement risk and reducing liquidity needs.
- **Enhanced compliance**: A shared platform could improve AML/CFT, anti-fraud and sanctions controls through streamlined validation, reduced duplication and potential for enhanced information-sharing.

Project assumptions

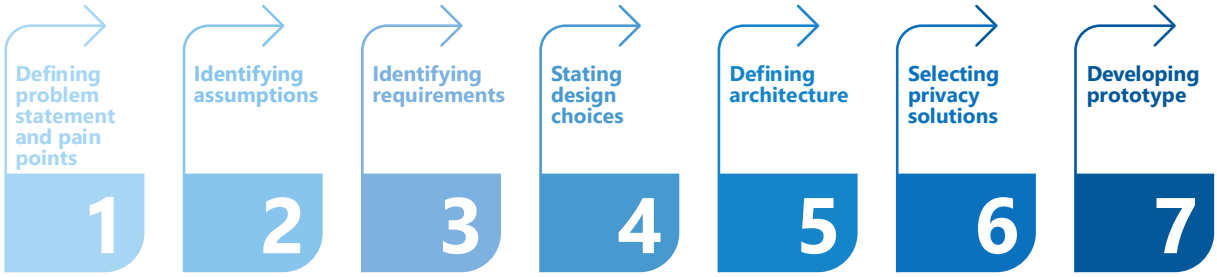
Project participants agreed on a set of foundational assumptions that define the scope of the work and the boundaries within which the Project Agorá platform operates:

- **Access policies are retained.** Eligibility, onboarding and participation in tokenised reserves and tokenised deposits remain the sole responsibility of the relevant central banks and commercial banks. Existing bilateral relationships and access controls are preserved and not altered by the platform.
- **Issuance of tokenised reserves and tokenised deposits is agnostic to funding sources.** The platform is agnostic to the issuance mechanism, which may reflect reserves or deposits, credit lines or other facilities.
- **The platform as the golden source of truth.** Balances and transactions recorded on the Project Agorá platform are treated as the authoritative record for tokenised deposits and tokenised reserves. Participants remain responsible for reconciling with their internal systems, and the prototype assumes continued interactions with legacy infrastructure.
- **Calibrated scope.** Given the ambitious objectives of Project Agorá, its experimental nature and available resources, the prototype does not prioritise production-grade capabilities such as scalability, throughput, latency or cyber security, nor functionalities such as liquidity savings mechanisms at this juncture. The focus remains on payments within the correspondent banking model; foreign exchange (FX) integration and other types of tokenised asset classes are out scope for the prototype.

Chapter 2: Business requirements and design choices

The development of the Project Agorá prototype reflects the translation of business needs into concrete requirements and corresponding design choices. The project was primarily driven by alleviating frictions in existing wholesale cross-border payment processes. Project participants translated these challenges, together with the project objectives and assumptions, into business requirements that shaped the design of the Project Agorá prototype (Figure 3).

Project Agorá approach to prototype **Figure 3**



Source: Project Agorá.

Understanding the business challenges

To inform the business requirements, Project Agorá participants undertook a focused analysis to evaluate the operational frictions affecting cross-border payments.[11] This analysis emphasised the dimensions most relevant to wholesale financial institutions: speed, efficiency, transparency and risk reduction.

- **Speed** is the time required for a payment to be processed and settled between the debtor and the creditor. It is influenced by factors such as accuracy, certainty, time zones and transparency, which determine the overall time for funds to reach the ultimate beneficiary.
- **Efficiency** relates to the smooth functioning of payment processes, including straight through processing, liquidity management, costs, routing and beneficiary validation, and timely resolution.
- **Transparency** concerns end-to-end visibility of transactions – from initiation to final credit – as well as access to relevant payment details such as fees and cross-currency amount.
- **Risk reduction** encompasses measures to mitigate settlement, operational, counterparty, market or liquidity risks.[12]

[11] Financial Stability Board, *Enhancing Cross-border Payments: Stage 3 roadmap*, October 2020.

[12] Project Agorá did not treat cost reduction as a primary design objective for the prototype. This reflects the assessment that many major cost drivers in wholesale cross-border payments arise from non-technological choices (eg FX pricing and market structure features). However, operational costs are materially increased by error handling, including investigations, returns, and reconciliations; therefore, some of the design choices may have secondary effects on costs.

High-priority cross-border payment pain points identified by Project Agorá		Table 1
Pain point	**Category**	**Description**
Predictability / availability (operating hours)	Speed, efficiency, transparency, risk reduction	Payments initiated outside overlapping market hours can delay cross-border transactions. In addition, certain flows, such as "payments against the sun", tend to experience longer delays than those that "follow the sun".
Sanctions/compliance screening, including hit ratio (false positives)	Speed, efficiency, risk reduction	False positives lead to additional checks and delays in clearing legitimate transactions. Differences in jurisdictional requirements may compound these operational challenges.
Sequential/serial processing	Speed	Payments are typically processed sequentially with both messaging and settlement occurring step by step. Each participant can only act once prior processes are complete, which slows execution. This sequential nature also affects efficiency, liquidity and error rates and may lead to duplicative checks across the payment chain.
Accuracy (data quality)	Efficiency	Discrepancies can arise from data entry errors, inconsistent date standards (eg purpose codes or routing identifiers such as ACH or BSB codes) or miscommunication between parties.
Transparency (payment status, fees)	Transparency	Transparency issues arise from limited clarity about a transaction status, fees and participating entities, often compounding data quality and accuracy issues. These challenges can be grouped into three areas: 1. *Payment and routing visibility*: limited insight into intermediaries and payment paths can delay processing, complicate tracking and resolution of exceptions scenarios. 2. *Payment status*: real-time updates are often lacking due to multi-step processes, multiple intermediaries and differences in service level agreements (SLAs). 3. *Fee transparency*: the level and allocation and timing of fees are not always clear.
Liquidity visibility, and allocation	Efficiency	Transparency for banks involved in transactions and access to liquidity positions are essential for efficient cross-border payments. Limitations in these areas can lead to delays and higher costs, including increased prefunding needs and more complex liquidity and treasury management. Cross-border payments can also be liquidity-intensive, depending on settlement method (eg gross settlement), with delays further increasing liquidity demands. Liquidity saving and settlement mechanisms, such as netting, can improve efficiency. In addition, treasury allocation outside operating hours is often required to manage liquidity and credit risk, ensuring funds are available for transactions occurring beyond regular business hours.
Settlement risk	Risk reduction	Settlement risk refers to the risk that a funds or securities transfer will not settle as expected, encompassing both credit and liquidity risk. A key objective in payments is to mitigate this risk through mechanisms such as payment versus payment (PvP) and on-us settlement.[1]
Reconciliation breaks	Efficiency	Reconciliation processes serve as a backstop for errors and settlement issues, but discrepancies are often identified only after settlement, when they are more difficult and costly to resolve. Moreover, reconciliation itself is resource-intensive, adding to operational costs.

Client outreach	Speed, Efficiency	Client outreach is essential for confirming payment expectations and resolving issues along the transaction chain. However, it can be time-consuming and complex, particularly in terms of identifying the appropriate contacts and managing manual interactions with clients and intermediaries.

[1] BIS-CPMI glossary, www.bis.org/cpmi/publ/d00b.htm?selection=65.

Source: Project Agorá.

Building on this framework, the project examined how these frictions arise in practice across wholesale cross-border payment chains. Table 1 summarises the key priorities identified for the prototype. These include delays arising from operating hour mismatches, data quality issues, reconciliation breaks, liquidity constraints and risks linked to sanctions screening.

A recurring theme is limited transparency, in terms of both payment status and fee predictability. This lack of visibility persists across multiple steps of the payment chain and amplifies other frictions, including operational complexity, reconciliation burdens and uncertainty for financial institutions and their clients.

These pain points were prioritised because they materially affect speed, efficiency, transparency and risk in cross-border payment chains and could be addressed through improved coordination on a programmable platform.

These pain points reflect the inherently sequential nature of wholesale cross-border payments, which require settlement across multiple entities operating on siloed systems. Tokenisation offers a way to address these challenges by enabling the secure sharing of data and transactions across participants.

Against this backdrop, the prototype focused on two transaction types that best leverage the composability and programmability of tokenisation: multi-party end-to-end (E2E) payments and payment versus payment (PvP) (Table 2). While other transaction types, such as book transfers, could also be supported, these two offer the greatest potential benefit, as frictions are less pronounced in simpler transactions.

E2E payments involve a single debtor and a single creditor, with settlement requiring a chain of balance updates across one or more intermediary financial institutions. In practice, such payments may arise from corporate transactions (eg the purchase of goods or services), as well as interbank activity (eg liquidity management and settlement of financial trades). The key challenge is to coordinate these balance updates so that funds move predictably from the debtor to the creditor, even across multiple institutions, currencies and jurisdictions.

PvP outcomes introduce a different structural constraint. They involve two linked settlement legs, each with its own debtor and creditor, that must complete together to eliminate principal risk. While PvP outcomes are often associated with foreign exchange activity, the platform treats them as linked balance updates rather than as trading transactions. The settlement requirement is that neither leg completes independently of the other, regardless of how or where the underlying obligation was generated.

The two main transaction types in the Project Agorá prototype				Table 2
	Number of debtors	**Number of creditors**	**Examples of payment triggers**	**Initiating party**
End-to-end transaction (E2E)	1	1	Corporate invoices, funding of accounts of financial institutions	Initiator (eg banks on their own behalf) Initiation service provider (eg banks on behalf of their customers)
Payment versus payment (PvP)	2	2	FX trades in exchanges	Initiator (eg banks on their own behalf) Initiation service provider

Source: Project Agorá.

Beyond the priority pain points, Project Agorá identified a broader set of frictions assessed as lower priority. These include delays and operational complexity arising from investigations, AML checks at transaction initiation, and the resource-intensive nature of post-transaction monitoring to meet funds transfer obligations.

Additional challenges relate to the lack of harmonised end-to-end data and compliance standards across jurisdictions, cumulative fees from multi-intermediary processing chains, and uneven access to risk-reducing settlement mechanisms such as PvP arrangements. The impact of counterparty and jurisdictional de-risking on access to cross-border payment services was also noted. While relevant, these were not prioritised for development of the prototype and are documented to reflect the broader problem landscape.

Business requirements

Based on the pain point analysis, Project Agorá identified a comprehensive set of business requirements to guide the development of the prototype. The requirements reflect longstanding challenges in wholesale cross-border payments, together with operational, legal and regulatory expectations for a future settlement environment. They inform the technical design and architecture of the prototype; they are not intended as measured operational outcomes nor as a full production-grade system specification.[13]

1. Jurisdictional autonomy and governance: The prototype must support wholesale cross-border payments across multiple jurisdictions while enabling jurisdictions to retain autonomy over domestic monetary arrangements, policy controls, access rules and operations. The prototype must also enable central banks to retain full control over their tokenised reserves.[14]

2. Issuance, redemption and transfer of tokenised deposits and tokenised reserves: The prototype must provide records of tokenised central bank reserves and tokenised commercial bank deposits in a way that preserves existing legal and balance sheet relationships. The records must support issuance, holding, transfer and redemption consistent with the responsibilities of issuers

[13] Some business requirements – not listed here – were purposefully deprioritised.

[14] This requirement has great impact on the choice of the platform architecture; see Chapter 4 for more information.

and holders, and must enable predictable, auditable settlement outcomes across jurisdictions. The prototype also must implement safeguards that allow issuing institutions to pause issuance, redemption, or transfers and act on behalf of account holders in exceptional circumstances without disrupting the platform as a whole.

3. Settlement and risk management: The prototype must ensure that wholesale cross-border transactions settle atomically, whether structured as E2E payments or PvP transfers to eliminate principal and settlement risk by preventing partial execution or inconsistent outcomes.

4. Pathfinding and identification: The prototype must support the identification, validation and agreement of viable payment paths across multiple participants. This includes identifying intermediaries, validating correspondent relationships and presenting alternative payment-chain options where available. Approval and transparency mechanisms must ensure that decisions are visible to relevant parties and aligned with participant preferences and constraints.

5. Cross-currency integrity: The prototype must ensure that, for payments involving more than one currency, cross-currency amounts are determined correctly, pricing logic is applied consistently for workflow purposes, and all transaction balance updates are settled in a coordinated manner.

6. Access, participation and authorisation models: The prototype must distinguish between direct and indirect participants, specify their eligibility to hold or transact in tokenised reserves and tokenised deposits, and establish role-based authorisation throughout the transaction life cycle. The prototype must enable participants to authorise parties to perform limited actions on their behalf without shifting accountability from the originating participant.

7. Compliance, pre-validation and screening: The prototype must support coordination of AML/CFT, fraud, sanctions and balance checks before settlement occurs. It must allow for participants to perform their own checks independently and to securely share only the necessary outcomes with other authorised parties in the payment chain. The prototype must allow transactions to proceed only once all mandatory pre-validation steps are satisfied and duplication is reduced.

8. Data standards, quality and interoperability: The prototype must incorporate ISO 20022 data standards and align with CBPR+ and High Value Payment Systems Plus (HVPS+) where applicable.

9. Reduction of exceptions and investigations: The prototype must reduce exceptions and manual investigations in cross-border flows by enabling structured early-stage checks, clear participant responsibilities at each workflow stage, and deterministic progression and termination outcomes that prevent ambiguous intermediate states.

10. Transparency, notifications and reporting: The prototype must enhance E2E visibility of payment status, confirmations and outcomes on a need-to-know basis. It should support real-time notifications, audit trails and monitoring of tokenised reserves and tokenised deposits, while limiting broader visibility to relevant participants.

11. Privacy and selective data-sharing: The prototype must preserve confidentiality of customer information, pathfinding preferences, compliance outcomes and institution-specific logic. The prototype must share minimum necessary information, only with the institutions directly involved at each step of the workflow on a *need-to-know* basis. Any data-sharing in the prototype must remain compliant with applicable legal and regulatory constraints on data-sharing.

12. Liquidity management and monitoring: To support treasury operations in an around-the-clock environment, the prototype must allow participants to monitor balances and liquidity positions held in tokenised reserves and tokenised deposits on the platform, at both granular and aggregated levels. The prototype must also provide the visibility and monitoring foundations needed for those operations and accommodate future enhancements such as liquidity saving or optimisation mechanisms, which are out of scope for the prototype.

13. Governance, roles and responsibility allocation: The prototype must preserve existing institutional roles or legal responsibilities. For example, customer relationships, compliance obligations and reconciliation with traditional systems must remain with issuing and participating institutions, and central banks and commercial banks must retain appropriate control over their tokenised reserves and tokenised deposits, respectively.

14. Platform reliability, security and scalability: The prototype must meet the non-functional requirements needed to operate a global settlement platform based on tokenised reserves and tokenised deposits. This includes performance, availability, resilience, deterministic settlement, strong security and confidentiality controls, observability and extensibility, while participants require these properties to ensure the platform can operate safely and reliably at scale across multiple jurisdictions and institutions.

15. Settlement finality: To achieve legal certainty (including appropriate insolvency protections) across participating jurisdictions, participants require a clearly defined settlement event (or trigger) for payments executed on the platform. Such a trigger could be reflected in an applicable rulebook(s) and enforceable within the relevant legal frameworks. The prototype must ensure that the workflow produces an unambiguous, auditable settlement outcome for multi-leg transactions, consistent with the platform's atomic settlement logic.

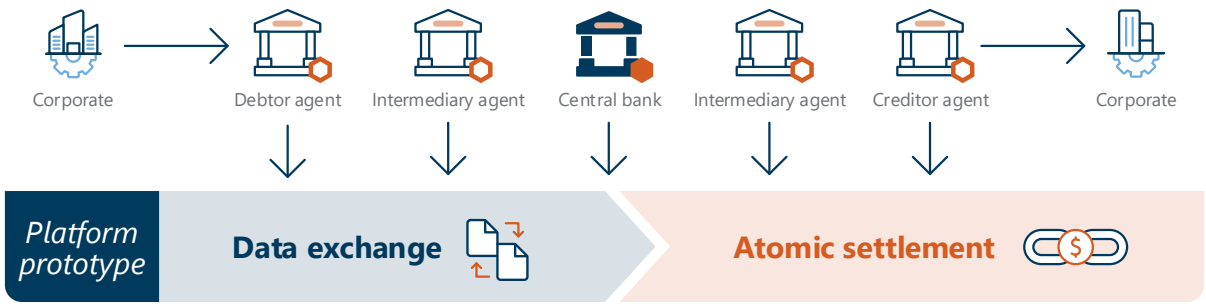
Design choices

Based on the frictions observed in wholesale cross-border payments and the business requirements identified above, a set of design choices was defined for the prototype. These do not materially alter the correspondent banking model or the current roles of participants. Instead, they bring forward the alignment of payment-related information to take place before liquidity is committed and settlement occurs. This decoupling of information from the movement of funds enables atomic settlement (Figure 4).

Taken together, the design choices below address fragmentation, limited visibility, and risk while remaining consistent with existing legal, regulatory, and operational responsibilities.[15]

[15] Some steps such as confirmation of payee, path discovery and compliance checks are not implemented for PvP.

Cross-border payments done in Project Agorá **Figure 4**



Source: Project Agorá.

1. Framing atomic settlement as coordinated balance updates. Wholesale cross-border payments ultimately result in a series of balance updates across financial institutions and their account holders. Project Agorá treats payment execution as a coordinated update of these balances, rather than as the outcome of bilateral instructions. Before execution, the debtor agent, creditor agent, and any intermediaries agree on the required balance movements to complete the end-to-end payment. These are conditionally linked so that either all occur or none do, enabling atomic settlement through programmable of DLT functionality. This supports settlement without relying on reconciliation or post-settlement claims to correct mismatches.

2. Confirmation of payee before payment initiation. Accurate beneficiary information upfront is necessary to identify the relevant balance updates. In current wholesale cross-border payments, beneficiary verification may be incomplete or inconsistent, with errors discovered only after funds have moved. Project Agorá incorporates the global best practice of confirmation of payee into the preparation stage. The debtor agent requests the creditor agent to confirm the beneficiary account and identity before settlement conditions are finalised. This reduces misdirected payments and downstream corrections, while preserving existing customer relationships.

3. Identifying and agreeing the payment path through a path discovery mechanism (PDM). In cross-border and cross-currency payments, the full chain of intermediaries is not always known at the outset. Today, routing decisions may be made dynamically, limiting transparency and increasing the risk of failure. Project Agorá introduces a path discovery mechanism (PDM) to identify the parties on a payment chain before execution. Where a payment instruction is submitted with incomplete path information, the platform can identify and propose viable intermediaries using shared reference data, reflecting customer, correspondent, nostro, central bank and other relevant account relationships. All proposed paths remain subject to approval by the relevant institutions. Each participant retains control over decisions related to its own involvement, while gaining earlier alignment on the full end-to-end path.

4. Sharing outcome of compliance checks before atomic settlement is initiated. Once the payment path is established, institutions must confirm that required compliance checks have been completed. Today, these checks are performed independently and repeatedly across the payment chain, with limited clarity about whether other parties have already completed them. Under Project Agorá, each institution continues to perform its own compliance and pre-validation checks,

including know your customer (KYC), AML, CFT, fraud and sanctions screening and others. What changes is that the outcomes of these checks can be shared (ie passed or failed), in a controlled manner with other authorised participants before atomic settlement is initiated.[16]

5. Locking liquidity and executing atomic settlement. With payment details, compliance outcomes and balance movements aligned, settlement can proceed with greater certainty. In current correspondent banking flows, liquidity is often committed sequentially, creating the risk that some legs settle while others do not. Project Agorá requires participating institutions to lock the balances required for settlement before execution. Settlement proceeds only once all required balances are locked. If any participant is unable to commit the required balance within the agreed window, the payment does not execute, any locked committed funds are unlocked, and the payment is aborted. This enables atomic settlement: either all balance updates occur, or none do. Partial completion risk is removed, while liquidity and credit decisions remain fully with each participant.

6. Executing payments to allow near real-time settlement (independent of external system hours). Execution is often constrained by the operating hours of domestic settlement systems and external infrastructures. By coordinating balance updates and settlement conditions directly on the platform, Project Agorá enables transaction execution whenever participating institutions have the required balances available on the platform, regardless of the operating hours of external issuance or redemption systems (ie real-time gross settlement (RTGS) or core banking systems). Issuance and redemption remain subject to existing constraints, but execution between participants would no longer be coupled to those windows in a Project Agorá-like platform.

Taken together, these design choices shift cross-border payment execution from a sequential, opaque process to one where key elements are aligned before settlement is attempted. By agreeing balance updates, validating participants and data, and confirming paths and payees in advance, Project Agorá reduces uncertainty around whether and how a payment will complete. Settlement becomes a controlled coordination exercise rather than a series of dependent hand-offs, improving predictability and reducing operational risk without changing institutional responsibilities or existing monetary arrangements.

[16] Since these outcomes rely on proprietary logic of each individual relevant party in the payment chain that is not expected to be fully encoded on the Project Agorá platform, transactions that require investigations may still impede straight-through-processing.

Chapter 3: The Project Agorá prototype

The Project Agorá platform is a multi-jurisdictional technical arrangement that relies on permissioned, shared ledger technology and additional off-ledger components to support the initiation and settlement of wholesale cross-border payments.

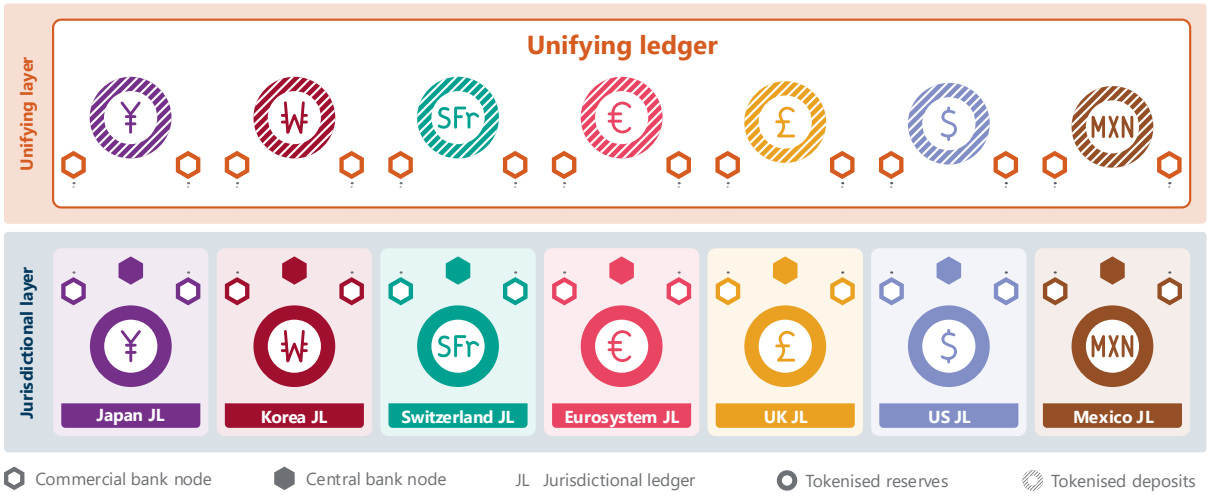
Tokenised reserves and tokenised deposits are recorded on the platform's shared ledgers. Tokenised reserves and tokenised deposits constitute balances in underlying reserve or deposit accounts at the relevant central bank or commercial bank, and record changes to those balances on the shared ledgers when payments are executed on the platform.

The platform architecture comprises two interconnected ledger layers (Figure 5):

- A **unifying layer**, consisting of a single shared ledger where tokenised commercial bank deposits are issued and accessible to all relevant participants.
- A **jurisdictional layer**, consisting of separate shared ledgers for each participating jurisdiction, where tokenised central bank reserves are issued.[17]

Each ledger is maintained by participant-operated blockchain nodes and governed by a common protocol governing how the ledger operates and how nodes interact with it. A cross-ledger coordination model (ie rules and procedures for communication between nodes operating on separate ledgers) enables communication and synchronisation between the unifying and jurisdictional layers. Deposit-taking commercial banks and eligible participants operate nodes on the unifying ledger, while central banks and eligible participants operate nodes on their respective jurisdictional ledgers.[18]

The Project Agorá layered architecture **Figure 5**



Source: Project Agorá.

[17] Tokenised commercial bank deposits can also be issued on a jurisdictional ledger.

[18] The design described here does not preclude the possibility that tokenised reserves may be recorded on the unifying ledger and/or tokenised deposits may be recorded on a jurisdictional ledger. In the prototype, node access across the unifying and jurisdictional ledgers is fixed along types of participating institutions; however, the underlying architecture is designed to support additional node access configurations.

Platform functionality is implemented through three types of smart contracts:

- **Asset smart contracts**, which define and manage tokenised central bank reserves and tokenised commercial bank deposits, including balances and token-level permissions.
- **Workflow smart contracts**, which coordinate payment execution by constructing payment paths, facilitating compliance checks, determining cross-currency amounts, securing participant approvals, locking balances and executing settlement.
- **Reference smart contracts**, which store supporting registry/configuration data such as participant and account information.

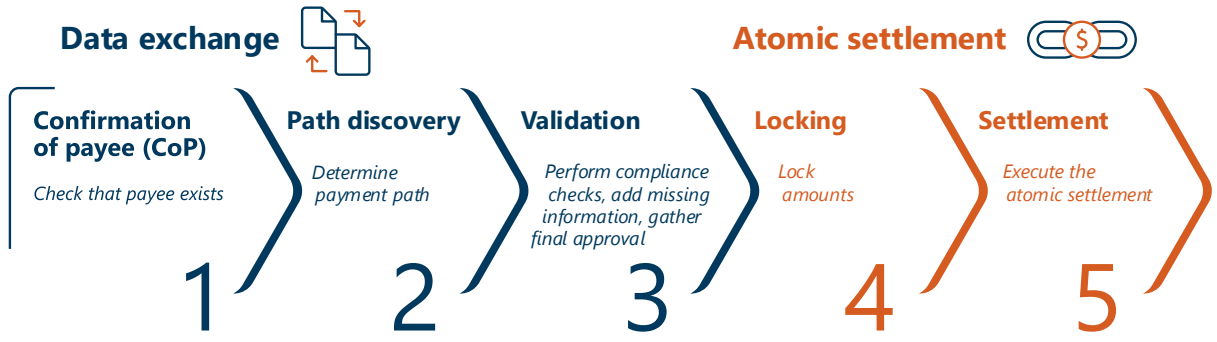
The three types of smart contracts interact to enable the processing of payments on the platform. For example, workflow smart contracts interact with asset smart contracts to enable the payments, including by constructing payment paths, facilitating appropriate compliance checks and obtaining "cross-currency amounts" when payments involve currency conversions. They also confirm approval of all participants in a payment for that payment to be processed, "locking" tokenised reserves and tokenised deposits prior to payment execution and, in connection with payment execution and settlement, updating asset smart contracts to record an increase or decrease in tokenised reserves and tokenised deposits.

A key architectural feature is the distinction between on-ledger and off-ledger activity. The shared ledgers record workflow state, enforce sequencing and anchor the minimum information required for coordination and settlement. Sensitive processes – such as compliance checks, private messaging and institution-specific decision-making – occur off-ledger, with only the necessary outcomes recorded on ledger. A workflow smart contract acts as a "payment coordinator": it guides the payment through the agreed stages (ie confirming the payee, agreeing the path, completing validations, locking funds and settling). It ensures that the payment only advances when each required participant has provided a signed confirmation that their step is complete, within the allowed time window.

Cross-border payment workflow in Project Agorá

Payments progress through five stages: (i) confirmation of payee; (ii) path discovery; (iii) validation; (iv) locking; and (v) settlement (Figure 6). Chapter 4 provides technical deep dives into each stage and the supporting components. The first three stages relate to data exchange among participants and the latter two stages concern atomic settlement.

Five-stage end-to-end payment life cycle **Figure 6**



Source: Project Agorá.

Data exchange

1. **Confirmation of payee (CoP):** This stage provides an early check that the payment instruction aligns with the intended recipient. The debtor agent initiates a CoP request and the creditor agent returns a confirmation outcome (ie match, no match). This stage is designed to reduce avoidable exceptions and investigations later in the payment life cycle.

   In the prototype, CoP coordination executes off the shared ledgers within a scoped execution context (privacy group / ephemeral Ethereum Virtual Machine (EVM), ie a short-lived, locally instantiated EVM runtime used by participants to execute private workflow logic) between the relevant participants, while the outcome needed to advance the workflow is anchored on the shared ledgers. Underlying customer data and matching logic remain within the creditor agent's institutional systems; only the minimum result necessary for workflow progression is disclosed to the debtor agent and recorded as a workflow outcome.

2. **Path discovery:** This stage identifies a viable path from the debtor agent to the creditor agent through potential intermediaries, ensuring reachability and policy constraints are met while preserving the confidentiality of participants' pathfinding preferences and internal decision logic.

   In the prototype, path discovery is performed via bilateral communication. Each agent engages a selected next-hop agent via private messaging and exchanges the minimum information required to explore path options. Unlike other stages of the workflow, path discovery does not use private smart contracts; it relies on bilateral private messages and institution-local pathfinding logic. Participants may backtrack and explore alternative options if an initial choice cannot reach the destination. Once a complete viable path is identified, the debtor agent validates it before proceeding. The workflow anchors the representation of the selected path on the shared ledgers to enable coordination in subsequent stages, without revealing sensitive path information.

3. **Validate (validate, amounts and ready):** This stage ensures that all institutions participating in the payment have performed the checks required before settlement, with deterministic progression and clear outcomes.

   a. **Validate:** Each participating commercial bank performs its required checks (ie sanctions screening; AML/CFT, KYC and fraud controls; and other policy validations) within its internal systems. The platform coordinates the exchange of the minimum outcomes needed to

progress the workflow, without centralising or revealing institution-specific logic. Where an institution requires additional information to complete checks, a scoped bilateral "needs more information" exchange may occur; however, the validation sub-step ultimately resolves to a definitive "pass" or "fail" outcome for workflow progression. Validation durations and timeout windows are configurable. The prototype uses illustrative timeouts and assumes required checks complete within configured windows; long-duration reviews (eg multi-hour or multi-day processes) may require extended windows or asynchronous handling approaches, which are outside the scope of the prototype. Central banks do not participate in payment validation; instead, they enforce policy through token-level and jurisdictional ledger controls.

b. **Amounts:** For cross-currency payments, the workflow determines the amounts to be settled in each currency leg. This includes single currency, dual currency and (where relevant) vehicle currency scenarios. Institutions may use internal pricing sources and policies; the workflow consumes only the endorsed results needed to build a coherent settlement instruction set.

c. **Ready:** Participants provide readiness signals indicating they are prepared to proceed to locking and settlement. Readiness incorporates the outcomes of validation and amount determination and confirms that each participant can proceed under the workflow rules.

Across these sub-steps, the key design objective is to ensure predictable progression while protecting sensitive information. Institution-local checks and sensitive computation remain off the shared ledgers; the minimum outcomes needed to progress the workflow are anchored on the shared ledgers as workflow attestations/outcomes.

Atomic settlement

4. **Lock (lock and delegate)**: This stage reserves the token balances required for settlement and establishes the authority required for coordinated execution. Reserved balances cannot be used elsewhere while the payment is awaiting settlement execution. In the prototype, locking is implemented using an asset contract locking construct:

   a. **Lock**: Participants reserve the required token balances (create a lock) in preparation for settlement. If a required lock cannot be created (for example, due to insufficient available balance), the workflow terminates before settlement and any partial preparatory actions are cancelled according to the payment coordinator-governed cancel outcome.

   b. **Delegate**: Participants temporarily delegate authority to the relevant payment-leg contract(s) so that settlement can be executed consistently according to the payment coordinator's final outcome.

Locking and delegation occur as part of a coordinated workflow: each participant retains responsibility for initiating locks on the assets they hold, while the workflow ensures the locking state is coherent across the payment path before settlement proceeds.

5. **Settle**: This stage executes the coordinated outcome across the relevant ledgers as a commit-or-cancel outcome governed by the payment coordinator. In this context, "atomic settlement" refers to a workflow-level outcome across payment legs, not a claim about finality or synchronous multi-ledger transaction execution. Once prerequisites are met (including validation, readiness and the locking), the payment coordinator advances the workflow to settlement.

Payment leg smart contracts then execute the instructions using the delegated locking construct, ensuring all legs either commit or cancel consistently, thereby preventing partial settlement outcomes across currencies and jurisdictions.

The workflow is designed to terminate cleanly at any stage if required conditions are not met. In such cases, the payment coordinator records a termination outcome and the settlement does not proceed; if termination occurs after locking, reserved balances are released in line with the payment coordinator's cancel outcome.

Together, these five stages provide a predictable, auditable and coordinated workflow for cross-border payments.

Chapter 4: Technical specifications of the prototype

The technical architecture and engineering design of the prototype comprise the Project Agorá platform architecture, the participant-operated Project Agorá suite, and the cross-cutting components that enable privacy-preserving, multi-ledger coordination. This includes key workflow mechanisms as well as assurance considerations, development and testing. Taken together, these elements present a system-level view of the Project Agorá prototype from a design and engineering perspective.

The Project Agorá ledger platform architecture

The Project Agorá ledger platform defines the shared execution environment in which payments, workflows and settlement occur. It comprises the unifying ledger and jurisdictional ledgers, the asset, workflow and reference smart contracts deployed on those ledgers, and a permissioned consensus model that governs transaction ordering and technical settlement.

Layered ledger model

The layered ledger architecture (Figure 5) combines a shared unifying ledger to coordinate cross-border payments with multiple jurisdictional ledgers to support domestic settlement in central bank reserves. In the prototype design, tokenised central bank reserves are maintained on their respective jurisdictional ledgers, while tokenised commercial bank deposits are maintained on the unifying ledger. This allocation reflects a design choice for the prototype and is not a fixed constraint of the architecture: the platform can support alternative allocations, provided assets implement the same contract interface and settlement constructs. For example, tokenised deposits may be issued on a jurisdictional ledger.

Each ledger operates independently, while a payment coordinator contract and payment leg contracts coordinate activity across ledgers. The governance, liability and operational responsibility model for the unifying ledger is outside the scope of the prototype and would require explicit multi-party agreements in any future implementation.

The unifying ledger provides the shared coordination layer for cross-border transactions. It hosts the payment coordinator contracts, payment leg contracts for unifying ledger-based assets, tokenised deposits in the prototype deployment, and workflow state required for multi-jurisdiction settlement. The unifying ledger acts as the logical hub for sequencing and coordinating the payment life cycle, without centralising domestic settlement functions or control.

Each jurisdiction operates its own jurisdictional ledger, hosting tokenised reserves issued by the central bank and any jurisdiction-specific settlement logic. Jurisdictional ledgers provide alignment with domestic monetary frameworks and regulatory requirements. They ensure that central bank reserves remain under full jurisdictional control while still participating in coordinated cross-border settlement.

Cross-border payments frequently require both central bank reserves and commercial bank deposits. The unifying and jurisdictional ledgers interact through:

- **Token locking** on the ledger where the asset resides.
- **Delegation of settlement authority** to payment leg contracts during the locking stage (lock and delegate as internal sub-steps).
- **Coordinated commit-or-cancel execution** of settlement across unifying and jurisdictional ledger legs governed by the payment coordinator.

Although transfers occur on separate ledger instances, workflow contracts ensure a coordinated outcome across legs, preventing partial settlement across currencies and jurisdictions.

Key features and benefits of the layered ledger architecture

- **Preserving jurisdictional autonomy** by allowing each central bank to maintain its own policy constraints, access rules and operational parameters while participating in coordinated cross-border settlement workflows.
- **Maintaining sovereign control of tokenised reserves** within each jurisdictional ledger, ensuring issuance, access and settlement of tokenised reserves remain governed domestically.
- **Providing a shared coordination layer for tokenised deposits** in the prototype, enabling multi-currency, cross-ledger workflows without centralising domestic settlement functions.
- **Standardising workflow semantics and contract interfaces across ledgers**, supporting composability and interoperability between tokenised reserves and tokenised deposits.
- **Supporting extensibility and future capabilities** (eg liquidity saving mechanisms, integration with tokenised securities for delivery versus payment (DvP) and additional workflow-level automation).
- **Improving coordinated visibility across ledgers**, enabling participants to follow payment progression through verifiable workflow state without disclosing confidential internal data.

Proof of authority consensus and QBFT

The unifying and jurisdictional ledgers operate under a permissioned consensus model designed for regulated financial institutions. The platform uses the Quorum Byzantine Fault Tolerance (QBFT) protocol within a proof of authority (PoA) governance framework. Validators are pre-authorised, identified institutions, ensuring that validation aligns with jurisdictional oversight and institutional accountability. Node participation and read access are governed by the permissioning model of each ledger. While smart contracts may record only minimal commitments for privacy-preserving assets and workflow outcomes, access to ledger data (including event streams) remains subject to network permissioning and participant roles.

Under the PoA model, validator membership is determined off chain and does not rely on token-based incentives or open participation. QBFT delivers deterministic technical settlement: once a block is confirmed by the validator set, it cannot be reversed. This behaviour provides stable transaction ordering and predictable workflow progression across the unifying and jurisdictional ledgers.

Ledger settlement ensures technical irreversibility of workflow state, not settlement finality of the underlying funds.[19]

Together, the PoA governance model and the QBFT consensus implementation provide a predictable, permissioned validation environment compatible with the operational expectations of regulated institutions, without introducing probabilistic settlement or incentive-driven behaviours found in public blockchain networks.

Asset smart contracts

The Project Agorá platform represents tokenised deposits and tokenised reserves through a unified asset contract model that applies consistently across them. Both asset types implement the same core functions – issuance, redemption, transfer, locking and delegated settlement authority – while differing in their issuers and the ledgers on which they reside.

Asset smart contracts implement a standardised interface designed to preserve the legal and balance sheet characteristics of the underlying forms of money. Both tokenised reserves and tokenised deposits support:

- Issuance and redemption through the authorised issuer (commercial bank for tokenised deposits; central bank for tokenised reserves).
- Transfers between institutions under existing settlement relationships.
- Locking of balances to reserve funds during the locking stage.
- Delegated authority allowing workflow contracts (payment legs) to act on locked balances during settlement, within a strictly scoped mandate.

This harmonised design ensures that asset behaviour is predictable irrespective of currency or jurisdiction, supporting coordinated commit-or-cancel settlement across unifying and jurisdictional ledger environments.

Tokenised deposits represent commercial bank deposits. In the prototype, tokenised deposits are recorded on the unifying ledger. They follow the unified contract model while reflecting the regulatory obligations, credit exposures and account structures of commercial institutions.

Tokenised reserves represent central bank reserves and are recorded on the jurisdictional ledger corresponding to each currency. Tokenised reserves follow the same functional model as tokenised deposits but are subject to jurisdiction-specific policy constraints, including issuance controls, access rights and central-bank-defined operational parameters.

The standardised tokenised deposit/reserve contract interface includes:

- *mint()* and *burn()* for issuance and redemption
- *transfer()* for value movement
- *createLock()* to reserve balances for settlement

[19] For a discussion of legal settlement finality, see Chapter 5.

- *delegateLock()* to grant temporary, payment-scoped authority to workflow contracts
- *spendLock()* to commit the prepared settlement action under the coordinator outcome
- *cancelLock()* to release the lock without settlement when the workflow terminates or cancels.[20]

By maintaining a common contract architecture across tokenised reserves and tokenised deposits, the platform ensures consistent asset handling across jurisdictions while allowing each issuer – commercial bank or central bank – to enforce its own policy rules.

Middleware and smart contract workflows

The Project Agorá prototype coordinates payments through a combination of: (i) on-main ledger workflow execution governed by smart contracts; and (ii) off-main ledger execution performed within institutional middleware and, where applicable, privacy group-scoped coordination. Smart contract workflows enforce deterministic sequencing, timeouts, asset locking and settlement execution. Middleware workflows execute institution-specific logic such as CoP checks, pathfinding decisions, validation and cross-currency amount determination. The platform anchors only the minimum outcomes required to progress the workflow on the shared ledgers.

Smart contract workflows (payment coordinator and payment legs)

Workflow smart contracts govern the on-chain stages of the payment life cycle. They enforce the rules through which payments progress, coordinate state transitions across the unifying and jurisdictional ledgers and ensure that settlement is deterministic and aligned with institutional controls.

The payment coordinator contract, deployed on the unifying ledger, orchestrates the on-chain workflow. It receives attested outcomes from institutional middleware (for example, validation outcomes, cross-currency amounts and readiness confirmations) through scoped coordination mechanisms and advances the workflow only when all required conditions are met. The payment coordinator enforces workflow timeouts and initiates settlement by enabling the payment legs to act on locked balances within a payment-scoped mandate. The payment coordinator does not perform CoP, path discovery, validation or cross-currency computation itself; it enforces state-transition rules based on endorsed outcomes produced by participants.

Payment leg contracts implement ledger-native settlement logic for each payment leg. After assets are locked, the payment coordinator enables each leg to act on the specific locked balances associated with that payment. Each leg then executes settlement in a deterministic operation that honours the payment coordinator's final outcome (commit or cancel), preventing partial settlement across unifying and jurisdictional ledger environments. Successful completion emits settlement events that provide an auditable record of technical settlement execution across ledgers.

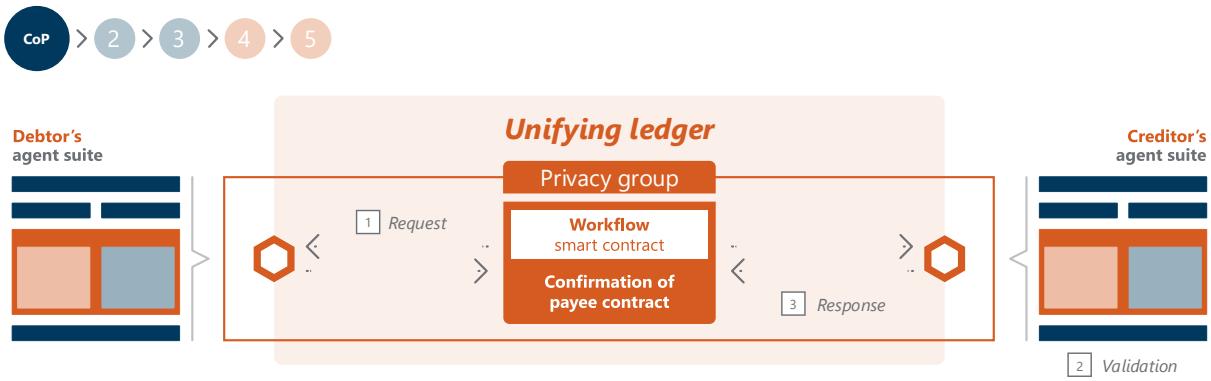
[20] In addition to timeouts, an explicit cancel operation is needed to support early termination and clean release of reserved balances when a payment aborts before completion (eg validation failure, readiness failure or participant withdrawal), rather than waiting for a timeout to elapse.

Middleware workflows

CoP: CoP is performed off the shared ledgers within the debtor and creditor institutions' middleware, using local account data and beneficiary information (Figure 7). Where coordination is required, a bilateral coordination channel is established between the debtor and creditor so that only the minimum CoP outcome is exchanged. Only the outcome needed to advance the workflow – not underlying customer data or matching logic – is anchored on the shared ledgers when required.

Confirmation of payee

Figure 7

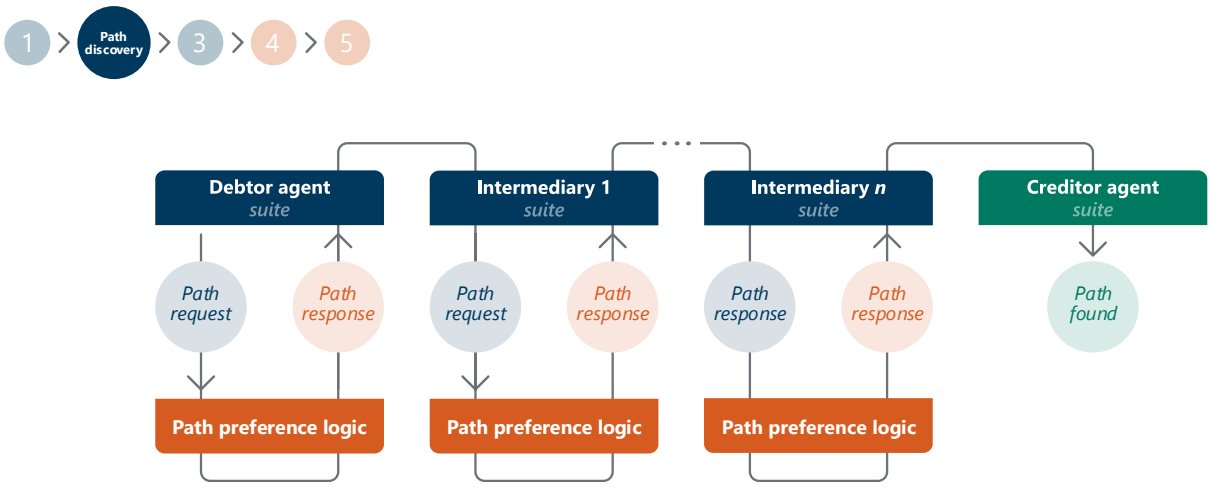


Source: Project Agorá.

Path discovery mechanism (PDM): PDM is an off-shared ledger workflow that identifies the parties necessary to execute the transaction, which would be referred to as "routing" in today's payments landscape (Figure 8). The PDM performs this function via hop-by-hop 1:1 private messaging. Each commercial bank along the chain evaluates options privately using internal correspondent relationships, preferences and bilateral agreements. The institution selects a next hop and exchanges the minimum necessary information with that next-hop institution through a bilateral channel.

Path discovery process

Figure 8



Source: Project Agorá.

Unlike other steps in the workflow, PDM does not rely on private smart contracts; it is implemented as distributed, bilateral messaging and institution-local pathfinding logic. Participants may backtrack and explore alternative paths if an initial choice cannot reach the destination. At the conclusion of PDM, the representation of a selected path is submitted to the payment coordinator and anchored on the shared ledgers so that subsequent stages can coordinate among the participants in the chosen path.

Verification workflow (validation, amounts, ready)

The verification workflow comprises the middleware-executed processes that ensure a payment is compliant, correctly quantified and ready for settlement. All logic in this workflow is performed in institutional middleware; the ledgers receive only endorsed outcomes.

- **Validation**: Each institution performs sanctions screening, AML/CFT, KYC and fraud controls and other policy validations within its own environment. Only summary outcomes are exchanged within the payment's privacy group. In the prototype, each participant submits a single endorsed response that includes three binary outcomes (pass/fail) — one for sanctions, one for AML/CFT, KYC and fraud, and one for "other". Privacy group members can view these category-level outcomes for participants in the group; the payment coordinator derives participant-level and workflow-level outcomes from them (any category fail → participant fail; any participant fail → payment fail). The coordinator advances the workflow only when all required participants return a passing outcome within the configured timeout window.
- **Amounts**: Where currency conversion is required, designated cross-currency providers compute the cross-currency amounts privately within their middleware. They may retrieve pricing data from internal engines or market sources and apply institution-specific policies such as spreads or rounding rules. Only the endorsed final amount(s) are submitted to the coordinator.
- **Ready**: Each participant performs final internal checks – liquidity, token availability, tolerance checks, and internal authorisation – within its own environment. Participants submit ready/not ready outcomes to the coordinator. The coordinator transitions to locking only if all required institutions return ready before timeout.

Reference smart contracts

The Project Agorá platform includes a set of reference smart contracts that provide shared registries and reusable components required for interoperable operation across the unifying and jurisdictional ledgers. These contracts do not execute payment workflows; rather, they supply common reference data that other contracts and off-main ledger systems rely on for consistency, discoverability and coordination.

- **Network registry**: allows participants to publish institutional identifiers, discovery endpoints and relevant contract addresses, enabling participants to identify one another across ledgers without exposing private pathfinding relationships or bilateral arrangements.
- **Token registry**: records metadata for tokenised assets supported on the platform, including issuer identity, contract address, asset type and jurisdictional attributes, enabling consistent interpretation of tokenised reserves and tokenised deposits across participants.

- **Corridor registry**: captures publicly declared cross-currency corridors and settlement capabilities. While private pathfinding preferences and bilateral relationships remain within each institution's middleware, corridor information provides the minimal public data needed for the PDM to identify eligible institutions for specific currency paths without disclosing sensitive commercial information.
- **Reserve account registry** (per jurisdictional ledger): a central bank-operated registry that discloses limited information about reserve account holders in that jurisdiction (for example, participant identifiers indicating which institutions hold reserve accounts and are reachable for settlement in that jurisdiction). This supports reachability and policy checks without exposing confidential bilateral relationships.

Note that responsibility for registering, managing and updating reference registry data (eg network, token and corridor registries) is an operating model consideration and is outside the scope of this prototype; it would require explicit definition in any future implementation.

Together, these reference contracts support a consistent, interoperable multi-ledger environment while preserving the confidentiality of institution-specific logic and bilateral arrangements.

Cross-ledger coordination (functional view)

Cross-ledger coordination in Project Agorá does not rely on a standalone cross-chain bridge. Instead, coordination is achieved through workflow enforcement on the unifying ledger payment coordinator, ledger-native execution of payment legs on each involved ledger and participant-operated middleware that submits endorsed outcomes and transactions to the appropriate ledger endpoints.

Functionally, coordination proceeds as follows:

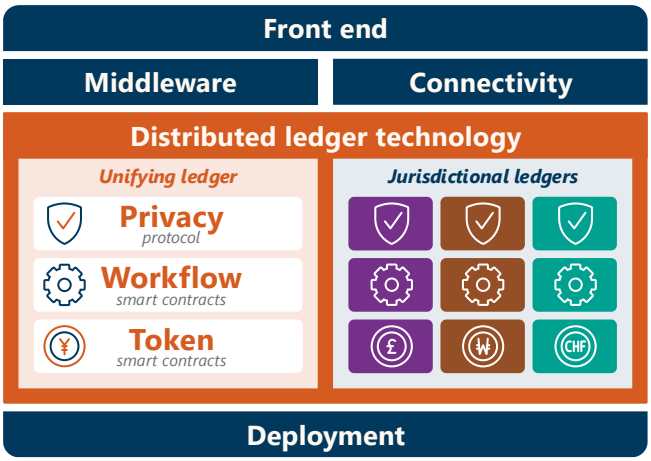
1. The payment coordinator on the unifying ledger acts as the authoritative workflow state machine for the payment, enforcing sequencing, timeouts and progression rules.
2. Participants' middleware consumes on-ledger events (from the unifying ledger and relevant jurisdictional ledgers) and participant-scoped coordination outcomes, performs institution-local logic, and submits endorsed outcomes to advance the coordinator state.
3. For actions that must occur on a jurisdictional ledger (eg reserve leg locking and settlement), the relevant participant (or authorised operator for that leg) submits the corresponding transaction to that jurisdictional ledger. Confirmation of those actions is observed through jurisdictional ledger events and used by middleware to progress the unifying ledger coordinator state.
4. Deterministic ordering within each ledger is provided by the ledger's consensus; deterministic workflow sequencing across ledgers is achieved through the coordinator's state-transition rules, which require specific confirmed outcomes (attested and/or event-observed) before advancing stages.

The Project Agorá suite

The Agorá suite (Figure 9) defines the participant-operated technology stack used by institutions to connect to, interact with and operate on the Project Agorá ledger platform. It includes the user interface, the Project Agorá middleware, connectivity and integration components, indexing services and the participant's ledger node configuration. Whereas the platform establishes the shared ledger and smart contract environment, the Project Agorá suite provides the local software and infrastructure each institution runs within its own environment to participate in the platform securely and consistently.

For the prototype, a web interface served as the primary operational interface. In a production setting, institutions would typically integrate via application programming interfaces (APIs) and internal systems, with the user interface used primarily for monitoring, exception handling and operational oversight; this would also require appropriate operational monitoring, patching and resilience measures for the participant-operated suite components, which were not assessed during the development of the prototype.

The Project Agorá suite **Figure 9**



Source: Project Agorá.

User interface layer

The user interface layer provides an operational view through which participants can initiate payments (in the prototype), monitor workflow progression and observe how the payment coordinator advances transactions across the unifying ledger and the jurisdictional ledgers. It presents multi-jurisdiction payment activity in a clear and operationally aligned manner.

The interface displays key information generated throughout the payment life cycle, including validation outcomes, cross-currency amount updates, readiness confirmations, lock and delegation status, and settlement results. It is driven by events emitted from the ledger platform and indexed by participant-operated services, providing near real-time visibility into both on-main ledger activity and the outcomes of off-shared ledger processing.

In addition to payment initiation and monitoring, the interface provides access to broader platform functions such as views of token holdings, account structures, participant networks, PvP activity and system diagnostics. These capabilities allow institutions to oversee positions, liquidity and platform interactions without exposing sensitive internal information.

The user interface is implemented as a modular, extensible application that institutions can tailor to their operational needs. It can support enhancements such as institution-specific role-based access control (RBAC), custom dashboards and alignment with internal systems, while underlying workflow execution and ledger interactions remain deterministic and governed by the platform architecture.

Connectivity and integration layer

The connectivity and integration layer provides the structured interfaces through which institutions interact with the Project Agorá platform. The Project Agorá suite exposes APIs documented using OpenAPI/Swagger specifications, enabling institutions to integrate horizontally with other platforms or networks and vertically with their internal operational systems.

These interfaces support payment initiation, account and token operations, workflow monitoring, and the consumption of settlement-related events. Through these endpoints, institutions can integrate the platform into their existing technology stacks with minimal friction, while retaining control over internal processing and decision-making.

At the connectivity layer, institutions may represent payment instructions using ISO 20022 messages (for example, pacs.008 or pacs.009). These messages are consumed by institutional middleware and translated into workflow outcomes and settlement instructions on the Project Agorá platform; ISO-formatted messages are not processed directly on the ledger. This approach allows institutions to leverage familiar standards at the integration boundary while preserving the platform's workflow-driven settlement model.

Connectivity capabilities also facilitate participation in Paladin (see below) privacy group communication, enabling secure bilateral or scoped multiparty messaging where required. Only suite-level connectivity aspects are described here; the broader privacy architecture and data governance mechanisms are covered later in the report.

Middleware

The middleware provides the participant-operated coordination and execution environment through which institutions run the private components of the workflow and connect institutional systems to the platform and serves as the primary compliance boundary for institution-specific decisioning. Institution-specific regulatory, compliance and risk decisions are executed within institutional middleware and remain the sole responsibility of each institution. The platform's on-ledger components enforce shared workflow rules (eg sequencing, state transitions and atomic settlement), but do not perform institution-specific compliance decisioning or assume responsibility for it. The middleware executes institution-specific logic and coordinates actions that result in on-main ledger state transitions and proofs. For example, it:

- executes institution-specific workflow logic (ie CoP checks, pathfinding decisions, validation, cross-currency computation and readiness checks).

- submits endorsed outcomes and transactions to progress the workflow (eg advancing coordinator state, initiating lock and delegation actions, triggering settlement execution in accordance with the workflow).
- ingests on-shared ledger events and off-shared ledger signals to maintain a coherent end-to-end view of each payment from the institution's perspective.
- transmits workflow-relevant information to the user interface and institutional monitoring systems.

Typical middleware-executed tasks include:

- CoP
- Path discovery evaluations (PDM hop selection)
- Compliance checks, including with respect to sanctions and AML/CFT, KYC and fraud
- Cross-currency amount determination
- Final readiness checks
- Bilateral "needs more information" exchanges (where required)

All processes above occur within the institution's technical environment and within its own regulatory, compliance and risk perimeter.[21] Only high-level outcomes – such as pass/fail validation results, endorsed cross-currency amounts or readiness confirmations – are returned to the payment coordinator to progress the workflow rather than underlying customer data, screening results, or internal risk signals.

Blockchain nodes

Each participant interacts with the Project Agorá platform through permissioned distributed ledger nodes running Hyperledger Besu, an enterprise-grade Ethereum-compatible blockchain client. These nodes form the execution environment for the smart contracts that facilitate payments, and they provide the authoritative record of workflow, asset and settlement state across the system.

While the prototype deployment may centralise certain node operations for practicality, the architecture is designed to support future deployments in which institutions and/or jurisdictions operate their own nodes in configurations aligned with their operational, regulatory or sovereignty requirements.

Ledger nodes perform several critical roles:

- Execute the asset, workflow and reference smart contracts that underpin tokens and payment coordination.
- Validate and store the state of the unifying ledger and relevant jurisdictional ledgers.
- Emit events consumed by institutional middleware, indexing services and user interfaces.

[21] Deployment note: the connectivity and middleware layers are described as logical components. In future, institutions may choose to deploy them as separate services or as a single integrated application depending on internal architecture and operational preferences.

- Enforce permissioning and access controls consistent with the platform's governance model.

Participation in consensus (ie validator responsibilities) is determined by the governance model and designated validator set for each ledger. Operating a node does not necessarily imply validator participation; this distinction and governance model is outside the scope of the prototype.

Deployment considerations

Operating the platform requires deploying (i) participant-operated Project Agorá suite components; and (ii) the shared ledger infrastructure (unifying and jurisdictional ledgers).

1. **Participant-operated components**: Each participating institution deploys its own instance of the Project Agorá suite, including middleware services, connectivity components and any associated local data stores and indexing services. In the prototype, these components were deployed using repeatable configuration and automation to support consistent setup across participants; production deployments would require institutions to align deployment and operational controls with internal policies and regulatory expectations.
2. **Ledger infrastructure**: The unifying ledger and each jurisdictional ledger must be deployed and maintained by authorised infrastructure operators under an agreed governance model. For jurisdictional ledgers, this typically aligns with the jurisdictional operator (which may be the central bank) and any authorised operators it designates. For the unifying ledger, governance and operational responsibility would be shared or delegated according to the participants chosen operating model.

The architecture supports deployment in single-cloud, multi-cloud or on-premise environments. This flexibility allows jurisdictions and institutions to adopt deployment models that reflect policy, regulatory and operational preferences while ensuring sufficient commonality to enable atomic settlement and integration with payment workflows between tokenised reserves and tokenised deposits on a shared platform. Operational security controls (identity and access management (IAM), key management hardening, monitoring and incident response), onboarding/offboarding procedures and operational continuity under node failures were out of scope for the prototype.

Technical components of the Project Agorá platform

This section describes the cross-cutting technical components that support coordinated, privacy-preserving, multi-ledger payments on the Project Agorá platform. These components operate alongside the layered ledger architecture and the participant-operated Project Agorá suite to enable secure coordination, interoperability, deterministic workflow execution and operational visibility across jurisdictions. They underpin the workflow mechanisms described later in the report.

The Project Agorá prototype coordinates payments using a hybrid model that links off-shared ledger computations to on-shared ledger workflow enforcement:

- **Middleware computes sensitive logic**: institutions perform CoP checks, pathfinding decisions, AML/CFT, KYC, fraud and sanctions checks, cross-currency calculations and readiness checks within their own systems.

- **Scoped private coordination exchanges endorsed outcomes**: where coordination with counterparties is required, institutions exchange only the minimum endorsed outputs through participant-scoped channels (bilateral messaging and, where applicable, privacy group-scoped coordination).
- **The ledgers anchor minimal outcomes and enforce deterministic workflow progression**: the payment coordinator and supporting contracts record only what is necessary to enforce sequencing, timeouts, locking/delegation and settlement execution.
- **Ledger events drive participants' next actions**: middleware and operator tools consume deterministic smart-contract events to remain synchronised and to trigger the next off-main ledger computation.

By combining participant-scoped private coordination with deterministic on-ledger enforcement, the Project Agorá prototype preserves institutional autonomy and confidentiality while ensuring participants remain synchronised in a single multi-ledger workflow, without relying on a central message broker or cross-chain bridge.

Privacy, confidentiality and data governance

Privacy is a foundational design requirement of the Project Agorá platform. The system must enable coordinated, multiparty cross-border payments while protecting customer data, institution-specific logic and commercially sensitive relationships. To meet these requirements, the prototype leverages Paladin, a programmable privacy framework for EVM-compatible ledgers. For the Project Agorá platform, two Paladin domain plugins are used:

- **Noto**: token-level privacy through an issuer-backed ("notary") token model.
- **Pente**: workflow-level privacy through privacy group-scoped coordination and ephemeral EVM execution for private contract logic.

Together, Noto and Pente provide a configurable privacy architecture that aligns with the confidentiality expectations of wholesale cross-border payments while enabling programmability and coordination across jurisdictions.

Paladin: programmable privacy framework

Paladin is a modular privacy framework designed to support programmable, policy-driven confidentiality in EVM-based distributed ledger environments. Rather than hardwiring a single privacy scheme into the ledger, Paladin provides extensibility points that can be configured or extended as privacy requirements, cryptographic tools and regulatory expectations evolve.

In Project Agorá, Paladin is used to:

- implement privacy-preserving token contracts (Noto) for tokenised reserves and tokenised deposits; and
- support workflow-level privacy (Pente) for participant-scoped coordination and private contract execution.

The design ensures the ledger enforces workflow correctness using minimal anchored outcomes, while sensitive data and institution-specific logic remain outside the shared ledgers. Additionally, privacy mechanisms do not remove regulatory obligations related to customer

identification, transaction monitoring, record keeping or audit access; they support selective disclosure while preserving institutional responsibility.[22]

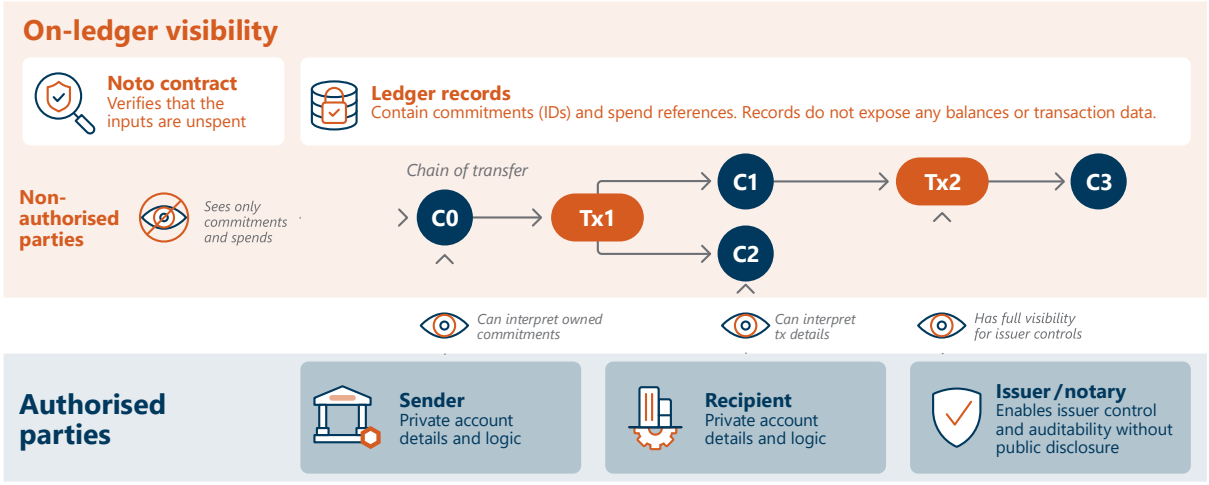
Noto: token-level privacy (issuer-backed/notary model)

Tokenised reserves and tokenised deposits in the prototype follow the Noto model (Figure 10). Noto is a reference implementation of an issuer-backed (sometimes called "notary") token model, in which the issuer retains full visibility over token state to support policy controls, redemption and auditability, while non-authorised parties cannot observe balances or transaction details.

Noto uses a commitment-based unspent transaction output (UTXO)-style state model rather than a single, globally mutable account balance:

- **State as outputs**: each transfer consumes one or more existing outputs and creates new outputs; there is no global balance field to update.
- **Private commitments**: each output is represented on chain as a cryptographic commitment (eg a salted hash commitment) that hides the underlying amount and recipient details from non-authorised parties.
- **Visibility by possession of private data**: there is no decryption or reconstruction mechanism on the public record. Parties who possess the relevant private data (typically the holder and the issuer, and optionally authorised auditors) can interpret their own states and prove/validate the chain of spent states. Other network participants see only commitments and valid spends.
- **Validated transitions**: the ledger verifies that inputs are unspent, outputs are well-formed, and issuer-defined constraints are met – without needing to see the underlying amounts or recipients.

Noto token privacy **Figure 10**



Source: Project Agorá.

[22] For further discussion of these obligations, see Chapter 5.

Because authorised parties maintain certain private data off the shared ledgers, institutions must ensure appropriate data durability, backup and recovery processes. The UTXO-style commitment model also shifts some complexity to participant systems, which must manage private state fragments, spend selection and wallet management within institutional environments.

This model enforces data minimisation at the token layer, the chain records commitments and spends, while semantically rich details remain with authorised parties. Noto also supports programmable hooks to enable policy controls without sacrificing confidentiality.

Privacy mechanisms minimise disclosure on the ledger, but they do not prevent authorised parties from producing audit evidence. Where audit access is required, authorised parties (eg issuer and designated auditors) can validate and prove token state transitions and workflow outcomes using access to the relevant private data and endorsements, consistent with applicable governance and legal requirements.

Visibility model: three layers of data disclosure

To avoid "all-or-nothing" disclosure, Project Agorá uses a layered visibility model:

- **Layer 1**: public/on-shared ledger workflow and reference data: Information recorded on the unifying ledger/jurisdictional ledgers that is required for coordination, sequencing, and auditability (eg workflow stage transitions, timeouts, and minimal attestations/outcomes needed to progress a payment).
- **Layer 2**: participant-scoped coordination data. Outcomes and coordination artefacts exchanged only among the institutions that must coordinate for a given payment step. This includes bilateral private messaging and privacy group-scoped coordination where appropriate. These artefacts are not public on the shared ledgers but can produce minimal anchors (commitments/events) needed for verifiability and deterministic progression.
- **Layer 3**: institution-local data and logic. Customer data, pathfinding preferences, proprietary pricing inputs and institution-specific compliance logic remain within each participant's systems and are never disclosed to the platform as raw data.

This layered approach allows institutions to share only the minimum necessary information at each workflow step while preserving confidentiality and jurisdictional constraints.

Pente: workflow-level privacy (privacy groups + ephemeral EVM mechanics)

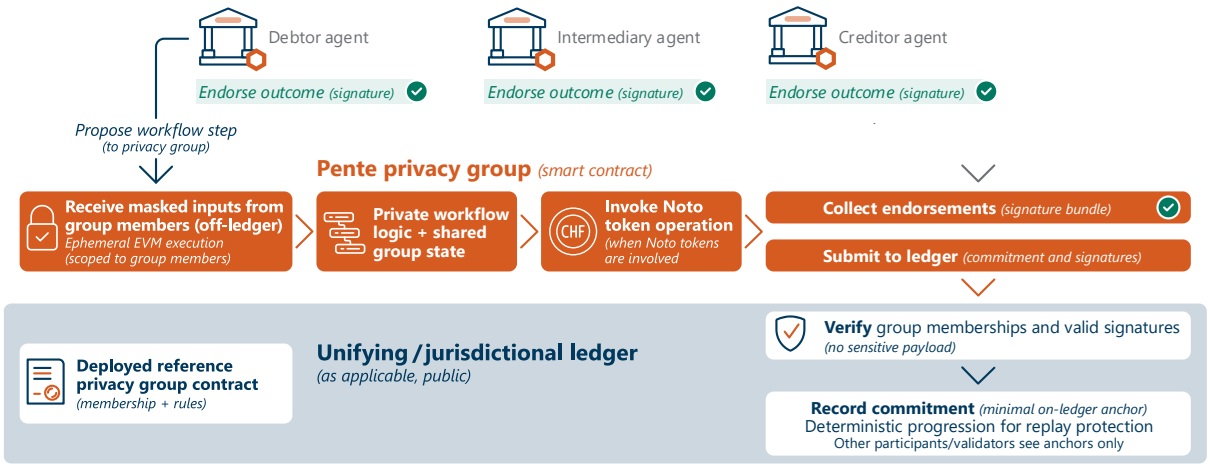
Pente provides workflow-level privacy by enabling subsets of institutions to coordinate private logic through privacy group-scoped execution (Figure 11). Pente is used where a workflow step benefits from a shared, participant-scoped contract state (for example, coordination of payment progression and settlement authorisations among the participants in a chosen payment path).

At a technical level, Pente provides:

- **Privacy group anchor and membership**: a privacy group is represented by an on-chain contract that defines its membership and rules (anchored on the unifying ledger or a jurisdictional ledger as applicable).
- **Ephemeral EVM execution (off the shared ledgers)**: workflow coordination logic can be executed in an ephemeral EVM scoped to the group membership. This execution is off the shared ledgers with respect to the public unifying ledger/jurisdictional ledger state.
- **Endorsements and signature verification**: participants endorse outcomes using typed data signatures (eg EIP-712). The base ledger verifies signatures and membership rules rather than storing sensitive payloads.
- **Anchored outcomes/commitments**: instead of recording raw values, the ledger records minimal commitments and/or attestations required for deterministic workflow progression and replay protection.[23]

Important scope note: Pente privacy groups are used for participant-scoped coordination where a shared contract state is needed (eg payment coordinator/leg coordination among the path participants). They are not used to externalise institution-local logic; substantive compliance decisioning, pathfinding logic and pricing logic remain within each institution's systems, with only endorsed outcomes exchanged.

Pente privacy group using Noto tokens **Figure 11**



Source: Project Agorá.

Key management

Key custody, hardware security module (HSM) vendor selection, key rotation policies and operational key-management governance are not specified in this report. In the prototype deployment, key management for participant components and managed services was handled

[23] Privacy groups are anchored on the ledger to define membership and verifiability, but their sensitive coordination logic and message content remain off the shared ledgers; only minimal commitments/attestations are anchored to support deterministic workflow progression.

using the hosting environment's managed key management capabilities. Any future implementation would require a full design of key custody, operational controls and governance aligned with participating institutions' security requirements.

Combined privacy model and extensibility

The Project Agorá privacy architecture combines Noto's token-level confidentiality with Pente's workflow-level, participant-scoped coordination to create a layered privacy model that supports deterministic multi-institution settlement while preserving confidentiality.

Because Paladin is modular, additional privacy-enhancing techniques – such as zero-knowledge proofs (ZKPs), secure multiparty computation (MPC) or other cryptographic approaches – can be incorporated over time without redesigning the layered ledger architecture or workflow contracts. This future proofing supports evolution as regulatory, cryptographic and operational expectations mature. While modular privacy approaches allow future enhancement, additional cryptographic techniques may introduce performance and operational complexity. Performance benchmarking of such techniques was not conducted in the development of the prototype.

Messaging

Messaging links off-shared ledger computations performed within each participant's middleware to the on-ledger workflow enforced by the payment coordinator. Rather than relying on cross-chain bridges between heterogeneous networks, the Project Agorá prototype uses a hybrid coordination model based on participant-scoped private communication (bilateral messaging and, where applicable, privacy group-scoped coordination) and deterministic smart contract events emitted by the unifying ledger/jurisdictional ledgers.

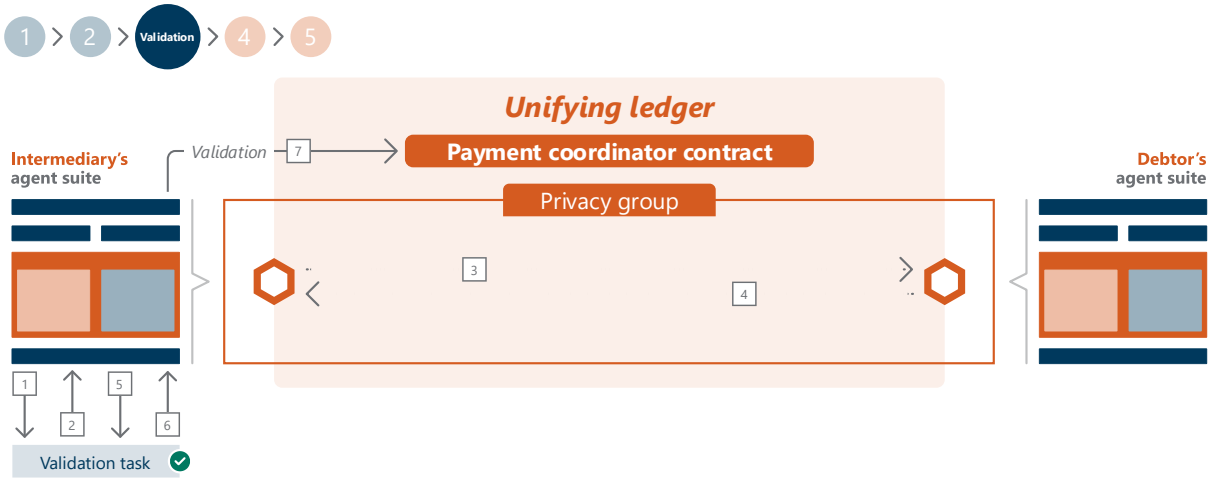
Participant-scoped private communication

The prototype uses participant-scoped private communication (Figure 12) to exchange endorsed outcomes between only those institutions that must coordinate at a given step:

- **Bilateral private messaging (not smart contract based)**: used where the workflow requires hop-by-hop coordination without shared private contract state (notably, PDM in the prototype).
- **Privacy group-scoped coordination (smart contract based)**: used where a fixed set of participants must coordinate against a shared private contract state (eg payment coordination among the selected path participants).

Messages exchanged within participant-scoped coordination channels (including privacy groups) are encrypted and visible only to authorised participants in that channel. In both cases, institutions compute sensitive logic locally and exchange only the minimum endorsed outcomes required for the workflow. The shared ledgers anchor only the minimal results needed to progress the coordinator state and enforce deterministic sequencing.

Participant-scoped private communication **Figure 12**



Source: Project Agorá.

Event-driven ledger coordination

On-ledger coordination is driven by events emitted by workflow and asset contracts, which signal transitions between workflow stages – such as the completion of CoP, receipt of validation outcomes, recording of endorsed amounts, readiness completion, locking and delegation, and settlement results.

These events are indexed by participant-operated services and consumed by middleware and operator tools, ensuring that each participant maintains an accurate near real-time view of payment state across the unifying ledger and any involved jurisdictional ledgers.

Hybrid on-/off-ledger coordination model

The prototype coordinates payments using a hybrid model that links off-ledger computations performed in institutional middleware to on-ledger workflow enforcement. Participant-scoped private communication is used to exchange only endorsed outcomes where needed, while the shared ledgers anchor minimal outcomes and enforce deterministic sequencing through workflow contracts.

Interoperability

Interoperability in Project Agorá refers to the ability of institutions, assets and workflow components to interact reliably across multiple jurisdictions without requiring a single centralised infrastructure or cross-chain bridging mechanism. The platform achieves this by combining the layered ledger architecture, standardised contract interfaces, participant-operated integration components and consistent execution semantics across unifying and jurisdictional ledgers.

Ledger-level interoperability through the layered architecture

The Project Agorá prototypes interoperability begins with the separation of responsibilities between the unifying ledger and jurisdictional ledgers. The unifying ledger provides a shared environment for cross-institution workflow coordination, while each jurisdictional ledger hosts jurisdiction-specific central bank reserves and settlement rules under domestic control.

Because unifying and jurisdictional ledgers share a compatible EVM execution model and contract interface structure, participants can interact with assets and workflow components across layers using consistent interaction patterns, without bridging, wrapping or reconciling incompatible ledger types.

Data-level interoperability through standardised formats

Workflow messages and payment information can be represented using structured formats that align with existing payment operations and enterprise integration patterns. This supports compatibility with domestic settlement infrastructures, correspondent banking interfaces and institutions' compliance/screening systems, and reduces integration friction. However, alignment of data structures alone does not guarantee end-to-end compatibility with existing infrastructures; practical integration depends on institutional systems, operational processes and jurisdiction-specific requirements.

Integration-level interoperability through participant systems

Institutions connect the Project Agorá platform to internal systems via the suite's APIs and the event-driven middleware architecture. This enables institutions to integrate compliance engines, cross-currency pricing sources, pathfinding preference logic, and accounting/position management systems directly into the workflow, without requiring wholesale replacement of domestic infrastructure.

Interoperability without bridges

A key architectural benefit of the Project Agorá platform is that cross-ledger workflows do not rely on standalone cross-chain bridges. Interoperability arises from:

- a single logical workflow coordinated via the payment coordinator;
- ledger-native execution of payment legs on each jurisdictional ledger;
- participant-scoped private coordination where required; and
- consistent execution semantics across compatible EVM-based ledgers.

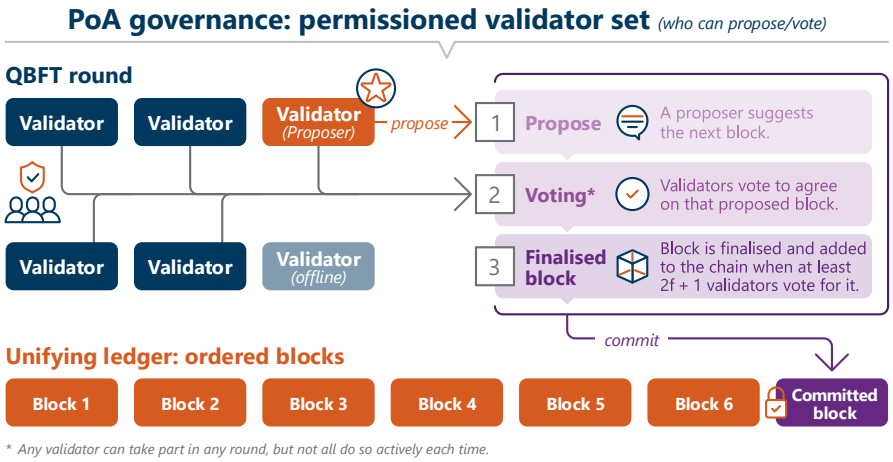
This reduces additional trust assumptions and operational complexity typically introduced by bridging architectures.

Consensus and ledger settlement (QBFT/PoA)

The Project Agorá platform relies on a permissioned consensus protocol to ensure predictable ordering and deterministic technical settlement of workflow state on the unifying and jurisdictional

ledgers (Figure 13). This is achieved through a PoA governance model and the QBFT consensus mechanism.

QBFT consensus **Figure 13**



Source: Project Agorá.

Deterministic technical settlement is important for coordinated multi-ledger workflows: participants need certainty that workflow state transitions, locking and delegation actions, and settlement outcomes have been committed and will not be reorganised. Ledger settlement ensures technical irreversibility of workflow state, not legal settlement finality of the underlying funds.[24]

Indexing and event retrieval

Indexing supports Project Agorá's operational model by enabling institutions to retrieve workflow state, monitor settlement progression and reconstruct relevant coordination flows across unifying and jurisdictional ledgers. Indexing services operate alongside the ledger platform and the participant suite, ensuring institutions have a coherent view of payment activity even as computations and coordination occur off the shared ledgers.

Ledger-level indexing

Workflow, asset and reference smart contracts emit events at key points in the payment life cycle – such as validation outcomes, readiness confirmations, locking/delegation actions and settlement results. Participant-operated services subscribe to these events and index them locally, enabling near real-time monitoring and efficient retrieval for audit and reconciliation.

Participant-scoped coordination indexing

Indexing also extends to participant-visible private coordination artefacts (for example, message metadata and endorsed outcomes exchanged through scoped channels, and privacy group

[24] See Chapter 5 for a discussion of a legal settlement approach for Project Agorá.

coordination outcomes visible to group members). This allows participants to reconstruct the sequence of coordination steps that led to a workflow outcome without exposing message content to non-participants.

Integrated event-driven operation

Together, ledger events and participant-scoped coordination artefacts support Project Agorá's event-driven operation. Institutions receive events and coordination requests, process them through middleware and submit endorsed outcomes that advance the workflow. Operator tools consume indexed data to present a timely end-to-end view of payment progression.

Operational and audit benefits

Indexing enables participants to reconstruct participant-relevant interactions for operational monitoring. This supports internal audit processes, facilitates supervisory review where appropriate and helps institutions meet operational and compliance obligations while preserving confidentiality.

Timeouts and workflow safety controls

The Project Agorá platform incorporates workflow-level safety controls to ensure payments either complete in full or terminate cleanly with no unintended movement of funds. These safeguards are embedded in the payment coordinator and supporting workflow contracts, operating independently of institution-local logic to ensure consistent behaviour across jurisdictions.

Each stage is governed by explicit timeout parameters enforced by the payment coordinator If a participant does not submit the required endorsed outcome within the permitted window, the coordinator records a timeout event and terminates the workflow. This prevents payments from remaining indefinitely in intermediate states and ensures that settlement is attempted only when prerequisites have been satisfied

Failures occur when an institution returns a negative validation or readiness outcome, when a required computation cannot be completed within its allowed window, or when mandatory stage conditions are not met. These failures are captured as explicit on-ledger events and cause termination of the workflow under uniform rules. Institution-local logic remains private; the coordinator enforces deterministic stage progression and termination semantics.

Safety controls for locking and settlement ensure that assets are reserved and can be acted upon only under tightly scoped delegated authority. The workflow proceeds to locking only once all required participants have returned the necessary endorsed outcomes (including readiness). If the workflow terminates before settlement, locks are released according to the workflow's outcome, preventing partial or unintended transfers.

Payment flow deep dive

This section provides a detailed view of the technical mechanisms that underpin the five workflow stages (confirmation of payee, path discovery, validation, locking and settlement), explaining how each stage operates within Project Agorá's privacy-preserving, multi-ledger architecture. These mechanisms rely on the coordinated interaction of institutional middleware, participant-scoped

private communication (bilateral messaging and, where applicable, privacy group-scoped coordination), and the payment coordinator's on-ledger enforcement of workflow rules.

Confirmation of payee

CoP provides an early safeguard in the payment life cycle by ensuring that beneficiary details supplied by the debtor agent correspond to the intended recipient. This reduces misdirected payments, avoids late-stage exceptions and aligns with established operational practices.

In the prototype, CoP coordination occurs off the shared ledgers between the debtor and creditor institutions using participant-scoped coordination. A scoped coordination channel is established so that only the relevant parties can exchange the minimum information required for the check. The creditor institution performs the CoP verification within its own middleware, using locally held customer/account data (including any internal address book or reference mappings). No raw customer data or proprietary verification logic is disclosed.

Once the creditor completes its check, it returns an endorsed result to the debtor agent. In addition to the match outcome (ie match / no match), the creditor may also return minimal operational details required for subsequent workflow stages – such as the token type and the receiving wallet/address that will be used in settlement – so that later stages can construct the settlement instruction set without disclosing sensitive underlying data.

The debtor agent submits the CoP outcome to the payment coordinator as an input to workflow progression. The payment coordinator records the minimum outcome required to govern progression and advances the workflow to path discovery when the CoP outcome meets the configured criteria. If the result is negative (or a timeout occurs), the payment terminates without proceeding to later stages.

Path discovery mechanism

The PDM identifies a viable path for a payment across participating institutions and jurisdictions while preserving confidentiality of pathfinding preferences and bilateral commercial relationships.

The PDM draws on two categories of information:

- Public reference and corridor data (eg network/corridor registries) that indicate which institutions are reachable for relevant currency corridors.
- Private pathfinding logic held exclusively within each institution's middleware, including preferred correspondents, bilateral agreements, internal policies and operational constraints.

In the prototype, the PDM is implemented as hop-by-hop, bilateral private messaging. Each institution evaluates its pathfinding options privately within its middleware, selects a next hop, and exchanges only the minimum necessary information with that next-hop institution through a 1:1 private communication channel. Unlike other workflow stages, the PDM does not use private smart contracts or a multi-party privacy group: pathfinding decisions remain institution-local, and coordination occurs through bilateral messaging.

Participants may backtrack and explore alternative paths if an initial choice cannot reach the destination under applicable constraints. Once a complete viable path is found, the debtor agent re-checks the final assembled path before submitting the selected path (or a representation of it) to the payment coordinator as the PDM outcome. The coordinator records the minimum path representation required for subsequent stages to coordinate among the participants in the chosen path, without revealing unnecessary pathfinding rationale or private preferences.

The following example shows how an institution might implement path preference logic based on the transaction amount in its own environment. It is simplified for clarity.

Example: payment pathfinding based on transaction amount (*)

```
threshold := input.config.threshold
amount := input.request.amount
# Direct relationship (e.g. a known direct counterparty)
direct_bic := input.request.direct_bic
# Central bank
central_bank_bic := input.request.central_bank_bic
path := {
    "type": "central_bank",
    "next_hop": central_bank_bic,
    "reason": "Amount above threshold, routed via central bank"
} if {
    amount > threshold
}
else := {
    "type": "direct",
    "next_hop": direct_bic,
    "reason": "Amount at or below threshold, routed directly"
}
```

(*) Illustrative example only; not a recommended implementation pattern.

Path construction

The debtor agent initiates path construction. At each hop:

1. The current participant receives the in-progress path (subject to restrictions on disclosure, consistent with existing practices).
2. The participant evaluates private pathfinding logic in its middleware.
3. The participant proposes and communicates a next hop bilaterally to the chosen next participant.
4. The process repeats until the creditor institution is reached.

If a participant cannot propose a viable next hop, the participant returns a path exhaustion response to the prior hop, and the path construction process may backtrack to explore alternatives.

If no viable path can be found within applicable constraints or timeouts, the payment terminates cleanly before entering Validation or settlement-related stages.

Once a complete path is constructed, the final sequence of intermediaries and any cross-currency providers is submitted to the payment coordinator as the PDM outcome. The coordinator records the minimum required representation and advances the workflow to the validation stage.

Privacy and interoperability characteristics

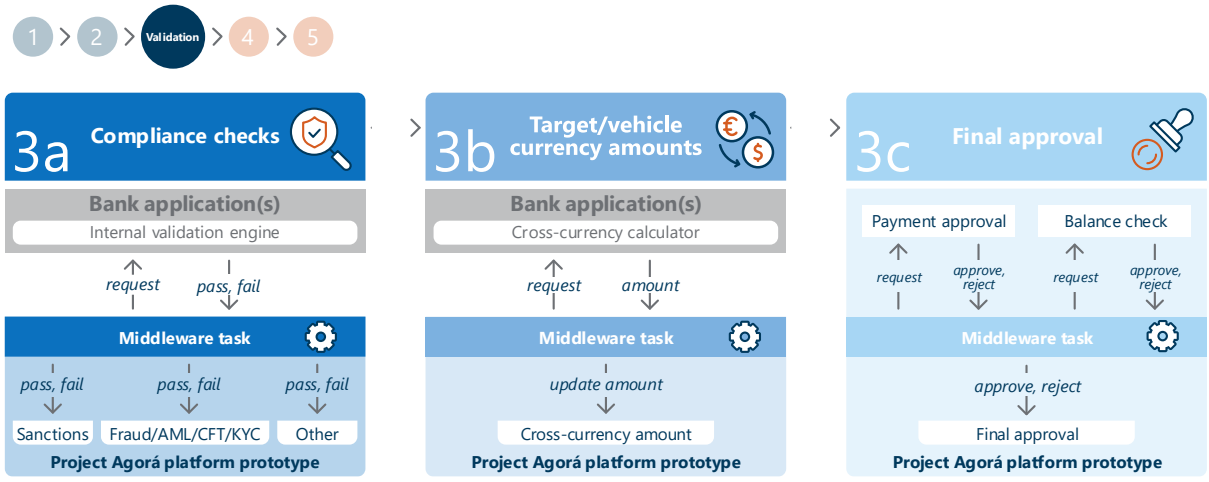
The PDM is designed to reveal only the minimum pathfinding information necessary to execute the workflow. Participants involved in the path learn only what is required to forward the payment along the selected path; institutions not involved in the path observe no pathfinding information. Interoperability is achieved by allowing institutions to reuse existing correspondent networks, policy rules and pathfinding logic without disclosure, while still producing a machine-verifiable path outcome for subsequent workflow stages.

Validation framework (validate, amounts and ready)

The Project Agorá prototype implements validation as a single life cycle stage with three internal sub-steps – validate, amounts and ready – to ensure all required checks are completed, cross-currency amounts are coherently determined when applicable, and participants are operationally prepared before entering locking and settlement (Figure 14).

The design follows three core principles. First, each institution performs its own checks and retains full control over internal logic and systems. Second, only endorsed summary outcomes required for workflow progression are shared; detailed data, methods and intermediate decisions remain within each institution. Third, the payment coordinator advances the workflow only when all necessary outcomes are received within defined time windows, enforcing deterministic progression and preventing ambiguous pre-settlement states.

Payment validation stages **Figure 14**



Source: Project Agorá.

Validate (compliance and risk checks)

In the validate sub-step, each commercial bank involved in the payment path conducts the regulatory and risk-based checks required under its jurisdiction and policy framework (Figure 15). These checks typically include sanctions screening, AML/CFT, KYC and fraud controls, transaction monitoring and other institution-specific policy assessments.

All validation logic is executed within the institution's middleware, drawing on internal compliance systems, customer records and risk engines. No underlying customer data or institution-specific methods are disclosed. Once checks are complete, the institution returns an endorsed summary outcome through participant-scoped coordination. In the prototype, this is implemented as one API submission that includes three binary (pass/fail) outcomes – one for each category (sanctions; AML/CFT, KYC and fraud; and "other").

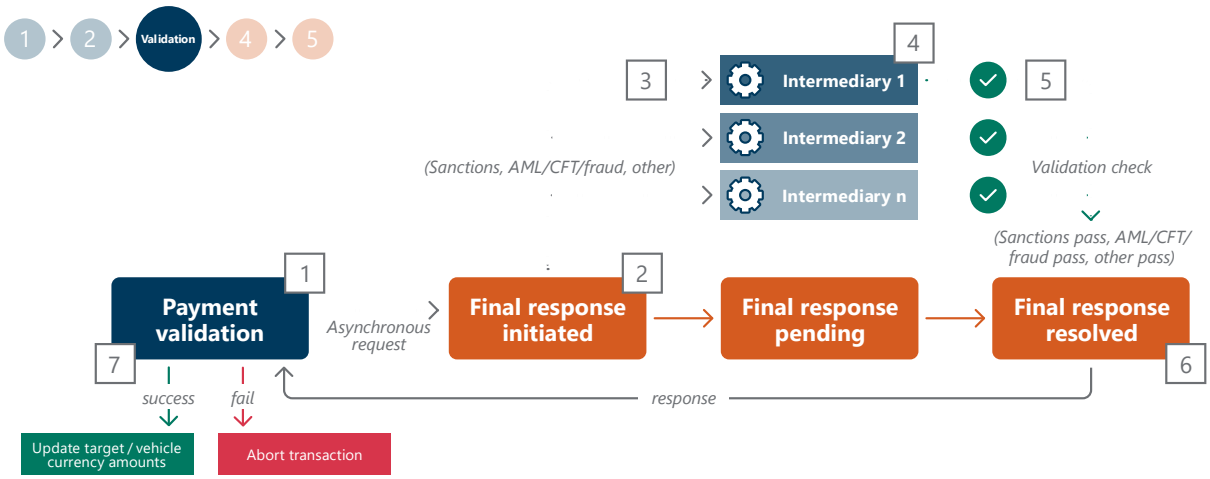
For each participant, the participant-level validate outcome is derived as follows:

- **pass** – all three category outcomes are pass; or
- **fail** – one or more category outcomes are fail, causing the payment to terminate.

Where an institution requires additional information to complete checks, a scoped bilateral "needs more information" exchange may occur with the relevant counterparty. Only the minimum additional details required are exchanged, and the institution then re-runs its internal checks before returning a definitive pass or fail outcome.

The payment coordinator aggregates validate outcomes across all required participants. The workflow can progress to amounts only when all required participants return a participant-level pass (ie all category outcomes passed for all required participants) within the configured timeout window. If any participant returns a fail (or times out), the aggregated validate outcome for the payment is fail, and the coordinator terminates the payment before any assets are locked or delegated.

Validation check steps **Figure 15**



Source: Project Agorá.

Amounts (cross-currency amount determination)

The amounts sub-step determines the final cross-currency settlement amounts when the payment involves one or more currency conversions. This sub-step is not invoked for single currency payments.

Designated cross-currency providers (as identified by the selected path) compute the required converted amounts within their own middleware environments. They may retrieve pricing data from internal engines or external sources, apply institution-specific policies (eg spreads, thresholds or rounding rules) and produce endorsed outputs.

Only the endorsed final amount(s) and associated currency information are submitted to the payment coordinator. No raw exchange rates, order books or proprietary pricing inputs are disclosed. In vehicle currency scenarios involving multiple conversions, amount computations occur sequentially, with each provider receiving the prior endorsed result and returning the next endorsed amount in the chain.

The coordinator records the endorsed amount outcomes as part of payment state (in minimal form) and advances the workflow to ready only when all required amount outcomes have been received within the configured timeout.

Ready (final pre-locking readiness)

The ready sub-step serves as the final checkpoint before the payment enters locking and settlement. At this point, the selected path and the final amounts are known. The purpose of ready is to allow each institution to confirm that it is operationally and technically prepared to proceed.

Each institution may perform additional readiness checks within its middleware, including:

- tolerance checks (eg comparing workflow-derived cross-currency outcomes with an institution's own pricing source within an acceptable threshold);
- liquidity and token availability checks to confirm sufficient balances to support locking; and
- any additional institution-specific authorisation requirements.

Based on these checks, each institution returns an endorsed ready or not ready outcome to the payment coordinator. All required participants must return ready within the configured timeout for the payment to progress. If any participant returns not ready or times out, the payment is terminated before locking begins.

The ready sub-step provides a final safeguard against unexpected market conditions, insufficient liquidity or changes in internal risk appetite. Only once all required participants have signalled readiness does the coordinator advance the workflow to locking.

The following example shows how an institution might implement a tolerance check in its own environment. It is simplified for clarity.

Example: illustrative readiness tolerance check (*)

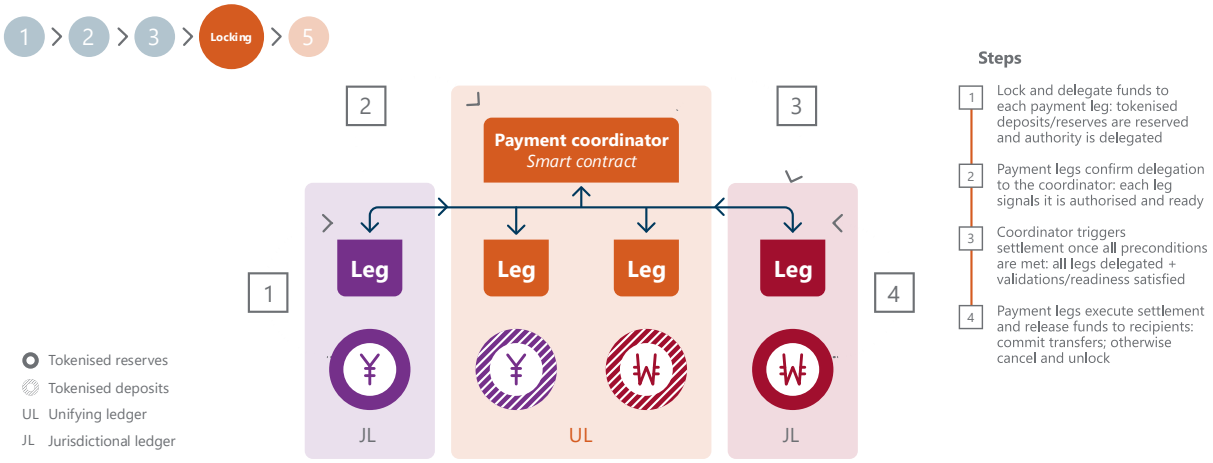
```
if payment.isCrossCurrency = false:
  return { approved: true, message: "Single-currency payment" }
else:
  tolerance := getTolerance(payment.targetCurrency)
  rate := getFxRate(payment.sourceCurrency, payment.targetCurrency)
  expected := payment.sourceAmount * rate
  actual := payment.targetAmount
  difference := abs(actual - expected) / expected
  return {
    approved: difference <= tolerance,
    message: difference <= tolerance ? "Amount approved" : "Amount rejected"
  }
```

(*) Illustrative example only; not a recommended implementation pattern.

Atomic settlement (lock, delegate, settle)

Atomic settlement is the point at which the workflow's prior stages culminate in a coordinated settlement outcome across multiple ledgers. In Project Agorá, settlement is governed by the payment coordinator and is executed as a coordinated commit-or-cancel outcome across all relevant payment legs (Figure 16).

Atomic settlement in the layered ledger **Figure 16**



Source: Project Agorá.

Because the platform uses a layered multi-ledger architecture, settlement coordination does not rely on cross-chain bridges. Instead, the coordinator and payment leg contracts enforce consistent progression using on-ledger state transitions and deterministic events, while

participants' middleware and participant-scoped coordination channels provide the endorsed inputs required to progress the workflow.

Lock

The lock sub-step reserves the assets required for technical settlement across the appropriate ledgers. For each payment leg, the relevant token contract reserves the required balances so they cannot be repurposed during the remainder of the workflow. Locking has three key characteristics:

1. **Ledger-native reservation**: assets remain on their native ledger (eg tokenised deposits on the unifying ledger in the prototype; tokenised reserves on the issuing jurisdictional ledger), preserving jurisdictional control.
2. **Payment scoping**: each lock is bound to a specific payment instance and settlement instruction set.
3. **Controlled release**: locks are held until the workflow reaches a coordinated conclusion, at which point they are either spent (commit) or released (cancel) according to the coordinator outcome.

Each institution submits the required lock and delegation transactions to the ledger where the relevant assets reside. Participant middleware observes unifying ledger/jurisdictional ledger events and endorsed outcomes and submits the required inputs to the payment coordinator on the unifying ledger to advance workflow state; the coordinator governs sequencing and outcomes but does not directly invoke contracts on other ledgers.

In contract terms, locking is implemented through a *createLock()* operation that reserves balances and prepares the atomic settlement trigger instruction to be executed later.

Delegate (and settlement authorisation)

Once all required assets are locked and all participants have reached ready, the workflow transitions to delegate. In this sub-step, participants grant narrowly scoped, temporary authority to the relevant payment leg contracts to act on the locked balances for this specific payment only.

Delegation is implemented through a *delegateLock()* operation that grants payment-scoped authority without transferring broader control of the underlying assets. Delegation remains valid only for the payment's settlement window and is constrained to the locked balances created for that payment.

To ensure that all payment participants explicitly authorise coordinated settlement, the prototype requires a signature bundle from them all. Participants produce signatures within a participant-scoped coordination context associated with the payment, and the coordinator collects these signatures into a bundle. This bundle is then used to authorise the final settlement execution across the relevant payment legs, ensuring that settlement cannot proceed unless all required participants have endorsed the settlement intent.

Settle (commit-or-cancel governed by coordinator)

In the settle sub-step, payment leg contracts execute the final technical settlement operations on their respective ledgers using the delegated authority and the collected signature bundle. Settlement is governed by the payment coordinator outcome:

- **Commit outcome**: payment legs spend the locks and apply the prepared settlement actions (*spendLock()*), transferring value according to the settlement instruction set.
- **Cancel outcome**: payment legs release locks without transferring value (*cancelLock()*), returning funds to participants' control.

Crucially, the payment legs do not "succeed" or "fail" independently in a way that determines the overall result. Instead, the locking and delegation construct ensures that each leg follows the coordinator's final outcome, preventing partial settlement across ledgers. Deterministic technical settlement on each ledger ensures that once settlement transactions are committed, the recorded workflow state becomes technically irreversible.

Payment versus payment

PvP settlement is a specialised form of coordinated settlement that links two payment legs in different currencies so that neither settles unless both can. PvP is particularly relevant in cross-currency trades and interbank transfers where institutions seek to eliminate principal risk arising when one leg is executed while the other remains unsettled.

The Project Agorá prototype supports PvP within the same layered multi-ledger architecture used for end-to-end cross-border payments. PvP reuses the same locking and settlement constructs as standard payments but applies a modified workflow structure: PvP does not require CoP, PDM or cross-currency amount determination. Instead, it focuses on the controls required to ensure both currency legs can be validated, locked, authorised and settled as a single coordinated outcome.

PvP workflow overview

A PvP transaction on the Project Agorá platform consists of two payment legs – one on each currency's relevant ledger surface – coordinated by a single PvP payment coordinator. Each participant performs required institution-local checks and confirms readiness within its own middleware (validation stage), after which both legs are locked and delegated (locking stage) and then settled together (settlement stage).

For readability, the PvP workflow can be described as:

- **Validation (including readiness)**: participants perform required checks and return endorsed outcomes.
- **Locking (lock and delegate)**: required balances for both legs are reserved and settlement authority is delegated to the relevant payment leg contracts.

- **Settlement (commit-or-cancel)**: both legs commit together or both cancel together according to the PvP coordinator outcome.

This structure ensures that the pre-settlement logic of each leg remains institution- and jurisdiction-specific, while the final settlement execution is synchronised across both currency legs.

PvP coordinator and payment legs (single-coordinator model)

PvP is orchestrated by a single PvP payment coordinator contract that governs the shared workflow state and final outcome. The coordinator tracks the readiness and locking state of both legs and advances to settlement only when prerequisites for both legs are satisfied within configured timeouts.

Each ledger involved hosts a single payment leg contract for the PvP transaction. Once locks are created and delegation is granted, each payment leg holds narrowly scoped authority to execute settlement actions on the locked balances for this specific PvP instance. The legs do not decide the success/failure of PvP independently; rather, they execute commit or cancel actions in accordance with the coordinator's final outcome, ensuring that partial execution across currencies does not occur.

Settlement outcome and safety properties

The PvP settlement outcome is governed by the PvP coordinator as a coordinated commit-or-cancel result:

- **Commit outcome**: both payment legs execute settlement using their delegated authority, applying the prepared settlement instructions and spending the locks.
- **Cancel outcome**: both payment legs cancel, releasing the locks without transferring value.

This coordinated outcome prevents principal risk by ensuring that neither currency leg completes without the other. Deterministic technical settlement on the relevant ledgers ensures that once settlement actions are committed, the workflow state transitions become technically irreversible. As with end-to-end payments, the prototype's settlement authorisation mechanism requires explicit endorsement by the relevant payment participants prior to settlement execution (described in the settlement deep dive).

Privacy and bilateral coordination

All sensitive negotiation – trade details, bilateral limits, risk calculations and any institution-specific decision logic – occurs within institutional middleware and participant-scoped coordination channels. Only endorsed outcomes required for workflow progression are provided to the PvP coordinator and anchored on ledger in minimal form, consistent with the platform's broader privacy and data minimisation model.

Prototype caveats and future extensions

While the prototype demonstrates core PvP coordination and settlement mechanics, it does not implement the full range of production-grade PvP features such as netting, batch PvP coordination, liquidity reservation windows, or integration with external trading venues and risk systems. The

architectural model nonetheless provides a strong foundation for extending PvP functionality, leveraging the same layered ledger architecture, deterministic workflow sequencing, and privacy-preserving coordination mechanisms.

Assurance and prototype development

Formal assurance activities required for production deployment – such as comprehensive cyber security testing, operational resilience assessment, performance benchmarking, threat modelling, and production-grade operational controls – were intentionally out of scope for the prototype. Nonetheless, the architecture and engineering approach were designed with these requirements in mind, providing a strong foundation for subsequent hardening and assurance work.

Accordingly, the assurance considerations described in this section focus on: (i) the architectural properties that support predictable and safe workflow behaviour in the prototype; and (ii) the development and testing practices used to demonstrate end-to-end flows and validate functional correctness.

Assurance considerations

The Project Agorá prototype incorporates architectural features that support predictable and controlled operation by design. These include permissioned consensus (QBFT/PoA) to provide deterministic technical settlement of workflow state, deterministic workflow sequencing with explicit timeouts and termination semantics, strict asset locking rules and scoped delegation of settlement authority to payment leg contracts during the settlement window.

These features contribute to workflow safety in the prototype in several ways:

- **Deterministic workflow progression**: the payment coordinator enforces stage preconditions, transition rules and timeouts, preventing payments from remaining indefinitely in intermediate states.
- **Safe termination semantics**: payments terminate cleanly if required participant outcomes are not received in time, or if a participant returns a negative outcome at a required stage, ensuring settlement is not attempted without prerequisites.
- **Controlled asset handling**: assets are locked prior to settlement and can be acted upon only under tightly scoped, payment-specific delegated authority, supporting coordinated commit-or-cancel execution.
- **Auditable state changes**: workflow and asset events provide an observable record of progression and outcomes for participants' operational and audit needs.

While these architectural properties provide a strong foundation, they do not replace the full assurance activities required for a production system. Any production deployment would require additional work across security testing, resilience and recovery design, operational monitoring, governance and control frameworks, and performance evaluation, consistent with the requirements of regulated financial market infrastructures.

Development and testing

The Project Agorá prototype was developed iteratively across four milestones, with each milestone introducing additional architectural components, workflow capabilities and ledger interactions. Development followed a modular approach: the layered ledger architecture, privacy framework, workflow smart contracts and participant-operated suite components were implemented independently and integrated through well defined interfaces. This reduced coupling between components and enabled changes in one area (eg workflow logic or privacy-group configuration) without requiring redesign of the underlying ledger platform.

Throughout development, new capabilities were validated through user acceptance testing (UAT) conducted jointly with participating institutions. UAT focused on demonstrating end-to-end payment flows and validating core workflow behaviour across realistic multi-institution scenarios. This included CoP, path discovery, validation (including cross-currency amount determination and readiness), locking and coordinated settlement. The tests also confirmed that institutional middleware, participant-scoped coordination mechanisms and the payment coordinator remained synchronised under different operational conditions, and that workflow progression and outcomes were observable through application interfaces and indexed events.

UAT was scenario-based and qualitative in nature, prioritising functional correctness, deterministic workflow sequencing, inter-institution interoperability and reliable reconstruction of participant state. Key areas covered during UAT included:

- End-to-end workflow execution across all life cycle stages
- Concurrent payment scenarios to validate isolation and deterministic sequencing between workflows
- Distributed path discovery behaviour, including multi-hop pathfinding, backtracking and clean termination when no viable path exists
- Validation flows across multiple participants, including pass/fail outcomes and "needs more information" exchanges resolving to definitive results
- Cross-currency amount determination and readiness confirmation prior to locking
- Multi-ledger locking and delegation sequencing across the unifying ledger and one or more jurisdictional ledgers
- Coordinated commit-or-cancel settlement execution across ledgers
- Timeout handling and workflow termination at different stages, including clean abort and release of locked balances
- Indexing and observability, confirming that participants could reconstruct workflow progression and outcomes using ledger events and participant-scoped coordination artefacts

Testing in this phase did not include performance benchmarking, stress testing, security assurance or operational resilience assessment. These areas were intentionally out of scope for the prototype.

Code compliance and engineering standards

Although the Project Agorá platform was developed as a prototype, its implementation followed disciplined engineering practices to support maintainability, reproducibility and correctness. The codebase was structured for modularity and clarity, and development processes included peer review and systematic validation of changes.

Core practices included:

- Unit and integration testing of key modules and representative workflows
- Automated checks for code quality (linting and style rules) and regression prevention where applicable
- Controlled change management through version control, review processes and documented interfaces between components
- Documentation within the codebase, including design notes and component-level usage information

These practices supported consistent evolution across milestones and facilitated collaboration among participating technical teams. They provide a foundation for future work, while recognising that production deployment would require additional assurance activities, operational controls and security hardening beyond the scope of this phase.

Chapter 5: Legal and regulatory analysis[25]

In support of developing the Project Agorá prototype, the project analysed the legal and regulatory considerations relevant to designing and building a programmable platform for wholesale cross-border payments based on the existing correspondent banking model. This chapter sets out the conclusions of this analysis.

Project Agorá aimed to design a prototype, with the objectives stated in Chapter 1. At the same time, Project Agorá remained aware of necessary legal constraints, rights and obligations of parties involved in a payment chain that serve public policy purposes such as monetary and financial stability, financial crime prevention and data privacy. The resulting design pushes the technological frontier of cross-border payments and contributes to ongoing thinking on the application of existing regulatory frameworks to tokenisation and DLT-based market infrastructures.

The legal and regulatory analysis found that the Project Agorá prototype does not present any direct conflicts with existing laws and regulations. Accordingly, implementation of a platform with this design is achievable within the current legal and regulatory framework. Additionally, no unmanageable challenges were identified in adopting this design in compliance with applicable legal and regulatory frameworks. The analysis also considers how compliance and contractual arrangements may be adapted to reflect the features of shared ledger infrastructures for cross-border payments. Recognising that jurisdictional laws and regulations pertinent to the adoption of new technologies in cross-border payments are likely to continue to evolve, the analysis also identifies legal elements which may warrant future consideration. Further, it considers aspects of the platform design and intended functionality that may need to be addressed in one or more rulebook(s).

The analysis does not cover the operational or governance arrangements applicable to participants in the protype and that would be necessary to bring the protype into production. Further, this legal analysis does not make definitive legal determinations regarding how this prototype would necessarily operate in practice, nor does it make regulatory recommendations.

Roles and responsibilities of platform participants

The Project Agorá platform is designed to allow participation of direct participants, initiation service providers and indirect participants. Direct participants are limited to central banks and commercial banks, which interact with the platform through implementations of the Project Agorá suite that they maintain. Initiation service providers are non-bank financial institutions maintaining a node on the unifying ledger for the sole purpose of initiating PvP transactions on behalf of participating commercial banks. Indirect participants include non-bank financial institutions (other than initiation

[25] This analysis does not represent legal or other advice or a legal opinion. The analysis is limited to a technical review of the content and structure of relevant legislation in the different jurisdictions and an assessment of its applicability to cross-border payment transactions with tokenised reserves and tokenised deposits on a Project Agorá-type platform. The analysis does not express, and should not be construed as expressing, in any way a view or opinion on the suitability, desirability, appropriateness or effectiveness of any law, legislative or policy approach adopted, or to be adopted, in any jurisdiction. It is the result of collective analysis and should not be attributed to any individual contributor or the organisation they represent, and it may not necessarily reflect the views of an individual contributor or the organisation they represent.

service providers) and corporates, which participate only as holders of deposit accounts at participating commercial banks. Balances that indirect participants hold in deposit accounts at participating commercial banks are recorded on the unifying ledger by means of tokenised deposits. However, an indirect participant may access the Project Agorá platform functionality only through its pre-existing relationship with a participating commercial bank.

No individuals may participate directly or indirectly in the platform, given the platform is not designed for retail payments.

The following provides additional information about the nature of the participation by each of these types of institutions:

- **Central banks**: A participating central bank maintains a node on its respective jurisdictional ledger and may choose to maintain a node on the unifying ledger; it would not be expected to maintain a node on any other jurisdictional ledger. Participating central banks are the only entities that may issue tokenised reserves. The tokenised reserves issued by a participating central bank are (as discussed above) recorded on its respective jurisdictional ledger. A participating central bank may participate in validation on the jurisdictional ledger on which it maintains a node. A participating central bank controls an asset smart contract applicable to the tokenised reserves it issues. A participating central bank is not expected to access or interact with workflow smart contracts or reference smart contracts in the unifying ledger for the purpose of cross-border payments. A participating central bank may, however, deploy workflow smart contracts or reference smart contracts on its respective jurisdictional ledger for its own use.
- **Commercial banks**: A participating commercial bank maintains nodes on the unifying ledger and on each jurisdictional ledger that corresponds to a participating jurisdiction in which it maintains balances in a reserve account at the applicable central bank that are recorded by means of tokenised reserves. A participating commercial bank may hold tokenised reserves in a participating jurisdiction only if that commercial bank: (i) is authorised to access central banking services in that participating jurisdiction and holds a reserve account with the relevant central bank; and (ii) elects to participate in the platform with respect to that participating jurisdiction. Only a participating commercial bank may be recorded as the holder of tokenised reserves issued by a central bank, and a commercial bank may hold tokenised reserves only in a participating jurisdiction with respect to which the commercial bank maintains a node on the applicable jurisdictional ledger.[26] A participating commercial bank issues tokenised deposits, which (as discussed above) are recorded on the unifying ledger.

  A participating commercial bank may participate in validation on both the unifying ledger and the jurisdictional ledger(s) in which it participates. A participating commercial bank controls an asset smart contract applicable to the tokenised deposits it issues, which in all cases may be held only by financial institutions or corporate depositors, not natural persons or other retail depositors. A participating commercial bank also interacts with relevant workflow smart contracts and reference smart contracts as necessary in connection with the issuance and redemption of tokenised deposits and to the extent that the processing of payments on the platform involves changes to amounts of: (i) tokenised deposits issued by the commercial bank (ie debits and credits to deposit accounts at the

[26] In other words, only a commercial bank that holds reserves at a particular central bank can receive or hold tokenised reserves issued by that central bank.

commercial bank); or (ii) tokenised reserves held by the commercial bank (ie debits or credits to a reserve account held by the commercial bank).[27] Payments on the platform involving changes to amounts of tokenised deposits issued by a participating commercial bank may involve the commercial bank acting, with respect to a particular payment, as the bank maintaining the account of the depositor that is the payor (ie the debtor's agent, or initiating institution), as the bank maintaining the account of the ultimate payee (ie the creditor's agent, or beneficiary institution), as a bank that facilitates the transfer of funds between the banks of the payor and the ultimate payee (ie an intermediary agent) or as a bank that maintains accounts at another commercial bank and is a payor (ie a debtor) or ultimate payee (ie a creditor) with respect to the payment on the platform.

- **Initiation service providers**: A non-bank financial institution such as a central counterparty or other financial market infrastructure may participate in the platform as an initiation service provider. In that capacity, the non-bank financial institution operates a node on the unifying ledger and interacts with relevant workflow smart contracts and reference smart contracts as necessary to initiate or support PvP transactions directly in the platform on behalf of participating commercial banks.
- **Non-bank financial institutions and corporates**: A non-bank financial institution other than an initiation service provider or corporate may participate in the platform only as a holder of a deposit account at a participating commercial bank or otherwise on behalf of holders of deposit accounts at a participating commercial bank. In these capacities, a non-bank financial institution or corporate participant may be a payor (ie a debtor) or ultimate payee (ie a creditor) with respect to a payment on the platform. A non-bank financial institution may also be a service provider that, through an arrangement with a participating commercial bank, initiates or handles payments on the platform as a service to debtors and/or creditors.

  When participating non-bank financial institutions are not initiation service providers, they do not interact directly with platform smart contracts that update balances and do not operate a node on either the unifying ledger or any jurisdictional ledger. In such cases, the participation of a non-bank financial institution or a corporate occurs only through a pre-existing customer relationship with a participating commercial bank, and all actions on the platform are performed by or through the applicable commercial bank on their behalf.

Tokenised reserves, tokenised deposits

The Project Agorá platform, through the issuance of tokenised reserves and tokenised deposits, enables the recording and updating of balances in different types of off-platform accounts. The use of tokenised reserves and tokenised deposits to effectuate payments preserves the underlying legal account relationship in place between the issuer of tokenised reserves or tokenised deposits (a central bank or commercial bank, respectively) and its depositor.

The balances recorded through the use of tokenised reserves are in all cases balances in reserve accounts at a central bank. The balances recorded through the use of tokenised deposits

[27] A commercial bank's interaction with workflow smart contracts relating to changes in amounts of tokenised reserves are structured so that the commercial bank has visibility only into a payment leg that involves changes to amounts of tokenised reserves held by that commercial bank.

are in all cases balances in deposit accounts at a commercial bank, and these accounts may be customer accounts, correspondent accounts or nostro accounts. The underlying account relationship, as established by the agreements between the relevant bank and its customer, continues to govern the legal relationship between those parties. The platform is designed to preserve these legal relationships, including to maintain continuity with established institutional arrangements, while enabling balances in the underlying reserve and deposit accounts to be recorded on the platform. Participating banks are also able to each determine how amounts of tokenised reserves or tokenised deposits recorded on the platform map to underlying accounts, including whether to establish a separate account with respect to any balances recorded through the use of tokenised reserves or tokenised deposits or whether balances within an individual account may be recorded in part through the use of tokenised reserves or tokenised deposits and in part by other technologies.

The balances in reserve accounts recorded through the use of tokenised reserves are liabilities of the central bank that issued the tokenised reserves to a commercial bank. A commercial bank's tokenised reserves, as recorded in the applicable smart contract on the relevant jurisdictional ledger, are associated with a balance of that commercial bank in a reserve account at the issuing central bank. Similarly, the balances in deposit accounts recorded through the use of tokenised deposits are deposit liabilities of the commercial bank that issued the tokenised deposits to a holder. The Project Agorá platform serves as the definitive record of the balances in reserve accounts or deposit accounts, respectively, that are recorded on the platform. Nonetheless, any bank that issues tokenised reserves or tokenised deposits may reconcile account balances recorded in the platform with other books and records, as it determines necessary and appropriate.[28] This reconciliation is not intended to affect the validity of payments processed on the platform. Rather, it is intended to ensure that payments processed on the platform are appropriately reflected in any other systems used by a participant.

Legal nature of tokenised reserves and tokenised deposits

In each participating jurisdiction, the principal consideration for evaluating the legal characterisation of tokenised reserves and tokenised deposits is whether using tokenisation to record balances in a central bank reserve account or a commercial bank deposit account alters the legal nature of the underlying account relationship or, instead, functions solely as a technical mechanism for recording balances and effectuating debits and credits to those balances.

The project has found that:

- No participating jurisdiction has adopted a statutory or regulatory framework that specifically governs tokenised representations of central bank reserves or of commercial bank deposits. In these jurisdictions, the legal characterisation of tokenised reserves and tokenised deposits would therefore be assessed under existing legal frameworks applicable to central bank reserves, commercial bank deposits, related arrangements and other types of assets, such as virtual assets or cryptoassets (or similar designations).
- These frameworks, especially those applicable to central bank reserves and commercial bank deposits, are generally technology-neutral and focus on the substance of the

[28] Central banks that issue tokenised reserves and commercial banks that issue tokenised deposits may choose how balances recorded on the platform are mapped to, and reconciled with, other books and records or legacy account systems that they maintain.

underlying legal relationships, rather than the technology used to record balances or process payments.

- Given the design requirements to maintain an underlying reserve or deposit account, and the platform's focus on preserving existing legal relationships, it is unlikely that legal frameworks applicable to virtual assets or cryptoassets, whether already in force or currently under development, would apply directly to the platform. However, because such frameworks may extend to payment-related activities, it is possible that they may still give rise to some considerations, even where such legal frameworks would not be directly applicable.
- Tokenisation of central bank reserve accounts or commercial bank deposit balances on the platform is intended to function solely as a technical mechanism for effecting debits and credits to those balances, without altering the legal nature of the underlying account relationship. Accordingly, tokenised reserves, and the underlying reserve accounts, should be characterised as equivalent to reserves recorded in a traditional (ie non-shared ledger systems) reserve account. Similarly, tokenised deposits should be characterised as equivalent to deposits recorded in a traditional deposit account.
- Neither tokenised reserves nor tokenised deposits themselves confer any legal or economic rights on any holder; such rights arise, in all instances, from the underlying debtor-creditor relationship between the issuing bank and its account holder (ie the holder of tokenised reserves or tokenised deposits, as applicable) pursuant to applicable account agreements or similar documentation, and not any rulebook(s) or other binding documentation governing a commercial bank's or central bank's participation in the platform in any participating jurisdiction. Nonetheless, to support this conclusion it will be important that platform documentation clearly provides that tokenised reserves and tokenised deposits do not themselves have independent legal significance or confer legal or economic rights separate from those arising under applicable account agreements.

In addition to the overview above, the key legal and other relevant elements of tokenised reserves and tokenised deposits within the Project Agorá prototype in regard to their adoption are set out below.

Tokenised reserves

- Central banks should retain exclusive control of the interaction between traditional reserve accounts and the issuance and redemption of tokenised reserves in their currency.
- Reserve balances held at the applicable central bank remain obligations of the central bank to the account holder.
- Tokenised reserves on the platform are equivalent to reserves recorded in traditional systems and are subject to local policies regarding their access, transfer and updates.
- The maintenance of local control was identified early on as an essential element to the platform's design. The Project Agorá platform supports this requirement by enabling the retention of control over the asset smart contracts associated with a central bank's tokenised reserves. This includes the ability to define the entities authorised to initiate balance updates and under what conditions.
- Platform documentation must align with central bank requirements to enable equivalent treatment of tokenised reserves on the platform, as compared with those in traditional

systems. In many participating jurisdictions this entails issuing the tokenised reserves in compliance with the operational standards related to requirements for appropriate control, oversight, data protection and operational resilience.

Tokenised deposits

- Banking and commercial law frameworks in each jurisdiction treat deposits as a debtor-creditor relationship between the bank and its depositor; tokenised deposits would be subject to these same existing frameworks.
- The analysis identified jurisdictional nuances in the requirements for documentation related to commercial deposits in regard to record-keeping. However, these nuances do not rise to a level such that the Project Agorá prototype could not operate with a great deal of commonality across participating jurisdictions.
- It may be necessary to consider whether account agreements should be updated to reflect that tokenised deposits do not confer legal or economic rights separate from those arising under applicable account agreements, as discussed below.
- The applicability of deposit insurance frameworks will be an important dimension of platform use. No participating jurisdiction maintains conditional eligibility for deposit insurance schemes based on whether deposits are recorded in tokenised or non-tokenised form, as current regimes are generally technology-neutral in this respect.
- However, the participating jurisdictions differ in the scope and operation of their deposit insurance schemes. Differences arise, for example, in coverage limits and in the categories of depositors eligible for protection.
- Deposit insurance eligibility for tokenised deposits is subject to related regulatory requirements that apply to insured deposits generally. In some participating jurisdictions, for example, insured banks are subject to extensive deposit record-keeping obligations. Application of these requirements to deposits recorded through shared ledger-based systems such as the platform may raise practical considerations, including the need to integrate platform-related activities with existing record-keeping and compliance systems, or to maintain certain record-keeping-related functionalities within jurisdictional borders.

Transactions on the platform: issuance, redemption and transfer

From a technology perspective, tokenised reserves and tokenised deposits are issued when balances are recorded on the platform. Therefore, issuance increases the amount of tokenised reserves or tokenised deposits held by a holder. Conversely, the amount of tokenised reserves or tokenised deposits held by a holder decreases when those tokens are redeemed. Finally, tokenised deposits and tokenised reserves are transferred by simultaneously increasing the amount of tokenised reserves or tokenised deposits held by one holder and decreasing by the same amount the amount of tokenised reserves or tokenised deposits (as applicable) held by another holder.

From a legal perspective, the key characteristics of the transactions on the platform are as follows:

- The issuance, redemption and transfer of tokenised reserves and tokenised deposits correspond to credits and debits to the relevant underlying accounts, in the same way that

balances would be updated in existing systems. The platform thus functions as a ledger and a mechanism for updating that ledger, rather than as a means of creating new financial instruments or imposing new rights and obligations between an issuer of tokenised reserves or tokenised deposits and the holder.

- The rights of a holder of tokenised reserves and tokenised deposits arise from the records maintained by the issuing central bank and commercial bank on the platform, respectively, as provided under applicable account agreements.
- The issuance of tokenised reserves and tokenised deposits does not imply the creation of new assets.
- The issuance, redemption and transfer of tokenised reserves and tokenised deposits are regarded as sufficient to complete a payment on the platform, provided that this is reflected in applicable account agreements. These agreements should also define who is entitled to make these updates and how they may do so.
- In the issuance, redemption and transfer of tokenised reserves and tokenised deposits each central bank retains capabilities equivalent to current oversight arrangements and jurisdictional control over sovereign money, including with respect to reserve balances and the systems in which they are recorded. As a result, minimum requirements for tokenised reserves could be explored that enable equivalent control and oversight powers for central banks. Such requirements will be a policy matter and an operational consideration for each central bank and are not in scope for the Project Agorá prototype.
- Commercial banks that issue tokenised deposits on the platform retain all current regulatory and supervisory obligations related to compliance. The ability to meet these obligations in transactions utilising the platform is discussed in later sections.

Contractual frameworks

The accounts with respect to which tokenised reserves and tokenised deposits record balances in the platform are governed by underlying contractual or other arrangements entered into between the central bank or commercial bank offering the account and its depositor. In this way, these accounts reflect the same legal relationships (ie asset-liability relationships) as is the case where balances in these accounts are recorded by means of traditional (ie non-shared ledger-based) records. However, recording balances in these accounts through the use of tokenised reserves and tokenised deposits may require updates or supplements to existing account agreements to permit the use of the platform, including representing balances by means of tokenised reserves or tokenised deposits (as applicable), effecting payments on the platform and consenting to sharing of data, as contemplated, through the platform.

In addition, direct participants in the platform will be subject to one or more rulebook(s) or other binding documentation that will establish, among other things: (i) applicable rules governing their participation in the platform; (ii) node operation; (iii) validation responsibilities; (iv) the point of settlement finality for payments on the platform; (v) allocations of liability; (vi) procedures for handling participant default or insolvency and other matters, consistent with national law requirements in each jurisdiction. Because the platform itself is a technical arrangement, there may be a need for documentation specific to individual jurisdictions, in addition to common operating rules for the platform as a whole. Based on the analysis carried out within the scope of Project Agorá, it may be the case that designation of components of the platform, or

its operations, as a payment system may be required in at least some of the participating jurisdictions. A direct participant would be subject to the applicable binding documentation in each participating jurisdiction in which it participates (ie by maintaining a node on the applicable jurisdictional ledger). Initiation service providers would also be subject to contractual arrangements governing their participation in the platform in any applicable participating jurisdiction. As indicated above, the participation of an initiation service provider is limited to initiating payments as a service provider on behalf of certain participating commercial banks.

Contractual enforceability

The Project Agorá platform's technical components, including asset smart contracts, workflow smart contracts and reference smart contracts, do not themselves govern the obligations of participants, but instead operate as mechanisms for performing or giving effect to the obligations that arise from binding underlying agreements. The operation of these smart contracts serves, among other things, as a means of carrying out contractual obligations,[29] evidencing required approvals or attestations, or enforcing agreed conditions (such as preventing the use of tokenised reserve or tokenised deposit amounts in a payment, unless specified preconditions are satisfied), but the legal significance of these operations derives from, and is dependent on, the underlying contractual framework rather than from the code itself.

In the participating jurisdictions, the enforceability of rights and obligations arising from participation in, and payments through, the platform would be assessed under generally applicable contract law frameworks that apply to the platform's applicable rulebook(s) or other binding documentation, rather than under a legal framework specific to smart contracts or shared ledger systems.

Project Agorá participants are likely to continue to rely on their existing underlying account agreements and related documentation to govern their relationships with customers or other account holders to the extent possible. It may be necessary to update or supplement these customer agreements to reflect platform-specific features and activities, including:

- Permitting some or all of a customer's deposit or reserve balance to be recorded on the platform.
- Authorising the participant to use the platform to initiate and settle payments on behalf of the customer or other account holder.
- Allocating rights and responsibilities in connection with platform-related payment activities, including in circumstances involving operational outages, erroneous or unauthorised payments, or fraud.
- Obtaining any necessary customer consent to utilise platform functionalities, including the sharing of certain data for the purpose of enabling the platform's confirmation of payee functionality and sharing the outcomes of compliance checks. (These items are discussed in more detail in the compliance section below.)

However, it is possible that these or other points may not require changes to existing account agreements and related documentation. In some jurisdictions, or within existing participant

[29] For example, asset smart contracts provide the means by which issuing banks issue, record and update amounts of tokenised reserves and tokenised deposits; workflow smart contracts coordinate the steps necessary to effect payments in accordance with agreed-upon conditions (both legal conditions established by contract and technical conditions established under the platform's technological design); and reference smart contracts store certain information required to support these processes.

contractual arrangements, these eventualities are already provided for in a manner consistent with regulatory requirements. The need for (and the scope of) any changes will be determined by each participant on the platform, subject to relevant regulatory provisions.

It is also expected that the governing framework for every jurisdictional ledger that operates in connection to the platform will be subject to certain minimum requirements. These may include technical specifications to ensure all jurisdictional ledgers that are part of the platform, whether designated as payment systems locally or not, use the underlying technology in a sufficiently similar manner, consistent with its purpose, applicable legal requirements and safeguards. These minimum standards may be agreed upon in a framework agreement, memorandum of understanding or other agreement entered into by the relevant participating central banks and/or operators in each participating jurisdiction.

Choice of law and conflicts of law

The cross-border characteristics of the platform make choices with respect to governing law and forum selection particularly important. Key considerations include:

- No participating jurisdiction has adopted a choice of law or conflict of law framework specific to tokenised representations of central bank reserves or commercial bank deposits recorded on shared ledgers. Contract law frameworks recognise the principle of party autonomy and are generally technology-neutral.
- Domestic legal frameworks in each participating jurisdiction typically recognise the parties' choice of governing law for contractual matters, subject to mandatory law and public policy limitations:
    - **Mandatory law**: including, but not limited to, bank regulatory, insolvency and resolution regimes; depositor protection frameworks; the protection of personal data; and third-party proprietary rights.
    - **Policy limitations**: such as where a chosen governing law would deny parties contractual remedies afforded under domestic law or undermine a core purpose of domestic contract law.
- The participating jurisdictions differ in how they identify the relevant jurisdictional nexus for proprietary disputes in the absence of an effective choice of law that binds third parties. In at least one participating jurisdiction, the applicable law for proprietary disputes is determined by reference to the place with the closest connection to the underlying relationship, which will often be the domicile or place of incorporation of the participant subject to the dispute. In other participating jurisdictions, this analysis may focus on factors articulated by reference to where control or possession is exercised, which may be difficult to apply to shared ledger-based claims.
- Due to these differences in the participating jurisdictions, it will be important to specify in the rulebook(s) or other platform documentation a specific governing law for all provisions. It may not be necessary that all provisions apply to all participating jurisdictions or that the same governing law applies in all participating jurisdictions or to all provisions. The possibility of multiple governing laws for the platform's governing documentation may help to address the mandatory law and public policy considerations discussed above.

Settlement finality

Final settlement of a payment occurs at a legally defined moment. This moment is defined as "the irrevocable and unconditional transfer of an asset or financial instrument, or the discharge of an obligation by a financial market infrastructure or its participants in accordance with the terms of the underlying contract".[30] Achieving settlement finality for payments conducted via the platform is a key objective for Project Agorá. This objective seeks to ensure that the arrangements that govern settlement finality under the laws of each participating jurisdiction: (i) provide certainty regarding the treatment of a transfer of funds from a payor to a payee in a transaction in the event a participant in the payment enters an insolvency proceeding; (ii) ensure, in case of an insolvency proceeding, that the relevant funds are funds of the payee; and (iii) establish that settlement finality protections apply to a payment simultaneously in each participating jurisdiction. Achieving settlement finality protections across participants is especially important and enables a way for the Project Agorá platform to support composed transactions, where multiple balance updates are involved. Otherwise, a situation could arise where one leg of the payment is protected in insolvency proceedings while the corresponding other leg is not, exposing this transaction to settlement (Herstatt) risk.[31]

The platform is designed to enable the initiation and settlement of payments by means of coordinated updates to shared ledgers that record balances of tokenised reserves and tokenised deposits. Consequently, no decrease or increase of any tokenised reserve or tokenised deposit balance occurs as part of a payment unless all balance decreases and increases necessary to complete the payment occur. In the final stages of an E2E payment life cycle, the payment coordinator contract ensures that all the relevant tokenised deposits and tokenised reserves are "locked" with technical authority for settlement delegated to the applicable smart contract. Once locking and delegation occur, the payment coordinator contract issues on the unifying ledger an atomic settlement instruction – the "atomic settlement trigger". If the atomic settlement trigger is issued, all of these actions – that is, all necessary updates to tokenised reserves or tokenised deposits – *must* occur. However, not all of these updates occur simultaneously. In the platform setup, updates to the unifying ledger may occur before updates to the jurisdictional ledgers do, and updates to the relevant jurisdictional ledgers in a payment may occur asynchronously, but all follow the issuance of the atomic settlement trigger.[32]

Settlement finality on the platform

Project Agorá's approach to settlement finality relies on the issuance of the atomic settlement trigger. The issuance of the atomic settlement trigger would be specified in applicable rules as

---

30 Committee on Payment and Settlement Systems and Technical Committee of the International Organization of Securities Commissions, *Principles for Financial Market Infrastructures*, April 2012, Principle 3.8.1.

31 Herstatt risk, also known as principal risk, is a type of settlement risk where one side of a transaction pays out its currency but does not receive the currency bought in exchange. European Central Bank, *Financial Stability Review*, December 2004.

32 Because updates to tokenised deposits on the unifying ledger will not occur at the same time as updates to tokenised reserves on the applicable jurisdictional ledgers, it is not possible to rely on the coordination of the timing of the updates to the shared ledgers to establish a single point of settlement finality for all legs of a payment in the platform, in the same manner that would be possible if all settlements occurred on a single ledger. Rather, it is expected that the issuance of the atomic settlement trigger itself will be specified as having an agreed-upon legal significance that determines the timing of settlement finality. The atomic settlement trigger has been determined as the appropriate point for this purpose because it is the single technological event that will cause all required updates to all relevant shared ledgers to occur, even though those updates may not occur simultaneously.

having the effect in each participating jurisdiction that the relevant payment is protected for insolvency law purposes.

Project Agorá's model for addressing settlement finality is as follows:

- A trigger on the unifying ledger would determine subsequent events that would occur on both the unifying ledger and jurisdictional ledgers, in particular, updating of relevant tokenised reserves and tokenised deposits. Before the trigger on the unifying ledger could be issued, all relevant amounts for the payment would be locked and delegated, and, as a result, could not be used until the payment was completed.
- The applicable rules in a rulebook(s) would specify for each jurisdiction that the atomic settlement trigger is the point at which the payment instruction becomes irrevocable, the point at which the payment is finally settled and related obligations discharged, or has some other significance. The determination of which legal consequence occurs in which jurisdiction would be determined based on when, under the relevant jurisdiction's laws, finality of settlement would be protected in an insolvency proceeding involving a participant in the payment.
- If a participating jurisdiction recognises that insolvency law protections apply when a payment instruction becomes irrevocable, including under the rules of a designated or authorised system, the participating jurisdiction could determine that this event is also the point at which obligations arising from the payment instruction are discharged. This event could, in such case, be the point at which relevant updates are made to the applicable jurisdictional ledger. However, the technical design of the platform and applicable rules would ensure that, if a payment instruction becomes irrevocable, the payment will necessarily become final, whether at the same time or at a later time. It would not be possible for a payment instruction to become irrevocable without the obligations arising from the payment instruction ultimately being discharged. This approach further ensures that the protections afforded under applicable insolvency laws apply, as such laws are not subject to modification or override by contractual arrangements. In addition, this model also enables extensibility to additional jurisdictions that may consider using the platform in future, as additional jurisdictions could determine whether the atomic settlement trigger is the point at which the relevant payment instructions become irrevocable or the point at which the payment is finally settled and related obligations discharged, depending on which event triggers the application of insolvency law protections.

This approach entails additional considerations that merit further analysis:

- The atomic settlement trigger causes events on both the unifying and jurisdictional ledger(s) necessary to complete a payment, and actions on the unifying ledger determine steps that must occur on the jurisdictional ledger(s) as a consequence of the platform's technical design.
- This approach to settlement finality could give rise to accounting or risk management considerations and would therefore warrant further consideration and refinement in the jurisdictional layer's implementation phases.

It should be noted that an operating model for the platform and its legal characterisation in each participating jurisdiction were out of scope for the Project Agorá prototype.

Compliance and data protection

Regulatory compliance

The use of shared ledger technology to record and update balances of central bank reserves or commercial bank deposits imposes additional obligations for participating institutions. In particular, applicable regulatory frameworks governing record-keeping, operational resilience, outsourcing and information security introduce further compliance requirements.

The platform design supports management of information in a manner that enables participants to update their records and maintain traceability of these changes as evidence of compliance. However, participants may need to consider incorporating certain requirements into their internal record-keeping and compliance procedures. Key considerations include:

- Commercial bank participants should be able to ensure that records maintained in the platform (such as tokenised deposit balances) can be reconciled with, supplemented by or integrated into records they maintain in other systems (including any applicable non-shared ledger-based record-keeping systems) in order to meet domestic record-keeping obligations.
- Commercial bank participants are expected to be able to demonstrate to applicable regulators that their platform-related activities, including payment processing, maintenance of reserve and deposit balances, and interaction and integration with the platform, are operationally resilient and that reasonable measures have been taken to ensure that operations can continue safely and reliably in the event of a disruption.
- In all participating jurisdictions there are requirements for participants and payment system operators to implement controls to address, among other things, continuity of critical services, integrity and availability of systems, effective incident management and recovery from operational failures.
- It will be incumbent upon platform participants to take measures to ensure that participants and account holders, as well as their means of access to the platform, are appropriately protected from the risks of unauthorised access, hacking, degradation, loss, cyber attack, theft, fraud, negligence and other serious operational malfunctions. The platform rulebook(s) or other binding documentation should be developed and could be used to support commercial bank participants in satisfying these and other applicable operational resilience obligations.
- In all participating jurisdictions, a commercial bank does not transfer responsibility to comply with applicable regulatory requirements by outsourcing an activity to a third party. Commercial bank participants remain responsible for compliance with applicable law and supervisory expectations, even to the extent they outsource payment processing, technology infrastructure or operational support to a platform operator or other third party. As a result, outsourcing arrangements, including any that may be put in place in relation to the use of the platform, will need to include contractual provisions regarding rights of the outsourcing commercial bank in respect of audits, inspections and access to information, as well as provisions addressing business continuity and exit or transition arrangements.
- The participating jurisdictions differ in how they assess which functions may be outsourced. In some participating jurisdictions, outsourcing of functions regarded as "essential" to

licensed banking activities may be prohibited, while in others such functions may be outsourced subject to enhanced governance and supervisory controls. A review should be conducted as to whether the function being outsourced constitutes an essential function. In several jurisdictions, participation in a payment or settlement system, particularly if it facilitates payment processing, maintenance of deposit accounts or related record-keeping, is likely to be treated as a significant or material outsourcing activity with, correspondingly, enhanced supervisory expectations.

- Although outsourcing arrangements may allocate risks or costs between the outsourcing institution and its service provider through indemnities or similar provisions, such arrangements do not affect each institution's accountability to its regulators. In practice, it will be important that the platform rulebook(s) and related agreements clearly allocate platform roles and responsibilities and provide participants with audit, inspection and related rights as necessary to comply with domestic outsourcing and supervisory requirements.

Financial crime prevention compliance

The Project Agorá platform enables a confirmation of payee (CoP) functionality coordinated through the unifying ledger. The debtor's agent, after completing its own screening of a payment, submits a CoP request through the platform to the creditor's agent, requesting confirmation that the specified creditor and associated account exist at the creditor's agent. The creditor's agent reviews the request and responds with either a positive "match" or negative "no match" confirmation. If the response is no match, the payment is terminated and does not proceed. The outcome of the CoP request is recorded on the unifying ledger as a cryptographic proof or hash indicating whether or not the CoP request was successful. No underlying debtor, creditor or account information is written to the unifying ledger in connection with the processes for making or completing a CoP request. A successful CoP outcome triggers the creation of the applicable payment coordinator contract and therefore enables the payment to proceed to subsequent stages.

After a payment path has been identified for a payment on the platform, the platform coordinates the completion of compliance checks by the commercial bank participants in the proposed payment. Participants are requested to issue flags for three different types of compliance checks: sanctions screening; AML/CFT, KYC and fraud control checks; and "other checks".[33] Each participant performs its own sanctions, AML/CFT, KYC and fraud controls, and any other institution-specific checks. The platform does not specify what information commercial bank participants must include as inputs for these checks. Accordingly, participants have discretion to determine what inputs they require to perform their compliance checks. Upon a participant's completion of its compliance checks for a payment, each participant submits coded attestations for each check to the payment coordinator contract reflecting the outcome of its review. These attestations use standardised binary outcome flags (ie Flag 0 = Fail, indicating a failed check, or Flag 1 = Pass, indicating a passed check). Receipt of any Flag 0 = Fail results in termination of the payment. An initiated payment may proceed only once Flag 1 = Pass attestations have been received from each participant involved in the payment. In the design chosen for the Project Agorá prototype platform,

[33] The Project Agorá Business Workstream broadly defined these categories of checks: AML/CFT checks are those to prevent illicit activities; fraud screening identifies and prevents unauthorised or suspicious transactions; sanctions screening ensures adherence to international and jurisdictional regulations; and "other checks" include reporting obligations and jurisdiction-specific checks (eg capital flow management regulations in Korea). The input into these checks is not strictly defined, and entities have the discretion to determine which inputs would meet the criteria.

commercial banks involved in a payment conduct their compliance checks in parallel with one another, rather than sequentially as typically done today, and the transfer of value only occurs after each participating commercial bank in a particular transaction has attested that they have no compliance issues with the payment. As a result, further consideration regarding the application of sanctions compliance obligations for current payment processes, such as freezing funds, may be necessary in future.

The platform itself does not conduct compliance checks and records only the attestations provided by participants. However, each transaction participant will be able to see the other transaction participants' three individual check outcomes (on sanctions; AML/CFT, KYC and fraud controls; and "other"), within the pre-defined privacy group.[34]

Confirmation of payee

This process touches on several areas of applicable law and regulatory policy regarding information-sharing. In this regard, users may want to consider both the regulatory frameworks applicable to these processes and additional matters that may influence the risk treatment applied by participants to this process. Across all participating jurisdictions, it should be possible, as a matter of local law, to implement the CoP model as contemplated for the platform. However, to do so, it would probably be necessary in several participating jurisdictions for commercial bank participants to obtain express customer consent before disclosing to another participant whether a particular customer and its associated account do or do not exist at that institution.

The need for express customer consent, in such cases, arises because several jurisdictions maintain bank secrecy or similar confidentiality regimes that restrict the disclosure of customer-identifying information absent customer consent or a specifically permitted legal basis.

Contractual confidentiality obligations in customer account agreements, in addition to bank secrecy and confidentiality regimes, may also restrict participants from disclosing information relating to the existence of a customer relationship or account, including in connection with disclosures made to other financial institutions in connection with payment processing. To the extent a participant has agreed to contractual provisions of this sort with customers, they would need to be reviewed to assess whether they permit the disclosures contemplated by the platform's CoP functionality or whether amendments or customer consents would be required. The requirement to obtain these consents, to the extent necessary, could be addressed through the platform's rulebook(s) or other binding documentation and could require updates to existing customer account agreements.

Generating and sharing compliance outcomes with the platform and transaction participants via the use of flag notices (Flag 1 = Pass and Flag 0 = Fail)

Project Agorá has concluded that:

- In several participating jurisdictions, constraints arise under bank secrecy, confidentiality or data protection frameworks to the extent that the outcome of a compliance check could, in context, be linked to a particular customer or account. Some participating jurisdictions apply confidentiality frameworks that extend to corporate customers and may restrict the disclosure of client-related information absent customer consent or a specific legal basis.

[34] In the Project Agorá prototype, a "privacy group" includes only some or all participants involved in the relevant payment.

In those participating jurisdictions, the sharing of outcome flags – even where no underlying data are disclosed – could trigger confidentiality obligations if the result can be combined with other information available to the recipient to identify the customer or account holder. However, restrictions under these obligations would not apply if the applicable customer provides consent to information-sharing, as contemplated for these compliance checks.

- Participants may be prohibited from "tipping-off," ie disclosing information that would reveal the existence of, or intent to file, a Suspicious Activity Report (SAR) or a Suspicious Transaction Report (STR). Reporting compliance checks in the manner implemented in the platform may not constitute tipping-off or a violation of SAR/STR confidentiality if appropriately calibrated. The factors supporting this view are: (i) the reporting of "fail" occurs before a participant conducts an investigation to determine if the payment is in fact reportable; (ii) a participant may consider institution-specific criteria in conducting checks, potentially making it difficult for third parties to draw conclusions about whether an SAR/STR will (or will not) be filed from a mere indication of "fail"; and (iii) the responses are provided without any contextual information. The Project Agorá prototype platform's design may provide certain safeguards to ensure that the proposed manner of reporting compliance checks will not rise to the level of tipping-off or compromise SAR/STR confidentiality, in participating jurisdictions where this may be a concern.
- Nonetheless, it cannot be concluded that sharing the outcomes of compliance checks in the manner implemented on the platform would not give rise to tipping-off concerns. Some participants consider that reporting a "fail" outcome – particularly in relation to AML/CFT, KYC and fraud controls – could indicate that an SAR or STR is being considered or filed. Accordingly, each participant would need to assess its own level of comfort with the platform's functionality for reporting coded compliance outcomes, taking into account their own risk tolerance and legal analysis. Documentation may also need to incorporate measures aimed at mitigating these risks.
- The reporting of compliance checks in the manner contemplated by the platform represents a novel approach and may require confirmation from relevant regulators that it satisfies applicable regulatory requirements within the relevant jurisdictions.
- The platform rulebook(s) or other binding documentation could reinforce confidentiality requirements, including with respect to tipping-off risks, by requiring participants, as a condition of participation, to: (i) ensure that the outcome flags they share, especially ones related to the failure of a required check, are not implemented in a way that indicates or could reasonably indicate that an SAR/STR will or may be filed; and (ii) obtain and maintain any customer consents necessary to permit the sharing of compliance outcomes in accordance with applicable local law.

Data privacy and confidentiality

The prototype contemplates direct and indirect participation in the platform by central banks, commercial banks and certain non-bank financial institutions and corporates, and does not contemplate any participation by, or processing of transactions for, natural persons. Therefore, in principle data protection frameworks should not apply to transactions on the platform. However, certain transactions may give rise to personal data being processed. In such exceptional instances, additional safeguards exist within the prototype's privacy architecture.

The platform's privacy architecture limits the visibility of protected or confidential data such as account identifiers, payment amounts and transaction metadata to the participants to which it is directly relevant, such as due to their involvement in a particular payment. Additionally, instead of protected or confidential data being recorded on the platform's shared ledgers, the unifying and jurisdictional ledgers record only non-reversible cryptographic proofs and signatures that may be used by participants that already have, separate from the platform, the underlying data to validate that the data recorded on one or more of the platform's shared ledgers correspond to those underlying data. These mechanisms ensure that protected or confidential data are shared only with the parties to which they are directly relevant and who have agreed to participate in the privacy group relevant to the transaction.

However, the following considerations are worthy of note:

- Participants will need to assess whether any data exchanged within payment-specific privacy groups or otherwise through the platform could contain information relating to an identifiable natural person. To the extent that personal data are included in payment-related messaging or otherwise exchanged across jurisdictions, the nature of such data-sharing does not appear materially different from the information exchanged today in connection with cross-border payments through traditional correspondent arrangements or other payment systems.
- While cryptographic proofs and tokenisation enhance security, they do not necessarily achieve full anonymisation under legal standards, in which case the platform and its participants may be subject to privacy obligations in respect of those data in some participating jurisdictions.
- The platform's rulebook(s) should include an obligation requiring participants to ensure that any cross-border transfer of information complies with applicable banking and data protection regulations.

Data localisation and cross-border transfers

No participating jurisdiction has adopted a legal or regulatory regime that categorically requires data relating to bank accounts, balances or payments to be stored exclusively within the jurisdiction. Instead, data localisation considerations arise primarily through supervisory or regulatory frameworks governing outsourcing, operational resilience, information security and regulatory access. These frameworks generally focus on whether regulated institutions retain effective control over data that are subject to specific controller and processing requirements, whether they ensure its availability for supervisory and resolution purposes and whether they maintain appropriate safeguards for its protection.

In certain participating jurisdictions, transfers of personal data outside the home jurisdiction require either an adequacy determination for the data-importing country, the implementation of recognised safeguards, such as standard contractual clauses or binding corporate rules, or reliance on other narrow legal bases, such as explicit consent or contractual necessity. Where an adequacy determination or the existence of other express requirements cannot be confirmed, data exporters may also be expected to put in place supplementary safeguards as necessary in order to ensure compliance with the legal requirements of the exporting jurisdiction. These frameworks may become relevant if the platform's design results in personal data being transmitted, accessed or

made available across borders, which could be the case with respect to certain customer or account holder information (for example, if the name of an employee of a corporate customer is included in data relating to that corporate customer's account or in payment remittance information).

The project has found that data localisation requirements vary across the participating jurisdictions:

- **European Union**: The General Data Protection Regulation (GDPR) does not impose data localisation but regulates cross-border transfers of personal data. The distributed storage of transaction records across nodes located in different jurisdictions may raise data governance challenges. French policy discussions around critical payment data highlight potential scrutiny of where data are stored or accessed.
- **Japan**: There is no general statutory data localisation requirement mandating that banks store or host data within Japan. However, cross-border transfers of personal information to third parties located in foreign jurisdictions are subject to additional requirements under applicable law, such as ensuring an adequate level of protection or obtaining informed consent.
- **Korea**: Financial institutions are prohibited from storing personal credit information and unique identification data overseas, and outsourcing arrangements must comply with localisation rules.
- **Mexico**: Mexican commercial banks are generally permitted to store and process information in their own infrastructure located in Mexican territory or abroad, while Mexico does regulate cross-border transfers of personal data. However, Mexican commercial banks are required to keep certain internal data, transactional log and accounting records in Mexico at all times to ensure continuity of operations, access and safekeeping, and regulatory access.
- **Switzerland**: Swiss banks must ensure that the Swiss Financial Market Supervisory Authority (FINMA) and their auditor can inspect data transferred under an outsourcing agreement. Additionally, access to such data must always be possible from Switzerland. This may be satisfied by creating a backup of the relevant information in Switzerland (which is regularly updated). If data on the platform were considered critical, it would be subject to FINMA's additional risk management requirements.
- **United Kingdom**: Regulation does not impose data localisation requirements but instead governs cross-border transfers of personal data, in which case general data protection regulations may apply.
- **United States**: No general localisation requirements exist, but US banks are subject to ongoing supervision by applicable federal and, if applicable, state supervisory agencies in respect of how data are handled, including related controls, governance and safeguards.

Further, across participating jurisdictions, participating banks remain subject to general safety-and-soundness and operational risk expectations that require institutions to maintain information systems, governance arrangements and internal controls that are appropriate to the nature, scale and risk profile of their activities, including with respect to the security, integrity and availability of customer and transaction data.

The platform's design does not require that a participant's protected or confidential customer or payment data be hosted outside its home jurisdiction, and each participating bank

may implement the Project Agorá suite and maintain its private data views in a manner that should enable participants to satisfy applicable local requirements.

Conclusions

The legal analysis undertaken across the participating jurisdictions has determined that the Project Agorá platform, in its current design, does not create direct conflicts with existing legal and regulatory frameworks. Tokenised reserves and tokenised deposits can be characterised as equivalent to central bank reserves and commercial bank deposits, for which balances are recorded using "traditional" (non-shared ledger-based) technologies. Tokenisation does not alter the legal nature of the underlying account relationship. As a result, the platform could, in principle, operate within technology-neutral legal frameworks that already govern the underlying accounts.

There are limited areas (for example, with respect to tipping-off risks in certain participating jurisdictions) where additional caution may be warranted when it comes to designing the implementation steps for the platform. However, it seems likely that concerns in these areas can be mitigated. Given the novelty of the protoype, certain safeguards incorporated in its design may need confirmation from regulatory authorities that they are appropriate and sufficient.

The analysis in relation to record-keeping, operational resilience, outsourcing oversight, deposit insurance applicability, customer confidentiality rules and settlement finality may warrant further elaboration in the individual participating jurisdictions. The contractual documentation governing platform participation and conduct on the platform would also need to be developed.

Chapter 6: The benefits and limitations of the Project Agorá prototype

The Project Agorá prototype illustrates how shared ledgers, interoperable tokens, programmable workflows, atomic settlement and privacy-preserving execution would allow the prototype to address many of the pain points associated with wholesale cross-border payments (Table 3). By combining the path discovery mechanism and the necessary pre-transaction confirmations – including beneficiary validation and compliance checks – the prototype brings forward the alignment of payment-related information so that those processes occur prior to the commitment of liquidity and settlement of funds. This enables atomic settlement and potentially reduces failed payments and the costly need to unwind transactions. While some steps necessarily retain sequential logic, the platform's shared coordination enables multi-hop execution and reconciliation with minimal delay and potentially greater predictability than today's systems.

How the prototype addresses identified pain points **Table 3**

Pain point	Description	How the prototype addresses the pain point
Speed	The time it takes for a payment to be processed and settled between the debtor and the creditor.	The prototype decouples information coordination between parties from movement of funds, reducing delays linked to sequential processing. Settlement occurs in seconds once funds or liquidity are locked.
Efficiency	Factors contributing to payment systems' overall effectiveness and smooth functioning to achieve straight through processing.	The prototype allows the implementation of certain controls (eg sanctions, AML/CFT) to occur in parallel, reducing serial/sequential processing and minimising late-stage failure risks after liquidity is committed. The prototype is designed to operate around the clock, which would mitigate delays arising from misaligned operating hours in today's jurisdictional payment systems.
Transparency	Visibility into the end-to-end transaction (ie, at payment initiation, in-flight, and when the ultimate beneficiary is credited) and relevant payment details and data (eg fees, cross-currency amount).	All parties involved in a transaction have access to the current payment status, while maintaining privacy from other parties. Payment status visibility can be extended to debtors and creditors in future.
Risk reduction	The strategies and measures to mitigate risks (eg settlement, operational, counterparty risk) in cross-border payments.	The prototype enables atomic settlement, ensuring that either all balance updates occur or none at all, eliminating credit risk and reducing settlement risk. The prototype shifts cross-border payment execution to a coordinated process, aligning key elements before settlement and lowering operational risk arising from disconnected processes.

Source: Project Agorá.

The prototype also seeks to address the lack of accuracy and consistency in payment data, a major source of errors and exceptions today. It leverages global standards that harmonise data in

payments, such as legal entity identifiers (LEIs) and ISO 20022 CBPR+, and implements best practices, such as CoP.

In addition, the platform's pathfinding feature enables intermediaries to make decisions based on shared information without revealing confidential bilateral relationships or private logic, allowing participants to understand the viability and progress of a payment in real time. The platform's unifying ledger approach also significantly lowers reconciliation burdens, as participating institutions view and interact with tokenised balances rather than maintaining duplicate ledgers across multiple systems. Altogether, these features provide a coordinated, programmable and privacy-preserving settlement environment that directly targets root causes of inefficiency, opacity and operational friction in today's global correspondent banking networks.

While the primary focus of the prototype is wholesale cross-border settlement, the architecture also demonstrates a broader capability: a structured model for the issuance, holding and inter-institution account management of tokenised reserves and tokenised deposits. These capabilities are treated as enabling foundations for the payment use cases explored in the report, but they highlight how programmable, privacy-preserving ledgers can support both settlement and the life cycle management of tokenised reserves and tokenised deposits.

Qualitative assessment of effectiveness of the prototype

To further assess the degree to which the prototype could mitigate specific wholesale cross-border payments pain points, a mapping exercise was conducted. This exercise ensured a structured and transparent link between the business frictions observed today and the process and architectural choices embodied in the prototype. It combined a structural and qualitative assessment to link the prioritised pain points to the prototype design.

Each pain point was first aligned with the relevant steps in the E2E payment process implemented in the prototype (Table 4), clarifying where frictions arise in today's flows and which elements of the revised process are intended to mitigate them. By anchoring pain points to concrete process steps – such as CoP, path discovery, validation, liquidity locking, and atomic settlement – the analysis established a clear connection between observed frictions and the mechanisms introduced by the prototype.

A red-amber-green (RAG) framework was then applied to provide an initial qualitative view of how effectively the prototype, as currently implemented, is expected to mitigate each prioritised pain point (Table 4). A "green" rating indicates material mitigation, for example through atomic settlement eliminating settlement risk or continuous platform availability improving predictability. "Amber" reflects partial mitigation, typically where benefits depend on participant behaviour, external system availability, or future enhancements, such as broader use of shared compliance outcomes or liquidity saving mechanisms. No "red" outcomes were identified for the prioritised pain points at this stage.

Prototype assessment					Table 4
	Step 1 Confirm payee	Step 2 Path discovery (optional)	Step 3 Validation	Step 4 Locking	Step 5 Settlement
1. Predictability/availability (operating hours)	●	●	●	●	●
2. Sanctions/compliance screening, including hit ratio	●		●		
3. Sequential/serial processing	●	●	●		●
4. Accuracy (data quality)	●	●	●		●
5. Transparency (payment status, fees)[35]	●	●	●		
6. Liquidity visibility and treasury allocation for non-operating hours				●	
7. Settlement risk				●	●
8. Reconciliation breaks	●		●		●
9. Client outreach	●	●	●		

Amber: addressed partially/moderately; green: effectively addressed.

Source: Project Agorá.

Overall, the mapping of pain points to the prototype confirms that the core design intent – improving coordination, transparency and certainty without altering institutional roles – is largely reflected in the tested solution. At the same time, benefits will only be quantifiable when applied to more realistic conditions. This assessment provides a concrete basis for interpreting the prototype results, refining expectations and informing potential future areas of work.

Illustrating the Project Agorá prototype through real-life scenarios

The prototype's functionality is best illustrated through a set of concrete payment journeys that show how a Project Agorá-like platform could reshape wholesale cross-border payment execution in practice. Examining real-world cross-border scenarios step by step makes visible how early information alignment, shared validation and coordinated execution change the dynamics of payment processing. These examples show how participants interact with the platform, how frictions are addressed in real time, and how outcomes differ from today's approaches.

Illustrative payment journey 1

Priority payment of services from Mexico to the US (Figure 17)

The personas

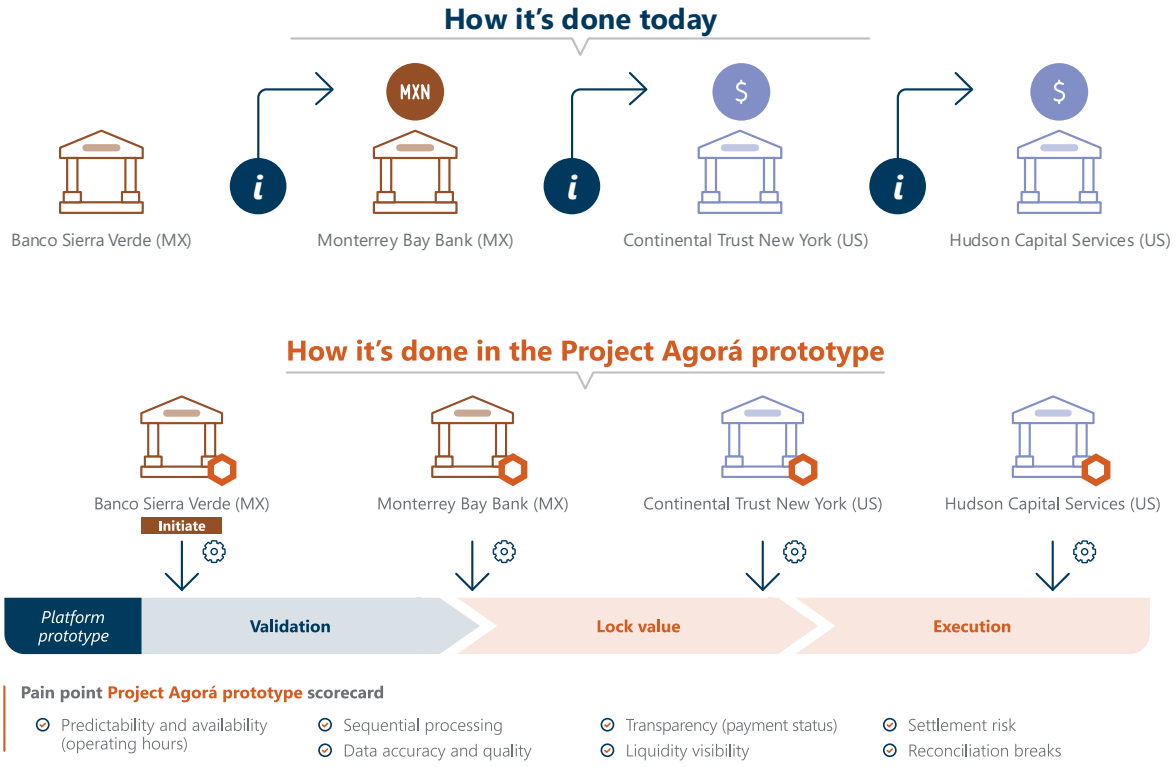
Banco Sierra Verde (BSV) is a small Mexican bank relying on Hudson Capital Services (HCS), a US financial institution, for the fraud monitoring engine that protects its e-commerce clients. Monterrey Bay Bank (MBB) acts as BSV's domestic correspondent, handling FX conversion, while Continental Trust New York (CTNY) maintains the USD nostro account used to credit HCS.

[35] Transparency of fees and costs are mitigated indirectly rather than fully resolved within the current scope of the prototype.

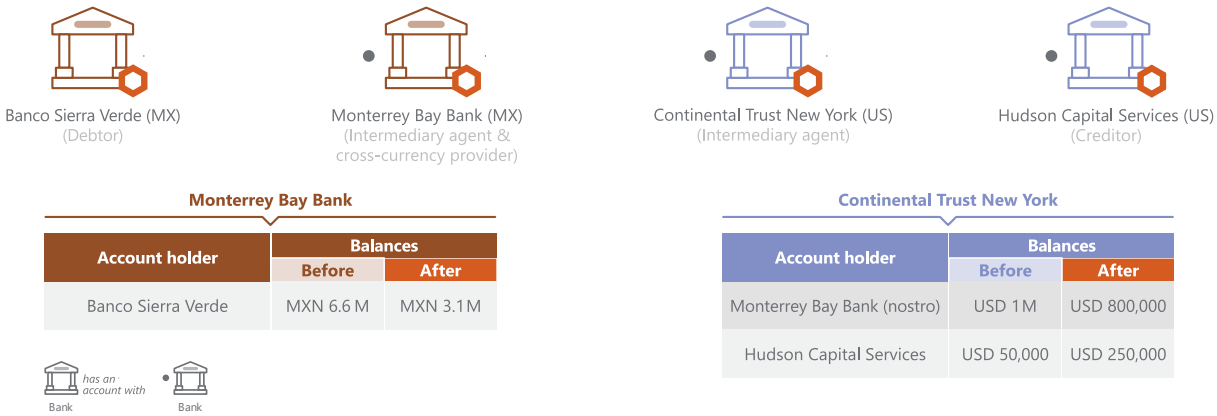
Journey 1 – Urgent payment due from Mexican bank to US firm

Figure 17

A. Today versus the Project Agorá prototype



B. Balance sheet updates involved in the atomic settlement



Monterrey Bay Bank

Account holder	Balances	
	Before	After
Banco Sierra Verde	MXN 6.6 M	MXN 3.1 M

Continental Trust New York

Account holder	Balances	
	Before	After
Monterrey Bay Bank (nostro)	USD 1 M	USD 800,000
Hudson Capital Services	USD 50,000	USD 250,000

Source: Project Agorá.

The conundrum

BSV must urgently settle an overdue USD 200,000 invoice owed to HCS. Because the invoice remains unpaid, HCS has suspended its fraud monitoring service, leaving BSV unable to process weekend e-commerce transactions during its busiest period. To restore operations on traditional rails, BSV

must route the payment through MBB for MXN–USD conversion and onward to CTNY to debit MBB's nostro and credit HCS. Despite the urgency, the transaction must still pass through a sequential chain of checks and intermediaries – an approach that is particularly challenging when timing is critical and operating hours are constrained.

Transaction flow today

Even in a simple, known-party transaction like this, the payment must move sequentially: BSV instructs MBB, MBB completes the MXN–USD conversion, and only then can CTNY process the USD leg to HCS. Each step depends on the previous one being completed within operating hours, making weekend execution uncertain and creating the possibility that earlier steps must be unwound if a downstream institution cannot process in time.

Transaction flow in the Project Agorá prototype

Since this is a transaction involving only financial institutions and the path is already known, the Project Agorá platform does not need to confirm the payee or discover a path. Instead of progressing step by step across separate systems, both legs of the payment are prepared in parallel on the unifying ledger, with each institution locking the required MXN-TD and USD-TD amounts up front. The flow therefore converges into a single coordinated payment instruction, reducing the number of sequential actions and removing the need to unwind earlier steps if a later participant cannot process in time.

Illustrative payment journey 2

Same-day international company payment (Figure 18)

The personas

HelvetiCure AG, a major Swiss pharmaceutical company headquartered in Basel, manages an extensive supply chain spanning numerous manufacturing partners across East Asia. Its primary banking partner is AlpenBank Zürich (ABZ). Under normal circumstances, the company's Korean subsidiary, HelvetiCure Korea Ltd, handles all local supplier payments through the group's account at Daehan Commercial Bank (DCB) in Seoul. One of its suppliers is BioSynK Co, a small Korean firm that also banks with DCB.

Unbeknownst to ABZ, the German institution Europa Bank Frankfurt (EBF) maintains correspondent banking relationships with Edelweiss Bank (EB) in Switzerland and HanMin Global Bank (HMGB) in Korea. These relationships enable a viable cross-border payment corridor from Switzerland to Korea using EUR as a vehicle currency, even though this path is not visible to ABZ through traditional channels.

The conundrum

On Tuesday morning, a time-critical shipment of temperature-sensitive enzyme essential for vaccine production arrives from BioSynK Co. The supplier requires same-day settlement in KRW before releasing the batch for export.

When HelvetiCure Korea Ltd attempts to process the payment locally, it encounters a liquidity bottleneck: the subsidiary's KRW account at DCB is temporarily unfunded due to a delayed

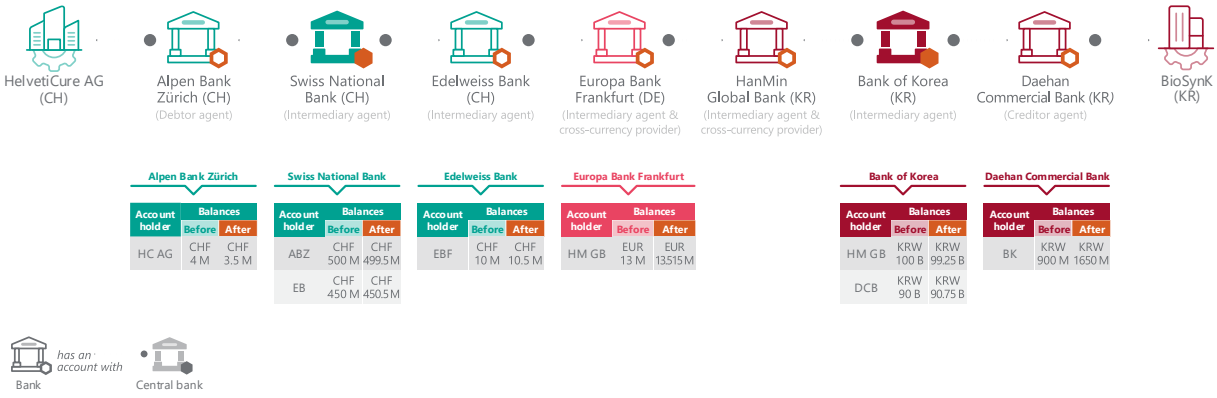
intra-group FX conversion from the previous business day. The treasury team in Basel is unable to move KRW into Korea quickly enough through normal channels, and the standard correspondent route has already passed its cutoff. With production at risk, the headquarters in Switzerland decides to initiate the KRW payment directly from Basel – despite having no established KRW corridor through traditional correspondent-banking partners.

Journey 2 – Critical payment from Swiss to Korean company

Figure 18

A. Today versus the Project Agorá prototype

B. Balance sheet updates involved in the atomic settlement



Source: Project Agorá.

Transaction flow today

Today, resolving an urgent cross-border payment relies on a slow, manual, relationship-driven process. HelvetiCure AG and its bank, ABZ, would need to make a series of bilateral phone calls to identify a correspondent chain capable of handling liquidity, FX conversion and settlement before cut-off. Each intermediary in the chain must then contact its own partners to confirm reachability, available liquidity and whether priority processing can even be arranged.

Priority handling often comes with extra fees and may require temporary, ad hoc agreements if no existing bilateral setup is in place. Because traditional correspondent networks typically offer limited end-to-end transparency, neither the corporate nor its bank would usually see the full settlement path, the intermediaries involved or real-time status updates. The entire process is slow, uncertain and operationally fragile – dependent on manual coordination, time zones and goodwill across multiple institutions.

Transaction flow in the Project Agorá prototype

HelvetiCure AG submits a payment instruction to its primary bank, ABZ, to credit BioSynK Co. ABZ, requests DCB to confirm the details of the beneficiary, triggering the CoP. This process anticipates potential unnecessary errors downstream due to inaccuracy of data. As ABZ does not have visibility into a viable end-to-end payment path, it submits only a partial instruction to the Project Agorá platform to credit BioSynK Co. and relies on the platform's PDM to determine a complete and executable settlement path – eliminating the need for manual coordination, negotiation or the urgency fees typically associated with traditional correspondent banking processes.

Since ABZ has no direct KRW corridor, PDM evaluates alternative settlement options that would normally be unknown or inaccessible to ABZ. The mechanism identifies a feasible path using EUR as a vehicle currency, leveraging existing correspondent links between EB/EBF and EBF/HMGB. The payment can be fully settled in tokenised reserves in both Switzerland and Korea.

Illustrative payment journey 3

Balancing liquidity across borders (Figure 19)

The personas

Crown Bank London (CBL) is a correspondent bank for North Harbor Bank (NHB) and Sakura Trust Bank (STB). Both institutions maintain GBP accounts with CBL in London and JPY accounts with CBL's branch in Japan.

Journey 3 – Liquidity balancing of UK and Japan correspondent accounts

Figure 19

A. Today versus the Project Agorá prototype

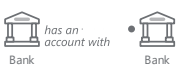
B. Balance sheet updates involved in the atomic settlement

Crown Bank London (UK)

Account holder	Balances	
	Before	After
North Harbor Bank (UK)	GBP 15 M	GBP 10.5 M
Sakura Trust Bank (UK)	GBP 1 M	GBP 5.5 M

Crown Bank London (JP)

Account holder	Balances	
	Before	After
Sakura Trust Bank (JP)	JPY 5,000 M	JPY 4,000 M
North Harbor Bank (JP)	JPY 500 M	JPY 1,500 M



Source: Project Agorá.

The conundrum

On a particular day at 09:15 London time, North Harbor Bank (NHB) contacts Crown Bank London (CBL) with an urgent request to increase its JPY balance at CBL's Japan branch. NHB must meet a

same-day margin call in Tokyo before the local payment system cut-off and proposes to fund the JPY position using surplus GBP held in its London correspondent account.

Almost simultaneously, in Tokyo late afternoon, Sakura Trust Bank (STB) contacts CBL's Japan branch requesting immediate additional GBP liquidity in London to cover a sterling funding shortfall ahead of end-of-day liquidity reporting. STB confirms that it is prepared to reduce its JPY balance in Japan to obtain the required GBP.

Both requests are time-critical. NHB faces a hard settlement deadline in Japan within hours, while STB must secure GBP liquidity before London market funding conditions tighten and internal treasury limits are breached.

Transaction flow today

CBL immediately convenes its London treasury desk and Tokyo operations team to review balances, cut off times, and the residual FX exposure. With the Japanese payment window closing, CBL decides to promptly settle the offsetting liquidity need via internal ledger transfers between the London and Japan books.

Transaction flow in the Project Agorá prototype

CBL matches the offsetting requests from NHB and STB and prepares a PvP instruction for execution in the Project Agorá platform prototype, resulting in the atomic settlement across the relevant correspondent accounts. The platform allows for an around-the-clock liquidity balancing of correspondent accounts, enabling CBL to rebalance GBP and JPY positions continuously on behalf of its correspondents, without depending on overlapping operating hours or traditional market windows. By leveraging the platform's programmability, banks could further encode rules, triggers, and matching logic directly into the workflow, materially reducing manual coordination and supporting more effective and flexible liquidity management for correspondent banking operations.

Limitations of the Project Agorá prototype

While the Project Agorá prototype demonstrates the feasibility of privacy-preserving, coordinated, programmable, multi-ledger settlement and that it could meaningfully improve wholesale cross-border payments, it was developed with an intentionally narrow scope. Key functions, including architectural design and workflow behaviour, were prioritised, while others were intentionally deprioritised.

The prototype does not evaluate production-grade requirements such as cyber security posture, operational resilience, throughput or latency characteristics, liquidity optimisation, failover mechanisms, or real-time monitoring capabilities. Interoperability with external infrastructures – such as domestic RTGS systems and core banking systems – was not tested, though the architectural model is designed to accommodate, if desired, such interoperability extensions. These areas were intentionally deprioritised in order to focus on core technical concepts and workflow models necessary for prototype delivery. The prototype was not tested using transactions originating from real-world production applications or live institutional systems. As a result, user behaviour, operational frictions and integration challenges that typically emerge in live environments could

not be fully observed. Testing with real application flows may therefore identify additional requirements, constraints or opportunities.

In addition, the project also aimed to deliver a prototype that met project objectives while considering legal constraints, making design choices in a legally aware manner. Project participants made design choices to adhere to those parameters while balancing the needs and aspirations of both the public and private sectors. As a result, the prototype does not fully mitigate some pain points. For example, while the prototype meaningfully improves transparency, data quality and settlement certainty among participating institutions, pain points such as client outreach, investigations or transparency of fees and costs are mitigated rather than fully resolved within the current scope.

While no legal barriers were identified that would preclude implementation of the platform in any participating jurisdiction, the legal analysis raises a series of policy, operational and contractual questions tied to future implementation and future potential evolution of wholesale cross-border shared ledger settlement infrastructures. These include the allocation of responsibilities between participants and potential service providers, the policy implementation of the settlement finality treatment across jurisdictions, including the determination of system rules, among others. Differences in legal effects across participating jurisdictions in the settlement finality approach could create operational risks in the enforcement of system rules or complicate the application of these rules in a consistent manner. Addressing these questions will be essential to enable any future deployment of a production-grade platform but were beyond the scope of Project Agorá.

Chapter 7: Key outcomes and areas for future exploration

Project Agorá successfully developed a prototype for a DLT-based system for cross-border payment settlement that meets policy, business, legal and regulatory requirements. The prototype design, validated through user testing, achieves its primary objective by demonstrating that a shared ledger can address many of the pain points in cross-border payments. More broadly, Project Agorá has delivered additional outcomes demonstrating the viability of key legal and operational foundations required for the future development of tokenisation-related initiatives. These key outcomes include:

- **Tokenisation using blockchain technology can significantly enhance cross-border payment workflows.** The prototype shows how processes that are traditionally fragmented can be integrated, enabling the coordinated crediting and debiting of multiple accounts. The project achieved this in a complex, multi-institution, multi-jurisdictional payment setting. While many projects exploring tokenisation have focused on either the issuance and settlement of assets exclusively, or the synchronisation of data, the project's focus on using tokenisation for both improved workflows and atomic settlement yields important lessons for future innovation.
- **Large-scale public-private collaboration is essential to unlock new potential.** In building a shared platform, the key to long-term viability is to build for diversity in business model and regulatory context. The breadth of participation ensured that the prototype accommodates diverse technical, legal and business requirements. As a result, the likelihood of broader adoption – a key element of a successful payment infrastructure – increases.
- **A shared ledger can preserve jurisdictional autonomy and flexibility.** The Project Agorá prototype's two-layer design allows central banks to retain control over their reserves while ensuring sufficient commonality that enables atomic settlement and integration with payment workflows between tokenised reserves and tokenised deposits on a shared platform. The jurisdictional layer is also designed to enable domestic transactions via each central bank, meeting central banks' policy goals and business needs.
- **Tokenisation does not fundamentally alter the legal nature of money.** Legal analysis in Project Agorá confirmed that tokenisation does not alter the legal characterisation of the underlying balances or the nature of the obligations represented by tokenised reserves and tokenised deposits. This clarifies that the development of tokenisation projects may proceed within existing legal and regulatory frameworks.
- **A shared ledger does not require shared data.** In Project Agorá, participants' data coexist but are not necessarily disclosed to other participants on the shared ledger. Privacy controls in Project Agorá allow data sharing when necessary and approved by participants, according to a range of preferences, but not as a default. The project demonstrated that data can be stored and transferred among the approved parties through a shared ledger platform of the type implemented in the prototype. In this way, Project Agorá demonstrates that data can be stored, transferred and shared, if needed, through a shared ledger platform subject to jurisdictional requirements and to meet data privacy objectives.
- **Interoperability of tokenised deposits is key to future use cases.** Settlement in tokenised central bank reserves is one way to enable deposits to operate seamlessly, supporting broader applications. Through a settlement mechanism, Project Agorá creates

a foundation to unlock the cash leg for even broader financial transactions, such as cross-border capital markets transactions.

Areas for future exploration

The development of the Project Agorá prototype has also highlighted areas for future exploration. Some issues emerged during the design and testing of the prototype, while others were identified at the outset of the project but intentionally kept out of scope. These areas include non-functional enhancements required to "harden" the prototype for potential production use; functional enhancements that could unlock additional capabilities; and further analysis of relevant legal and regulatory considerations.

Non-functional enhancements to explore

Key areas for further development include strengthening the platform's technical robustness, expanding functionality and deepening integration with existing financial infrastructures:

- **Cybersecurity assurance**: Formal threat modelling, penetration testing, secure configuration hardening, cybersecurity posture, key management and security operations design.
- **Operational and cyber resilience**: High-availability design, failover and recovery mechanisms, cyber incident response and operational monitoring.
- **Performance and scalability**: Benchmarking throughput/latency, stress testing under concurrent load and optimisation of indexing and event processing.
- **Interoperability with external infrastructures**: Deeper integration testing with domestic RTGS systems, FX platforms, netting utilities or treasury systems.
- **Privacy enhancements**: Evaluation and potential integration of additional privacy techniques (eg ZKPs or MPC) where appropriate.

Functional enhancements to explore

Certain wholesale cross-border payments pain points identified in the broader analysis – such as post-transaction monitoring and advanced compliance tooling – were intentionally left out of scope for the prototype, even where the potential benefits are clear. Similarly, liquidity saving mechanisms and full integration with traditional systems were not prioritised.

Looking ahead, further enhancements could strengthen the business case and value proposition of a Project Agorá-type platform. Examples include:

- **Enhanced information-sharing and coordination**: Expanding the ability to share information and activity for AML/CFT, sanctions and anti-fraud controls. The prototype adheres to current industry practice, whereby each participant is solely responsible for meeting its legal and regulatory obligations. It may be worth exploring the potential efficiency gains from different types of coordinated approaches within a shared platform.

- **Liquidity management solutions**: Addressing potential liquidity demands arising from gross settlement, particularly as volumes scale. This could include the development of a liquidity savings mechanism for tokenised reserves, drawing on concepts from RTGS systems (such as offsetting) adapted to atomic settlement environments on DLTs.
- **Interoperability and compatibility standards**: Advancing collaboration on standards both within and across platforms is key. Project Agorá's focus on the "cash leg" of cross-border payments is seen as strategically important. Technically, a Project Agorá-type solution could support a range of use cases beyond wholesale cross-border payments, including tokenised assets. Given the role of network effects in payment systems, a clear approach to intra-platform compatibility and external interoperability will therefore be critical.
- **Enhanced token management**: Enabling the issuance and management of tokenised deposits on multiple ledgers (jurisdictional and unifying ledgers).
- **Workflow extensions**: Richer liquidity management tooling, batching/netting and expanded PvP/DvP scenarios.

Additional analysis of legal and regulatory issues

Further analysis of legal and regulatory issues would support both functional and non-functional enhancements. This work could include assessing the application of domestic data protection and localisation regimes where payment data involve identifiable individuals; designing mechanisms that enable compliance checks without creating risks of unauthorised disclosure; exploring the conditions under which participants may rely on other participants' compliance outcomes, subject to legal and regulatory constraints; and examining how the platform's architecture aligns with supervisory expectations on operational resilience and cross-border outsourcing.

The legal analysis undertaken for the prototype also highlights the importance of more detailed and comprehensive work on governance, rules and oversight to be reflected in rulebook(s) as part of further exploration. Early identification of key themes at this stage provides a foundation for continued public-private collaboration. Key rulebook elements to be analysed include:

- **Participation and eligibility**: Criteria and onboarding requirements, including distinctions across participant categories (eg central banks, commercial banks and payment initiation service providers), and differences in national definitions of eligible institutions.
- **Legal nature of relationships and assets**: Confirmation that existing relationships between participants and their customers remain unchanged; clarification that tokenised reserves and deposits represent account balances and do not create independent legal rights.
- **Requirements for tokenised reserves and tokenised deposits**: Minimum requirements for issuance, redemption of tokenised reserves and tokenised deposits on the shared ledgers to ensure atomic settlement in the cross-border payment workflow.
- **Ongoing participation requirements**: Compliance with AML/CFT, sanctions and other financial crime obligations, including appropriate provisions in customer agreements.
- **Scope of permitted activities**: Clear delineation of which participants may initiate, validate or execute payments, and under what conditions.

- **Permitted assets and transaction types**: Definition of acceptable tokenised instruments and payment formats.
- **Settlement finality and legal effect**: Common treatment of key processing steps, including recognition of the unifying ledger trigger as the point of settlement finality and the application of insolvency protections; alignment with jurisdiction-specific rules on irrevocability and discharge of obligations.
- **Accounting and risk management**: Standardised approaches to recording transactions and managing risks, to the extent feasible within jurisdictional constraints.
- **Exception handling**: Procedures for errors, reversals and other exceptional events.
- **Liability and compliance standards**: Provisions covering representations, indemnities and limitations of liability.
- **Governance and operations**: Allocation of responsibilities among participants and any platform operator(s).
- **Data governance**: Requirements to ensure data are processed only for specified, legitimate purposes and in line with applicable consent and minimisation principles.
- **Reporting and record-keeping**: Standards to ensure accurate, reliable and retrievable records, consistent with financial market infrastructure principles.
- **Legal framework**: Governing law, dispute resolution mechanisms and forum selection for platform-related matters.

Project participants, including central banks, have expressed strong and sustained interest in further exploring the potential benefits of the prototype. Future work is expected to involve an enhanced role for the private sector, supported by continued and active engagement from participating central banks.

Glossary

Account holder: Holder of tokenised reserves or tokenised deposits.

Project Agorá suite: The participant-operated software components – including the user interface, connectivity and integration layer, middleware, indexing services and ledger access tools – that institutions deploy to interact with the Project Agorá platform.

Atomic settlement: A settlement model in which all relevant payment legs across the affected unifying and jurisdictional ledgers execute as a single coordinated outcome governed by the payment coordinator: commit (settle) or cancel (abort). This prevents partial movement of funds across currencies and jurisdictions. In this report, atomicity is used in the workflow sense (coordinator-governed commit-or-cancel across legs), not as a statement about legal settlement finality or synchronous multi-ledger transactions.

Account: An account in Project Agorá has the same definition as one in the traditional banking system, ie a (digital) representation of an end user's set of claims against the issuer.

Balance: The amount of money tokens in an account at a given time.

Bridge: A mechanism used to transfer assets or messages between distinct ledger networks, often introducing additional trust assumptions (eg custodial or validator-based bridging). The Project Agorá prototype does not rely on a standalone cross-ledger bridge; cross-ledger coordination is achieved through workflow contracts, deterministic events, and participant-operated middleware submitting transactions to each ledger.

Commit-or-cancel outcome: A settlement outcome model in which the payment coordinator determines a single final outcome for the workflow. Payment legs then execute that outcome consistently across ledgers: commit transfers (spend locks) or cancel and release locks (without moving value).

Commitment (private commitment): A cryptographic value recorded on the ledger that represents hidden token state or workflow outcomes (eg token outputs or endorsed workflow outcomes). The underlying data (amounts, recipients, decision details) are visible only to authorised parties who possess the associated private data.

Confirmation of payee (CoP): A privacy-preserving check performed by the creditor institution to verify beneficiary details before the payment workflow proceeds. The check is executed within the creditor's institutional systems; only the minimum endorsed outcome is shared as required for workflow progression.

Corridor registry: A reference registry that captures declared cross-currency corridors and settlement capabilities. It provides minimal public information to support discovery while leaving private pathfinding preferences and bilateral commercial relationships within institutional systems.

Creditor: The party to whom an amount of money is due. In the context of the payment model, the creditor is also the credit account owner and acts as a payee (*).

Creditor's agent: A financial institution servicing an account for the creditor (*).

Debtor: The party that owes an amount of money to the creditor. In the context of the payment model, the debtor is also the debit account owner and acts as a payor (*).

Debtor's agent: A financial institution servicing an account for the debtor (*).

Delegate (locking sub-step): The internal sub-step within the locking stage in which participants grant temporary, payment-scoped authority to payment leg contracts to act on locked balances for settlement. Delegation is narrowly scoped, time-bound and specific to a single payment instance.

Delegation (delegated lock authority): Temporary, scoped authority granted to a payment-leg contract to act on a specific lock for a specific payment. Delegation enables coordinated settlement execution while preserving participants' control over assets outside the delegated scope.

End-to-end (E2E) payment: In the context of Project Agorá, end-to-end payment consists of a transaction involving one debtor and one creditor, hence one payment with multiple legs.

EVM (Ethereum Virtual Machine): A runtime environment for executing smart contracts in an Ethereum-compatible manner.

Ephemeral EVM: A short-lived Ethereum Virtual Machine (EVM)-compatible execution environment used in workflow-level privacy coordination to execute private smart-contract logic off the shared ledgers. Each participant instantiates the environment locally for the workflow step, executes the logic, and the instance is discarded after use. Participants endorse outcomes using typed-data signatures; only minimal anchored outcomes (eg commitments/attestations) are recorded on the shared ledgers as required.

Hyperledger Besu: An open source, enterprise-grade Ethereum client used to run EVM-compatible permissioned networks.

Indexing service: A participant-operated service that subscribes to ledger events and participant-scoped coordination artefacts to provide fast retrieval, monitoring, and operational reconstruction of workflow activity.

Initiating party / Initiator: The party initiating the payment to an agent can be either the debtor (in a credit transfer) or the creditor (in a direct debit) (*).

Initiating party / Initiator service provider: The party initiating the payment to an agent. In the payment context, this party initiates the payment on the debtor's or creditor's behalf.

Intermediary agent: Agent (central banks or financial institutions) between the debtor's and the creditor's agents. There can be several intermediary agents specified for the execution of a payment (**).

ISO 20022: International standard published by the International Organization for Standardization (ISO) that defines a common methodology and repository for developing financial messaging schemas. Specific data models and message formats used across payment systems, securities settlement, and trade finance.

Issuer: Issues and redeems tokenised reserves or tokenised deposits, which constitute liabilities of the issuer when held by other participants.

Jurisdictional ledger: A shared ledger within the jurisdictional layer of Project Agorá. Each participating jurisdiction has its own jurisdictional ledger (one per jurisdiction/currency area), operated under that jurisdiction's governance (typically under the relevant central bank's authority). The jurisdictional ledger hosts tokenised reserves for that jurisdiction and applies jurisdiction-specific policies and controls (eg access rules, issuance/redemption constraints and domestic settlement logic) while supporting coordinated cross-border workflows through the platform's cross-ledger coordination model.

Lock (locking sub-step): The internal sub-step within the locking stage in which token balances are reserved for settlement. Locked balances cannot be spent outside the workflow and are associated with a specific payment instance and settlement instruction set.

Middleware: The institution-operated execution environment where sensitive logic – such as CoP checks, PDM pathfinding decisions, sanctions and fraud/AML/KYC checks, cross-currency calculations and readiness checks – is performed privately. Middleware also coordinates actions that result in on-main ledger workflow progression and indexes events and participant-scoped coordination artefacts for operational visibility.

Network registry: A reference registry that allows participants to publish identifiers, discovery endpoints and relevant contract addresses to enable cross-ledger discoverability without exposing private pathfinding relationships.

Noto (token privacy model): A token privacy model implementing an issuer-backed ("notary") token design that provides token-level privacy using cryptographic commitments. The ledger records commitments and spends; authorised parties (typically the holder and issuer, and optionally auditors) can interpret their own token state using private data and can validate the chain of spent states without requiring decryption of on-ledger data.

Paladin: A programmable privacy framework for EVM-compatible ledgers used in Project Agorá to provide modular privacy through domain plugins such as Noto (token privacy) and Pente (workflow privacy groups and ephemeral EVM execution).

Participant-scoped coordination: Private coordination among only those institutions required for a specific payment step. In the prototype, this includes bilateral private messaging (notably for PDM) and privacy group-scoped coordination where a shared private contract state is needed.

Party: Entity involved in a payment (*).

Path discovery mechanism (PDM): A distributed pathfinding mechanism that identifies a viable payment path through intermediaries while preserving confidentiality of pathfinding preferences and bilateral commercial relationships. In the prototype, PDM is performed via hop-by-hop 1:1 private messaging and institution-local pathfinding logic (not via multi-party privacy-group smart contracts).

Payment coordinator: The workflow smart contract that orchestrates the payment life cycle by enforcing sequencing rules, aggregating endorsed outcomes, applying timeouts and triggering locking and settlement stages. For readability, this report describes the life cycle in five stages (CoP, PDM, validation, locking and settlement), while the implementation may represent more finely grained internal sub-steps within certain stages.

Payment leg contract: A smart contract responsible for executing settlement operations for a specific currency leg on a single unifying or jurisdictional ledger. It acts on locked balances under narrowly scoped delegated authority and executes commit or cancel actions in accordance with the payment coordinator's final outcome.

Payment versus payment (PvP): In the context of Project Agorá, PvP consists of a transaction involving two debtors and two creditors, hence two payments paired for atomic settlement.

Pente (workflow privacy model): A workflow privacy model providing privacy group-scoped coordination and ephemeral EVM execution for private smart-contract logic. It enables participant subsets to coordinate against shared private contract states, while anchoring only minimal outcomes on the shared ledgers.

Privacy group (Pente privacy group): A scoped collaboration construct that defines membership and coordination rules for a subset of institutions. It is used to exchange endorsed outcomes and, where applicable, host private contract state using ephemeral EVM execution off the shared ledgers, with minimal anchored outcomes recorded on the shared ledgers.

Private message / participant-scoped message: An encrypted message exchanged through participant-scoped coordination mechanisms (eg bilateral private messaging or privacy-group messaging where used). These messages convey endorsed outcomes required for workflow progression while preserving confidentiality.

Private data views: Enable participants to access and store a participant-specific view of sensitive data to which that participant has access. Through these views, a participant may view private subsets of data relating to the data recorded on the platform's shared ledgers, preserving verifiability and consistency of those data, but without providing other participants access to sensitive data to which they should not have access. This component enables participants to link the non-reversible cryptographic proofs and signatures recorded on the unifying ledger and jurisdictional ledgers to the underlying payment data held by a participant but is in no event recorded on the platform's shared ledgers.

Proof of authority (PoA): A permissioned governance model in which validator nodes are operated by pre-authorised institutions. Validator trust derives from institutional accountability and governance rather than open participation or token-based incentives.

Prototype: An experimental implementation used to demonstrate feasibility and validate core architectural mechanisms and workflow behaviour in a controlled setting. It is not designed to meet all operational, security, resilience, governance or assurance requirements expected of live financial market infrastructures.

Participating jurisdictions: May include one or more countries, but in all cases correspond to a currency area. The jurisdictions currently in scope for the platform are the Eurosystem, Japan, Korea, Mexico, Switzerland, the United Kingdom and the United States.

Quorum Byzantine Fault Tolerance (QBFT): The consensus protocol used by the unifying or jurisdictional ledgers to provide deterministic technical settlement of the ledger state. It supports predictable ordering of workflow state transitions and settlement-related actions under a permissioned validator model.

Ready (validation sub-step): The internal sub-step within the validation stage in which each participant confirms it is operationally and technically prepared to proceed to locking and settlement (eg liquidity availability, tolerance checks, internal authorisation). If any required participant returns "not ready" or times out, the workflow terminates before locking begins.

Reconcile / reconciliation: Operational processes used to match records across systems after the fact (eg comparing internal ledgers, messages, and settlement records). The Project Agorá workflow aims to reduce the need for post facto reconciliation by enforcing deterministic workflow sequencing and anchoring endorsed outcomes and settlement events on the ledgers, while institutions retain their own internal accounting and reporting processes.

Reference smart contract: A smart contract that provides shared registry or configuration data used by other contracts and participant systems (eg network registry, token registry, corridor registry, reserve account registry).

Reserve account registry (per jurisdictional ledger): A jurisdictional reference registry operated by the central bank that discloses limited information about reserve account holders in that

jurisdiction (eg participant identifiers indicating which institutions are reachable via that jurisdictional ledger).

Shared ledgers: Refers collectively to the Project Agorá ledger and the jurisdictional ledger(s) operated by permissioned participants and used as the common record of authoritative on-ledger workflow state and token movements needed to coordinate and execute settlement. This is in contrast to off-ledger components (eg participant middleware, bilateral/private messaging and privacy-scoped execution environments) where sensitive processing and data exchange occur and are not recorded on the shared ledgers beyond minimal anchored outcomes.

Signature bundle: A set of signatures collected from all required payment participants to authorise final settlement execution. In the prototype, participants produce signatures within participant-scoped coordination, and the payment coordinator uses the resulting bundle to authorise settlement actions across the relevant payment legs.

Token registry: A reference registry containing metadata for tokenised assets supported on the platform, including issuer identity, contract address and attributes needed for consistent interpretation across participants.

Tokenised deposits: Representations of commercial bank deposits implemented as tokenised records under an issuer-backed model. In the prototype deployment, tokenised deposits are primarily issued on the unifying ledger, though the architecture can support alternative allocations.

Tokenised reserves: Representations of central bank reserves issued on the jurisdictional ledger corresponding to each currency under central bank control and jurisdiction-specific policy constraints.

Unifying ledger: A shared ledger within the unifying layer of Project Agorá. The unifying layer consists of a single unifying ledger that acts as the common coordination surface for multi-jurisdiction workflows. It hosts cross-institution workflow coordination logic (including the payment coordinator and related reference contracts) and, in the prototype deployment, tokenised deposits. The unifying ledger enables participants to coordinate sequencing, locking/delegation and settlement across jurisdictions without centralising domestic settlement control, which remains on the relevant jurisdictional ledger(s).

Validate (validation sub-step): The internal sub-step within the validation stage in which institutions perform sanctions screening, fraud/AML/KYC and other policy validations within their own systems and return endorsed summary outcomes required for workflow progression.

Validation (stage): A life cycle stage that ensures participating institutions have completed required checks and are ready to proceed before locking and settlement. In the prototype, validation comprises internal sub-steps: validate, amounts (where applicable), and ready.

Vehicle currency scenario: A cross-currency path where multiple conversions occur sequentially (eg A→B→C), with each conversion step endorsed and used to produce the next amount in the chain.

(*) Terms defined in ISO 20022 MDR

(**) Terms adapted from ISO 20022 MDR