# Faster Payments QIAT

Proposer: **Ripple**

February 21, 2017

## TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Original Proposal</td>
<td>2</td>
</tr>
<tr>
<td>Q&amp;A Response</td>
<td>67</td>
</tr>
<tr>
<td>Draft QIAT Assessment</td>
<td>85</td>
</tr>
<tr>
<td>(Includes proposer comment in Appendix A &amp; B)</td>
<td>99</td>
</tr>
<tr>
<td>Task Force comments</td>
<td>112</td>
</tr>
<tr>
<td>Proposer response to Task Force comments</td>
<td>121</td>
</tr>
<tr>
<td>Final QIAT Assessment</td>
<td>132</td>
</tr>
</tbody>
</table>
Faster Payments Task Force Proposal

Ripple
Real-Time Cross-Border Payment Service

April 29, 2016

Submitted by:
Ryan Zagone
Director of Regulatory Relations, Ripple
zagone@ripple.com
BACKGROUND

Strategy 2 of the Federal Reserve’s Strategies for Improving the U.S. Payment System paper is to “Identify effective approach(es) for implementing a safe, ubiquitous, faster payments capability in the United States”. The Faster Payments Task Force was created to support this strategy and has designed the Faster Payments Effectiveness Criteria (Effectiveness Criteria) and process for assessing alternative faster payments proposals. The Effectiveness Criteria is consistent with Strategy 2, as well as the broader set of “desired outcomes” set out in the Strategies Paper. These desired outcomes include:

**Speed:** A ubiquitous, safe, faster electronic solution(s) for making a broad variety of business and personal payments, supported by a flexible and cost-effective means for payment clearing and settlement groups to settle their positions rapidly and with finality.

**Security:** U.S. payment system security that remains very strong, with public confidence that remains high, and protections and incident response that keeps pace with the rapidly evolving and expanding threat environment.

**Efficiency:** Greater proportion of payments originated and received electronically to reduce the average end-to-end (societal) costs of payment transactions and enable innovative payment services that deliver improved value to consumers and businesses.

**International:** Better choices for U.S. consumers and businesses to send and receive convenient, cost-effective and timely cross-border payments.

**Collaboration:** Needed payment system improvements are *collectively* identified and embraced by a broad array of payment participants, with material progress in implementing them.

All proposals submitted through the Task Force’s assessment process will be assessed against the Effectiveness Criteria to determine how well solutions can achieve the desired outcomes associated with improving the U.S. payments system.

---

1 “Proposal” is defined in the *Glossary of Terms* as, “The written document that provides a detailed description of a faster payments solution, and demonstrates how it meets the Effectiveness Criteria for a faster payments solution”.

© 2016 Federal Reserve Banks. Materials are not to be used without consent.
**Purpose of the Template and Instructions for Use**

This proposal template has been developed to assist proposers in detailing their proposal for a full end-to-end faster payments solution. The template is designed to increase the consistency of information provided by proposers, as well as to provide the breadth and depth of information needed for the Qualified Independent Assessment Team (QIAT) to understand and assess a proposal against the Effectiveness Criteria. Proposers submitting proposals for assessment by the QIAT should use this template and complete all parts and sub-sections as described in the instructions.

This template includes three parts. Part A requires proposers to describe and illustrate (via a flow chart) what the solution does at each stage of the end-to-end payments process (from initiation of the payment through to the reconciliation of the payment). This description should be provided for the solution overall, as well as for each use case that is supported by the solution. Proposers will also be required to complete a table indicating which parts of the criteria each use case addresses (for example, the solution may enable contextual data capability for business-to-business payments, but not for person-to-person payments). Part B requires proposers to describe business considerations for the solution. These business considerations include: a detailed timeline to achieve initial implementation and then to achieve ubiquity; the intended value proposition of the solution and how it supports competition; and integration considerations. The detail in Part B will help the QIAT understand the feasibility of the solution and will help support its assessment against the Effectiveness Criteria. Part C requires proposers to provide a self-assessment and justification of how the solution meets each of the criteria outlined in the Effectiveness Criteria.

Proposers should refer to the Effectiveness Criteria when completing all parts of the proposal template.

---

2 A full end-to-end faster payments solution (or “Solution”) is defined in the Glossary of Terms as, “The collection of components and supporting parties that enable the end-to-end payment process. A faster payments solution might include new components, the adaptation of existing components, and/or a combination of the two.

- Components include any of the following:
  - Rules, standards/protocols, and procedures
  - Physical or technical infrastructure, networks, systems and other resources needed by all parties to use or enable the rules, standards/protocols and procedures
  - Centralized or shared services, if any
  - Legal framework and enforcement mechanisms

- Parties include any of the following:
  - Governing bodies, operators, depository institutions, non-bank account providers and third-party service providers”.

© 2016 Federal Reserve Banks. Materials are not to be used without consent.
Proposal Review Process

Once a proposal has been submitted, a qualitative assessment of the proposal against the Effectiveness Criteria will be conducted by the QIAT. During the assessment process, the proposer will have the opportunity to provide additional information and/or a response to the assessment. The proposer may also choose to withdraw its proposal at any point in during this initial assessment meaning that the proposal will not be shared with the Faster Payments or Secure Payments Task Forces. No confidential or proprietary information should be shared in a proposal. Any information shared in a proposal that is not subsequently withdrawn will be provided to the Faster Payments Task Force, and ultimately published in the Final Report.

Following the completion of the QIAT’s assessment and the compilation of any responses received from the proposer, the assessment will be provided to the Faster Payments Task Force for review. The proposal will be reviewed in its entirety, including the assessment and the proposer response, and Task Force members may offer comments to the proposer and the QIAT. Similarly, the Secure Payments Task Force will review the proposal and provide comments on the security-related aspects to the proposer and the QIAT. The proposer may respond to Task Force comments and may revise its proposal for final QIAT review. The proposer may also choose to withdraw its proposal at this point meaning that the proposal will not be published as part of the final report.

The QIAT will finalize its assessment of the revised proposal with consideration given to comments by both Task Forces. Once the assessment has been finalized, the proposal, QIAT final assessment, and Task Force comments will be published in a final report along with corresponding material for all other solution proposals that underwent and completed the proposal review process.

Instructions for Submission and Proposal Review Process Timeline

Proposals should be provided in Word or PDF format, submitted on 8½ x 11 inch paper with 1 inch borders and Times New Roman font size 12. It is advised that proposers limit the total length of each proposal (including optional appendix) to a maximum of 200 pages. Proposers choosing to attach an optional appendix should ensure that it is highly organized with a table of contents and any reference to the appendix in the main body of the text should be clearly cross referenced. As noted above, the QIAT will have a dialogue with proposers and will request additional explanation if required. Proposals should be written to the primary audience of the QIAT, and the Faster Payments and Secure Payments Task Forces.

All inquiries regarding the proposal template and submission process should be directed to:
Instructions providing details on where proposals are to be submitted will be provided in a separate communication prior to the submission window opening on April 1.

The following table outlines the proposal assessment process and timeline. Key dates for proposers are indicated in bold type.

<table>
<thead>
<tr>
<th>Timeline and key dates</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Proposers to submit proposals</td>
<td>Proposal submission window open from 9am ET April 1, 2016 to 5pm ET April 15, 2016</td>
</tr>
<tr>
<td>2. Draft 1 of QIAT assessment and discovery period between QIAT and proposers</td>
<td>Conducted from April 15, 2016 to July 7, 2016</td>
</tr>
<tr>
<td>3. Proposers to provide written response to QIAT assessment or notification of decision to withdraw</td>
<td>Due no later than 5pm ET August 9, 2016</td>
</tr>
<tr>
<td>4. Task Force review of proposal assessments commentary period</td>
<td>Conducted from August 10, 2016 to October 4, 2016</td>
</tr>
<tr>
<td>5. Proposer to submit final revised proposal, and written response to Task Force comments or notification of decision to withdraw</td>
<td>End-October 2016</td>
</tr>
<tr>
<td>6. Final QIAT assessment provided to proposers</td>
<td>November 2016</td>
</tr>
<tr>
<td>7. QIAT report of all fully assessed proposals including Task Force commentary and proposer responses</td>
<td>November 29, 2016</td>
</tr>
</tbody>
</table>
Legal Considerations

All submissions are at the discretion of the proposer or proposers, and are subject to the terms outlined in the Faster Payment Task Force Proposal template and the terms of the Faster Payment Task Force Participation Agreement. Please limit your responses to matters reasonably necessary to the creation, development, and deployment of your proposed solution.

All Faster Payments Task Force Members who contribute to a proposal are considered to be proposers, and a proposal should identify all Task Force Members who have contributed. If a Secure Payments Task Force Member contributes to a proposal, that Secure Payments Task Force Member should sign a Faster Payments Task Force Agreement and be included as a proposer.

Proposers should identify the proprietary intellectual property contained in its proposal. This identification should include whether the proposer owns the intellectual property or whether the intellectual property has been licensed or will require licensing from another entity (in the event the proposer has licensed technology from another entity), the terms the proposer will license its intellectual property under and the terms of license(s) required from other entities. These terms could include FRAND, royalty bearing, or non-royalty bearing, by way of example. Such disclosures should be made under Part C, sub-section 5 “Legal Framework” (justification for L.5, Intellectual property criterion), which asks whether a proposal has undertaken or will undertake a due diligence review for the subject matter disclosed by a proposal, and an approach to resolve or manage any risks that arise from third-party intellectual property rights implicated by a proposal. In making these disclosures, proposers should identify any technology that is disclosed by its proposal, which the proposer has knowledge potentially infringes or misappropriates the intellectual property of any other entity or person, and the basis on which the proposer has this knowledge.

If a proposer does not currently have access to Federal Reserve System (FRS) services referenced in a proposal or the proposal relies upon new or the expansion of existing FRS services, the proposal must clearly acknowledge that the FRS has not in any way committed to provide the services to the proposer.

Proposers are reminded of their obligations to comply with applicable anti-trust laws in preparing their proposals. Proposers should not share confidential or proprietary information in a proposal. Any information shared in a proposal that is not subsequently withdrawn will be provided to the Faster Payments Task Force, and ultimately published in the Final Report. While
all information contained in a proposal is ultimately at the discretion of the proposer(s), if a proposer inadvertently includes confidential or proprietary information in a proposal, the proposer should immediately notify the QIAT.
EXECUTIVE SUMMARY

Ripple Overview

Ripple is a real-time interbank payment service. Ripple’s technology allows financial institutions (FIs) to directly transact with each other and settle transactions in real time, 24/7/365. While the technology can be used for both domestic and cross-border payments, this proposal focuses on Ripple’s ability to enable cross-border payments that meet emerging market demands and the effectiveness criteria.

Ripple’s solution consists of a software application that enables:
1. Bi-directional messaging and data transfer
2. Real-time settlement and
3. Liquidity management.

Ripple enables settlement of cross-border payment between the originating and beneficiary FIs in under one second. The full end-to-end payment process can be completed in under five seconds, plus the time of the FI’s internal compliance process.

Ripple synchronizes simultaneous transactions on the FIs’ books, instead of relaying payments sequentially as is done today. This process minimizes the settlement risk and reduces the cost of cross-border payments, enabling FIs to improve existing payment services and introduce new products that were not previously feasible.

Ripple provides payers and FIs the total cost of the payment prior to authorization, end-to-end traceability, and the ability to send low-value cross-border products that are not feasible with today’s infrastructure.

Ripple is designed to complement an FI’s payments business. Ripple’s solution can be integrated directly into an FI’s payment hub, or may be integrated into a 3rd party provider’s platform that FIs are already connected to. This flexible approach allows direct integration for banks with custom technology or a scalable integration for banks that rely on external or off-the-shelf services.
Regardless, the bank continues to own the customer relationship. The existing consumer protections, customer onboarding, due diligence, and transaction monitoring programs remain intact. Payments that a bank facilitates via Ripple are “pushed” to the beneficiary bank who delivers the funds to the payee.

Cross-Border Payments Today: A Fragmented Process

For cross-border payments, originating and beneficiary FIs are not currently able to directly connect and transact with each other. FIs rely on a chain of siloed intermediaries that relay payments across a diverse set of messaging and settlement protocols. This fragmented process results in delays, high processing costs, and opportunities for errors.

Banks send one-way payment messages through a global network provider yet must rely on a complex patchwork of correspondents and intermediaries for settlement. For instance, an originating FI and its correspondent connect via a central counterparty. A series of one-way messages are sent to initiate a transaction. The sending correspondent charges a processing fee and dictates an FX fee for the transaction, then passes the payment to the receiving correspondent. The receiving correspondent then charges a processing fee and connects to the beneficiary FI through a central counterparty. This process – which includes messaging fees and processing costs at each step in the chain – can take between two to four days given the institutions and currencies involved.
The reliance on intermediaries and the lack of coordination between their ledgers results in processing costs, lengthy settlement times, and the potential for error, given that the messaging and funds movement occur over separate channels. Further, the payment process is opaque, meaning the originating and beneficiary FIs do not have visibility into the status of the payment. They are unable to track where the payment is during the several days of transmission, and lack visibility into the fees, FX cost, and timing of delivery – limiting the ability to provide the customer with crucial information about the payment.

For broad, global reach, banks must fund and maintain accounts with many correspondents, locking up valuable capital. Alternatively, businesses must open accounts in all of the countries in which payment reach is needed, locking up capital and assuming FX risk. For non-core markets, banks and corporates are likely unwilling or unable to afford the capital costs of accessing such corridors. They go without payment access to these markets.

These structural inefficiencies have resulted in several key issues:

1. **Limited access** - The reliance on intermediaries limits banks’ access to liquidity, currencies, and other financial institutions.
2. **Lack of certainty** - The fragmented, opaque process as well as one-way messaging limits the ability to track and confirm payments.
3. **Delays** - Relying on a relay process through several intermediaries results in delayed settlement, up to two to four days for some corridors.
4. **High costs** - The liquidity and processing costs, operational inefficiencies and non-competitive FX market result in a total cost of $1.6T\(^3\) per year for all participants in the ecosystem – including payment originators, banks and liquidity providers.

The inefficiencies and high cost structure of today’s system makes cross-border payments only viable for high-value transactions. Low-value B2B and remittance payments – as well as high-volume payments – are increasingly in demand, yet not feasible within the existing infrastructure. These limitations create barriers to global growth and financial inclusion.

---

Ripple: A Closer Look

Ripple bridges today’s fragmented structure by enabling direct connectivity between the originating and beneficiary FIs. Ripple tightly integrates the messaging with funds movement and replaces the relay process with synchronized, atomic settlement. Additionally, Ripple can provide access to a competitive FX marketplace, supplementing a bank’s own liquidity and reliance on one provider as is the case today.

This design eliminates the risk of a failed payment occurring midway through the chain of intermediaries, and provides banks visibility into fees, payment status and timing of each payment.

Multiple liquidity sources can reduce FX spreads and provides efficient access to new corridors. Altogether, Ripple reduces the total risk, inefficiency and cost of cross-border payments.

Ripple’s Key Capabilities
Ripple’s key capabilities are designed to lower the risk and total cost of cross-border payments.

Bi-directional messaging
Ripple enables banks to directly connect and communicate with each other via bi-directional (two-way) messaging. Through a private, secure connection, banks easily share pre-transaction information including transaction fees, delivery time, and FX rate. Banks can deliver this
information to the consumer for review and approval, before confirming the payment. Such transparency is not easily possible with one-way messaging over today’s fragmented payment chain.

**Real-time settlement**
Payments initiated with Ripple settle in real-time (less than one second), 24/7/365. Ripple’s technology allows for settlement of funds to happen synchronously across not just the originating and beneficiary FIs. This synchronicity of settlement (what we refer to as an atomic settlement) ensures that either the funds are settled across the entire chain or the funds are immediately returned to the payer. There can never be a situation where one leg of the payment settles and the next leg fails.

This eliminates one-leg risk, or settlement risk between the originating bank, beneficiary bank, intermediaries and liquidity providers. As the messaging and settlement are closely integrated, banks can track the status of payments and receive confirmation of delivery once funds are deposited to the beneficiary’s account – features not possible today. With this functionality, FIs can provide much improved payment information to their customers.

**Liquidity management**
FX liquidity is a crucial part of a cross-border payment. Ripple provides the flexibility to use multiple liquidity models, as opposed to FX being dictated by the single correspondent as is done today.

Using Ripple, financial institutions that have their own trading desk or nostro relationships can continue to use their own liquidity to fund payments. However, banks can also access liquidity provided by trusted third parties, broadening payment reach without having to hold capital with an intermediary or in another country. This is particularly useful for smaller institutions with limited excess capital and for exotic corridors that may lack the payment volume to make it feasible for access today. When sourcing liquidity from the marketplace, Ripple selects the authorized provider with the lowest cost FX, incentivizing efficiency and competition.
Benefits

These key capabilities create several benefits over existing cross-border payment rails:

Access
Ripple provides banks direct access to other institutions, instead of relying on a disjointed chain of intermediaries for settlement. Support for multiple liquidity models, including a competitive marketplace of third-party FX providers, enables access to new corridors and sources of liquidity.

Certainty
Ripple’s technology tightly integrates payments messaging with funds settlement, allowing for unprecedented visibility into a transaction’s lifecycle. Bi-directional messaging enables banks to exchange customer information, fees and delivery times before executing the transaction. End-to-end transaction visibility and settlement confirmation provides banks certainty of their cross-border payments.

Speed
Ripple’s distributed technology enables direct bank-to-bank funds settlement in under one second, as opposed to two to four days with traditional models. This allows banks to improve existing payment services and develop new, differentiated products for consumers and businesses.

Cost
Ripple drives broad cost efficiencies for cross-border payments. Greater certainty and lower failure rates reduces risk and operational costs for the FIs. Faster settlement reduces the inflight capital costs for payers and payees. The competitive FX marketplace of third-party providers allows FIs, particularly small institutions, to access new and existing corridors without posting capital in those countries. Capital can be re-deployed, and payment reach can be achieved more efficiently. Lower total costs enable banks to feasibly provide low-value cross-border payment products for the first time.
USE CASE COVERAGE

Supported Use Case Coverage Summary

Ripple enables direct bank-to-bank settlement in over 60 countries, regardless of use case. The flexible messaging functionality, real-time tracking, and liquidity service empower banks to determine which type of use case they would like to enable between each other, depending on the demands of its customers.

By changing the architecture and cost structure of the payment, Ripple improves banks’ existing payment services and enables new use cases not feasible in today’s system. Banks can introduce highly differentiated products and services to their customers, meeting the demand for faster, low-cost, global payments.

Banks are integrating with Ripple to enable:

**Low-value Remittance Service for Retail Customers (P2P):** Ripple lowers the total cost of settlement, enabling banks to profitably offer low-value international payments to their retail customers for the first time. This service helps meet the rising demand for remittance payments and enables financial inclusion. An example video of such a service is available [here](#). Previously the price of cross-border payments (~$40 per transaction) made low-value payments prohibitively expensive.

**International Corporate Payments (B2B):** Banks can offer real-time, on-demand international payment services for their corporate customers, enhancing their corporate treasury solutions portfolio and allowing their corporate customers to achieve superior working capital management. The delays and uncertainty of today’s cross-border payments force corporates to open and fund accounts in countries around the world, so that cash is available overseas if an immediate payment is needed. With Ripple, corporates can initiate cross-border payments in real-time from their sole domestic bank account, allowing the corporate to repatriate its capital and deploy it in more efficient ways.

**International Transaction Banking Service:** Banks can serve as a provider of Ripple transactions to other institutions. With the ability to settle funds internationally in real-time,
banks can repackage and provide this service to other regional banks or non-bank financial institutions that have cross-border payment needs.

**Cross-Border Intra-Bank Currency Transfers:** Banks with branches in different countries must use intermediaries to move their own funds. They suffer the same delays and inefficiencies seen in cross-border payments. Banks can use Ripple to transfer their own funds between entities in different countries at a fraction of the time and cost, allowing the bank’s treasury to allocate capital more efficiently across international operations.

<table>
<thead>
<tr>
<th>Supported use case coverage summary</th>
<th>Use case</th>
<th>Supported (Y/N)</th>
<th>Cross-border (Y/N)</th>
<th>Examples of payments supported</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Business to Business (B2B)</td>
<td>Y</td>
<td>Y</td>
<td>A business pays a foreign supplier for components.</td>
</tr>
<tr>
<td></td>
<td>Business to Person (B2P)</td>
<td>Y</td>
<td>Y</td>
<td>An employer issues a paycheck to an employee; a company issues a credit to a customer.</td>
</tr>
<tr>
<td></td>
<td>Person to Business (P2B)</td>
<td>Y</td>
<td>Y</td>
<td>A customer pays tuition to a university abroad.</td>
</tr>
<tr>
<td></td>
<td>Person to Person (P2P)</td>
<td>Y</td>
<td>Y</td>
<td>Remittance payments, including low-value payments.</td>
</tr>
</tbody>
</table>
Cross-border Use Case Coverage (If Applicable)

For those use cases supporting cross-border, provide the jurisdictions and systems with which the solution interoperates in the table below.

<table>
<thead>
<tr>
<th>Cross-border use case coverage</th>
<th>Non-US Corridor(s) and Systems</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business to Business (B2B)</td>
<td>FIs can use Ripple to access over 60 currencies as of April 2016.</td>
<td></td>
</tr>
<tr>
<td>Business to Person (B2P)</td>
<td>See above.</td>
<td></td>
</tr>
<tr>
<td>Person to Business (P2B)</td>
<td>See above.</td>
<td></td>
</tr>
<tr>
<td>Person to Person (P2P)</td>
<td>See above.</td>
<td></td>
</tr>
</tbody>
</table>

Ripple is an inter-bank solution for cross-border payments. The FIs that use Ripple connect directly with FIs or networks in other countries, enabling real-time settlement between those institutions. Ripple enables indirect connectivity to other currencies as well. Details of reach and ubiquity are described in the Payment Lifecycle section below.

In addition to direct integration with FIs, Ripple is integrating into third-party payment hubs that FIs are already connected to. This approach gives the FIs access to Ripple via their existing connections. Ripple has announced several channel partners that enable access to over 60 currencies. Ripple’s public channel partnerships are available at Ripple.com.
Proposal Assumptions (Optional)

Proposers may choose to provide a list of assumptions used in the creation of their proposal. Assumptions should be limited to those that are unique to the proposal and cannot be adequately addressed elsewhere in the document. The QIAT will take into account any assumptions listed in making their assessment of the proposal.

For example, as noted in the “Practical and Conceptual Considerations” section of the Faster Payments Effectiveness Criteria, many of the criteria require the solution proposer to describe various elements of the payment system rules for the proposed solution. In a multi-operator environment, it is possible that a single entity will be given rule-making authority by multiple operators that desire a standardized ruleset. Solution proposers planning to pursue such an approach may list this rule-making authority as an assumption. However, it should be noted that for the purposes of meeting the Effectiveness Criteria related to “Legal Framework”, proposers should coordinate with either the designated rule maker or articulate preferences for rules when preparing their solution proposal, even though rules may not be finalized until later.

Distributed Financial Technology and Operational Resiliency

Today, financial systems are generally centralized, meaning there is one central counterparty that operates the system. The financial institutions taking part in the network connect to this central operator. The central operator is a single point of failure for the system. If it goes offline, no transactions can be made by any participant in the entire system.

Distributed financial technology was a breakthrough allowing systems to be created and transactions to be initiated without the need for a central operator. Instead, the participants on the network connect directly to each other, distributing the operations across themselves. There is no central operator or single point of failure.

In this way, a distributed architecture allows networks to maximize operational resiliency. One participant may go offline, but that does not affect the ability for other institutions to continue to transact.
This distributed design parallels the design of the Internet: connections across many participants without a central operator. One cannot “turn off” the Internet. While one participant or service provider may go offline, the connections between other users and providers remain active. By adopting distributed financial technology, payment systems can realize the same resiliency as the Internet.

Distributed financial technology can take many forms: blockchains, distributed ledgers, and open protocols. While blockchains have been the primary focus of attention over the past few years, this proposal leverages an open protocol called Interledger. Interledger connects and synchronizes transactions across FIs’ existing ledgers. Within this proposal, there is no blockchain or new ledger (i.e., distributed ledger). A detailed discussion of Interledger is presented in the Ripple Connect Deep Dive section below and Settlement description of the payment lifecycle.
PART A: DETAILED END-TO-END PAYMENTS FLOW DESCRIPTION

Part A is composed of three sub-sections:

- Section 1 focuses on the broad solution, looking across the eight stages of the payment lifecycle.
- Section 2 focuses on the details of the solution by describing the solution’s supported use cases across the eight stages of the payment lifecycle.
- Section 3 provides a summary table of whether the Effectiveness Criteria are addressed by each supported use case.

Part A, Section 1: Solution Description

Overview of the Solution’s Components

There are four major components of the real-time cross-border payment solution:

1. Financial Institution
2. Ripple Connect (software application)
3. FX Connector
4. Notary

1. The Financial Institution

The financial institution (FI) offers its customers payment products that are enabled by Ripple. An FI integrates Ripple into its ledger and creates an escrow account on its books. The escrow account will be explained in the Settlement Section below. All activity of a Ripple payment occurs on the books of the FIs involved in the transaction. There is no central or third party operator.

The FI continues to own the customer relationship and the front-end application (phone app, website, or branch network). In this way, the FI’s internal processes for onboarding, authentication, and transaction monitoring remain in place. The example below shows two FIs and the accounts of two customers: the sender and receiver of the payment.

2. Ripple Connect

Ripple Connect is the name of the plug-and-play software module that processes international payments for banks. FIs license Ripple Connect and integrate it into their payment hub or core
ledger. Ripple Connect enables the bi-directional messaging and real-time settlement. A deep dive on the functionality of Ripple Connect is presented below.

3. FX Connector

An FX Connector holds accounts with two or more FIs, providing liquidity for transactions between those institutions. FIs can be their own FX Connector, using nostro and vostro accounts that they may hold with each other. Alternatively, FIs can rely on third-party connectors, such as currency brokers or today’s existing correspondent banks. While a correspondent bank is not required to provide connectivity on Ripple, as is the case today, a correspondent bank may continue to provide FX liquidity as a connector.

Importantly, the connector is a customer of the FIs and is subject to each FI’s onboarding, due diligence and compliance processes. Typically an FI will establish a contract with the connector, stating the amount of funds (liquidity) the connector will hold in the account and the counterparties the FI is willing to transact with.

Once a connector has been onboarded by the banks, it will deposit local currency into its accounts (i.e., U.S. dollars in a U.S. bank and Euros in a European bank). The FX Connector will then use an API to broadcast its FX quote. The API is FIX-compatible, the standard quoting protocol for institutional FX traders. When a payment is initiated, Ripple Connect will use the APIs to determine the FX quote being offered by the FX Connector and deliver that FX quote to the originating FI.

The example below shows one FX Connector with both its U.S. Account and European Account. FIs may choose to have more than one FX Connector. In the event that two FIs have several common FX Connectors, Ripple will source liquidity from the FX Connector with the tightest spread, creating a competitive marketplace for liquidity.

4. Notary

A notary is an entity that confirms debits and credits have successfully occurred across multiple ledgers. The notary acts as a source of truth on the status and success of a payment. A notary is
established between the Ripple Connects at each FI. A notary is run by a software package that confirms cryptographic messages signaling the status of the payment issued by Ripple Connect.

The FIs will actively select a notary they mutually trust to confirm their transactions. Notaries can be run by FIs themselves, FIs not involved in the payment, or trusted third parties such as technology companies or outside vendors. The FIs have complete autonomy to select the notary they wish to use; FIs may select different notaries for each counterparty they are making payments with.

The image below shows the two FIs, their escrow accounts, and Ripple Connect installed at each institution, enabling connectivity.

**Deep Dive on Ripple Connect**

Ripple Connect is the software product FIs license to enable real-time cross-border payments. Ripple Connect has two primary functions: messaging and settlement.

1. **Messaging Functionality:** The messaging functionality within Ripple Connect allows FIs to share contextual payment data, fees, and confirmations of acceptance and delivery. The messaging function within Ripple Connect does not have a proprietary standard or format that must be used. The originating and beneficiary FIs determine the messaging standard their systems are designed to support and format the messages accordingly.
Ripple Connect simply extracts, transmits and delivers whatever payment data and format the originating and beneficiary FI wish to send. Ripple Connect does not translate or alter the data or format.

This design provides needed flexibility for payment systems that support multiple use cases and are cross-border in nature. The messaging functionality is extensible, allowing FIs to include additional contextual data about the payment. This enables support for various use cases. The flexible messaging functionality is suitable for a cross-border environment where there are many different standards being used. The design “future-proofs” Ripple Connect, allowing FIs to adopt new standards without having to update the software.

The messaging functionality was designed with cost effectiveness in mind. Unlike existing messaging services, Ripple Connect does not impose a fee per message. The ability for originating and beneficiary institutions to connect directly means messaging does not have to be passed through many intermediaries, eliminating the potential for error or misinterpretation. Such a design reduces the complexity and cost of resolving messaging errors.

2. **Settlement Functionality via the Interledger Protocol**: For real-time settlement, Ripple Connect makes use of an open source protocol called Interledger. Interledger is a standard that synchronizes the movement of value on ledgers. While messaging is used to share contextual data about a payment, Interledger assesses and affects settlement on the FIs’ ledgers. This process is explained in the settlement section below.

Interledger is a protocol, or standard, used to coordinate the transfer of value. Protocols are broadly used for interoperability. For instance, HTTP or SMTP are broadly used protocols that enable data to be transferred over the Internet. HTTP is a standard incorporated into many products (apps, web browsers, etc) to enable the movement of data.

Similarly, Ripple Connect is one commercial application that uses the Interledger Protocol to transfer value. Other products can make use of this standard to enable value transfer and interoperability between ledgers or systems. Within this proposal, Interledger is used to transfer currency, but it can be used to transfer any asset held on a ledger.
The name “Interledger” reflects the fact that it facilitates transactions across multiple existing ledgers. Interledger does not have its own ledger that FIs have to connect to and remain in sync with. All the activity occurs on the FI’s ledgers and is private to the ledgers involved in the transaction.

This design is different from traditional networks (both centralized and distributed), which have their own ledger that FIs connect to and must remain in sync with. Systems that have their own ledger face scalability limitations; the process used to update the ledger and keep the network participants in sync with the ledger limit capacity (i.e., transactions per second). Increasing scalability within these designs can be complex and burdensome.

Interledger is a technology that synchronizes transactions on FIs’ own books. FIs do not have to sync with an additional ledger, reducing complexity. To increase capacity, FIs simply add an additional server to process more transaction instructions. As shown with the growth of Internet traffic, scalability of protocols is easily achieved and potentially unlimited.


Security Within Ripple Connect: Ripple Connect is installed behind the FI’s firewall in its secure environment. Financial institutions’ internal systems will communicate to Ripple Connect over secure HTTPS connections using OAuth 2.0 for authentication. All traffic between Ripple Connect at the originating and beneficiary FI is encrypted and occurs over secure HTTPS as well.

Importantly, the information sent between the Ripple Connect is accessible only by the originating and beneficiary FI. The data is not accessible to Ripple (the company) in any way.

Interledger Overview: https://youtu.be/UdCxrqP6w3I
Ripple (the company) neither accesses nor stores this information. The information is private and accessible only to the originating and beneficiary FIs, who are responsible for retaining their own communication records.

As a technology vendor, Ripple (the company and our products) are held to the security and risk expectations established within the FFIEC’s Technology Service Provider guidance. The software is also subject to the FI's due diligence as part of their vendor management procedures. As enterprise software, Ripple’s products meet industry standards for security and encryption.

**Compliance Implications:** By licensing the Ripple Connect software to banks, Ripple is considered a technology service provider within the United States. Ripple is subject to the Bank Service Company Act and the FFIEC’s guidance on the “Supervision of Technology Service Providers.” Such designation means Ripple may be subject to examination by the primary regulators of its U.S. FI customers. Additionally, Ripple is subject to the FI’s vendor management requirements and IT change management program.
Ripple Connect Technical Requirements

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Red Hat Enterprise Linux (RHEL) 7.1 or 6.7</th>
</tr>
</thead>
<tbody>
<tr>
<td>SELinux</td>
<td>Ripple recommends that SELinux be set to: SELINUX=enforcing and SELINUXTYPE=targeted See Enabling and Disabling SELinux in the official Red Hat documentation for more information about enabling SELinux.</td>
</tr>
<tr>
<td>OS Dependencies</td>
<td>• pkgconfig</td>
</tr>
<tr>
<td></td>
<td>• ntp</td>
</tr>
<tr>
<td></td>
<td>• ntpdate</td>
</tr>
<tr>
<td></td>
<td>• openssl-devel</td>
</tr>
<tr>
<td></td>
<td>• openssl</td>
</tr>
<tr>
<td></td>
<td>• psmisc</td>
</tr>
<tr>
<td></td>
<td>• sysstat</td>
</tr>
<tr>
<td></td>
<td>• python</td>
</tr>
<tr>
<td></td>
<td>• expect</td>
</tr>
<tr>
<td>Architecture</td>
<td>x86 (64-bit)</td>
</tr>
<tr>
<td>RAM</td>
<td>4 GB</td>
</tr>
<tr>
<td>CPU</td>
<td>2 Cores</td>
</tr>
<tr>
<td>Storage</td>
<td>50 GB</td>
</tr>
<tr>
<td>Supported Database Connections</td>
<td>• PostgreSQL</td>
</tr>
<tr>
<td></td>
<td>• Microsoft® SQL Server® 2012</td>
</tr>
<tr>
<td>Deployment Options</td>
<td>RPM</td>
</tr>
<tr>
<td>RPM Dependencies</td>
<td>Node.js v0.12</td>
</tr>
</tbody>
</table>
PAYMENT LIFECYCLE

Once integrated with Ripple, the payment lifecycle occurs in seven steps:

1. Authentication
2. Initiation
3. Approval by Payer’s Provider
4. Clearing
5. Payer Authorization
6. Settlement
7. Receipt and Reconciliation

Step 0. Integration and Onboarding

First, FIs integrate Ripple Connect into their system. FIs can license Ripple Connect from Ripple or work with an authorized integration partner. Approved integration partners are available at Ripple.com. These partners can either assist the FI with a direct integration, or have integrated Ripple into their payment hubs which FIs may already be connected with.

Once Ripple Connect has been integrated, the FI will select and authorize the other FIs it wishes to conduct payments with. FIs will conduct due diligence on the counterparties it seeks to make payments with to ensure proper security, compliance and risk controls are in place at the institution. Based on its due diligence findings, the FI has the full autonomy to select only the counterparties it is comfortable or allowed to engage with. By authorizing other FIs, the institutions establish a trusted relationship for payments. Counterparties that an FI does not authorize are unable to message, send or receive payments.

Once integrated, the FI will offer a payment service within its user interface (phone app, website, etc.) that is powered by Ripple.

1. Authentication

Ripple is used by an FI to enable cross-border payments for its customers. The FI continues to own the customer relationship. The payment service enabled by Ripple is embedded in the FI’s existing delivery channels (mobile app, website, etc.). Customer onboarding, due diligence, and user authentication are completed by the FI per its existing processes for each delivery channel. Ripple does not alter these processes. The speed of authentication is dependent on the FIs internal processes.

The customer has a relationship and payment experience with the FI. The consumer or business does not engage directly with Ripple. The customer may not know the FI is using Ripple to
enable the payment service, just as they are not necessarily aware of the services FIs use to facilitate payments today. Given the relationship is between the customer and the FI, all existing consumer protection laws remain relevant and applicable.

2. Initiation
Payment initiation occurs directly between the customer and the FI, via the FI’s existing channels (app, website, etc). The FI will determine the payment and receiver information required to ensure compliance with its own procedures and its jurisdiction’s laws. The speed of initiation is dependent on the FIs internal processes.

The encryption and storage of this data is determined by the security features within the FI’s channels. Ripple Connect does not have access to this information.

The FI initiates push payments over Ripple on behalf of its customers. Pre-authorized and pull payments may be future capabilities. All features and benefits of Ripple remain intact regardless of the use case or channel that a customer uses to initiate a payment.

3. Approval by the Payer’s Provider
Upon receiving all necessary payment information, the FI will ensure the payer has sufficient funds to cover the payment. The payer is a customer of the originating FI, meaning the FI has direct visibility into the payer’s account balance to assure good funds are available. The originating FI will use Ripple Connect to determine the FX connector(s) that have sufficient liquidity (good funds) available for the payment. (See Clearing for more information.) This process takes milliseconds, depending on the speed of the FI’s internet connection. Altogether, the FI confirms good funds within the “very effective” timeframe of under two seconds.

The FI may require payments to be fully funded, or may opt to extend the customer credit to cover the payment. This is determined between the FI and the customer. As Ripple supports multiple use cases, the customer may be a retail consumer or a commercial/corporate customer. The appropriate consumer protection and/or payment regulations apply to the transaction, depending on the customer type.

4. Clearing
Once the FI has received the necessary information from the sender and confirmed good funds are available, the originating FI uses Ripple Connect to communicate with the beneficiary institution. The two FIs use Ripple Connect to share payment information and determine fees,
FX rates, and delivery times. As the clearing process occurs over HTTPS, the timing of clearing is dependent on each FI’s respective internet speed, typically within five seconds.

### Ripple Connect’s Clearing Process

The Ripple Connect portion of the clearing process occurs in two stages:

1. **Pre-transaction messaging**: Using the messaging function within Ripple Connect, the originating FI shares payment and customer information with the beneficiary FI. The beneficiary FI confirms that the beneficiary is an account holder in good standing and that it is willing to accept the payment. The beneficiary FI will share its fee and an estimated delivery time with the originating FI.

   As described in the Deep Dive of Ripple Connect, the information shared via messaging is encrypted and accessible only by the FIs. Ripple (the company) neither accesses nor stores this information.

2. **Identifying the FX Connector and FX fee**: Ripple Connect will then leverage the Interledger Protocol to (1) identify the FX connectors that have accounts and liquidity at both the originating and beneficiary FIs and (2) determine the FX quotes offered by those connectors. The FX connectors use APIs to communicate their FX fees. If the originating and beneficiary FIs have more than one common connector, Interledger is designed to source liquidity from the connector with the lowest FX quote.

   Ripple Connect delivers the beneficiary FI’s fee and the FX quote to the originating FI. The fees and FX quote are locked in for a time period determined by the FIs and the liquidity provider during the onboarding process.

### 5. Payer Authorization

Next, the originating FI compiles the cost information provided by Ripple Connect and delivers this to the payer for review and authorization. Ripple enables complete visibility into the fees and FX cost *before* the payer authorizes the transaction. This transparency provides the payer certainty into the amount of funds that will be delivered to the payee.

© 2016 Federal Reserve Banks. Materials are not to be used without consent.
Fee transparency and payment certainty on Ripple is unprecedented and a significant advantage over payment systems today. The chain of intermediaries and opaque process make it impossible to determine the fees, FX rate, and amount of funds to be delivered before authorizing the payment. The payer and originating FI must wait two to four days for settlement to occur until they are able to message the beneficiary FI to discover the amount of funds that were delivered.

Ripple’s ability to pre-disclose all fees prior to sending the payment not only improves the customer experience, but also enables compliance with laws in some countries, specifically the United States.

Payment authorization may occur within the same channel in which the payer initiated the transaction. This video provides an example of the payment process from the payer’s perspective, including review of the total cost and authorization.

After the payer has authorized the payment, the originating FI will message payment instructions to the beneficiary FI who confirms the transaction and replies with a unique payment ID that will be used to track payment through the remaining steps of the process.

6. Settlement
Settlement Overview
After successfully completing its internal compliance processes, the FI will use Ripple Connect to settle the payment. Ripple Connect leverages the Interledger Protocol to instruct synchronized transfers on the books of the originating and beneficiary FIs. Settlement occurs in under one second.
Synchronized transactions provide certainty that funds are credited from the payer and delivered to the payee, eliminating the settlement risk that plagues payments facilitated through today’s opaque relay process. Ripple’s design ensures that the payment either immediately settles or the funds are immediately returned to the payer. This compares to today’s system where payments can fail along the chain, with the payer and originating FI learning about the issues several days later. Investigating the issue and locating the breakdown is expensive and cumbersome given the opaque process.

Instant settlement means funds are no longer stuck in flight for two to four days, with the FI holding capital against the payment.

Messaging and settlement capabilities of Ripple Connect are available 24/7/365. The FIs can establish operating hours for when they wish to send and receive payments given their own systems’ scheduled time for maintenance, yet Ripple provides 24/7 functionality.

Within the scope of this proposal, Ripple settles payments in commercial bank money; however the technology, particularly Interledger, can be used with central banks for settlement in central bank money.

The entire process, from debiting funds from the payer to delivering funds to the beneficiary FI, takes less than one second. Importantly, the FI will complete its compliance process before instructing Ripple Connect to transfer funds.

Compliance Responsibilities
The FI maintains full responsibility for ongoing compliance with Anti-Money Laundering (AML) and Office of Foreign Assets Control (OFAC or, more broadly, “sanctions”) legislation and regulations. Financial institutions are also responsible for ongoing monitoring of transactions conducted through Ripple in accordance with their existing transaction monitoring program requirements.
U.S. Financial institutions also maintain responsibility for compliance with foreign correspondent account recordkeeping and due diligence requirements specified under Section 312 of the USA PATRIOT Act. Use of Ripple does not alter these obligations of the financial institution.

The speed of completion depends on the FI’s internal processes. Today’s compliance processes for cross-border payments are designed for low-volume payments that settle in two to four days. While the FI’s compliance processes may not change, the timing of some components may be accelerated or moved earlier in the process, in light of the technology’s immediate settlement of the payment. Optimizing these processes will result in faster end-to-end payment cycles and create a competitive advantage for the FI.

**Detailed Settlement Process and Funds Flow**
To illustrate the settlement flow, we will assume a payer at USA Bank will send $100 to a payee in Europe at Euro Bank.

At this point in time, the banks have completed all pre-transaction messaging, the FX Connector and FX rate has been determined, and the cost information has been presented to the payer. The payer has reviewed the quote, authorizing a payment in which €76.90 will be delivered to the payee.

Currently, the funds remain in the payer’s account, as shown by the graphic below.
Settlement Step 1 - Escrow
Following authorization and compliance processes, Ripple Connect uses the Interledger Protocol to affect funds movement on the FIs’ ledgers. The first step is the movement of funds into the originating and beneficiary FIs’ escrow accounts.

Interledger instructions are sent informing the originating FI to debit $100 from the payer’s account and credit $100 to its escrow account, as shown on the books of USA Bank.

Simultaneously, Interledger instructions inform the beneficiary FI to debit €76.90 from the connector’s account and credit €76.90 to its escrow account, as shown on the books of Euro Bank.

Step 2: Notary Approval
The Ripple Connects at each FI will provide a cryptographic signature that the escrow accounts have been funded. The Ripple Connects at each FI then connect to the authorized notary who will validate these cryptographic signatures.

If the notary confirms the accurate signatures (indicating the payment is fully funded in each escrow account), the payment is deemed final and irrevocable. The process continues to the next step, execution.
However, if escrow accounts are not fully funded, the notary will inform the FIs to release the escrowed funds back to the payer at the originating FI and back to the FX Connector at the beneficiary FI.

The synchronized escrow function and the notary approval process is designed to ensure the payment is fully funded with good funds. This process minimizes settlement risk and lost payments that may occur in relay processes. The commercial agreement and legal framework explained below define payment finality per this notary process.

Step 3: Execution
Following approval by the notary, the FIs will receive Interledger instructions to release funds from their respective escrow accounts. USA Bank will transfer funds from its escrow account to the FX Connector’s account and Euro Bank will transfer funds from its escrow account to the payee’s account.
In the end, the payer is left with $100 less, the payee has €76.90 more, the FX Connector has collected an FX fee and its balances have shifted among its U.S. and European accounts. This entire process takes less than one second.

The entire settlement process occurred on the books of the FIs in commercial bank money. Ripple neither custodies funds nor is a party to the transaction, rather it is a software solution that allows the FIs to safely synchronize book entries on their own ledgers. Instead of relying on a relay process across several institutions as is done today, Ripple coordinates the funds transfers directly on the FIs’ books.

While the example above described settlement between two FIs, Interledger can be used to facilitate settlement between any two entities that have a ledger with an escrow function. Interledger can be used to connect payment systems and facilitate real-time settlement between the two networks.

Legal Framework
A clear and robust legal framework is an essential part of any payment system. With respect to consumer protection, as the consumer payer and the payee remain customers of the FIs and have no direct interaction with Ripple, the consumer laws that generally apply to FIs (e.g., Regulation E) remain applicable. Similarly, prudential regulation and supervision that apply to FIs today will, as a general matter, continue to apply.

Commercial matters including roles, responsibilities, rights, and obligations are governed by a commercial framework and a contractual participation agreement developed by Ripple.
The purpose of such a framework is to establish certainty and clarity as to the FIs’ rights and liabilities vis-a-vis each other when using Ripple technology, including when certain rights arise and certain liabilities are extinguished. This framework builds upon and supplements Article 4A of the Uniform Commercial Code to appropriately tailor the rules to the unique Ripple technology transaction structure. [The agreement and framework are not public documents.]

The FIs will hold Ripple accountable for the functionality of Ripple Connect. Ripple is considered a vendor, subject to the FI’s vendor management program and the FFIEC’s Technology Service Provider guidance in the U.S. Classification and regulatory expectations of Ripple as a technology service provider will vary by jurisdiction.

7. Receipt and Reconciliation
The FIs use Ripple Connect and the payment ID created in the Payer Authorization step to track the status of the payment and update the payer and payee in real time 24/7/365. With real-time tracking and bi-directional messaging, the FIs can quickly identify and resolve any issues that may arise during or after settlement, including exceptions, disputes and investigations. This compares to cross-border payments today where it is timely and costly to detect and resolve errors that occur along the chain of intermediaries.

Once the funds have been delivered to the payee, the beneficiary FI’s Ripple Connect sends a final confirmation notice to the originating FI who notifies the payer that the payment is complete. This process takes place within milliseconds.

The example above illustrated real-time settlement between the FIs and direct delivery of funds to the payee. While this is the fastest approach to funds availability, the beneficiary FI may opt to add an additional step in the process, where it holds the funds after settlement for a period of time before final release to the payee.

An FI may opt to do this to protect itself against the possibility of an unauthorized, erroneous or fraudulent payment. Such a decision is up to the FI and dependent on its risk and compliance policy. Even with such a delay, the settlement still occurs in real-time between the FIs, but delivery to the payee is delayed. The participation agreement and commercial framework define the rights and obligations for handling disputed and fraudulent payments.
The FIs will store all communications, payment tracking status, and delivery confirmation per the needs of their reconciliation process and the requirements of their compliance procedures. While the data is delivered via Ripple Connect, Ripple (the company) cannot access and does not store such information. This transfer of data occurs directly between the FIs.

The FIs are responsible for storing this information internally, subject to the security and encryption policies at each FI. The format and additional contextual information shared via Ripple Connect are delivered in a user-friendly way so that FIs can use their internal tools for analysis and trend identification. As the FIs own the data, they are responsible for fraud detection and reporting.

**Enabling Ubiquity Through Multi-hop Payments**

The payment example presented above requires the originating and beneficiary FI to share a common connector. Without a common connector, the transaction cannot be completed between the FIs. Yet, establishing a common connector between every FI quickly becomes unrealistic.

Interledger resolves this limitation through multi-hop payments. While two FIs may not share a common connector, the connectors they do have may be linked through another FI or network. Interledger can create a chain of connectors and FIs that ultimately connect the originating and
beneficiary FIs. Think “six degrees of separation” for payments. The payment example described above would become one link in the Interledger chain.

The Interledger chain may begin to reflect the chain of intermediaries used to facilitate cross-border payments today. However, there is one crucial difference: the way the payment is processed. Today, cross-border payments are facilitated through a relay process. The payment is sequentially moved from one intermediary to the next. Each link in the chain is disjointed from the others, creating settlement and counterparty risk throughout the payment. A problem could occur at the second or third leg in the payment, requiring several days to reverse the previous legs.

Interledger replaces relay payments with a fully synchronized process designed to create certainty and minimize settlement risk. When settling a payment, Interledger synchronizes the escrow and execution process across the entire payment chain. The payment either fully executes across the entire chain, or all the funds are released from escrow back to their original accounts. Interledger allows FIs to ensure all legs of the payment are fully funded in the escrow accounts before the funds are released to beneficiary of each transaction within the chain.

**Multi-hop Example**

Assume Bank A seeks to make a payment to Bank Z on behalf of their customers. Both banks are directly Ripple-enabled; however, they do not share a common connector. Bank A uses FX Connector 1 while Bank Z uses FX Connector 2. At this time, the FIs are unable to make a payment.
However, Ripple Connect is able to use a pathfinding algorithm to determine that Bank M has accounts for both FX Connector 1 and FX Connector 2. Via two Interledger transactions, Bank M can link the payment for Bank A and Bank Z. The transaction chain will include two parts: (1) between Bank A and Bank M and (2) between Bank M and Bank Z. Interledger will synchronize these transactions to provide certainty of good funds and minimize settlement risk.

Large FIs who hold accounts for many intermediaries can play a central role as the “link” (Bank M) between payments, similar to correspondents’ role today. As large FIs may be the connector, given their global reach and low cost of capital relative to smaller FIs, the large FI can collect an FX spread for facilitating this connection.

The “link” can also be a payment network or any other entity that has a ledger with an escrow function. Interledger can link a payment through traditional centralized payment networks or through a distributed network (“blockchain”). For instance, the payment may be routed through the Ripple Consensus Ledger, a distributed ledger that contains XRP, a digital asset that can be used by FIs or connectors. The FIs determine the connectors and “links” they are comfortable including in their chain.

In this example, there is only one link (Bank M), but an infinite number of links can be added to facilitate the end to end payment. The escrow process and coordinated debits and credits on the books of the FIs ensure settlement risk is minimized, even if many links are used.
Multi-hop Payment: Synchronized Escrows
The settlement process in a multi-hop payment occurs in the same way as described in the funds flow above. First, funds are escrowed across the entire payment chain, starting with the origination FI. In this example, Bank A and Bank M will fund their escrows, which will be confirmed by their notary. Once complete, the next leg of the payment will fund their escrows, which will be confirmed by their notary as well.

Once the entire leg is funded and confirmed by the last notary, there is certainty that the payment is fully funded with good funds. If the escrow is not fully funded at any step in the process, the notary will provide notice to release the escrow funds back to the owner. As the escrow happens entirely on the FIs’ books, this process occurs at the speed of the FIs’ internet connection (delivering Interledger instructions) and Ripple Connect’s ability to process the instructions. This typically occurs in milliseconds.

Multi-hop: Synchronized Execution
After the escrow portion is complete, the payment is executed, meaning funds are released from the escrow to the payee. The execution process occurs in “reverse” order, starting with the last leg of the payment, proceeding through the chain to the payer. If the execution were to proceed in “forward” order, malicious actors would have no incentive to pass confirmation messages on and would stop as soon as the transfer crediting their account was executed. With reverse order,
connectors effectively pay out first and are then reimbursed when they pass the execute command to the previous ledger. The confirmation that good funds are available in the escrow for payout minimizes settlement risk for the connector.

Multi-hop payments coordinated through Interledger ensure ubiquity while minimizing settlement risk.
### Summary: Speed of the payment

<table>
<thead>
<tr>
<th>Step</th>
<th>Summary</th>
<th>Time with Ripple</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Approval and determination of good funds</strong></td>
<td>As a customer of the FI, the payer’s funds are immediately visible to the FI. The FI will use Ripple Connect to determine the available liquidity at the beneficiary FI. This process occurs at the speed of each FI’s respective internet connection.</td>
<td>Milliseconds</td>
</tr>
<tr>
<td><strong>Clearing</strong></td>
<td>The bi-directional messaging and extensible format enables FIs to directly share contextual data.</td>
<td>Under 5 seconds</td>
</tr>
<tr>
<td><strong>Settlement</strong></td>
<td>Compliance checks and exception handling occur per FIs’ internal processes. Ripple Connect leverages the Interledger Protocol to instruct synchronized transfers on the books of the originating and beneficiary FIs.</td>
<td>Compliance process: subject to the speed of the FI’s internal processes Funds movement: Under one second.</td>
</tr>
<tr>
<td><strong>Availability of good funds</strong></td>
<td>Ripple enables immediate availability of funds as the payment is settled into the payee’s account, but the FI can establish a delay if desired.</td>
<td>Immediate; FI may establish a delay per its own risk and compliance program</td>
</tr>
<tr>
<td><strong>Monitoring</strong></td>
<td>FIs use Ripple Connect and the unique payment ID for real-time monitoring of the payment status. Automated notifications allow the FIs to confirm receipt and delivery.</td>
<td>Real-time, 24/7/365</td>
</tr>
<tr>
<td><strong>End-to-End Process</strong></td>
<td>Ripple: Approval, messaging, settlement, funds availability + FI: internal compliance process</td>
<td>Under 5 seconds + the time of the IF’s compliance process</td>
</tr>
</tbody>
</table>
The end-to-end process occurs in **under five seconds** (plus time for the FI’s internal compliance program), **with real-time payment tracking available 24/7/365**.

This compares to cross-border payments using today’s infrastructure which takes **two to four days** to complete with **no tracking or status notification**.
Part A, Section 2: Use Case Description

In this section, the proposer should describe what the solution does at each stage of the end-to-end payments process for each use case that the solution supports (business to business; business to person; person to business and/or person to person, as indicated in the table “Supported use case coverage summary”, above). Proposers should include flow diagrams of the messaging and payment flows and the roles of stakeholders (end users, technology providers, processors, including the proposer(s) for the solution) through the eight stages of the end-to-end payment process of their solution. The description and diagrams should be specific to each supported use case and should highlight all processes and features that are unique to the use case being described. For example, the solution may be designed to enable contextual data capability for business-to-business payments, but not for person-to-person payments. The business-to-business use case description should, therefore, include all the additional processes and features related to enabling contextual data capability.

Ripple is an inter-bank settlement solution optimized for real-time cross-border payments. Ripple can be used to underpin a variety of use cases. See the Use Case section above for more information.

The operation and underlying features of Ripple remain unchanged for whichever use case is used. The FIs may customize the messaging content or contextual information needed for a specific use case, which is easily supported through Ripple’s extensible messaging functionality. See the messaging and payment lifecycle description above, as it remains unchanged for all use cases.
Part A, Section 3: Use Case by Effectiveness Criteria

For each use case that the solution supports (business to business; business to person; person to business and/or person to person, as indicated in the table “Supported use case coverage summary”, above), complete the following table. For each criterion relevant to the lifecycle stage, enter a “Y” if the use case addresses the Effectiveness Criteria (at least to a “somewhat effective level”) or an “N” if it does not (blanks will be assumed as “N”). For example, the solution may be designed to enable contextual data capability for business-to-business payments (U.4, Contextual data capability criterion), but not for person-to-person payments. Proposers should enter a “Y” for any functionality that will be in place at the date of implementation or for which there is a credible plan to implement the enhancement at a future date (as described in Part B, sub-section 1 “Implementation Timeline”).

For solutions where lifecycle stages occur simultaneously, the proposer should enter a “Y” or an “N” based on the criterion listed (rather than focusing on the categorization by lifecycle stage). The table is intended to be a summary of the description in Part A, Section 2.

The end to end solution consists of the FI and Ripple Connect. The operation and underlying features of Ripple remain unchanged for whichever use case is used. The FIs may customize the messaging content or contextual information needed for a specific use case, which is easily supported through Ripple’s extensible messaging functionality.

<table>
<thead>
<tr>
<th>Use case by effectiveness criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lifecycle stage</td>
</tr>
<tr>
<td>Authentication</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Initiation</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Process</td>
</tr>
<tr>
<td>---------------------------------</td>
</tr>
<tr>
<td>S.7</td>
</tr>
<tr>
<td>S.9</td>
</tr>
</tbody>
</table>

**Approval by the Payer’s Provider**

<table>
<thead>
<tr>
<th>Y.3</th>
<th>Y (see Settlement)</th>
</tr>
</thead>
<tbody>
<tr>
<td>S.7</td>
<td>Y</td>
</tr>
<tr>
<td>S.9</td>
<td>Y (see Clearing)</td>
</tr>
<tr>
<td>F.1</td>
<td>Y</td>
</tr>
<tr>
<td>F.5</td>
<td>Y</td>
</tr>
</tbody>
</table>

**Clearing**

<table>
<thead>
<tr>
<th>Y.4</th>
<th>Y</th>
</tr>
</thead>
<tbody>
<tr>
<td>S.7</td>
<td>Y</td>
</tr>
<tr>
<td>S.9</td>
<td>Y</td>
</tr>
<tr>
<td>F.2</td>
<td>Y</td>
</tr>
</tbody>
</table>

**Payer Authorization**

<table>
<thead>
<tr>
<th>Y.2</th>
<th>Y</th>
</tr>
</thead>
<tbody>
<tr>
<td>U.3</td>
<td>Y</td>
</tr>
<tr>
<td>S.2</td>
<td>Y</td>
</tr>
<tr>
<td>S.7</td>
<td>Y</td>
</tr>
<tr>
<td>S.9</td>
<td>Y (see Clearing)</td>
</tr>
</tbody>
</table>

**Settlement**

<table>
<thead>
<tr>
<th>Y.4</th>
<th>Y</th>
</tr>
</thead>
<tbody>
<tr>
<td>S.7</td>
<td>Y</td>
</tr>
<tr>
<td>S.9</td>
<td>Y (see Clearing)</td>
</tr>
<tr>
<td>F.4</td>
<td>Y</td>
</tr>
</tbody>
</table>

**Receipt and Reconciliation**

<table>
<thead>
<tr>
<th>Y.1</th>
<th>Y</th>
</tr>
</thead>
<tbody>
<tr>
<td>U.2</td>
<td>Y</td>
</tr>
<tr>
<td>U.3</td>
<td>Y</td>
</tr>
<tr>
<td>U.6</td>
<td>Y</td>
</tr>
<tr>
<td>S.5</td>
<td>Y</td>
</tr>
<tr>
<td>S.6</td>
<td>Y</td>
</tr>
<tr>
<td>S.7</td>
<td>Y</td>
</tr>
<tr>
<td>S.9</td>
<td>Y</td>
</tr>
<tr>
<td>F.3</td>
<td>Y</td>
</tr>
<tr>
<td>F.5</td>
<td>Y</td>
</tr>
<tr>
<td>E.7</td>
<td>Y</td>
</tr>
</tbody>
</table>
PART B: BUSINESS CONSIDERATIONS

In this part, the proposer should describe important business considerations to demonstrate the feasibility for the solution. Proposers may detail their qualifications or past experience in implementing faster payments in the sub-sections below if they view it will support the description.

1. Implementation Timeline

Ripple Connect and the solution components take four months (16 weeks) to implement including planning, design, building, testing, and launch. The table below shows a typical integration plan and timeline. The steps are details in the Integration Effort section below.

<table>
<thead>
<tr>
<th>Ripple Production Timeline</th>
<th>Month 1</th>
<th>Month 2</th>
<th>Month 3</th>
<th>Month 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phase</td>
<td></td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Planning &amp; Requirements</td>
<td>FI, Ripple</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integration Ripple Connect</td>
<td>FI, Ripple</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integration to Core Ledger/ Banking Product Systems</td>
<td>FI, Ripple</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integration to Support Systems</td>
<td>FI, Ripple</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interface to liquidity provisioning</td>
<td>FI (Trading Desk), Liquidity Provider</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integration from Channels</td>
<td>FI Product Group(s)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Design</td>
<td>FI, Ripple</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Build</td>
<td>FI, Ripple</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integration Ripple Connect</td>
<td>FI, Ripple</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integration to Core Ledger/ Banking Product Systems</td>
<td>FI</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integration to Support Systems</td>
<td>FI</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interface to liquidity provisioning</td>
<td>FI (Trading Desk), Liquidity Provider</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integration from Channels</td>
<td>FI Product Group(s)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Testing</td>
<td>FI, Ripple</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Go-Live</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2. Value Proposition and Competition

Ripple provides all FIs, especially small and medium institutions, direct access to cross-border payments, empowering them to better serve their customers and compete for cross-border payments for the first time.

FIs are no longer reliant on and restricted by their correspondent’s geographic reach. FIs can integrate and transact directly, eliminating today’s intermediaries and processing fees. By accessing the competitive liquidity marketplace, FIs can reach new corridors without locking up their own capital. FIs are able to better meet the needs of their customers, without reliance on limited features and costs of using a correspondent. These design elements lower the cost and risk of cross-border payments, while increasing market competition.
As a flexible platform, Ripple gives FIs tools to improve their existing services or build new products. FIs can add value-added services such as real-time status updates or new services such as low-value remittance products. FIs determine the use case and product they will enable via Ripple given their customers’ demands and product strategy. Some FIs are focused on the P2P market to certain countries, while others may seek to enable a B2B payment product to a previously inaccessible country.

FIs license Ripple Connect from Ripple (the company) or an approved channel partner. Licensing fee and integration cost are dependent on the FI’s internal system and customization (if required). Ripple offers a variety of licensing plans to fit the needs of different FIs: annual subscriptions, volume-based pricing, etc.

Some FI’s use third party payment hubs, such as Earthport, to process cross-border payments. Ripple has partnered with such firms to integrate Ripple into the platforms FIs are already connected to. This becomes a fast and efficient way for banks to become Ripple-enabled. Through additional partnerships, Ripple plans to broader the reach and lower the cost of accessing Ripple.

3. Integration Effort

The following description describes generic integration points at an FI. While each FI’s architecture may vary causing some customization, the functions below and their interactions will generally remain the same.

Banks may choose to integrate the Ripple solution by implementing its full capabilities through either single or multi-phase integration. Banks’ implementation strategies will necessarily be dependent on their respective business and solution architectures, but regardless of the approach all will need to implement a new functionality specifically designed for the Ripple solution integration. FIs integrate with the Ripple solution through licensed software and Ripple-provided Representation State Transfer Application Programming Interface (REST API), and may physically reside in one or more systems.

The illustration above provides for five integration points, each with its own function, interaction, interface, and stakeholders as explained below:

1. Ripple Connect
   The FI typically interacts with Ripple Connect directly through the REST API to allow for the initiation of quoting flow, submission of payment
settlement, and sending and receiving delivery confirmations, among other capabilities. Ripple, an authorized channel partner, or a bank’s enterprise payment service provider will usually handle this integration point and the expected level of effort is one month.

2. Core Ledgers/Banking Product Systems
This integration point typically interacts with the bank’s core ledger system to transfer funds as part of payment processing and update the ledger following transactions; real-time payment posting is made possible through this integration point. This integration point normally interfaces with the bank-provided core ledger/banking product systems. Ripple, an authorized channel partner, or a bank’s enterprise payment service provider will usually handle this integration point and the expected level of effort is one month.

3. Support Systems
This integration point typically interacts with the bank’s payment supporting systems to pre- and post-process payment transactions through a bank-provided support systems interface. This integration point permits the Ripple solution to use bank provided payment support services such as customer identification and validation, sanction list checks, and fee calculations among others. A bank’s support service providers will usually handle this integration and the expected level of effort is two weeks.

4. Liquidity Management Systems
This integration point typically resides in the bank’s liquidity management system and interacts with the Ripple solution directly through REST API or through the bank’s enterprise services to perform the defined liquidity management function; the bank’s liquidity management system will need to be enhanced to provide appropriate and secure user interfaces to facilitate liquidity management. This integration point permits liquidity providers, whether a bank’s FX trading desk, treasury, or a third-party liquidity provider, to get authorization, fund and monitor liquidity positions, participate in payment execution, and redeem funds as needed. A bank’s FX trading desk, treasury, or a third-party liquidity provider can usually handle this integration and the expected level of effort is one month.
5. Channels
This integration point will allow selected payment channels, such as mobile banking, to take advantage of the Ripple solution. This integration point typically interacts with the FI’s payment hub/integration platform which forwards payments to be processed directly through the REST API. A bank’s mobile, online, or enterprise payment service provider can handle this integration and the expected level of effort is 1-2 months, 1, or 0.5-1 month, respectively.

Please note that enhancement to other bank systems to take advantage of the Ripple solution’s real-time payment settlement may be necessary depending on each bank’s system architecture.

Integration Maintenance
Banks should maintain their Ripple solutions by upgrading to the latest version in order to take advantage of new capabilities and apply critical patches as they are released. Due to the interconnectivity between banks’ Ripple solutions it is imperative that partnering banks maintain compatibility between their respective software versions. Ripple’s product release notes contain advisory statements and recommendations to assist banks in determining whether and how to upgrade their software to maintain compatibility.
PART C: SELF-ASSESSMENT AGAINST EFFECTIVENESS CRITERIA

This section should be used by proposers to assess how the solution meets each of the criteria outlined in the Effectiveness Criteria (considering all use cases supported by the solution). Proposers should include in their self-assessment any functionality that will be in place at the date of implementation or for which there is a credible plan to implement the enhancement at a future date (as described in Part B, sub-section 1 “Implementation Timeline”). For example, the Effectiveness Criteria specifically acknowledges that proposers may not have cross-border functionality at implementation but may have a credible plan to implement it at a later date.

Proposers should use the tables below to indicate their self-assessed rating on the Effectiveness Scale outlined for each criterion, as well as a detailed discussion of why the rating is justified and how the solution meets each criterion (e.g., U.1, U.2, etc.), including each consideration (e.g., U.1.1, U.1.2, etc.). Proposers may use the far-right column (“Proposal Page Number”) in the tables to cross-reference the section/page number for the relevant description provided in Part A or Part B, above.

Proposers should note that a number of the criteria have been written in a way that provides flexibility for a range of different approaches to address the criteria or for the solution to determine how certain terms and parameters are defined. Proposers should ensure their justification of how the solution meets each criterion includes a clear explanation of the approach taken in the solution, and how solution-determined terms and parameters are defined. For example, S.2.3 (Payer authorization criterion) requires the solution to enable the payer to revoke any pre-authorization of payments easily and timely. The proposer’s justification for S.2 should include how the revocation is “easy” for the payer and the time it takes (i.e., number of minutes, hours, or days) for the revocation to take effect. Similarly, E.6.2 (Scalability and adaptability criterion) requires the solution to demonstrate the capacity to handle projected volumes and values (determined by the solution), including heightened transaction volumes and values during peak times or periods of stress. The proposer’s justification for E.6 should include its assumptions for determining the heightened volumes and values and how they relate to normal periods (e.g., heightened volumes are equal to twice the projected volumes during normal periods).

NOTE: VE = Very Effective  
E = Effective  
SE = Somewhat Effective  
NE = Not Effective
Proposers should refer to the Effectiveness Criteria for an explanation of what Very Effective, Effective, Somewhat Effective and Not Effective mean for each criterion.

1. **Ubiquity**

   Provide a self-assessed rating in the table below and then justify how the solution meets criteria for: accessibility, usability, predictability, contextual data capability, cross-border functionality, and applicability to multiple use cases.

   **Self-assessed rating:**

<table>
<thead>
<tr>
<th>Effectiveness Criteria</th>
<th>Effectiveness Criteria Self-Assessment (Check One)</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria Name</td>
<td>#</td>
<td>Consideration Name</td>
</tr>
<tr>
<td>Ubiquity</td>
<td>U.1</td>
<td>Accessibility</td>
</tr>
<tr>
<td>Ubiquity</td>
<td>U.2</td>
<td>Usability</td>
</tr>
<tr>
<td>Ubiquity</td>
<td>U.3</td>
<td>Predictability</td>
</tr>
<tr>
<td>Ubiquity</td>
<td>U.4</td>
<td>Contextual data capability</td>
</tr>
<tr>
<td>Ubiquity</td>
<td>U.5</td>
<td>Cross-border functionality</td>
</tr>
<tr>
<td>Ubiquity</td>
<td>U.6</td>
<td>Applicability to multiple use cases</td>
</tr>
</tbody>
</table>

   **Justification for U.1: Accessibility**

   Ubiquity and accessibility can be achieved in two phases: indirect and direct access.

   **Indirect access:** In the early days of adoption, Ripple will reach ubiquity through indirect access to the technology. Only one FI in the country needs to be integrated to provide the benefits of Ripple to its currency.

   Early adopters of Ripple’s technology can offer faster cross-border payment services to other FIs. For instance, an FI that needs to make a fast cross-border payment will first send the payment over domestic rails to the Ripple-integrated FI. The Ripple-integrated FI facilitates
the cross-border payment to a Ripple-integrated FI in the payee’s country, who sends the funds over the local rail to the payee’s FI.

The cross-border leg of the payment is settled in a few seconds as opposed to several days; the speed of the domestic payment rail becomes the limiting factor. Indirect access to Ripple through other FIs quickly enables ubiquity and the ability to access faster cross-border payments.

**Direct access:** Over time, more FIs are likely to access Ripple directly through either their own integration or use of a payment service that becomes Ripple-enabled. Ripple is working with several channel partners who are integrating Ripple into their core systems and payment hubs – platforms that FIs are already connected to. This enables access with minimal additional effort from the FI. By leveraging channel partners and integrating into payment hubs FIs are already using, Ripple can achieve direct ubiquity.

While direct access offers the greatest speed and efficiency, indirect access quickly enables accessibility and ubiquity. In the short run, indirect access will allow Ripple to “effectively” achieve accessibility.

**Multi-hop payments:** Multi-hop payments enable scalability and payment reach between FIs who do not have common connectors. Multi-hop payments reduce the number of connector relationships, allowing ubiquity to be reached efficiently and safely. See the multi-hop payment description for more information (p. 36).

**Financial Inclusion:** A key part of accessibility is enabling greater financial inclusion. The risk and high cost of cross-border payments today put such services out of reach for many consumers. As the global economy has become more interconnected, the demand for cross-border payments, especially low-value remittance payments, is increasing yet cannot be met by today’s systems.

By minimizing settlement risk and driving many efficiencies, Ripple lowers the cost of facilitating cross-border payments by 40% to 60%. With this cost reduction, Ripple enables FIs to introduce low-value payment products feasibly and profitably for the first time. By optimizing the cost structure of the payment, Ripple directly improves access to payment services and increases financial inclusion.

---

**Justification for U.2: Usability**

Ripple is used by an FI to enable cross-border payments for its customers. The FI continues to own the customer relationship. The payment service enabled by Ripple is embedded in the FI’s existing delivery channels (mobile app, website, etc). All features and benefits of Ripple remain intact regardless of the use case or channel that a customer uses to initiate a payment. See the Initiation and Authorization sections for more information (pg. 27, 28).

Given Ripple enables good funds to be delivered to the payee 24/7/365, along with end-to-end tracking of payment status, Ripple’s self assessment is “very effective,” especially in light of delays, cost and lack of visibility into cross-border payments today. See the Settlement section for more information (pg. 29).

**Justification for U.3: Predictability**

As an inter-bank payment solution, Ripple functions the same regardless of the use case or type of payment the FI is sending. This provides clarity and predictability to the FI for how the payments are processed. See the Initiation and Authorization sections for more information (pg. 27, 28).

The participation agreement and commercial ruleset define roles, rights, obligations of the FIs on the network. Additionally, the consumer protection safeguards in place today remain unchanged given the payer and payee remain customers of the FI. See the Legal Framework section for more information (pg. 34).

The FI will use Ripple to underpin an existing payment service or develop a new product. As part of the end to end solution, the FI selects the appropriate channels and user interface will develop.

**Justification for U.4: Contextual Data Capability**

The messaging functionality within Ripple Connect allows FIs to share contextual payment data, fees, and confirmations of acceptance and delivery. It is extensible to support a variety of use cases and does not require use of a proprietary standard. See “Deep Dive on Ripple Connect” for more information on messaging and contextual data (pg. 21). Ripple’s self assessment is “very effective.”
**Justification for U.5: Cross Border**

Ripple enables settlement of real-time cross-border payments in less than one second, compared to two to four days today. Ripple provides direct connectivity to other currencies via an FI’s own liquidity or through a competitive market of third-party liquidity providers. This market provides access to other currencies without requiring an FI to pre-fund or outlay capital – a cost effective and capital efficient way to enable access to new corridors. Ripple’s self assessment is “very effective.”

**Justification for U.6: Multiple Use Cases**

Ripple enables multiple use cases. See the “Use Case” section (pg. 14). Ripple’s self assessment is “very effective.”

2. Efficiency

Provide a self-assessed rating in the table below and then justify how the solution meets criteria for: enables competition, capability to enable value-added services, implementation timeline, payment format standards, comprehensiveness, scalability and adaptability, and exceptions and investigations process.

**Self-assessed rating:**

<table>
<thead>
<tr>
<th>Effectiveness Criteria</th>
<th>Effectiveness Criteria Self-Assessment (Check One)</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Criteria Name</strong></td>
<td><strong>Consideration Name</strong></td>
<td><strong>VE</strong></td>
</tr>
<tr>
<td>Efficiency E.1</td>
<td>Enables competition</td>
<td>X</td>
</tr>
<tr>
<td>Efficiency E.2</td>
<td>Capability to enable value-added services</td>
<td>X</td>
</tr>
</tbody>
</table>

© 2016 Federal Reserve Banks. Materials are not to be used without consent.
Justification for E.1: Enables competition

For cross-border payments today FIs are dependent on a few large correspondents for liquidity and funds delivery. FIs must lock up capital with multiple correspondents for broad payment reach, and are forced to accept the FX quote dictated by the correspondent (pg. 9).

Ripple is designed to drive competition and market access in cross-border payments. FIs can directly connect with the counterparties they desire to transact with, or they can connect indirectly through another Ripple-enabled FI. FIs of any size can integrate with Ripple, providing greater choice of indirect partners.

FIs can use their own liquidity (via nostro and vostro accounts) to fund payments – as is done today – or they may access a competitive marketplace of third-party FX providers (aka: connectors). This market allows FIs to access both core and non-core corridors without locking up their own capital. The third-party providers supply the liquidity for the payment. When executing a payment, Ripple will source liquidity from the authorized provider with the lowest FX cost, creating an openly competitive FX market. FIs select and onboard their approved third-party providers, so they have complete visibility into the provider and its liquidity.

Being a platform for inter-bank settlement, Ripple empowers the FIs to create the use case and product that best suits their customers’ needs and market position. Small FIs are now able to directly offer cross-border payment services, driving competition in what is currently a closed market. See the Deep Dive section for more information (pg. 21).
**Justification for E.2: Capability to enable value-added services**

As a platform that supports multiple use cases, Ripple empowers the FI to build value added services into its existing services and new products. For instance, the flexible messaging functionality allows FIs to share contextual information about the payment that can be used for a value-added service by the FIs. The real-time tracking of payment status is an additional benefit FIs can pass on to their customers. See the Ripple Benefits overview (pg. 13).

**Justification for E.3: Implementation timeline**

At a minimum, only one FI in a country needs to be integrated to provide the benefit of Ripple to their currency. The Ripple-enabled FI can provide indirect access to other FIs in the country by connecting over the country’s domestic payment rail. Additionally, an FI can integrate directly for improved speed and efficiency. The sales pipeline of both large and small FIs shows increasing interest in direct access. See the Ubiquity U.1 for more information (pg. 46, 51).

As of April 2016, Ripple has completed 30 pilots at FIs globally. The company has 90 active customers in the pipeline planning products and integrations. There are 10 commercial deals underway that will result in live products in the coming 12 months. Some FIs have already launched live products. Ripple’s engagements with channel partners enables access to over 60 currencies.

Given the sales pipeline, channel partner arrangements, and non-public pending deals, Ripple will be broadly available and utilized for cross-border payments by 2018. Ripple aims to enable global ubiquity.

**Justification for E.4: Payment format standards**

See the “Messaging Functionality” Section within the Ripple Connect Deep Dive (pg. 21).

**Justification for E.5: Comprehensiveness**

Ripple’s inter-bank solution, in conjunction with the FI’s internal authentication and compliance processes, enables a complete solution with new features that systems do not have today: flexible messaging, real-time settlement of cross-border payments, real-time tracking and payment status, and a competitive liquidity market for FX.

**Justification for E.6: Scalability and adaptability**
Ripple’s use of a protocol enables scalability and resiliency not previously possible in payment systems. The flexible messaging format enables adaptability to whichever current and future standards FIs wish to use. See the following sections:
(1) Settlement Functionality via the Interledger Protocol, pg. 22
(2) Distributed Financial Technology and Operational Resiliency, pg. 17
(3) Messaging Functionality within the Deep Dive on Ripple Connect section, pg 21

Justification for E.7: Exceptions and investigations process
Ripple Connect’s flexible messaging functionality allows FIs to share contextual information about the payment in a user-friendly format. The FIs can use this information and bi-directional messaging to resolve exceptions and complete investigations more efficiently than today’s limited, one-way messaging allows. While Ripple Connect’s messaging and data capabilities support the FIs’ internal investigations and exception handling process, these processes are internal to the FI. See pg. 21 for messaging overview.

3. Safety and Security
Provide a self-assessed rating in the table below and then justify how the solution meets criteria for: risk management, payer authorization, payment finality, settlement approach, handling disputed payments, fraud information sharing, security controls, resiliency, end-user data protection, end-user/provider authentication, and participation requirements.

**Self-assessed rating:**

<table>
<thead>
<tr>
<th>Effectiveness Criteria</th>
<th>Effectiveness Criteria Self-Assessment (Check One)</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Criteria Name</strong></td>
<td><strong>#</strong></td>
<td><strong>Consideration Name</strong></td>
</tr>
<tr>
<td>Safety and Security</td>
<td>S.1</td>
<td>Risk management</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>S.2</td>
<td>Payer authorization</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>S.3</td>
<td>Payment finality</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>S.4</td>
<td>Settlement approach</td>
</tr>
</tbody>
</table>

© 2016 Federal Reserve Banks. Materials are not to be used without consent.
<table>
<thead>
<tr>
<th>Safety and Security</th>
<th>S.5</th>
<th>Handling disputed payments</th>
<th>X</th>
<th>21</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety and Security</td>
<td>S.6</td>
<td>Fraud information sharing</td>
<td></td>
<td>21</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>S.7</td>
<td>Security controls</td>
<td>X</td>
<td>23</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>S.8</td>
<td>Resiliency</td>
<td>X</td>
<td>17</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>S.9</td>
<td>End-user data protection</td>
<td>X</td>
<td>23</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>S.1 0</td>
<td>End-user /provider authentication</td>
<td>X</td>
<td>27</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>S.1 1</td>
<td>Participation requirements</td>
<td>X</td>
<td>34</td>
</tr>
</tbody>
</table>

**Justification for S.1:**

The participation agreement and commercial rules include a risk framework. Maturity of the risk framework will develop with the adoption of the solution, as unforeseen risks are identified and mitigated. See the legal framework section (pg. 34).

**Justification for S.2 Payer Authorization:**

Ripple enables unprecedented certainty and transparency in the payment authorization process. Through data provided by Ripple Connect, the originating FI can present the total cost, including fees and the FX rate, to the payer for review and approval before authorizing the transaction. This transparency provides the payer certainty into the amount of funds that will be delivered to the payee.

Fee transparency and payment certainty on Ripple is unprecedented and a significant advantage over cross-border payments today. The chain of intermediaries and opaque process make it impossible to determine the fees, FX and amount of funds to be delivered before authorizing the payment. The payer and originating FI must wait two to four days for
settlement to occur until they are able to message the beneficiary FI to discover the amount of funds that were delivered.

For more information see the Payment Authorization Section (pg. 28).

**Justification for S.3 Payment Finality:**

See “Step 2: Notary Approval” of the Settlement Section (pg. 32).

**Justification for S.4 Settlement Approach:**

Settlement occurs via synchronized transactions on the books of the originating and beneficiary FI. Settlement via Ripple Connect can occur 24/7/365, however, FIs have the ability to establish settlement windows if they wish. As the funds of the payer, payee and FX Connector are on the books of the FIs, the FIs have instant 24/7/365 visibility into the balances of the accounts.

This proposal illustrated real-time gross settlement of a cross-border payment. FIs can also use Ripple to deferred net settlement. The FIs would establish terms, risk limits, and settlement periods for this arrangement.

See the Settlement section for additional information (pg. 29).

**Justification for S.5 Handling Disputed Payments:**

Ripple’s participation agreement and commercial framework define the process, rights, and obligations for addressing disputed payments between the FIs. The agreement holds FIs responsible for compliance with all consumer protection laws. The messaging functionality and direct connectivity enables FIs to efficiently resolve issues. See pg. 34 for the legal framework/participation agreement and pg. 21 for a deep dive of the messaging functionality.

**Justification for S.6 Fraud Information Sharing:**

Ripple provides bi-directional messaging enabling the transfer of payment data (pg. 21). The messaging format is extensible, allowing FIs to share contextual and possibly fraud information. Ripple Connect consolidates payment information in a user-friendly format. However, the data is owned by the FIs and is not accessible by Ripple. As their is no central operator and payments are made directly between FIs, the FIs are responsible for the fraud detection, reporting and resolution of transactions that they process.
Justification for S.7: Security

See “Security Within Ripple Connect” section within the Deep Dive on Ripple Connect (pg. 23).

Justification for S.8: Resiliency

See section: “Distributed Financial Technology and Operational Resiliency” (pg. 17).

Justification for S.9 End-User Data Protection

All information at rest is stored by the FIs per their encryption and security procedures. Ripple does not govern this process. As the payer and payee are customers of the FIs (not Ripple), information needed for account set-up, transaction set-up and problem resolution is collected, managed and stored by the FI per its procedures.

Ripple Connect transfers data between the FIs. All traffic between Ripple Connect at the originating and beneficiary FIs is encrypted and occurs over secure HTTPS connections using OAuth 2.0 for authentication. Ripple (the company) does not have access to this information. It is private between the FIs. See “Security Within Ripple Connect” section within the Deep Dive on Ripple Connect (pg. 23).

The FIs determine what end user data is needed to facilitate the payment. The FIs may require an account number (BIC, IBAN, etc) to route the payment.

Justification for S.10 End-User Authentication:

As the payer and payee are customers of the FIs, the FIs are responsible for the end user authentication per their respective policies and procedures (pg. 27). Upon integrating Ripple, an FI will perform due diligence on the other FIs it seeks to make payments with. In this process the FI will assess the onboarding and compliance policies of the counterparty to ensure reliable onboarding and authentication processes. This process is performed by the FIs as part of the end-to-end solution. The data transmitted between the FIs via Ripple Connect is encrypted and only visible between the FIs.

Justification for S.11:
See the Legal Framework section within the Settlement portion of the payment lifecycle (pg. 34).

4. **Speed (Fast)**

Provide a self-assessed rating in the table below and then justify how the solution meets criteria for: fast approval, fast clearing, fast availability of good funds to payee, fast settlement among depository institutions and regulated non-bank account providers, and prompt visibility of payment status.

**Self-assessed rating:**

<table>
<thead>
<tr>
<th>Effectiveness Criteria</th>
<th>Effectiveness Criteria Self-Assessment (Check One)</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria Name</td>
<td>#</td>
<td>Consideration Name</td>
</tr>
<tr>
<td>Speed (Fast)</td>
<td>F.1</td>
<td>Fast approval</td>
</tr>
<tr>
<td>Speed (Fast)</td>
<td>F.2</td>
<td>Fast clearing</td>
</tr>
<tr>
<td>Speed (Fast)</td>
<td>F.3</td>
<td>Fast availability of good funds to payee</td>
</tr>
<tr>
<td>Speed (Fast)</td>
<td>F.4</td>
<td>Fast settlement among depository institutions and regulated non-bank account providers</td>
</tr>
<tr>
<td>Speed (Fast)</td>
<td>F.5</td>
<td>Prompt visibility of payment status</td>
</tr>
</tbody>
</table>

These self-assessment ratings are based on the cross-border payment between two FIs directly connected via Ripple. As discussed in the Ubiquity self assessment above, FIs not connected to Ripple can benefit from the solution through indirect access. First, the FI will

© 2016 Federal Reserve Banks. Materials are not to be used without consent.
send the payment over local rails to a Ripple-enabled FI for it to facilitate the cross-border payment. In this scenario, the speed of the local rail payment should also be considered to determine the end-to-end time of the payment. However, the self assessment below is limited to the cross-border leg of the payment, the focus of this proposal.

**Justification for F.1: Fast Approval of Good Funds**

The payer is a customer of the originating FI, meaning the FI has direct visibility into the payer’s account balance to assure good funds are available. The originating FI will use Ripple Connect to determine the FX connector(s) that have sufficient liquidity (good funds) available for the payment. This process takes milliseconds, depending on the speed of the FI’s internet connection. With this information the originating FI can confirm good funds within the “very effective” timeframe of under two seconds. See pg. 27.

**Justification for F.2: Fast Clearing**

The clearing process occurs directly between the FIs using Ripple Connect. The timing of clearing is dependent on the FIs’ internet speed, typically within five. See the Clearing Section for more information. See pg. 27.

**Justification for F.3: Fast availability of good funds to payee**

Ripple enables immediate availability of funds as the payment is settled into the payee’s account, but the FI can establish a delay if desired. See the Receipt Section for more information. See pg. 35.

**Justification for F.4: Fast Settlement**

Ripple Connect leverages the Interledger Protocol to instruct synchronized transfers on the books of the originating and beneficiary FIs. Settlement occurs in under one second, plus the time needed for the FIs to complete their internal compliance processes. See the Settlement Section (pg. 29).

**Justification for F.5: Prompt Visibility of Payment Status**

The FIs use Ripple Connect and the payment ID created in the Payer Authorization step to track the status of the payment and update the payer and payee in real time 24/7/365. See the Receipt and Reconciliation Section (pg. 35).
5. Legal Framework

Provide a self-assessed rating in the table below and then justify how the solution meets criteria for: legal framework, payment system rules, consumer protections, data privacy, and intellectual property.

**Self-assessed rating:**

<table>
<thead>
<tr>
<th>Effectiveness Criteria</th>
<th>Effectiveness Criteria Self-Assessment (Check One)</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legal Framework L.1</td>
<td>X</td>
<td>34</td>
</tr>
<tr>
<td>Legal Framework L.2</td>
<td>X</td>
<td>34</td>
</tr>
<tr>
<td>Legal Framework L.3</td>
<td>X</td>
<td>34</td>
</tr>
<tr>
<td>Legal Framework L.4</td>
<td>X</td>
<td>34</td>
</tr>
<tr>
<td>Legal Framework L.5</td>
<td>X</td>
<td>23</td>
</tr>
</tbody>
</table>

**Justification for L.1, L.2 and L.3:**

With respect to consumer protection, as the consumer payer and the payee remain customers of the FIs and have no direct interaction with Ripple, the consumer laws that generally apply to FIs (e.g., Regulation E) remain applicable.

The messaging function with Ripple Connect enables the FI to better comply with existing laws. For instance, the FI’s ability to present the total cost of the payment to the payer before authorization allows banks to increase transparency and cost certainty to the customer and comply with fee pre-disclosure requirements required by Section 1073 of the Dodd-Frank Wall Street Reform and Consumer Protection Act.

With respect to the roles, responsibilities, rights, and obligations of FIs using Ripple technology, such commercial matters are governed by a commercial framework and a contractual participation agreement that FIs sign upon integrating Ripple. The participation
agreement and commercial framework define the rights and obligations for handling disputed and fraudulent payments between the FIs.

See (1) Compliance Responsibilities subsection, pg. 30 and (2) the Legal Framework subsection within the Settlement Section of the Payment Lifecycle, pg. 34.

**Justification for L.4 Data Privacy:**
As part of the solution, the FIs will determine the payer and payee information required to ensure compliance with its own procedures and its jurisdiction’s laws. The information sent via Ripple Connect is accessible only by the originating and beneficiary FI. Ripple (the company) neither accesses nor stores this information. The FIs will store communications, payment tracking status, and delivery confirmation per the needs of their reconciliation process and the requirements of their compliance procedures (pg. 21).

As the data belongs to the FIs, it is stored per the encryption and security procedures of the FIs. Ripple Connect is installed behind the FI’s firewall in its secure environment. Financial institutions’ internal systems will communicate to Ripple Connect over secure HTTPS connections using OAuth 2.0 for authentication. All traffic between Ripple Connect at originating and beneficiary FI occurs over secure HTTPS as well (pg. 23).

To ensure end user privacy, the participation agreement and commercial framework define the permissible and restricted uses of personal data shared during the payment cycle. FIs are bound by this agreement (pg. 34).

**Justification for L.5: Intellectual Property**

The solution has undertaken a due diligence review of potentially applicable intellectual property rights. Ripple Connect is a closed-source software solution licensed by Ripple to FIs.

The Interledger Protocol is an open source standard being developed in the Interledger Payments Community Group at the World Wide Web Consortium (W3C), the main international standards organization for the World Wide Web. Interledger is and should remain free for everyone to use without fear of infringing any third party IP rights.

Ripple is not aware of any third party IP rights that would be infringed by Interledger. Ripple is establishing procedures for third parties to bring any IP concerns to Ripple’s attention.
6. Governance

Provide a self-assessed rating in the table below and then describe how the solution meets criteria for: effective governance and inclusive governance.

**Self-assessed rating:**

<table>
<thead>
<tr>
<th>Effectiveness Criteria</th>
<th>Effectiveness Criteria Self-Assessment (Check One)</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Criteria Name</strong></td>
<td><strong>#</strong></td>
<td><strong>Consideration Name</strong></td>
</tr>
<tr>
<td>Governance</td>
<td>G.1</td>
<td>Effective governance</td>
</tr>
<tr>
<td>Governance</td>
<td>G.2</td>
<td>Inclusive governance</td>
</tr>
</tbody>
</table>

**Justification for G.1:**

The governance of the solution is defined by the participation agreement and commercial framework, described on pg. 34. Given the infancy of the solution and the network of FIs as of April 2016, the governance will mature as the solution gets broader adoption.

**Justification for G.2:**

Governance of the Interledger Protocol is managed within the well-established World Wide Web Consortium (W3C), the main international standards organization for the World Wide Web. This open group includes participants from financial services, technology, government and other sectors.
Ripple

Real-Time Cross-Border Payment Solution

Update to the QIAT
August 26, 2016

Submitted by:
Ryan Zagone
Director of Regulatory Relations, Ripple
zagone@ripple.com
Introduction

Ripple appreciates the consideration of this update to our faster payments proposal. Following the submission of the original proposal in April 2016, several market developments and solution improvements have occurred.

This paper addresses the follow updates:

1. Emerging payment demands driving increased adoption of the solution
2. Updated details of the solution
3. The formation of a governance body and payment scheme
4. Unique Realities of a Cross Border Payment Solution
5. The Path To Interledger

We appreciate your review and are happy to address any questions.

Ryan Zagone  
Director of Regulatory Relations  
Ripple

Liza Partington  
Regulatory Relations Specialist  
Ripple
1. Emerging payment demands driving increased adoption of the solution

Today, cross-border payments are relayed across several intermediaries. The fragmented and opaque process prohibits originating and beneficiary institutions from knowing the status of the payment, the fees that will be taken, and the amount of funds that will ultimately be delivered. Given the side effects of this process – including delays, costs and risks – only large-value batch payments are viable with today’s infrastructure.

Banks and payment providers are seeking new solutions in response to two primary cross-border payment demands: (1) improved transparency and certainty of high value payments and (2) the ability to efficiently send low-value payments.

**Market Demand 1: Improved High-Value Payments**
Customers are seeking an improved cross-border payment experience for the payments they currently send overseas. Customers expect transparency to the payment – the ability to track the payment in real-time with clear estimates for the time of delivery. Customers are also seeking greater certainty of fees and the exact amount of funds that will be delivered, all before the payment is initiated.

As the current process does not provide this certainty and transparency, many corporates result to a workaround for some payment needs, opening bank accounts and depositing cash in all the countries in which they make payments. This enables the corporate to quickly make payments of a certain amount. However, the corporate assumes FX risk, which it may not have an expertise in managing; incurs operational cost of maintaining these accounts; and suffers a large opportunity cost of locking up capital all around the world.

An improved cross-border payment process that provides efficiency and certainty is needed.

**Market Demand 2: The Ability to Send Low-Value Cross-Border Payments**
A wide variety of stakeholders are seeking access to low-value, high-volume payment services. As today’s current infrastructure was built to support high-value batch payments, the services in demand are generally not cost effective or not offered at all. Broad macro trends are calling for efficient low-value payment options:

**Remittances:** Consumers have grown accustomed to immediate global connectivity, which has led to a change in their expectations for the speed and reach of payments. As globalization has driven individuals to become more
dispersed and interconnected, there is an increasing demand for low-cost P2P payment services, particularly for small-dollar cross-border transactions.

**Small and medium sized companies**: Smaller companies have long sought access to materials and markets overseas. Yet, the cost and complexity of managing cross-border payments often cannot be justified for a few low-value payments per month. Given their anticipated low payment volume, these companies often minimize activity that would require cross-border payments. To enable growth, these companies are seeking solutions that allow them to efficiently send a low-volume of small- and medium-sized payments.

**A new generation of digitally-based companies**: A new crop of digitally-based marketplace companies has emerged with a specific need for low-value global payments. These companies, such as Uber, Amazon and Airbnb, have a global mindset and customer base from day one. They have supply chains that are increasingly sophisticated with a focus on minimizing working capital.

The nature of these companies’ operations require many small payments to be sent globally in real-time. Today’s high-value, batch payment solutions do not suit the needs of this new generation of companies. Given these companies large size and quick growth, meeting their payment needs is a priority for many banks and payment providers.

These two demands are driving increased adoption of Ripple. Instead of using a relay process as is done today, Ripple securely synchronizes settlement across the originating and beneficiary banks. This coordinated approach provides transparency, certainty, global reach, and efficiency for both high- and low-value payments.

Ripple is an enterprise solution designed to be integrated by a variety payment providers. Ripple’s solution can be used by banks, payment networks and non-bank payment providers such as remittance companies or telecom-operated mobile money systems. Ripple’s work with Western Union on cross-border and intercompany settlement is one example of a non-bank payment company use case.

Ripple enables payment providers to better meet their customers’ needs, resulting in greater financial inclusion while lowering barriers to global commerce.

Recent adoption includes:
- [Seven Leading Banks Join Ripple’s Global Network](#)
- [Santander UK to Launch Ripple-Powered Payments App in 2016](#)
- [Live Transaction Between ATB (Canada) to Reisebank (Germany) in Seconds](#)
- [Japanese Bank Consortium Building a New Payments Network with SBI Ripple Asia](#)
- Non-public deals to provide interoperability between mobile money operators
2. Updated Details of the Solution

Speed, Reach and Funds Availability
Ripple is a real-time enterprise solution for payment companies ("Providers"), including banks, payment networks, and non-banks payment providers.

Ripple enables providers to send cross-border payments with transparency, speed and certainty. Ripple’s solution operates 24/7/365, settling payments in good funds in commercial bank money. Ripple settles gross payments or netted positions between providers. Section 3 of this paper discusses the commercial framework for these transactions.

The limiting factor is the operating window of the originating and beneficiary providers. If their systems do not process 24/7/365, they can establish operating windows that are indicated to other providers. This flexibility allows Ripple to accommodate institutions with a variety of system requirements, yet as providers’ ability to process cross-border payments 24/7/365 becomes increasingly standard, Ripple is ready to enable this functionality.

If the originating and beneficiary providers are both connected to Ripple, the payment is processed and settled within seconds – down from two to four days as is the standard for cross-border payments today. In this scenario, the payment is not bound by settlement windows at central banks or existing domestic rails. Ripple does not need to connect to an existing payment rail to settle transactions when both the originating and beneficiary providers are connected to Ripple.

Our initial proposal noted that speed of settlement between providers is within five seconds plus the time of the providers’ compliance processes. The time of the compliance process is a limitation of all cross-border payment services. This limitation is not unique to Ripple, rather it is reality of all systems, if one considers the compliance process part of the payment or not. As compliance requirements and processes vary by country and provider, any estimate provided would not accurately reflect the reality in all jurisdictions.

Once the provider has completed its compliance obligations, the time of settlement via Ripple is defined and can be made known to the end user. This varies greatly from the status quo, where the speed of the payment is not known and dependent on processes at several intermediaries that the originating provider does not have visibility into.

Ripple noted that the settlement between providers is known and within five seconds, yet the solution provides flexibility for the beneficiary provider to delay funds availability. This feature would not be necessary in a domestic payment system, where payments are subject one regulatory framework. However, this capability is necessary to allow providers in various countries to meet local compliance obligations. Ripple’s real-time tracking and delivery
confirmation features allow providers to have and deliver up-to-date information on the status of the payment.

This discussion assumes both the originating and beneficiary providers are using the Ripple solution. We recognize that this is not a realistic assumption in the early days of the network. However, Ripple does offer tangible benefits to cross-border payments so long as at least one provider is using Ripple in the sending and destination country.

The originating provider can send a payment over a domestic network to a Ripple-enabled provider also on the network. This Ripple-enabled provider can send the cross-border leg of the payment in 5 seconds to a Ripple-enabled provider in the destination country. The payment can be sent over a domestic network to the ultimate beneficiary provider. Despite the multiple hops to the payment, Ripple optimizes the cross-border leg adding speed and transparency to what is the slowest and opaquest leg of a payment today. The timing of the payment would be dependent on the settlement windows of the domestic networks, yet as domestic networks are increasingly faster, the total time of the cross-border payment is roughly T+1, down from two to four days.

Existing Ripple customers currently leverage this arrangement. One customer can reach every bank in the United States, United Kingdom and Europe (SEPA), with payment settlement and funds delivery occurring next day, down from three to four days per the provider’s previous arrangement. Payments made to counterparties also using Ripple are settled in seconds.

**The Providers’ Role in the Solution (Regarding Compliance and Security)**

Together, the Ripple technology and the provider enable a complete cross-border payment solution. The providers are responsible for onboarding consumers, fulfilling their Know Your Customer procedures and end user authentication requirements for payments. The details of many of these requirements are defined by the regulators in the provider’s jurisdictions.

Providers maintain their responsibility for compliance screening and transaction monitoring. The Ripple technology does not interact directly with end senders or receivers, rather it is designed to empower the providers to maintain the end customer relationships.

Upon receiving a payment request from a customer, the provider will screen the request to ensure the payment meets its compliance requirements. The provider holds the customer information, not Ripple. Upon the provider approving the transaction, it will be processed over Ripple.

Providers store the payment information themselves, per their own IT security and data management procedures. Ripple (the company) neither can access nor store the payment data. Data that is transferred between providers via the solution is encrypted and sent via HTTPS, but not stored by Ripple or the software. The storage is left to the individual providers, enabling
flexibility for providers in various countries to comply with their own IT security and data privacy regulations.

Ripple does supply guidance to providers on how to securely install and maintain the software. The installation of the software is typically done behind the provider’s firewall and subject to its IT risk and change management procedures. The software includes layered security, encryption, and cryptographic signature features that ensure the validity and privacy of data. Ripple’s account managers continuously engage with providers to ensure they have properly and securely installed and use the software.

Integration and Software Updates
Integration cost
Ripple views its payment system as a foundational platform upon which several value added services will be offered. Future value added services may include a liquidity sourcing and management service and customizable risk monitoring tools. These value added services provide primary opportunity to monetize the platform. Connecting providers and enabling global reach is a first and necessary step in building this platform.

Given these intentions, it is necessary to provide a variety of cost structures to ensure the solution is accessible and affordable for providers of different sizes and payment volumes.

Providers can license and integrate Ripple directly, an option well-suited for providers with sophisticated systems or seeking multiple uses of the platform. Alternatively, Ripple has partnered with several existing payment technology vendors to integrate Ripple into the services currently being licensed to providers. This is a cost-efficient option for providers with standard core systems or who have low payment volumes but still wish to offer cross-border service.

In addition to multiple integration models, Ripple has multiple cost models to accommodate large and small providers. Ripple offers a flat rate licensing option which includes unlimited payments by the provider, a fee per payment model, and a hybrid plan to meet the preferences of the provider.

Details on the governance and process of software updates
The governance of enterprise software is crucial for uninterrupted service and operational resiliency. Ripple has kept this top of mind in designing the product and software update process.

As noted in the original proposal, providers run a piece of software called “Ripple Connect” which enables them to connect to other counterparties. Ripple Connect is installed behind the firewalls of the provider, subject to the provider’s IT risk and vendor management standards. This software facilitates the messaging between providers; identifies the fees and status among participants in the payment; and coordinates the settlement between providers.
Ripple releases scheduled updates to Ripple Connect on a quarterly basis (4 per year). Hotfixes for any discovered security patches are issued on an ad hoc basis. Ripple follows a semantic versioning approach to upgrading our product (http://semver.org/).

To ensure uninterrupted service, all software releases are backwards compatible. It is not necessary that all banks run the same version of Ripple Connect or upgrade in unison for the solution to operate. Providers do not need to simultaneously update for compatibility; however, additional feature sets included in each release have incentivized clients to continuously upgrade. To ensure adoption and utility of new features, Ripple’s SLAs require clients to be no further than two releases behind the current version.

New releases are made available to providers via our partner-facing repository where they can download our software. The software is made available in a standard RPM. Banks are aware of our release cadence (quarterly) and are also notified by their account service representative when a release is posted to the partner repo. Our Client Services team assists with any upgrade questions or feedback.
3. Formation of a Governance Body and Payment Scheme

The initial proposal described Ripple's ability to support a variety of messaging standards and data fields. The flexibility allows a variety of providers (banks, non-banks, and networks) to use Ripple for multiple use cases.

While this flexibility offers great potential, it can also create fragmentation in the absence of any foundational coordination. To ensure common agreement on messaging, data and functional standards, for example, each provider could enter into bilateral contracts with each of its counterparties and agree to comply with such standards. However, requiring bilateral agreements between each provider can create complexity, introduce unnecessary transaction costs, and hinder broad scalability.

Ripple recognized this limitation. Over the past year, Ripple has helped establish a provider-run governance body to ensure consistent, interoperable use of the solution. The governance body maintains a scheme that contains (1) commercial rules and (2) technical standards for the execution of interbank payment transactions over Ripple technology.

The commercial rules provide a common understanding on how payments are settled, as well as the roles and responsibilities of a provider in connection with such settlement. The functional standards define messaging formats, which are based on standards defined by international standard-setting bodies such as the International Organization for Standardization (ISO). The functional standards are designed to ensure compatibility with many banks’ existing cross-border payment procedures. Member providers must follow these rules and standards, with the governance body responsible for enforcing compliance.

This payment scheme obviates the need for participants to create bilateral agreements with each and every one of their counterparties. Rather, a provider need only execute a single agreement with the governance body, under which it agrees to adhere to the payment scheme. Thus, upon integrating Ripple, a provider may join the payment scheme and adopt the framework, enabling interoperability with all other institutions that are following the payment scheme. The payment scheme has a membership structure designed to ensure accessibility regardless of the size or complexity of the provider.

Details of the structure, members, and terms of the governance body were not yet public at the time of this submission. Yet, this payment scheme ultimately lays the groundwork for effective provider-run governance that enables ubiquity and interoperability among Ripple-enabled institutions.

Details Regarding the Commercial Rule Set

The commercial rule set provides the well-defined, basic foundation for providers to transact with each other using Ripple technology. At the same time, the commercial rule set allows for
flexibility among individual providers in the particular service features they choose to provide to the end users --- the payer and payee.

It clearly defines the legal roles and responsibilities of providers with respect to their interbank payment activity using Ripple technology, consistent with any applicable law in relevant jurisdictions. It also provides providers clarity and certainty as to their rights and obligations vis-à-vis each other, including when they arise and when they are extinguished.

More broadly, the legal certainty provided by the commercial rule set facilitates transactions between providers over Ripple technology, enhances transparency and accountability, and establishes trust for transaction participants.

The commercial rule set provides a framework for providers using Ripple technology for interbank payments, including in the following areas:

➔ Authorization of transaction counterparties,
➔ Communication and exchange of transaction information between providers,
➔ Acceptance, rejection, cancellation, expiration, and enforceability of payment messages,
➔ Posting of F/X orders and cancellation of orders,
➔ The obligation of a sending bank to pay a receiving bank for an accepted payment message,
➔ The obligation of a receiving bank, upon acceptance of a payment message, to pay or cause another bank to pay the beneficiary,
➔ Liability for erroneous payment messages, and
➔ Other miscellaneous issues.

A key guiding principle in developing the commercial rule set was the Principles for Financial Market Infrastructures, issued by the Committee on Payments and Market Infrastructures and Board of the International Organization of Securities Commissions --- particularly Principle 1 regarding legal basis (“An FMI should have a well-founded, clear, transparent, and enforceable legal basis for each material aspect of its activities in all relevant jurisdictions”).

Accordingly, the commercial rule set is based upon the Model Law on International Credit Transfers (adopted by the United Nations Commission on International Trade Law in 1992), which was drafted to establish greater legal certainty and internationally harmonize the law relating to cross-border credit transfers. The commercial rule set also draws from Article 4A of the Uniform Commercial Code (which has been adopted by all 50 U.S. states), with a focus on Article 4A’s provisions relating to interbank rights and obligations.

International banking industry standards and practices for funds transfers were also considered. The commercial rule set takes those bodies of law as a starting point, with appropriate adjustments for the Ripple payments framework and local law applicable to providers.
Details Regarding Messaging Formats
The governance body’s technical standards outline the messaging format to be used amongst participants. The format builds off traditional messaging standards to ensure minimal integration effort for participants. The information captured in the messaging is largely based on an MT103 with the ISO 20022 pacS structure and nomenclature.

Ripple’s messaging functionality allows for extensibility, capturing additional payment metadata as well as the original message the payment was originated from. This gives providers the opportunity to enter additional information regarding a payment that they could not previously.

This unique functionality gives providers the ability to have back-and-forth conversations about payments, either manually, by human intervention initially, or automatically using systems. Dynamic conversations such as these are useful for situations when account numbers are incorrect or compliance concerns have arisen.
4. Unique Realities of a Cross Border Payment Solution

There are several unique considerations that must be made when reviewing a cross-border payment solution. The assessment must reflect the realities of cross-border payments, which may vary greatly in some instances from the expectations of a domestic payment system.

Requiring one standard for user experience, regardless of the provider’s jurisdiction, is not feasible in a cross-border system in the way it is in a domestic system as each country has unique standards, regulations and compliance requirements.

This section addresses primary areas that require proper context and consideration: end-user experience, fee disclosure, payment status notifications and fraud functionality.

Addressing End-User Experience, Fee Disclosure, and Payment Status

Flexibility is a Necessity in Cross-Border Solutions
When assessing aspects such as uniform end-user experience, fee disclosure and the sender’s visibility into payment status, one must consider the different realities that exist in cross-border scenarios than in domestic systems.

Domestic payment solutions are generally governed by only one primary regulatory framework, with secondary considerations for some state-specific items. For instance, initiation and authorization would be designed to reflect one primary set of regulations (i.e.: consumer protections rules, disclosure requirements, and fee schedules). Given one primary framework, domestic solutions can easily require and ensure a consistent experience that complies with all regulatory requirements.

However, a cross-border solution must weigh the regulatory requirements of all the jurisdictions within its reach. Given the wide variance in requirements regarding fee disclosure; control and transparency of the payment; consumer protections; and release of funds to the recipient, requiring a standard that complies with all jurisdictions’ laws is unlikely. For this reason, historically, there has been no uniform experience or expectations for cross-border payments.

Further, Ripple supports a variety of use cases: P2P and B2B payments as well as low-value and high-value payments. Requiring one uniform experience across a variety of use cases will not effectively meet the needs of different customer types; a customized experience is needed to best suit the characteristics of each type of payment.

Taking into account these realities of cross-border payments, it is neither feasible nor appropriate for Ripple to require a uniform end user experience, or enforce one country’s rules on providers in other jurisdictions. Rules requiring fee pre-disclosure or visibility of payment
status vary by country. No standard exists. With this in mind, Ripple was designed with
flexibility, transparency and access to data that allows the providers to fully meet the regulatory
requirements in their own respective jurisdictions.

Given different regulatory requirements and use cases, a flexible framework and end user
experience is a necessity for providers to be able to fully meet their compliance obligations. For
this reason, Ripple focused on a design that provided the necessary flexibility providers in
different jurisdictions need to comply with their own laws.

**Recognizing Improvements In User Experience**

While standardization of user experience is not appropriate for cross-border payments, the
assessment should give consideration to the improvement in user experience that the solution
enables.

Today, cross-border payments are sent via a relay process across several intermediaries. Each
intermediary takes a fee and processes the payment by its own procedures. The fragmented,
inconsistent process is opaque, providing no visibility to the providers, sender or receiver. For
payments processed through correspondent banks, the originating bank (and the sender) do not
know the cost breakdown, timing of delivery, status of the payment or amount of funds that will
be delivered to the recipient.

The lack of transparency has created a poor user experience for cross border payments.
Further, the lack of cost data has hindered banks in the United States from easily complying
with fee pre-disclosure requirements that were enacted as part of the Dodd-Frank Wall Street
Reform and Consumer Protection Act. While regulatory requirements that ensure consumers
understand fees exist, providers are not easily or fully able to comply due to the lack of
information about the payment.

Ripple was designed to provide transparency and certainty, enabling providers to offer a far
improved end user experience. While the experience is not standardized for the reasons
discussed above, providers do know the total cost of the payment, the timing of the delivery,
and the exact amount of funds that will be delivered before initiating the payment. Once the
payment is initiated, providers have visibility into the status of the leg of payment processed
over Ripple.

The providers that are integrating Ripple today are incorporating this data into their product to
create a superior customer experience. Providers in the United States (and other jurisdictions)
are taking advantage of the cost information they now have available to them to more fully and
easily comply with fee pre-disclosure requirements for the first time.

Altogether, Ripple offers the transparency and certainty that allows providers to offer a vastly
improved user experience, with the flexibility needed to meet regulatory requirements across a
variety of jurisdictions. The design of transparency and flexibility were intentional, reflecting the unique realities of cross-border payments.

**Addressing Fraud and Information Sharing**

**The Realities of Cross-Border Payment Fraud Today**

Today, the fragmented relay process used for cross-border payments creates opportunities for fraud to occur. For instance, contextual data can be removed from the message midway through the payment chain to redirect funds, hide a portion of the payment path, or avoid triggering a sanctions or compliance alert. This is referred to as wire stripping, one of the more well-known frauds in cross-border payments.

The lack of transparency creates challenges to identifying fraud when it has occurred. Piecing together the payment paths, messages, and ledger records of all intermediaries in a payment is a challenging process. Respondent banks typically have to pay audit fees for their correspondent banks to provide payment information. Not only is the investigation timely and complex, it is also expensive for providers.

Given that information about a single payment is distributed across many intermediaries, fraud information sharing today is crucial in seeing the complete picture.

**Ripple: Designed to Limit and Easily Identify Fraud**

Ripple replaces the fragmented relay process with a coordinated, transparent approach for providers using the solution. Regardless of whether the transaction is direct between two providers or a multihop payment between multiple parties, the payment path over Ripple is known in advance by all participants.

Ripple synchronizes the transaction across all parties. By replacing the relay process with a transparent, coordinated process, Ripple eliminates opportunities for banks to alter payment information and commit wire stripping (or, in Ripple’s case, remove information from the transaction messaging layer). Ripple’s design limits the opportunity for fraud, enabling a safer financial system.

If fraud were to have occurred, Ripple provides transparency needed to easily investigate the incident. The providers have on hand a complete record of the transaction information, including the messaging content and path of the payment. By not having to piece together information from various intermediaries, Ripple enables providers to have a more efficient and timely investigation process, without the cost and reliance on others to provide necessary payment path information.

As previously mentioned, Ripple’s messaging function includes certain flexible, open-ended fields and enables a two-way conversation between banks. This functionality may be useful in
identifying and potentially resolving fraud issues. Use of this functionality will likely be manual in
the early days of adoption. As providers become more sophisticated and the governance body
defines additional expectations for use of open-ended messaging fields, this functionality is
expected to become increasingly automatic.

Ripple reduces the likelihood of some more common fraud techniques and provides greater
transparency to investigate fraud when suspected. Yet information sharing across participants is
still important in identifying fraud trends that may be occurring at the system-wide level. The
governance body discussed earlier is especially well-suited to aggregate fraud information from
participants, identify trends and communicate information back to participants.

Reducing the likelihood of fraud and providing greater transparency for investigations, paired
with the governance body’s ability to facilitate high-level information sharing fosters a safer
cross-border payment solution.
5. The Path To Interledger

From our early days, Ripple’s mission has been to make cross border payments truly efficient. Our initial work and product was centered around the use of a distributed ledger (“blockchain”). We completed 30 pilots with a number of global payment providers and in the process learned a great deal about the benefits and limitations of distributed ledger technology.

Unlike today’s correspondent banking system which creates many opportunities for delays and errors, distributed ledger technology streamlines the payment path by coordinating transactions directly between providers. This synchronization between providers ultimately results in a process that minimizes settlement risk for all parties involved.

Speed of payments is significantly increased with distributed ledger technology as funds can be processed and settle in a matter of seconds - a vast improvement over the current 2-4 day settlement period. From a security perspective, unlike the opaque relay process in correspondent banking, distributed ledger technology allows for complete transparency into the payment flow, giving providers, customers, and regulators full disclosure as to where the payment lies along its path to settlement. It became clear to us during our pilot phases, that blockchain technology creates a faster, more efficient, truly global payments network.

However, this technology also presented a series of limitations. At its core, a distributed ledger solution is a network, meaning it suffers the same challenges faced by existing networks: scalability, privacy and interoperability. As global payments grow in volume, distributed ledger technology becomes harder to scale. The technology does not allow for that kind of interoperability which is the key to a scalable network of global providers.

Partners also requested increased privacy than a distributed ledger solution provided. While no customer data or personally identifiable information was visible on the distributed ledger, partners wanted to limit visibility to the parties directly involved in the transaction. It was important to us to address these concerns and limitations when building a more functional and effective solution.

This feedback and awareness of the drawbacks of distributed ledger technology led us to the Interledger protocol. Instead of connecting banks via a shared ledger, Interledger is a protocol that connects banks’ ledgers directly. Interledger is a set of instructions that allows banks to coordinate debits and credits with certainty, visibility and efficiency. Interledger is an open protocol being worked on within the W3C, the standards body for the World Wide Web.

With distributed ledger technology, payment instructions are sent from the ledger back to the providers to appropriately debit and credit their accounts. With Interledger, those instructions remain, but are no longer tied to a ledger, rather, operate in the form of a protocol directly
between the providers. Interledger successfully encapsulates the strengths of distributed ledger technology while circumventing the limitations of a shared ledger.

Interledger effectively eliminates the issues that come hand in hand with distributed ledgers, allowing providers and payment systems to interconnect with one another. Interledger sets the foundation for a scalable, interoperable global payments system.

The Role of Distributed Ledger Technology with Digital Assets
While Ripple does not feel that a distributed ledger is the best tool for fiat-to-fiat payments, it is well suited for an important use case: transacting digital assets.

In our initial proposal, we describe how providers can use multi-hop payments through a bridge network or bank to expand reach. One such bridge network that can be used is a distributed ledger where a digital asset, such as Ripple’s native asset XRP, can be used in transactions. XRP enables providers to have global reach without requiring the high costs of pre-funding nostro accounts around the world.

Providers use a digital asset like XRP to transact directly with counterparties, without the cost of holding an account or funds in other countries. This enables providers to make payments globally from capital held solely in their domestic country.

XRP is an independent digital asset – meaning it is not pegged to any fiat currency or issued by one or a group of entities. Trades of XRP on the open market determine its price. It is convertible into whatever fiat currencies traders are willing to quote an exchange for.

The design of an independent digital asset is essential for cross border payments, as it is not contained to any one country or tied to any particular currency. This allows XRP to be truly global in reach.

Alternative approaches have been considered by others in the market, yet we see limitations that make them ill suited for cross-border payments. Some have considered a digital asset that is issued by one entity, or group of entities, yet we expect this design will struggle to achieve adoption and reach outside of the founding entities. This design requires all users around the world to trust a select few parties who created the asset. While such a design could be viable for certain use cases, it will struggle to achieve scale and reach needed for a cross-border payment tool.

Another option floated has been a digital coin that is backed by cash. Yet, backing a coin with cash makes it a liability, not an asset. This is a crucial difference, as trading liabilities requires moving cash across borders for final settlement, re-creating today's fractured system but with added friction.
Ripple's experience with distributed ledger technology, progression to a protocol solution and development of an independent digital asset altogether enable a scalable, secure, efficient system for cross-border payments.
Faster Payments QIAT

PRELIMINARY ASSESSMENT

**Proposer:** Ripple

**Summary Description of Solution:** Ripple uses Distributed Financial Technology (an open protocol called Interledger) to enable cross-border payments using direct two-way messaging between financial institutions (FIs) that join its network. The solution enables payers to see the total cost of the payment prior to authorization and settles transactions between FIs in real-time, 24x7x365.

It does so through several components. The first is “Ripple Connect,” a plug-and-play software module that FIs license and integrate into their payment hub or core ledger. The second is “FX Connector,” which holds accounts with two or more FIs, providing liquidity for cross-border transactions between those institutions. The third is the “Notary,” an entity that FIs select to confirm that debit and credit have successfully occurred across multiple FI ledgers. The Notary is based on a software package that confirms cryptographic status messages regarding payment issues by Ripple Connect.

Ripple has helped establish a provider-run governance body to maintain a scheme that contains 1) commercial rules, and 2) technical standards for the execution of interbank transactions over Ripple technology. Outside the scheme, providers need to develop bilateral agreements with every counterparty. Within the scheme, providers integrate Ripple and adopt the scheme framework to enable interoperability with other providers participating in the scheme.

While the assessment of the Ripple proposal was conducted against the same Effectiveness Criteria applied to all other proposals, the QIAT acknowledges the differences in starting points between cross border and domestic payments that impacts criteria such as user experience.

EXECUTIVE SUMMARY OF THE PROPOSAL

- **Major strengths**
  - If the originating and beneficiary provider are both on the Ripple Network, then the solution processes and settles payment within 5 seconds plus the time of the provider’s compliance processes
  - The solution bolsters the certainty of the cross-border payment experience by providing end-to-end transaction visibility to banks, as well as settlement confirmation. Ripple enables more transparency in the total cost of a payment to the payee prior to authorization, if participating banks are willing to provide this transparency. However, effective transparency will depend on how participating banks deploy the solution to end users.
  - The solution facilitates additional liquidity options, as banks can use their own liquidity to fund payments but can also access liquidity through a competitive marketplace, wherein Ripple would select the authorized provider with the lowest-cost FX
  - The solution is flexible enough to be integrated directly into an FI’s payment hub, or it may be integrated into a third-party provider’s platforms to which FIs are already connected

- **Areas for improvement and enhancement**
  - The solution does not address common standards and processes across FIs. This will present a challenge to the solution’s ability achieve the user experience and speed of payments outlined in the proposal, particularly as FIs have control over many elements of the end-to-end payment process (e.g., authentication, availability of good funds, notification to end users). However,
the new provider-run governance body should now help solve this through a commercial rule set, though further details are not yet available.

– More detail is needed on how the solution will address cross-border differences in messaging formats, processing rules, regulatory issues and conflicts across countries such as consumer protection and data privacy.

– Ripple cannot access transaction data, which promotes privacy but prevents network-wide fraud monitoring unless the FIs choose to participate. In addition, dispute-handling rules are not specified in the proposal, although it does refer to a participation agreement and commercial framework that governs the relationship between Ripple and participating FIs.

■ Use cases addressed

– The proposal focuses on the cross-border payment use case, including low-value remittance payments (P2P), international corporate payments, international transaction banking payments services, and cross-border intra-bank currency transfers.

■ Proposer’s overall ability to deliver proposed solution

– Ripple has 30 pilots at FIs globally, with access to over 60 currencies through channel partners. However, no deployment at scale has been completed to date.
Ubiquity

U.1 Accessibility

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

Ripple facilitates payments to/from all types of payment accounts in the FIs that are part of the network (U.1.1). Ripple supports payments from both banks and Regulated Non-bank Account providers (e.g., Western Union). Payments through the solution can reach any and all payees, as long as there is one Ripple-integrated FI in the payer’s country (other FIs first send to the Ripple-integrated FI through existing domestic payment systems) and one in the payee’s country (the Ripple-integrated FI sends funds over the existing domestic payment systems to the payee) (U.1.2). While Ripple does not facilitate domestic payments to/from all accounts for the cross-border use case addressed in the proposal, by focusing on cross-border, the solution supports multi-currency payments (U.1.3). Ripple outlines a plan for widespread adoption by starting with an indirect access model (with only one FI integrated with Ripple), moving to a direct access model over time (FIs access Ripple directly through their own integration or use of a payment services that becomes Ripple-enabled), and then moving to the use of multi-hop payments to scale and reach FIs that do not have common connectors (U.1.5).

The solution demonstrates technical feasibility for providers to adopt it through examples of FIs that are live; providers are motivated to participate by the benefits of improved transparency and speed in cross border payments. Integration will require providers to change processes and operating systems, to build new functionalities (e.g., escrow accounts) (U.1.5).

U.2 Usability

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

Ripple’s technology enables FIs to provide cross-border payment services to customers. An FI can use Ripple to provide a straightforward, simple End User experience using a variety of access across channels, devices, and platforms as decided by the FI (U.2.1). Ripple is accessible 24x7x365 (U.2.3).

Ripple does not provide the above functionalities and capabilities itself; it relies on its providers to do so (U.2.1, U.2.3). FIs have a great deal of flexibility in how they provide Ripple to customers and determine how to provide a user-friendly experience to customers. This flexibility for FIs is intentional in order to accommodate the different regulatory requirements by country for cross border payments. Although the solution is available 24x7x365, the provider FI can establish its own operating hours for sending and receiving payments. The FI also controls how well varying levels of End-User technological proficiency and usability needs are addressed (U.2.4).

Additionally, Ripple does not address enablement of payment with limited information or minimum requirements for authentication. No directory is provided as part of the solution (U.2.2).
U.3 Predictability

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale:
Ripple provides predictability to the FI for how payments are processed in its baseline core features (U.3.1). The solution’s design ensures delivery of the baseline features and communication of those features to providers (e.g., cost of payment prior to payer authorization); providers are then responsible for delivering baseline features to end users (U.3.2). Standard communication protocols through the Interledger protocol are used and a consistent message format is determined by the provider-run governance body established to ensure consistent, interoperable use of the solution (U.3.3). Since the FI is responsible for the End User’s experience, Ripple itself cannot ensure reliability or standardization in that experience; however the commercial ruleset provides a way to do so through provider agreement (U.3.4).

However, the solution does not define error resolution protections, rights and liabilities, indicating the commercial rule set may do so (U.3.5). The solution also does not provide a generic, brand-agnostic term to distinguish the solution from other payment systems (U.3.6).

U.4 Contextual data capability

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale
Ripple supports the transfer of information to end-users by enabling messaging functionality to share contextual payment data, fees, and confirmations of acceptance and delivery (U.4.1). Ripple has helped establish a provider-run governance body to maintain a scheme that includes technical standards for the execution of interbank payment transactions over Ripple technology. This body defines the message format based on standards defined by international standard-setting bodies (U.4.3).

The proposal would benefit from providing more detail on the integration of contextual data with interfacing business and personal finance systems (U.4.2).

U.5 Cross-border functionality

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale:
Ripple enables FIs the ability to operate cross-border payments faster than the 2-4 days common today, if the originating and beneficiary providers are both connected to Ripple (U.5.1). The solution enables interoperability with other Real-Time Payment systems in other countries by using domestic networks when the originating and/or beneficiary provider is not on the Ripple network (U.5.2). Ripple enables visibility into the fees and FX cost before the payer authorizes the transaction (U.5.3) and relies on the commercial ruleset to ensure FIs make the advance disclosure. Ripples provides an FX quote and fees through an FX Connector (third party FX providers) or an FI’s own liquidity (nostro and vostro accounts) for conversion from one currency to another (U.5.4).
U.6 Applicability to multiple use cases

<table>
<thead>
<tr>
<th>Rating</th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

Rationale:
The solution focuses solely on the targeted use case of cross-border P2P and B2B payments. It may also be extensible to domestic payments, though the proposal does not describe this use case.

Efficiency

E.1 Enables competition

<table>
<thead>
<tr>
<th>Rating</th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

Rationale:
Ripple allows users to have a choice of providers same as today (E.1.). End Users that switch providers can continue to use Ripple if the FI participates in the network. The commercial ruleset ensures disclosures (E.1.3). All providers are allowed to provide services as long as they meet participation requirements (E.1.4).

However, the solution would benefit from more detail on how it allows entities to easily switch or use multiple providers (e.g., receive money using the Ripple network to payment accounts at different FIs) (E.1.2).

E.2 Capability to enable value-added services

<table>
<thead>
<tr>
<th>Rating</th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

Rationale:
Providers integrate with the solution using RESTful APIs. Providers, regardless of size or incumbency, can offer value-added services as long as they meet participation requirements (E.2.1, E.2.2). Future value added services may include liquidity sourcing and management service and customizable risk monitoring tools. The solution enables providers to disclose to customers that value added services are optional (E.2.3).

E.3 Implementation timeline

<table>
<thead>
<tr>
<th>Rating</th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

Rationale:
To achieve faster cross-border payments, Ripple needs to connect to a network of banks, with at least one FI in each country. Ripple has completed 30 pilots at FIs globally and has 90 active customers in the pipeline, 10 commercial deals underway, and channel partners’ enabling access to over 60 currencies. However, there has not yet been a commercial deployment at
scale. In addition, further details are needed on funding, hurdles, which entities are expected to adopt the solution first, market share, and growth projections (E.3.1).

### E.4 Payment format standards

<table>
<thead>
<tr>
<th>Rating</th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

Ripple supports a variety of messaging standards but does not set a particular standard for use (E.4.1). The provider-run governing body will define the messaging format, based on standards defined by international standard-setting bodies (E.4.5).

More clarity would be helpful on the exact message format the governing body intends to use. In addition, the proposal does not describe the mechanism for updates to message formats to facilitate innovation (E.4.4).

### E.5 Comprehensive

<table>
<thead>
<tr>
<th>Rating</th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

The solution focuses on clearing and settlement. In concert with FIs, which are responsible for the other aspects of the end-to-end payment process, it is able to deliver an end-to-end payment process from initiation to reconciliation (E.5.1). The solution’s technical design supports all of its features (E.5.2).

### E.6 Scalability and adaptability

<table>
<thead>
<tr>
<th>Rating</th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

The technical design supports the projected use cases focused on cross-border payments (E.6.1). Ripple governs the closed network and can provide updates to adapt technical design to ongoing developments through upgrades to the Ripple Connect software 4 times a year with backwards compatibility (E.6.3).

Further detail would be helpful on the projected transaction volumes and how the solution supports those volumes and values under peak times or periods of stress (E.6.2).

### E.7 Exceptions and investigations process

<table>
<thead>
<tr>
<th>Rating</th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

Ripple provides transaction data to FIs with each payment for full visibility and its messaging function includes flexible, open-ended fields that enables a two-way conversation between banks that could be used in identifying and potentially resolving fraud or other issues.
The solution does not, however, provide any other tools, messages, alerts, or notifications to help address exceptions (E.7.1). FIs must each handle their own investigations and exception-handling process and find ways to resolve disputes with other FIs (E.7.1, E.7.2). Since Ripple does not see the transaction data, it does not record or retain this information or aggregate exceptions data to spot patterns (E.7.2, E.7.3).

Safety and Security

S.1 Risk management

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

Rationale:
The proposal refers to a participation agreement and commercial rules that include a risk framework. The participation agreement and commercial framework cover commercial matters (including roles, responsibilities, rights and obligations, including FI rights and liabilities, when using Ripple) but the details provided on the commercial rule set would benefit from further clarity on the risk management aspects.

S.2 Payer authorization

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

Rationale:
Payers authorize to their FI with each payment initiation (S.2.1). Payment authorization occurs in the same channel in which the payer initiates the transaction and Ripple enables visibility into the fees and FX cost before the payer authorizes the transaction, though the enforcement of this user experience through operating rules is not clear. The solution does not address pre-authorization of payments (S.2.2, S.2.3).

S.3 Payment finality

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

Rationale:
Instead of the FI, a notary confirms the accuracy of the cryptographic signatures that indicate that the payment is fully funded in each escrow account, and thus that there are good funds. The payment becomes irrevocable once the notary approves. Following approval, the FIs will receive Interledger instructions to release funds from their respective escrow accounts (S.3.1, S.3.2).

However, no mechanisms or processes are defined for protecting or compensating the payer in the event that the payment is disputed beyond compliance with consumer laws (S.3.3).
S.4 Settlement approach

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale:
The Ripple solution settles in commercial bank money (S.4.3) using synchronized transactions on the books of the originating and beneficiary FIs through the Interledger protocol. Within the Ripple system and using the same liquidity provider, this real-time gross settlement can occur in less than one second. It is up to the FIs or the governing body to use real-time gross settlement or deferred net settlement to exchange value with the Ripple liquidity providers; it is also up to the FI to define terms, risk limits, and settlement periods and operating hours (S.4.1, S.4.3).

The commercial rules provide a common understanding of how payments are settled, but more clarity would be helpful on how the solution manages credit and liquidity risk arising from the use of commercial bank money in settlement and in cases of deferred net settlement that causes a lag between transaction finality and settlement (S.4.3).

S.5 Handling disputed payments

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale:
Similar to S.1, the proposal refers to a participation agreement and commercial framework that define the process, rights, and obligations for addressing disputed payments between FIs, but no further detail is provided on each sub-criteria. In addition, the proposal does not describe mechanisms for any party to the transaction to request prompt voluntary return of funds from the Payee (S.5.3).

S.6 Fraud information-sharing

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale:
Ripple reduces the likelihood of some common fraud techniques and provides greater transparency to investigate fraud. The solution facilitates information sharing that supports management and monitoring of fraud through Ripple Connect, which consolidates payment information in a user-friendly format to allow FIs to share contextual and fraud information if they so choose (S.6.1).

However, Ripple does not see transaction data and does not require providers to share information in order to manage and monitor fraud (S.6.1). Ripples does not aggregate, manage or protect data owned by entities other than providers for purposes of Fraud information sharing (S.6.2). Ripple does not provide timely updates and alerts for fraud (S.6.3). In the solution, FIs are responsible for fraud detection, reporting, and resolution of the transactions they process. Ripple does not have information sharing mechanisms through a central authoritative trusted source to support differential access to content or to aggregate Fraud information to spot patterns (S.6.5-S.6.7). The provider-run governance body could choose to aggregate fraud information among participants to spot patterns (S.6.7).
S.7  Security controls

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

Rationale:

The traffic between Ripple Connect and FIs is encrypted and occurs over secure HTTPS (S.7.1). Much of the security, such as data retention and disposal controls, relies on FIs (S.7.2).

Additional detail would be helpful on the other sub-criteria including technical access components and controls – how the solution can ensure data encryption, quality and integrity controls, data breach prevention and detection, layered security controls, operational and procedural components and controls – physical security, operations security and monitoring, and Ripple’s managerial policies and oversight - adaptability to enterprise-level security architectures, motivation of investments by all Parties to improve the security of each transaction. The commercial rule set developed by the governing body could cover these topics but not detailed.

S.8  Resiliency

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

Rationale:

The solution uses distributed financial technology, which means that there is not a central operator or single point of failure in the solution. If one participant goes offline, that does not affect the ability for other institutions to continue to transact.

However, the proposal does not address target availability metrics, business continuity and disaster recovery plans, mechanisms to minimize the chance of triggering systemic risk, the resources devoted to business continuity and resiliency and regular contingency testing across all operators and providers within the Ripple network (S.8.1-S.8.5).

S.9  End-user data protection

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

Rationale:

The solution does not have requirements for end-user data protection outside of the data transferred by Ripple Connect between the FIs, which is encrypted and occurs over secure HTTPS connections using OAuth 2.0 for authentication (S.9.1).

End user data information at rest is the responsibility of the FI and the protection of sensitive information needed for account set up, transaction setup, problem resolution, and to process and complete a payment is all determined by the FI. Ripple does not define requirements for provider controls or mechanisms to protect sensitive information and does not provide a mechanism for enabling payers and payee to transact without knowing one another’s account number (S.9.1-S.9.3). The commercial rule set developed by the governing body could cover these topics but not detailed.
S.10 End-user/provider authentication

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

Rationale:

FIs are responsible for end-user authentication and for due diligence on other FIs to which it wants to send money without any Ripple-imposed minimum requirements (S.10.1). This due diligence includes assessing the onboarding and compliance policies of the counterparty. The payment scheme run by the governing body is likely to develop authentication requirements but further details would be helpful.

The solution does not describe mechanisms to ensure the payment reaches the intended Payee Account, to apply strong Authentication procedures based on the risk-weighting of a transaction (this is up to the FI), and does not describe how new Authentication models are adopted and old models decommissioned (S.10.2-S.10.6).

S.11 Participation requirements

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

Rationale:

A commercial rule set governs commercial matters pertaining to the solution, including roles, responsibilities, rights, and obligations (S.11.1, S.11.2).

The proposal would benefit from further detail on the process to monitor and ensure compliance by all providers against these requirements that providers must meet (S.11.3).

Speed (Fast)

F.1 Fast approval

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

Rationale:

The Ripple technology supports approval within two seconds when both the originating and beneficiary providers are using the Ripple solution since the originating FI can use Ripple Connect to determine the FX Connector with sufficient liquidity available for payment within milliseconds. However, Ripple does not describe operating rules to enforce fast approval, nor to ensure 2x7x365 operations.

F.2 Fast clearing

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

Rationale:

The Ripple technology supports clearing within five seconds when both the originating and beneficiary providers are using the Ripple solution. The clearing process occurs between the FIs through Ripple Connect over HTTPS typically within five seconds. The two FIs share payment
information and determine fees, FX rates and delivery times. However, Ripple does not describe operating rules to enforce fast clearing – it would be under the purview of the governing body.

F.3 Fast availability of good funds to payee

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The Ripple technology enables immediate availability of good funds when both the originating and beneficiary providers are using the Ripple solution, but allows FIs to delay funds’ release (hold the funds after settlement for a period of time) to the payee to protect against unauthorized, erroneous, or fraudulent payment. Ripple does not describe operating rules to enforce fast availability of good funds to the Payee – it would be under the purview of the governing body.

F.4 Fast settlement among depository institutions and regulated non-bank account providers

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The Ripple technology enables real-time gross settlement or deferred settlement in commercial bank money within 5 seconds plus the time of the provider’s compliance processes when both the originating and beneficiary providers are using the Ripple solution. Ripple does not describe operating rules to enforce fast settlement – it would be under the purview of the governing body.

F.5 Prompt visibility of payment status

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The Ripple technology supports tracking of the payment at various stages of the payment process with visibility of status within five seconds. FIs use Ripple Connect and the payment ID to track the status of the payment in real time and update the payer and payee as to that status. Ripple does not describe operating rules to enforce prompt visibility of payment status to the Payer and Payee – it would be under the purview of the governing body.

Legal

L.1 Legal framework

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>
**Rationale:**
The solution relies on FIs’ legal frameworks. The proposal provides no detail on the solution’s participation agreements and commercial rules as they pertain to its legal framework.

The proposal acknowledges a need for a Legal Framework, but it is not yet complete. The QIAT has interpreted the Effectiveness Criteria such that solutions at this stage of development earn a rating of “Somewhat Effective.”

**L.2 Payment system rules**

Very Effective  Effective  **Somewhat Effective**  Not Effective

**Rationale:**
The solution generally relies on FIs’ legal framework and more detail would be helpful on its commercial rules as they relate to payment system rules. Key features of the payment system rules—such as payment finality—can be inferred from the proposal, but detail is not available on error resolution and other aspects of payment system rules.

The proposal acknowledges a need for Payment System Rules, but they are not yet complete. The QIAT has interpreted the Effectiveness Criteria such that solutions at this stage of development earn a rating of “Somewhat Effective.”

**L.3 Consumer protections**

Very Effective  Effective  **Somewhat Effective**  Not Effective

**Rationale:**
The solution generally relies on FIs’ legal framework. As the consumer payer and payee remain customers of the FI, the consumer laws that apply to FIs remain applicable. The proposal does not provide details on the solution’s commercial rule set as they pertain to consumer protections. The solution does not address how consumer protection laws can be met cross border, particularly when there are different regulations and requirements by country.

**L.4 Data privacy**

Very Effective  Effective  **Somewhat Effective**  Not Effective

**Rationale:**
FIs determine the payer and payee information required to ensure compliance with its own procedures and jurisdiction’s laws (L.4.1). The Ripple participation agreement and commercial framework define the permissible and restricted uses of personal data shared during the payment cycle though no details are shared. FIs are bound by this agreement (L.4.1). Data shared between FIs over Ripple Connect is encrypted (L.4.2).

The Proposal does not address how end-users can view the data that is collected on them (L.4.4), as well as the approach to data breaches at the Payment System or end user/provider (L.4.5). In addition, the proposal does not address how to manage and reconcile the diversity of data privacy rules by country.
L.5 Intellectual property

- **Very Effective**  Effective  Somewhat Effective  Not Effective

**Rationale:**
The solution has taken a due diligence review of intellectual property (IP) rights and is establishing procedures for third parties to bring any IP concerns to Ripple’s attention. Interledger, the open protocol used by Ripple, is an open-source standard and thus should remain free for everyone to use.

**Governance**

G.1 Effective governance

- **Very Effective**  Effective  Somewhat Effective  Not Effective

**Rationale:**
Ripple’s governance is defined by participation agreements and its commercial framework. It has helped establish a provider-run governance body to ensure consistent, interoperable use of the solution. However, details of the structure, members, and terms of the governing body are not yet public.

The QIAT has interpreted the Effectiveness Criteria such that solutions at this stage of development earn a rating of “Somewhat Effective.”

G.2 Inclusive governance

- **Very Effective**  Effective  Somewhat Effective  Not Effective

**Rationale:**
Ripple’s governance is defined by participation agreements and its commercial framework. The Interledger protocol’s governance is provided through the World Wide Web Consortium, which includes a broad set of participants. Ripple has helped establish a provider-run governance body to ensure consistent, interoperable use of the solution. However, details of the structure, members, and terms of the governing body are not yet public.

The QIAT has interpreted the Effectiveness Criteria such that solutions at this stage of development earn a rating of “Somewhat Effective.”
APPENDIX A: ASSESSMENT SUMMARY

|= QIAT Assessment ⊗ = Proposer Self-Assessment

### UBIQUITY

| U.1: Accessibility | ⊗ ☑ |
| U.2: Usability | ☑ |
| U.3: Predictability | ☑ |
| U.4: Contextual data capability | ☑ |
| U.5: Cross-border functionality | ☑ |
| U.6: Multiple use case applicability | ☑ |

### EFFICIENCY

| E.1: Enables competition | ☑ |
| E.2: Capability to add value-added services | ⊗ ☑ |
| E.3: Implementation timeline | ⊗ ☑ |
| E.4: Payment format standards | ☑ |
| E.5: Comprehensive | ⊗ ☑ |
| E.6: Scalability and adaptability | ⊗ ☑ |
| E.7: Exceptions and investigations process | ⊗ ☑ |

### SAFETY AND SECURITY

<p>| S.1: Risk management | ☑ |
| S.2: Payer authorization | ⊗ ☑ |
| S.3: Payment finality | ☑ |
| S.4: Settlement approach | ☑ |
| S.5: Handling disputed payments | | ☑ |
| S.6: Fraud information sharing | | ☑ |</p>
<table>
<thead>
<tr>
<th>SAFETY AND SECURITY (cont’d)</th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
<tbody>
<tr>
<td>S.7: Security controls</td>
<td>☐</td>
<td>☑</td>
<td></td>
<td>☑</td>
</tr>
<tr>
<td>S.8: Resiliency</td>
<td>☐</td>
<td>☑</td>
<td></td>
<td>☑</td>
</tr>
<tr>
<td>S.9: End-user data protection</td>
<td>☐</td>
<td>☑</td>
<td></td>
<td>☑</td>
</tr>
<tr>
<td>S.10: End-user/provider authentication</td>
<td>☐</td>
<td>☑</td>
<td></td>
<td>☑</td>
</tr>
<tr>
<td>S.11: Participation requirements</td>
<td>☐</td>
<td>☑</td>
<td></td>
<td>☑</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SPEED (FAST)</th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
<tbody>
<tr>
<td>F.1: Fast approval</td>
<td>☐</td>
<td>☑</td>
<td></td>
<td>☑</td>
</tr>
<tr>
<td>F.2: Fast clearing</td>
<td>☐</td>
<td>☑</td>
<td></td>
<td>☑</td>
</tr>
<tr>
<td>F.3: Fast availability of good funds to payee</td>
<td>☐</td>
<td>☑</td>
<td></td>
<td>☑</td>
</tr>
<tr>
<td>F.4: Fast settlement</td>
<td>☐</td>
<td>☑</td>
<td></td>
<td>☑</td>
</tr>
<tr>
<td>F.5: Prompt visibility of payment status</td>
<td>☐</td>
<td>☑</td>
<td></td>
<td>☑</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LEGAL</th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
<tbody>
<tr>
<td>L.1: Legal framework</td>
<td>☐</td>
<td>☑</td>
<td></td>
<td>☑</td>
</tr>
<tr>
<td>L.2: Payment system rules</td>
<td>☐</td>
<td>☑</td>
<td></td>
<td>☑</td>
</tr>
<tr>
<td>L.3: Consumer protections</td>
<td>☐</td>
<td>☑</td>
<td></td>
<td>☑</td>
</tr>
<tr>
<td>L.4: Data privacy</td>
<td>☐</td>
<td>☑</td>
<td></td>
<td>☑</td>
</tr>
<tr>
<td>L.5: Intellectual property</td>
<td>☐</td>
<td>☑</td>
<td></td>
<td>☑</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>GOVERNANCE</th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
<tbody>
<tr>
<td>G.1: Effective governance</td>
<td>☐</td>
<td>☑</td>
<td></td>
<td>☑</td>
</tr>
<tr>
<td>G.2: Inclusive governance</td>
<td>☐</td>
<td>☑</td>
<td></td>
<td>☑</td>
</tr>
</tbody>
</table>
APPENDIX B: PROPOSER RESPONSE TO QIAT ASSESSMENT

Ripple thanks the QIAT for their detailed review of our proposal, and we look forward to receiving Task Force feedback. Ripple has focused its proposal on solving the costs, delays, and risks that plague cross-border payments today.

In July 2016, the Bank for International Settlements noted these problems and the resulting decline in access to cross-border payment services.¹

"Until recently, banks have maintained a broad network of correspondent relationships, but there are growing indications that this situation might be changing. In particular, some banks providing these services are cutting back the number of relationships they maintain and are establishing few new ones." (pg. 6)

"One of the main drivers seems to be the growing tendency for banks to assess the profitability of their business lines, customers and even jurisdictions in a world where the cost of correspondent banking has increased and capital and liquidity are scarcer and more expensive. While the correspondent banking business seems profitable in aggregate, parts of this business are not and, as a result, correspondent banks have been dropping their less profitable customers or jurisdictions." (pg. 12)

"As a result, some respondent banks are likely to maintain relationships, whereas others might risk being cut off from international payment networks.” (pg. 1)

It is important to reflect these pressures in the assessment of Ripple and other cross-border solution proposals, as they differ greatly from the realities of domestic systems.

The BIS report highlights messaging and new technology, among others, as ways to reverse the decline in access to cross-border payment services. Ripple’s improved messaging capabilities, greater efficiency, and the ability for banks of all sizes to connect directly to other institutions addresses some concerns highlighted by BIS and potentially eases headwinds facing cross-border payments.

The QIAT’s initial assessment highlighted many advantages of the Ripple solution, including speed, certainty of payment status, and transparency into the total cost of the payment. These characteristics of Ripple are significant upgrades to cross-border payments.

However, there are two key areas where Ripple’s self assessment differs from the QIAT ratings: (a) the “Ubiquity” criteria and (b) items related to both the “Safety and Security” and “Legal” criteria.

Generally, the difference in ratings stem from updates to our proposal that were made public (non-confidential) after the time of submission and assessment. We provide the following updated details to justify our self assessment and urge reviewers to consider these points in their feedback.

I. Updates Impacting “Ubiquity” Criteria Assessments

Applicability for Multiple Use Cases
(related to U.6. Applicability to Multiple Use Cases)

Ripple is a cross-border solution designed to meet the criteria laid out in U.6. (“Applicability to Multiple Use Cases”). Ripple is flexible to support a variety of payment types.

Today’s cross border infrastructure was built to support high-value batch payments, meaning low-value cross border payments are expensive or not offered at all. Consumers and companies of all sizes are all looking to make low-value, high-volume payments feasible and cost effective for the first time.

Given this market demand, Ripple is currently being deployed at several providers with initial targeted use cases of low-value P2P and low- and high-value B2B.

Ripple is extensible to other payment types and is working with a pipeline of institutions to offer additional payment services, including B2P and P2B. The solution is flexible enough to fulfill each of the use cases outlined by the Effectiveness Criteria, as referenced on pages 15 and 16 of our initial proposal:

➢ B2B: A business pays a foreign supplier for components.
➢ B2P: An employer issues a paycheck to an employee; a company.
➢ P2B: A customer pays tuition to a university abroad.
➢ P2P: Remittance payments, including low-value payments.

Given Ripple’s targeted use cases and extensibility to all use cases highlighted by the Effectiveness Criteria, we have assigned a self assessment of “Very Effective.”

The feedback provided by the QIAT cites that Ripple does not address the domestic use case in our proposal. Item U.6. does not require domestic services, so this feedback did not explain the QIAT rating. While this proposal is focused on cross-border solutions for U.S. banks, Ripple can be used for domestic payments, particularly cross-network payments.
Usability
(related to U.2. Usability)

As providers are deploying Ripple to enable a variety of use cases around the world, flexibility in design is essential for there to be effective usability. The assessment of this criteria must take into consideration the global nature of Ripple, as designing usability in a cross-border solution differs greatly from that of a domestic solution where there is likely one dominant language and cultural understanding of technology.

As noted in the QIAT assessment, the provider continues to own the customer relationship and will integrate Ripple into its customer interface. Addressing U.2.1., Ripple’s flexible design allows it to receive instructions for payment from a variety of channels and devices including mobile, web interface, payment hubs, and providers’ platforms.

Regarding U.2.2., Ripple provides a messaging functionality that allows providers to initiate a payment with whatever information is acceptable to the originating and beneficiary institutions. This flexibility enables providers to define the information they require for initiation depending on payment type and reflecting the risk and regulatory requirements that vary by jurisdiction. The technology and commercial rules (discussed in the next section) are agnostic to the identification of the beneficiary (whether by account number or otherwise). Given the variety of use cases, cross-border nature of Ripple, and data privacy concerns that exist in a cross-border environment, Ripple does not include a directory, but does allow providers the flexibility to define the minimum information needed to initiate a payment.

Regarding U.2.4., by enabling the provider to own the customer relationship, the end-user experience is customized for the specific customer type – corporate or retail – and the cultural preferences of the region. Yet the underlying processing of the payment via Ripple is uniform across all providers. This design ensures certainty, transparency and speed of payment, with a customer experience that reflects jurisdictional regulatory requirements and cultural preferences. This balance is essential in a global solution that addresses many languages and a variety of technological proficiencies. With this design, Ripple is being deployed to support payments initiated across basic cellular phones in developing regions and advanced smartphones and web interfaces in developed countries.

Considering the variety of use cases and cross-border functionality of Ripple, we feel the solution meets or exceeds the effectiveness criteria for U.2.1, U.2.2 and U.2.4.

However, the solution does not guarantee end user accessibility on a 24/7/365 basis (U.2.3.) Ripple operates and processes payments 24/7/365, but the provider’s end user interface may not be accessible on this basis given its own system maintenance or down time. This is the one subcriterion under “Usability” that is not fully met due to the provider.

As three of the four subcriteria are fully met, with Ripple providing 24/7 functionality to enable the fourth subcriterion to be met, we have assigned an “effective” rating, as we mostly satisfy the criteria. We urge the QIAT and task force to reconsider or provide additional justification for a “somewhat effective” rating.
II. Updates Impacting “Safety and Security” and “Legal” Criteria Assessments

Announcement of Ripple Governance Body: Ripple’s proposal references the creation of a governance body that will manage crucial functions of the network. At the time of the proposal, the governance body was not yet public, limiting the amount of detail that could be shared.

On September 23, 2016, Ripple publicly announced the formation of this governance body: the Global Payments Steering Group (GPSG).2 GPSG is an interbank group that has created and will oversee the maintenance of Ripple payment transaction rules, formalized standards for activity using Ripple, and frameworks that promote scalable implementation as the network grows. The GPSG will ensure a common set of standards and protocols that maintain critical integrity and security. This allows providers to offer seamless service to customers across the globe.

GPSG’s founding members are Bank of America Merrill Lynch, Santander, UniCredit, Standard Chartered, Westpac Banking Corporation, and Royal Bank of Canada. GPSG is a tiered membership structure supporting the inclusion of other payment providers as they enter the Ripple network. CIBC will also join the GPSG as a new member.

The creation of the GPSG and its work products will have a direct impact on the “Safety and Security” and “Legal” criteria, among others. Specifically, the GPSG justifies our self assessment ratings for risk management, security controls, end-user data protection and data privacy; legal framework; payment system rules; and effective governance.

We share the following information for consideration and support of our self assessment ratings.

Legal Framework and Payment System Rules

The commercial rules developed by Ripple in collaboration with the GPSG provide the well-defined, basic foundation for providers to transact with each other using Ripple technology -- and the rules have been implemented by members of the GPSG. Although the commercial rules themselves are confidential by their terms, a summary of the substance of key provisions follows. The intent in sharing this summary is to provide a high-level view of certain key concepts to ensure an accurate assessment rating.

Defined terms include the following key parties:

The framework and rules define key parties referenced in Ripple’s original proposal to provide contractual agreement and certainty. Key parties include:

➢ Receiving provider (the provider to which a sending provider’s payment instruction sent over Ripple technology is addressed)

---

2 https://ripple.com/insights/announcing-ripples-global-payments-steering-group/
➢ Sending provider (the provider sending a payment instruction to the receiving provider over Ripple technology)
➢ FX connector (as described further in Ripple's original proposal)

Authorization process: The commercial rules and the design of Ripple technology allow providers and FX connectors to choose the parties that they transact with over Ripple technology and to limit their counterparties to only those that they have granted authorization. Providers must credential each other before they can communicate with each other using Ripple technology.

These controls allow providers and FX connectors using Ripple technology to manage their transaction counterparties and protect themselves from doing business with entities that they do not know or wish to transact with. The commercial rules formally document the authorization process, including the rights and obligations of providers and FX connectors vis-à-vis each other. For example, the commercial rules state that an entity cannot act in the capacity of a FX connector in a transaction over Ripple technology with a provider, unless that entity has sought the authorization of the provider and the provider has authorized it through Ripple technology.

Following the authorization process, the commercial rules and Ripple technology allow providers and FX connectors to unilaterally cease transacting with each other in such capacity, if they choose. This feature allows providers and FX connectors to ensure they comply with applicable sanctions and anti-money laundering laws, as well as mitigate and manage their risk as they deem appropriate.

The commercial rules formalize this process and include protections for the impacted providers and FX connectors. For example, if an authorized FX connector chooses, in its own discretion, to unilaterally cease to act in such capacity with a provider, it must give that provider not less than five business days' prior written notice (unless a shorter period of notice is agreed to by that provider or required under applicable law). This notice period is intended to give the provider adequate time, in case any is needed, to identify another entity to serve in the role of FX connector.

Communication: The commercial rules formally document (i) how providers may send payment instructions to each other through Ripple technology, (ii) how a sending provider may initiate that process on Ripple technology, and (iii) how an FX connector’s FX rate is communicated through Ripple technology to the sending provider. The commercial rules additionally provide for how a sending provider may cancel (using Ripple technology) a payment instruction it has already sent to a receiving provider, including identifying the moment in time after which a sending provider may no longer do so (the initiation of the settlement process, as described below).

Furthermore, the commercial rules detail how providers transacting with each other may request from and share with each other certain information about the payment transaction that each, under its own internal compliance policies, requires in order to perform its own due diligence checks and screening. For example, U.S. law generally requires banks to retain and pass on to the next bank in a funds transfer chain certain information for certain transmittals of funds (often called the “Record Keeping Rule” and the “Travel Rule,” 31 C.F.R. §§ 1020.410, 1010.410). The commercial rules are not prescriptive on the precise transaction information providers must request from each other, instead giving each the freedom and discretion to make that determination. This approach accommodates the
diversity among providers and the likelihood that the information a provider chooses to request would likely vary depending on applicable local law and each provider’s own internal compliance policies.

The commercial rules include provisions drafted to support such information sharing and define requirements for providers to protect and safeguard sensitive information that they receive from each other. As discussed in greater detail below (the confidentiality discussion in the End-User Data Protection section), the commercial rules require a provider receiving such information from another provider to: (i) provide adequate security measures in order to maintain the confidentiality of such information and (ii) not to disclose or use such information for any purpose other than to perform its own due diligence checks and screenings as required under its own internal compliance policies and applicable law.

Payment instruction acceptance and rejection: The commercial rules allow a receiving provider to accept or reject, in its own discretion and using Ripple technology, a payment instruction it has received from a sending provider. In particular, the commercial rules permit a receiving provider to reject a payment order for any reason or for no reason --- defining the payment instruction as a request by the sending provider to the receiving provider to pay the beneficiary. The commercial rules formally document how a receiving provider may either accept or reject a payment instruction and how notice is given of such to the sending provider over Ripple technology.

Settlement process and finality: If a receiving provider has accepted a payment instruction received from a sending provider, the commercial rules address: (i) the sending provider’s obligation to pay the receiving provider the amount of the payment instruction, (ii) how the sending provider has discharged that obligation, (iii) the moment in time when that the sending provider’s obligation to pay has been finally and irrevocably discharged, and (iv) what happens if the funds transfer is not properly completed (for example, if the receiving provider does not then make payment to the beneficiary identified in the payment instruction).

➢ With respect to the first item, the commercial rules state that a sending provider does not become obligated to pay the amount of the payment instruction to the receiving provider until the sending provider has initiated the settlement process on Ripple technology. As detailed in the commercial rules, the sending provider initiates this process by confirming that it has made a certain book transfer (as described further in Ripple's original proposal, “Settlement Step 1 – Escrow” in Part A).

➢ With respect to the second item, the commercial rules state that the sending provider discharges its obligation to pay the receiving provider by means of the settlement process over Ripple technology, which the commercial rules formally document (the substance of which is described in Ripple’s original proposal, “Detailed Settlement Process and Funds Flow” in Part A).

➢ With respect to the third item, the commercial rules state that the notary’s approval (described further in Ripple's original proposal, “Settlement Step 2 – Notary Approval" in Part A) --- which is communicated to both the sending provider and the receiving provider through Ripple technology --- constitutes the final and irrevocable discharge of the sending provider’s obligation to pay the receiving provider. The commercial rules also formally document the automated release of funds that immediately and automatically occurs upon notary approval (as described further in...

The commercial rules clearly and precisely identify notary approval as the moment in time when final settlement has occurred, taking into account the benefits of Ripple technology’s speed and transparency to providers. Identifying final settlement at this moment in time additionally allows the receiving provider to protect itself from credit risk to the FX connector: the receiving provider can implement controls in Ripple technology to make overdrafts in the FX connector’s account impermissible, precluding the possibility of notary approval in such circumstances.

➢ With respect to the fourth item, the commercial rules recognize that settlement between the sending provider and the receiving provider over Ripple technology will often precede or be contemporaneous with payment to the beneficiary. The commercial rules include a requirement that following final settlement between the sending provider and receiving provider (as described in the third item directly above), the receiving provider must confirm to the sending provider that it has paid the beneficiary identified the payment instruction in the amount indicated.

However, there may be instances where the receiving provider does not make such payment to the beneficiary and the funds transfer has not been properly completed. In these circumstances, the commercial rules provide that the sending provider’s obligation to pay the receiving provider (described in the first item above) has been excused. Thus, if the sending provider has already paid the amount of the payment instruction through operation of the Ripple settlement process (described above), then the receiving provider must refund such payment in the amount of the payment instruction. This refund may be done through Ripple technology or by other means, as the providers choose.

The commercial rules include additional key provisions, such as loss allocation (for example, for unauthorized transfers as described above), required security measures (discussed in greater detail in the Security section below), confidentiality obligations (discussed further in the context of the End-User Data Protection section below), and compliance with applicable law (including applicable transaction recordkeeping and reporting requirements and sanctions/asset control and anti-money laundering laws, rules, and regulations).

Finally, the commercial rules provide for amendment upon a certain specified threshold of consensus among the members of the GSPG. The amendment framework positions the commercial rules to address a payment system that is far from static and continues to innovatively evolve — it prevents the commercial rules from becoming outdated or locking providers into a set of rigid requirements that no longer reflect marketplace needs or technology advancements. Rather, the commercial rules can be amended quickly as necessary over time by providers (members of the GPSG) themselves.


**Risk Management**


The QIAT assessment noted that additional detail on the commercial ruleset would allow for a more informed assessment of risk management.
The commercial rules, together with the design of Ripple technology, allow providers to manage risks effectively and efficiently, as well as reduce and eliminate certain key risks.

➢ **Systemic risk**: Today, most providers do not have a direct relationship with each other and must rely on a certain central counterparties (such as regional payment systems or a dwindling number of correspondent banks) to connect with each other. This centralized framework is vulnerable to systemic risk – a central counterparty’s failure to function as expected could lead to adverse knock-on effects on the institutions and broader market it serves.

In contrast, Ripple’s commercial ruleset creates a clear and well-established legal framework that allows providers replace their dependence on central counterparties with a diverse and robust network of FX connectors. The commercial rules mitigate systemic risk by supporting, with the design of Ripple technology, a decentralized cross-border payment network. The commercial rules allow providers to connect to a network of FX connectors, and a provider can promptly and effectively obtain a substitute FX connector for critical payments in the event one fails to function as expected.

➢ **Replacement-cost risk** (usually associated with pre-settlement risk): As discussed above, the commercial rules create a robust legal framework that supports a decentralized cross-border payments framework. This decentralized framework stands in contrast to a hub-and-spoke model, where it would be a challenge to replace the central counterparty should it fail to function as expected and a transaction is left unsettled.

Thus, replacement-cost risk would be relatively high were the “hub” to fail: institutions are exposed to the cost of replacing the original transaction with the central counterparty at current market prices. However, the commercial rules’ decentralized framework allows providers to promptly and efficiently substitute counterparty FX connectors prior to settlement should the need arise – transactions are not concentrated in any one or few central counterparties, minimizing replacement-cost risk.

➢ **Principal risk** (often associated with settlement risk): The commercial rules and the design of Ripple technology provide for atomicity – that is, payments, including cross-border payments involving more than one currency, are either fully settled in real-time or they do not occur at all. This process stands in contrast to payment systems that operate with delayed settlement and sequential processing.

For example, the delivery of one currency against delivery of another currency involves the settlement of two linked obligations (an exchange of dollars to euro involves the delivery of dollars from one party to the other and the delivery of euro from that other party to the first). Risk arises when one obligation is settled, but the other obligation is not (dollars are irrevocably transferred, but no euro payment is received). A failure to complete the settlement of both linked obligations could, in turn, result in high replacement costs (that is, the cost of replacing the original contract at market prices that may be rapidly changing, as discussed above).

However, providers can eliminate this risk when the final settlement of the obligations is linked – which the commercial rules and the design of Ripple
technology accomplish. The commercial rules and the design of Ripple technology establish a settlement mechanism that eliminates principal risk by ensuring that the final settlement of one obligation occurs if and only if the final settlement of the linked obligation occurs (as discussed in greater detail in the Legal Framework and Payment System Rules section above).


Security
Data being transferred by the providers through Ripple Connect (in flight data) is secured by the encryption built into the product, as the assessment noted. However, the assessment did note a lack of information on the security of data at rest – that is data held by the providers. In addition to the functionalities built into Ripple Connect, the commercial rules developed by Ripple in collaboration with the GPSG establish standards for providers in how they secure the data they hold.

The commercial rules contractually obligate providers to take all commercially reasonable security measures applicable to the financial industry in order to detect fraud and prevent unauthorized access. In recognition that security practices in the banking industry evolve in order to keep pace with bad actors seeking to exploit vulnerabilities, a deliberative decision was made to refer to industry practice regarding the exact security procedures deemed commercially reasonable.

In addition, the commercial rules allocate liability for unauthorized transfers in a way that incentivizes providers to protect against fraud. Specifically, if an unauthorized transfer arises as the result of a provider’s negligence and security gaps, that provider is responsible for direct damages up to the amount of the transfer. This liability allocation places the onus on providers to assure compliance with applicable security procedures and to safeguard confidential security information and facilities.


End-User Data Protection
GPSG’s commercial ruleset defines clear expectations for data protection, including end-user data. The commercial rules recognize that much data exchanged between providers in connection with payment transactions is confidential, and that providers are subject to regulations such as anti-money laundering laws that require them to retain and pass on certain transaction information.

Accordingly, the commercial rules were drafted to help protect providers disclosing such information in connection with their transactions and to define requirements for providers to protect and safeguard sensitive information that they receive from each other. A provider would contractually agree to the commercial rules prior to conducting transactions with other providers, ensuring that these confidentiality provisions would be in place at the outset.
Specifically, the commercial rules include the following components with respect to confidentiality obligations:

➢ The definition of “Confidential Information” was drafted to take into account the interests of both the disclosing party (to protect its confidential information with as broad a definition as possible) and the receiving party (to minimize its burden under the commercial rules with a narrower definition). Because providers generally intend to both disclose and receive confidential information in connection with a transaction, a balanced definition is in the best interest for all providers.

Accordingly, the definition captures all information relating to transactions governed by the commercial rules which a provider discloses or makes available to another provider, with exclusions from the definition for information that: (i) is or becomes lawfully available to the public, (ii) is accessible to the receiving party from a third party that is not bound by any duty of confidentiality, (iii) was already known to the receiving party on a non-confidential basis, or (iv) was independently arrived at by the receiving party without using the disclosing party’s confidential information.

➢ The obligations of the party receiving confidential information are also core provisions of the commercial rules. The recipient is subject to broad affirmative duties to safeguard the confidentiality of the disclosing party’s information. The commercial rules tie this obligation to a certain standard of care: the same degree as the receiving party would protect its own confidential information, but at least with a commercially reasonable degree of care applicable to the financial services industry.

The commercial rules include additional specific obligations for the receiving party. First, the receiving party is restricted in how it can use the disclosing party’s confidential information – it may not use that information other than to exercise its rights or perform its obligations in connection with the commercial rules (which includes a requirement that providers comply with applicable law). Second, the receiving party is prohibited from disclosing the disclosing party’s confidential information to third parties without the disclosing party’s consent, except to the receiving party’s representatives on certain conditions.

➢ The commercial rules provide for instances where the receiving party is required by applicable law, court order, or governmental agency to disclose the other party’s confidential information. The commercial rules also require the receiving party to endeavor to provide notice to the other party of such disclosure (unless it is legally prohibited from doing so) before making the disclosure. This notice requirement is intended to allow the other party to make a timely objection to a compelled disclosure.

The commercial rules and the design of Ripple technology allow for providers to provide payment services to payers and payees without knowledge of any account number, if they wish. The commercial rules and technology are agnostic as to the identification of the beneficiary (whether by account number or otherwise), the method of payment to the payee (whether by book transfer to an account of the payee or otherwise), and the method of payment from the payor to its bank (whether by book transfer from an account of the payor or otherwise).

Resiliency
(related to S.8. Resiliency)

By supplying software to providers, Ripple is classified as a software vendor and is subject to the providers’ vendor management and IT change management program requirements. These programs – generally required by financial services regulators in each jurisdiction – are designed to ensure the security, resiliency and reliability of technology. These programs and their due diligence standards are often unique to each institution, reflecting its operations, size, complexity and risk controls.

In the United States, Ripple is considered a technology service provider and subject to the expectations established in the Federal Financial Institutions Examination Council’s (FFIEC) “Supervision of Technology Service Providers” booklet, part of the Information Technology Examination Handbook.

Ripple has designed an operational resiliency and business continuity plan that aim to satisfy these expectations as well as the expectations of our clients in other jurisdictions.

This work includes the (1) development and implementation of a business continuity and disaster recovery plan, (2) independent, 3rd-party risk audits of our software and products, (3) internal service availability metrics, (4) a tiered incident severity system with defined response and resolution times and (5) user support expectations.

Ripple has a quality assurance team that reviews and test product performance. Together, these efforts result in a solution that meets enterprise and financial institution expectations for resiliency under normal and stressed operating conditions. These expectations are either defined in contract with a provider and/or validation of each is required before a provider will integrate.

Given this work, we have issued a self assessed rating of “very effective” for S.8.

[end]
RIPPLE PROPOSAL

TASK FORCE ASSESSMENT COMMENTS

Please share your concerns about this proposal’s assessment against the Effectiveness Criteria.

Overall assessment, DISAGREE with QIAT assessment. The reviewers believe Ripple should be rated lower, as it has many challenges especially when at key effectiveness criteria the responsibility and liability among the criteria items are shifted to the FIs. Ripple could be part of the overall interoperability, especially as it relates to cross-border transactions. However, there are major gaps for domestic use.

The only solid use case is the cross-border payment, which eliminates the need for a correspondent bank, and through having global FIs adopt the Ripple solution and become part of the network, Ripple is able to transfer cross-border payments as closest to real time. However, the other important and most common use cases of any payment solution provider are not prioritized, making Ripple a challenging solution for real-time faster payments in the U.S.

Given that the solution only addresses cross-border, I thought that the assessment was a little too lenient. Not every use case calls for cross-border so just ignoring that and calling something effective or somewhat effective when domestic payments are ignored doesn't make sense to me.

Real-time settlement still requires a substantial investment by both banks to ensure funds are on deposit somewhere (either a one-to-one bank relationship or via a connector). The solution breaks down quickly when both FIs are not connected directly to each other or via Ripple Connect. Because of that I don't think it is very effective. Additionally, Ripple was very evasive when I asked them if banks needed individual relationships to be established outside of the Ripple Connect relationship and if that is the case, then it is very onerous for smaller players to negotiate agreements and/or maintain accounts with a variety of international banks.

The proposal is not in conformance with the requirements of a full solution proposal. The requirements were designed to ensure that McKinsey and Task Force time and resources are focused on end-to-end solution proposals that can be thoroughly and credibly assessed against the criteria. This proposal does not meet the requirements. Proposal has answered all sections of the template but in many cases the response does not provide information that would allow the QIAT to evaluate the proposal. The Proposal Template included instructions for Part C: Self-Assessment against Effectiveness Criteria that asked proposers to include a "detailed discussion of why the rating is justified and how the solution meets each criterion" (page 22 of template). It does not include specific information in Part C as to how or why the proposed solution meets each of the criteria. As a result, the QIAT is unable to evaluate the solution with the information provided. Altering the existing process defined to offer an opportunity for the proposer to include more explicit information in its submission to make the proposal “assessable” would be unfair to proposers who provided complete proposals before the submission deadline. A few of the reasons why the proposal did not meet the requirements are as follows: The solution did not include the unbanked. The solution focused on B2P and P2P cross-border payments only and did not
include B2B or P2B cross-border payments. The solution has no common standards across FIs, no disputed payment rules, no deployment scale or commercial deployment. The solution does not ensure reliability; protect payer; aggregate, manage, or protect data owned by FIs. The solution has no end-user data protection, operating rules, participation agreements, and legal and governance are incomplete.

Please submit any comments about this proposal’s assessment against the Effectiveness Criteria.

There are a few assessments which I would rate lower—E4, payment format standards—are not defined and subject to additional input from a governing body; should be "somewhat effective." The legal and governance frameworks are still a work-in-process—L1, L2, G1 and G2—I disagree with the QIAT arbitrary assessment of "somewhat effective." "Not effective" is more appropriate at this stage.

Even though the proposal deals with cross-border payments only, it would have been useful for the QIAT to dig deeper into the issue of processing Distributed Financial Technology at scale. Few laymen, and for that matter not many IT professionals, are knowledgeable enough to adequately address this topic. The QIAT could have helped us separate the myths from the reality.

Agree as assessed. While the solution is very limited in scope, if the criteria are applied against the stated scope, the assessment is accurate.

Solution seems to be very fast for approval and settlement; use case is primarily cross-border payments.

I believe generally speaking Ripple fairly represented the use case limitations and likewise demonstrated the effectiveness levels against the criteria within the proposal. However, their own self-assessment was at odds with McKinsey's assessment. Given the scope that Ripple set out to solve which seemed to be accomplished, McKinsey's assessment against the entire criteria was generally fair.

Lacking in security, legal and governance criteria as noted in assessment.

Originally designed for trans-border funds movement, Ripple has been adapted for purposes of this proposal to act as a domestic carrier as well. This, despite the lack of connective tissue on legal structure (save for bilateral agreements between participating banks), legal structure, and governance. The concept is viewed as sound, but, as yet, incomplete.

Cross-border model between FIs that join its network. Rules and legal framework are not clearly defined.

(1) Standardizes the cross-border payment experience (2) can integrate directly with a financial institution or connect to a 3rd party platform that a financial institution is already connected to (3) meets speed criteria (4) more usability and transparency in cross-border payments experience (5) governance from 6 FIs on the network that create standards and framework instead of Ripple doing, tiered governance structure that will allow other FIs.
Ripple seems to offer a realistic time frame within the governance requirements. It also seems to take into account P2B with the hardware aspects while being able to show a realistic initiative to interlope with existing hardware such as POS terminals. One thing to mention, the base applications of the manufacturers will need higher levels of security within these applications as well as greater education towards Small Businesses on how this process would work. Many small businesses are not even EMV compliant, many still balk on the equipment to mention, and many of the ISOs and processors may only be able update this equipment based on their back-end processing application files. Even with all of this being said, even though the initiative is realistic for governance and interoperability, the timeframe may be much longer than perceived.

My feeling is that Ripple is not yet mature as a payments system. While the engineering details are well worked out, the business case has yet to be proven. The current experiments and trials with blockchain technology by some of the larger banks have not yet, that I have seen, shown that there are any advantages of blockchain solutions outside of a small, specialized use case of the transmittal of digital intellectual property/secure document transmittal. It might be informative to see if any of the other faster payments systems globally are using a blockchain technology. I am not aware of any.

The QIAT completed a comprehensive review of the proposal. As indicated by the QIAT, the proposal is focused on cross-border payments, albeit proposer indicates it could also be leveraged for domestic payments which is initial objective of the FED initiative.

The QIAT identifies that the solution depends on a change in the cross-border payment model such that all the FIs would need to be members of the same network and have direct two-way connectivity between themselves. Where this direct two-way connectivity is the case, and with the limited number of points that the payment needs to process, it then allows for speedy settlement of cross-border payments.

As indicated by the QIAT, proposer is piloting their solution today but on a very small scale where no large-scale deployments have been done.

Ripple's proposal focused on their core strengths in processing P2P and B2B cross-border payments and as such the assessment was accurate.

Proposal trying to adapt its cross-border payment solution towards a domestic transaction processor. Appears to address most of the effectiveness criteria, but will need to address how to expand the bilateral agreements between a broader and more diverse group of participating financial institutions. Will require work around legal structure and governance. Did not see how it would effectively support interoperability with other payment structures.

Concur with QIAT comments.

Rating for “enables competition” should be very effective given the use case that the solution provides and its competitive landscape. Rating for contextual data seems too high given the format for the data (esp. B2B) is not defined, nor would be consistent. Rating for “fast approval” rating appears too high,
given that there is not a consistent approval process and timing for all using the solution. Rules and governance are rated too highly given that they are not yet defined/fully shared.

While Ripple has an international implementation, the concepts of what they propose can certainly be adapted to domestic processing which seemed to be discussed (not in detail) in the proposal. The QIAT may have been more firm about this point than was necessary in evaluation U6 (for example). In all, the QIAT did assess properly but possibly more critical over the international versus domestic comments.

Bank to bank network based on distributed ledger, with existing rules and governance. Payments settled within 5 seconds among participating banks. No UX. Good for bank to bank but an incomplete solution.

U.3. Predictability. Unless Ripple can define how error resolution rights will be expressed, then the solution cannot be “effective.” Other parts are adequate; we would suggest a rating for U.3. of “somewhat effective.”

The assessment seems fair given Ripple’s 1) cross-border focus doesn't address all use cases 2) acknowledged start of a standards, legal, and governance framework. 3) lack of error resolution process. Acknowledged benefit of the use of Interledger (open protocol) to enable payments that join the network. Framework appears to be able to work for small to medium FIs provided their payment providers integrate Ripple Connect.

E.2 Capability to enable value-added services should be rated as Effective as the solution does not currently support Domestic transfers.

S.2 Payer authorization was rated as Very Effective while E.4 Payment Format Standard was only rated as Effective as it wasn't specific on the message format while the S.2 comments reflected it did not address pre-authorization of payment. Both of these categories should be Effective based on the comments provided.

I agree, with one reservation: I do agree with the proposer's response regarding the assessment of U.6. The criterion does not specify domestic use cases.

Though the panacea is for a “grand, unified” solution to the Fed's request for proposals, the reality is a solution set comprised of robust components, and Ripple was transparent in its intent to address cross-border payments only.

With regards to the proposer's other comments I agree with the assessment as I think it to be accurate given the information provided at the time of the assessment.
TASK FORCE SOLUTION-ENRICHING COMMENTS

Ubiquity

More development in the solution to be able to offer in a domestic transfer environment similar to what is being offered for International transfers.

Would have liked to see a framework for domestic payments spelled out.

The solution could be enriched by including additional business use cases such as P2P, P2B, B2B, and B2P. Also, the proposal could be enriched to describe the interoperability capabilities between like or different faster payment solutions for the cross-border use cases presented.

By definition, ubiquity is not obtained (nor strived for) given the focus on cross-border – yet more words on how reach could be extended to all US bank accounts would be helpful.

Certainly addresses P2P and cross-border needs but does not appear to solve for the other use cases.

U.1 Accessibility – Somewhat Effective, the FIs must be a part of the Ripple network which can be challenging as adoption of Ripple has mainly been for cross-border use, and domestic transfers are done through existing infrastructure. This means reliance on current payment processors and infrastructure, but not leveraging Ripple as it is targeted more to cross-border payments.

U.2 Usability- Not Effective, Ripples leaves functionalities and capabilities to the providers. Some should be left to the providers so they can align with their clients, but some essential functions that are key to real-time payments (e.g., operating hours) have been left to the providers to have full control, causing an issue for the real time payments that should be available 24/7/365.

U.5 Cross-border functionality-Somewhat Effective, the core of Ripple is eliminating the intermediary bank(s) and going directly to the FIs enabling faster and the closest real-time cross-border transactions; however, the set-back for Ripple is that there must be FIs within the network who have the Ripple technology integrated in order to be able to deliver the cross-border payments.

U.6 Applicability to Multiple Use Cases – Not Effective, if there is a global FI within their Ripple Network, then cross-border payments will have a key advantage of real-time transferability, but this only one use case, and Faster Payments, must be able to support at least the most common use cases, which is not the case for Ripple.

Because of its nature, the proposal seems to be calling for partnership to very effectively deliver in many areas including Ubiquity. In my reading, it seemed more direct, the link to business applications through technical standards. With that said, it is the issue of having an offering that is not currently connected to business applications – however, I can see how this would be done and believe Ripple has addressed this section better than may appear in the evaluation.

While the proposal defers addressing some of the Ubiquity requirements (a common theme among these proposals), Ripple does demonstrates some key strengths, including one of the most developer
and innovation-friendly platforms for international transfers and a price point that can't be beat. It's with high confidence that we believe Ripple could deliver consistent and familiar end-user experiences where and when applicable.

This is not a complete solution.

Doesn’t address all use cases.

Doesn’t facilitate domestic payments. Provides financial institutions the ability to establish their own timeframe outside of 24/7/365 on cross-border payments. Not a domestic solution.

Meets the needs of the solution.

Ubiquity will be a long time coming for Ripple (or any blockchain system.) What I don't see in their proposal is anything effective about a "translator function" to enable a payment to originate or end outside of their system, although perhaps they feel this is the responsibility of the banks that might operate a Ripple technology based system.

Efficiency

More fully describe the bi-directional messaging and how those messages might be integrated into other banks’ systems and processes – either to support required payment tasks or to provide other value-added services. Describe how indirect access in a country (via one FI) would be implemented and tasks required of the indirect participants.

E.1 Enables competition – Somewhat Effective, further information is needed as how easily a provider can switch among “multiple providers” and what time frame, risk, down time if any could the change bring.

E.4 Payment format standards – Somewhat Effective, messaging standard is not set, rather Ripple states “provider-run governing body will define messaging format”—leaving an important criteria of interoperability at risk.

E.6 Scalability & adaptability – Somewhat Effective, no metrics/estimates are provided as to how Ripple will handle scalability and the capability of the same in volumes and values.

E.7. Exceptions and investigations process, Not Effective, the FIs that are participants of the Ripple network are responsible for communicating with one another and solving any issues with a transaction. Thereby, shifting the liability between FIs with no tools within the Ripple solution to investigate any exceptions within a transaction.

Ripple takes many of the promising aspects of distributed systems and applies them in a way that is pragmatic and digestible to the FI community. Its relative growth over the last year or two, its governance board, and its standards work demonstrate the company's maturity. Its biggest proof point
will be continuing to distribute and deliver a business model and value proposition that banks want to adopt worldwide.

Resiliency issues.

Appears to provide for an efficient solution.

Blockchain payments are relatively efficient except in the sense of being timely. Although data varies quite widely, transactions have been recorded taking several minutes to complete.

Safety and Security

The solution could be enriched by including how fraud protection and fraud monitoring is maintained within the system.

The solution needs more work on fraud monitoring solutions since Ripple does not have access to the data, they lack the ability to address system wide fraud detection. That also means that claims processing and dispute resolution would have to be deferred to others.

S.2 Payer Authorization – Effective, more information is needed for pre-authorization of payments.

S.3 Payment finality – Somewhat Effective, no information in place by Ripple in the “event that the payment is disputed beyond compliance with consumer laws.”

S.4 Settlement Approach – Somewhat Effective, although Ripple can settle within one (1) second, at the end it turns over the control to the “FIs or governing body” to make the decision if the transaction(s) will be settled in real-time or not or “deferred net settlement” including operating hours, which contradicts the Faster Payments real-time criteria.

S.5 Handling disputed payments- Not Effective, as stated in E.7, the disputed transactions is shifted to the FIs and Ripple does have the tools within the solution.

S.6 Fraud information sharing – Not Effective, similar to S.5, and E.7, Ripple doesn’t have any tools within the solution to mitigate fraud, and instead all responsibility is shifted to the participating FIs and providers, who have eventually could set a “provider-run governance body” according the solution proposer.

S.9 End-User data protection – Not Effective, similar to S.6, S.5, and E.7, Ripple shifts all responsibility to the FIs, and the proposer’s solution does not have the tools to protect the data among its FIs and providers, posing a risk to the end-user’s data and not aligning with the Effectiveness Criteria.

S.10 End-User/provider authentication – Not Effective, similar to S.9, S.6, S.5, and E.7, shifts all responsibility to the FIs, posing a risk to the overall transaction.

The diverse compliance requirements (both domestic and international) for any FI wishing to adopt a cross-border payment solution is rightfully burdensome. Ripple does not dismiss the reality that, while
although applicable to every solution, a bar is set slightly higher with new entrants with new ideas. However, a strong pipeline and advisory council reinforces Ripple’s ability to facilitate, interoperate, and execute against these requirements.

No requirements for end-user data protection

Data privacy

Financial Institutions have to handle fraud/dispute etc. no info sharing or support.

No directory is part of the solution.

Blockchain's security is, in my view, still unproven simply because there have not been a lot of attempts by necessarily skilled parties to break it. Ripple would need to develop some proof that the system is secure either as a matter of engineering or some other functionality and submit it to attempted break-in testing.

**Speed (Fast)**

F.1 Fast approval, F.2 Fast clearing, F.3 Fast availability of good funds to payee, F.4 Fast settlement among depository institutions & regulated non-bank account providers – Somewhat Effective, given that “Ripple does not describe operating rules to enforce fast approval, nor to ensure 2x7x365”— they shift the decision to whomever are the FIs / providers. This puts at risk the real-time Effectiveness Criteria and it will be up to the providers and FIs to decide if the payment will be fast, secure and in real time. Same rating for all F.1 to F.4.

Near real-time.

Contrary to what is often believed, blockchain transactions are not at all necessarily fast and can take minutes and multiples of minutes to be certified as having completed. I don't know that Ripple has addressed this or not.

**Legal**

Please ensure the legal framework is inclusive of small to medium FIs.

The proposed solution could be enriched by providing some insight into the legal framework that needs to be developed between various messaging systems, processing rules, and regulatory oversight related to consumer protection and data privacy.

More definition around each participant’s required processes, as it pertains to end-users, would be helpful – including definition of B2B information that would be passed with a transaction, and handling disputes.
Too much reliance on the FI for the legal framework. There has to be some overarching framework to ensure consistency and the user experience.

L.1 Legal framework & L.2 Payment system rules – Not Effective, shift of Legal Framework is dependent on each FI, posing a risk to how a faster payment in real-time could really operate under the Ripple solution, as the solution does not provide a legal framework, but instead shifts all responsibility to the FIs and/or providers.

L.3 Consumer protections—Not Effective, Same as L1. & L.2 everything is shifted to the FIs and/or providers.

L.4 Data privacy – Not Effective, same as L.1, L.2, and L.3, responsibility is shifted to FIs.

Need to develop some operating rules instead of relying on FIs to develop their own rules.

The legal status of a blockchain transaction has not yet, as far as I know, been ruled on by a court of law. Until there is a challenge by an aggrieved party and a court rules in Ripple's favor this remains an unsettled issue.

**Governance**

Please ensure that when establishing the governance over the network that it is fully inclusive to small and medium FIs.

The proposed solution could be enriched by providing some insight into how disputes will be governed between countries utilizing the Ripple solution and the differences in various banking laws/governance.

Describe more fully how inclusive governance is achieved.

Needs to be better defined. There is too much ambiguity in the proposed governance model.

G.1 Effective governance & G.2 Inclusive governance, Somewhat Effective – “Ripple has helped establish a provider-run governance body to maintain a scheme.” Effective – define by a “participation agreement commercial framework.” Inclusive – “Governance of the Interledger Protocol is managed within the well-established World Wide Consortium (W3C).” Formation of a Governance Body and Payment Scheme.

Need to develop additional governance instead of relying solely on participation agreements.

It wasn't clear to me how much of a role, and of what type, Ripple would want in governance. It is something they need to make clearer.
Ripple

Response To Task Force Commentary

January 2017

Submitted by:

Ryan Zagone
Director of Regulatory Relations

Liza Partington
Regulatory Relations Specialist
Ripple’s Response to Task Force Commentary

Ripple greatly appreciates the time and effort put forth by the Federal Reserve, the QIAT team, and Task Force participants. Your review and comments provided useful solution-enriching feedback that helped validate Ripple’s approach.

Over 93% of Task Force responders agreed with the QIAT’s assessment that Ripple greatly improves the speed, certainty and transparency of cross-border payments. We thank the responders for the time they took to review the proposal and offer this input. Your feedback is incredibly useful.

We would like to take this opportunity to address some themes that emerged from the feedback and resolve uncertainty that was present in small subset of comments. The following response provides greater detail on three areas:

1. Ripple’s Focus on Improving Cross-Border Payments
2. Additional Detail on the Solution’s Legal and Governance Structure
3. Addressing Comments Regarding the Reliance on Providers for Fraud Monitoring

We hope this additional input provides the necessary clarity to understand Ripple’s self assessment ratings and resolve some inconsistencies with QIAT ratings. We are happy to assist with any further questions.

1. Ripple’s Focus on Improving Cross Border Payments

Addressing the Unique Challenges of Cross-Border Payments
The Task Force sought proposals to improve the domestic and cross-border payment functionalities available in the United States. There was no requirement to cover domestic payments in the request for proposals or in the effectiveness criteria. With this in mind, Ripple proposed an end-to-end, cross-border payment solution that improves upon the unique pain points of this payment type: settlement days of up to four days, lack of visibility of the payment status, and no transparency into fees and FX costs.

The initial proposal was clear that this solution is focused on improving cross-border payments. While some commenters questioned the lack of a domestic functionality, it is critical to note that the realities of cross-border and domestic payments are inherently different. In domestic (single currency) systems, it is feasible to have a central operator with payments settled through a central bank account. However, cross-border payments are fragmented across geographies, currencies and jurisdictions. There is added complexity of currency exchange with complex, sequential processing with no central coordinator acting as an intermediary.
Because the technology solutions that underpin domestic and cross-border systems are each solving fundamentally different problems, they will likely have to be unique in their technology and design. Ripple’s solution was designed to specifically address the unique challenges facing cross border transactions.¹

Ripple agrees it would be ideal for faster payment solutions to offer both domestic and cross-border functionality. However, the technology underpinning those solutions will differ. It’s this belief that lead Ripple to use emerging industry standards (ex: ISO 20022) and open-source technology so that it can be easily integrated into domestic solutions.

**Ripple: Supports Broad Use Case Coverage Through Optimizing The Process of the Payment**

Today, cross-border payments are relayed across several intermediaries one step at a time. Aside from resulting in two-to-four day settlement delays, this sequential process prohibits originating and beneficiary institutions from knowing the status of the payment, the fees and FX cost, and the amount of funds that will ultimately be delivered. The delays, costs, risks and uncertainty inherent in this sequential process make today’s cross-border system only viable for large-value batch payments.

Ripple replaces the sequential payment process with a coordinated process. With Ripple, the payment either fully executes across all intermediaries or it does not execute at all. This synchronized process enables transparency and certainty, while eliminating settlement risk.

Through this coordinated process, Ripple enables banks to make low-value cross-border payments efficiently for the first time. This is an important expansion in cross-border payment use cases that has not been achieved in current systems.

As a payment rail, Ripple is agnostic to payment type. It supports high and low value payments across all use cases. Given Ripple’s unique new offering of low-value payments, banks are initially using the solution to meet market demand for this type of payment, specifically low-value person-to-person and business-to-business payment services. The solution is already capable of other use cases; these two low-value use cases were highlighted in the proposal given their novelty for cross-border payments.

While not discussed in our initial proposal, Ripple is also fitting and capable of processing B2P payments. This is especially relevant for low-value wages to workers overseas. As digitally-based platform businesses have grown (such as Uber or Airbnb), they have an increasing demand for individual low-value payments to individual suppliers. Ripple is well suited for this emerging payment demand. We have added details on this use case below (low-value transactions for digitally-based platform businesses).

Given the immediate support for several initial use cases and the ability to process low-value cross-border transactions for first time, Ripple gave itself a “very effective” rating for U.6 (Applicability to Multiple

¹The proposal notes that Ripple’s solution can be used to enable interoperability between domestic systems, which can resemble challenges faced in cross-border transactions (i.e.: synchronizing ledgers with certainty).
Use Cases). However, the QIAT failed to consider the realities of cross-border payments in its assessment of “somewhat effective”. A commenter points out:

“The QIAT may have been more firm about this point than was necessary in evaluation U6. In all, the QIAT did assess properly but possibly more critical over the international versus domestic comments.”

Another commenter noted that the “rating for ‘enables competition’ (E.1) should be ‘very effective’ given the use case that the solution provides and its competitive landscape.” A “very effective” rating would match Ripple’s self assessment and we believe more accurately reflects how Ripple improves cross-border payments to support many use cases and low-value payments.

We appreciate these comments. By changing the process of the payment from sequential to coordinated, Ripple unlocks entirely new use cases and payment types.

**Additional Detail of the Use Cases and Emerging Payment Demands**
Below we provide additional detail on how Ripple addresses the market demands for: (1) increased transparency and certainty of high value payments and (2) efficient low-value, cross-border payments.

1. **Ripple Enables Improved High-Value Payments**

Customers of payment providers, especially corporates, are seeking an improved cross-border payment experience for the payments they currently send overseas. Customers expect transparency of the payment – the ability to track the payment in real-time with clear estimates for the time of delivery. Customers are also seeking greater certainty of fees and the exact amount of funds that will be delivered, all before the payment is initiated.

As the current process does not provide this certainty and transparency, many corporates result to a workaround for some payment needs, opening bank accounts and depositing cash in all the countries in which they make payments. This enables the corporate to quickly make payments of a certain amount. However, the corporate assumes FX risk, which it may not have an expertise in managing; incurs operational cost of maintaining these accounts; and suffers a large opportunity cost of locking up capital all around the world.

An improved B2B cross-border payment process that provides efficiency and certainty is needed. Ripple’s solution is designed to fill that void.

Ripple allows providers to offer real-time, on-demand international payment services for their corporate customers, enhancing their corporate treasury solutions portfolio and allowing their corporate customers to achieve superior working capital management. The delays and uncertainty of today’s cross-border payments force corporates to open and fund accounts in countries around the world, so that cash is available overseas if an immediate payment is needed. With Ripple, corporates can work with their
provider to initiate cross-border payments in real-time from their sole domestic bank account, allowing the corporate to repatriate its capital and deploy it in more efficient ways.

This improvement, which is currently supported by Ripple, is especially relevant in high-value and B2B payments.

2. Ripple Enables Efficient Low-Value Cross-Border Payments

A wide variety of stakeholders are seeking access to low-value, high-volume payment services. As today’s current infrastructure was built to support high-value batch payments, the services in demand are generally not cost effective or not available at all. Broad macro trends are calling for efficient low-value payment options and Ripple’s solution provides them:

Remittances: Consumers have grown accustomed to immediate global connectivity, which has led to a change in their expectations for the speed and reach of payments. As globalization has driven individuals to become more dispersed and interconnected, there is an increasing demand for low-cost P2P payment services, particularly for small-dollar cross-border transactions. The price of cross-border payments (~$40 per transaction) makes low-value payments prohibitively expensive.

Small and medium sized companies: Smaller companies have long sought access to materials and markets overseas. Yet, the cost and complexity of managing cross-border payments often cannot be justified for a few low-value payments per month. Given their anticipated low payment volume, these companies often minimize activity that would require cross-border payments. To enable growth, these companies are seeking solutions that allow them to efficiently send a low-volume of small- and medium-sized payments.

A new generation of digitally-based companies: A new crop of digitally-based marketplace companies has emerged with a specific need for low-value, global, B2P payments. These companies, such as Uber, Amazon and Airbnb, have a global mindset and customer base from day one. They have supply chains that are increasingly sophisticated with a focus on minimizing working capital. The nature of these companies’ operations requires many small payments to be sent globally in real-time. Today’s high-value, batch payment solutions do not suit the needs of this new generation of companies. Given these companies large size and quick growth, meeting their payment needs is a priority for many banks and payment providers.

Ripple is initially focused on P2P, B2B, and B2P services to meet the emerging needs described above. While these use cases are the initial focus, Ripple is flexible and can support a wide variety of use cases to meet the growing demands of various marketplace stakeholders.

2. Additional Detail on the Solution’s Legal and Governance Structure
Overview of the Legal and Governance Structure

The Task Force requested greater detail on the governance and legal framework that has been developed for the solution. Limited information was shared in the initial proposal because the details of Ripple’s governance solution had not yet been made publicly available. Since then, the steering group of six global banks that helped develop the governance and legal frameworks have been announced publicly. Ripple provided additional detail in a “Proposer Response to the QIAT Assessment” [see page 104 of the Ripple Proposal packet shared with the Task Force]. Further detail is available below.

On September 23, 2016, Ripple publicly announced the formation of an advisory body focused on the governance and legal framework: the Global Payments Steering Group (GPSG). This group worked together for the previous twelve months to develop a commercial framework, technical standards and network rules for payments made over Ripple. These bodies of work were crafted to reflect Ripple’s technology and the global nature of the network.

GPSG’s founding members include Bank of America Merrill Lynch (United States), Santander (United Kingdom and Spain), UniCredit (Italy/European Union), Standard Chartered (Singapore), Westpac Banking Corporation (Australia), and Royal Bank of Canada (Canada).

The outputs of this advisory group – the payment transaction rules, technical standards, and commercial framework – enable scalable implementation of Ripple as the network grows. They provide a critical set of common set of standards and protocols that allow providers to offer payment reach across the globe. These documents cover such topics as establishing the messaging standard (ISO 20022), defining settlement finality, providing a framework for dispute resolution, and detailing the rights and obligations of providers when using Ripple.

Commenters noted that criteria for E.4 (Payment Format Standards) and U.3 (Predictability) did not appear to be satisfied. However, the GPSG’s bodies of work fully define payment format standards and provide the certainty needed for the predictable use of Ripple’s solutions.

Some commenters sought greater detail on the inclusiveness of the GPSG framework [Criteria G2]. GPSG is an advisory body that developed the initial legal and governance framework. The goal of this work is to create certainty and standards across all banks using Ripple - both large and small. Given this, GPSG seeks banks of all sizes to both use the rules and standards, and provide input as these documents are updated. We expect additional banks, including smaller banks, to adopt GPSG’s standards and provide input. In fact, CIBC, a Canadian bank, will join GPSG to use and provide input on the documents.

Several comments disagreed with the QIAT’s rating of “Somewhat Effective” for criteria pertaining to the legal and governance framework [L1, L2, G1, G2]. Commenters felt these components were incomplete or a work in progress. We acknowledge that at the time we submitted our initial proposal in April 2016, neither GPSG nor its completed work products had been announced publicly. After the public announcement of GPSG, Ripple submitted more information to the QIAT to support our self-rating of “Very Effective” for Legal and Governance criteria.

We invite commenters to review our in-depth appendix submitted as a response to the QIAT assessment, which provides an extensive and detailed description of both the legal and governance frameworks,

2 https://ripple.com/insights/announcing-ripples-global-payments-steering-group/
further supporting our self-rating. Components such as the authorization process; communication via commercial rules; payment instruction, acceptance and rejection; settlement process and finality; risk management; security; data-protection, are all included in this thorough response.

To ensure greater clarity, we will re-address and elaborate on some of the primary themes from the comments we most recently received.

**End-User Data Protection/Data Privacy:**

Some commenters expressed concern over the protection of end-user data, and general data privacy. GPSG’s commercial ruleset defines clear expectations for data protection, including end-user data. The commercial rules recognize that much data exchanged between providers in connection with payment transactions is confidential, and that providers are subject to regulations such as anti-money laundering laws that require them to retain and pass on certain transaction information.

Accordingly, the commercial rules were drafted to help protect providers disclosing such information in connection with their transactions and to define requirements for providers to protect and safeguard sensitive information that they receive from each other. A provider would contractually agree to the commercial rules prior to conducting transactions with other providers, ensuring that these confidentiality provisions would be in place at the outset.

Specifically, the commercial rules include the following components with respect to confidentiality obligations:

- The definition of “Confidential Information” was drafted to take into account the interests of both the disclosing party (to protect its confidential information with as broad a definition as possible) and the receiving party (to minimize its burden under the commercial rules with a narrower definition). Because providers generally intend to both disclose and receive confidential information in connection with a transaction, a balanced definition is in the best interest for all providers.

  Accordingly, the definition captures all information relating to transactions governed by the commercial rules which a provider discloses or makes available to another provider, with exclusions from the definition for information that: (i) is or becomes lawfully available to the public, (ii) is accessible to the receiving party from a third party that is not bound by any duty of confidentiality, (iii) was already known to the receiving party on a non-confidential basis, or (iv) was independently arrived at by the receiving party without using the disclosing party’s confidential information.

- The obligations of the party receiving confidential information are also core provisions of the commercial rules. The recipient is subject to broad affirmative duties to safeguard the confidentiality of the disclosing party’s information. The commercial rules tie this obligation to a certain standard of care: the same degree as the receiving party would protect its own confidential information, but at least with a commercially reasonable degree of care applicable to the financial services industry.
The commercial rules include additional specific obligations for the receiving party. First, the receiving party is restricted in how it can use the disclosing party’s confidential information – it may not use that information other than to exercise its rights or perform its obligations in connection with the commercial rules (which includes a requirement that providers comply with applicable law). Second, the receiving party is prohibited from disclosing the disclosing party’s confidential information to third parties without the disclosing party’s consent, except to the receiving party’s representatives on certain conditions.

- The commercial rules provide for instances where the receiving party is required by applicable law, court order, or governmental agency to disclose the other party’s confidential information. The commercial rules also require the receiving party to endeavor to provide notice to the other party of such disclosure (unless it is legally prohibited from doing so) before making the disclosure. This notice requirement is intended to allow the other party to make a timely objection to a compelled disclosure.

The commercial rules and the design of Ripple technology allow for providers to provide payment services to payers and payees without knowledge of any account number, if they wish. The commercial rules and technology are agnostic as to the identification of the beneficiary (whether by account number or otherwise), the method of payment to the payee (whether by book transfer to an account of the payee or otherwise), and the method of payment from the payor to its bank (whether by book transfer from an account of the payor or otherwise).

**Payment Format Standards:**

A commenter expressed a concern that the payment format standards did not appear to be defined, urging that the effectiveness criteria rating for E.4 to be lowered to “somewhat effective.”

In fact, payment format standards are defined by the technical standards which were developed by GPSG. Ripple uses ISO 20022 format with an extensible data field for status tracking which is also defined by the technical standards. Use of ISO 20022 enables interoperability with a growing number of systems also adopting this format, while the extensible nature of Ripple’s messaging layer provides flexibility for new features and mechanisms to be added over time. Given the cost effective nature of adopting this standard and the reference to a standards development organization, Ripple gave a self-rating of “very effective.”

**Rules to Define and Enforce Fast Approval, Clearing, Good Funds and Settlement (F.1 through F.4):**

Some commenters expressed concern over a perceived lack of rules to enforce fast approval through settlement, which would jeopardize the certainty and speed of the payment. The rules and technical standards developed by GPSG do indeed provide certainty for these items. For instance, the frameworks developed by GPSG define time frames in which providers must accept or reject a payment. They also create predictable processes for providers to follow if a payment message is not responded to within the
defined time frame. These rules along with the transparency into the payment status through the messaging functionality provide the process and legal certainty for payments.

Ripple’s solution operates 24/7/365. Payments that have been accepted and approved by providers settle between the providers in seconds. A provider will know within a defined time frame is the payment cannot be processed or accepted.

**Handling Risk:**

Commenters felt concerned about the level of responsibility that the financial institutions take on in the Ripple solution, particularly in regards to the legal and governance framework. One commenter felt that this model posed more risk than the typical legal framework. It is critical to understand that the creation of the legal framework was a collaborative effort between Ripple’s legal team and each member bank’s legal department. The robustness of the framework actually lends itself to a system that allows providers to manage risk more effectively and efficiently, and in some cases, reduce or eliminate certain risks.

- **Systemic risk**: Today, most providers do not have a direct relationship with each other and must rely on certain central counterparties (such as regional payment systems or a dwindling number of correspondent banks) to connect with each other. This centralized framework is vulnerable to systemic risk – a central counterparty’s failure to function as expected could lead to adverse knock-on effects on the institutions and broader market it serves.

  In contrast, Ripple’s commercial ruleset creates a clear and well-established legal framework that allows providers to supplement their dependence on one central counterparty with a variety of FX connectors. In the event that liquidity from an FX connector becomes unavailable, a provider can promptly and effectively obtain a substitute FX connector for critical payments. This design and legal framework ensure operational resiliency and availability of the network, even in light of an individual participant losing connectivity.

- **Replacement-cost risk** (usually associated with pre-settlement risk): As discussed above, the design of the technology along with the commercial rules create a robust legal framework that supports a decentralized cross-border payments framework. This decentralized framework stands in contrast to a hub-and-spoke model, where notification of a failed payment could come several days after initiation and it would be a challenge to replace the central counterparty should it fail to function as expected.

  Thus, replacement-cost risk would be relatively high were the “hub” to fail: institutions are exposed to the cost of replacing the original transaction with the central counterparty days later at current market prices. However, the technology and commercial rules allow providers to have real-time visibility into the status of the payment and the legal certainty to efficiently substitute counterparty FX connectors prior to settlement should the need arise. Together, this visibility and framework greatly minimize replacement-cost risk.
Principal risk (often associated with settlement risk): The commercial rules and the design of Ripple technology provide for atomicity – that is, payments, including cross-border payments involving more than one currency, are either fully settled in real-time or they do not occur at all. This process stands in contrast to payment systems that operate with delayed settlement and sequential processing.

For example, the delivery of one currency against delivery of another currency involves the settlement of two linked obligations (an exchange of dollars to euro involves the delivery of dollars from one party to the other and the delivery of euro from that other party to the first). Risk arises when one obligation is settled, but the other obligation is not (dollars are irrevocably transferred, but no euro payment is received). A failure to complete the settlement of both linked obligations could, in turn, result in high replacement costs (that is, the cost of replacing the original contract at market prices that may be rapidly changing, as discussed above).

However, providers can eliminate this risk when the final settlement of the obligations is linked – which the commercial rules and the design of Ripple technology accomplish. The commercial rules and the design of Ripple technology establish a settlement mechanism that eliminates principal risk by ensuring that the final settlement of one obligation occurs if and only if the final settlement of the linked obligation occurs.

3. Addressing Comments Regarding the Reliance on Providers for Fraud Monitoring

Fraud Monitoring
Some commenters noted a drawback of Ripple’s solution is its “dependence” or heavier reliance on providers than existing systems, citing a reliance on the financial institutions for functions like fraud monitoring.

The reality for cross border payments today is that financial institutions are entirely responsible for identifying fraud. Each bank in the payment chain (respondent and correspondent banks) review transactions per their own fraud detection tools. There is no central operator or entity that conducts fraud monitoring in cross-border payments today.

Ripple follows this status quo, with the financial institutions identifying fraud for the transactions initiated with the solution. Ripple places no additional burden on a financial institution than what is currently in place for cross-border payments.

While cross-border messaging platforms do provide daily summaries of transaction messaging, often described as a fraud service, the financial institution itself must assess these reports internally to identify fraud or suspicious activity. The process is still carried out by the financial institution.
Data privacy and the fact that there is no global central operator for cross-border payments explain why financial institutions carry out the fraud monitoring.

**Security**
As fraud is often linked to the security of the connection to the product, Ripple has implemented several security features and threat countermeasures. The Ripple Solution components require that communication between parties to the transaction are private and encrypted using industry standard Transport Layer Security (TLS) v1.2. The provider’s access to the Ripple Solution is authorized using the OAuth 2.0 open protocol while authentication of inter-service communication is performed using client certificate authentication.

Ripple ensures the integrity of the transaction data being communicated between the parties by implementing keyed-hash message authentication code (HMAC) within the application. Using this HMAC process, a secret key is required to sign and send a valid message and only the parties to the transaction can compute if the key is valid. The cryptographic HMAC simultaneously verifies both the integrity of the data and the authenticity of the message, while the application level client certificate authentication ensures that only the holder of the private key is authorized to access the service.

Through these and other tactics, Ripple ensures information is not viewed or altered by unauthorized parties.

Further, providers are expected to adhere to the Ripple Solution Security Guide which requires notification to the company in a defined timeframe if a variety of security incidents occur. This ensures Ripple is aware of potential vulnerabilities, can quickly address the issue, and/or notify other providers of the potential vulnerability.

In summary, Ripple does not rely on the provider or financial institution for fraud monitoring any more than cross-border processes today. Yet, Ripple does provide sophisticated security measures to ensure the validity of payment messages.

We hope these comments have been helpful in better understanding Ripple’s solution. We extend our thanks to the time and effort Task Force members took in review our proposal.
Faster Payments QIAT

FINAL ASSESSMENT

Proposer: Ripple

Summary Description of Solution: Ripple uses Distributed Financial Technology (an open protocol called Interledger) to enable cross-border payments using direct two-way messaging between financial institutions (FIs) that join its network. The solution enables payers to see the total cost of the payment prior to authorization and settles transactions between FIs in real time, 24x7x365.

It does so through several components. The first is “Ripple Connect,” a plug-and-play software module that FIs license and integrate into their payment hub or core ledger. The second is “FX Connector,” which holds accounts with two or more FIs, providing liquidity for cross-border transactions between those institutions. The third is the “Notary,” an entity that FIs select to confirm that debit and credit have successfully occurred across multiple FI ledgers. The Notary is based on a software package that confirms cryptographic status messages regarding payment issues by Ripple Connect.

Ripple has helped establish a provider-run governance body to maintain a scheme that contains 1) commercial rules, and 2) technical standards for the execution of interbank transactions over Ripple technology. Outside the scheme, providers need to establish bilateral agreements with every counterparty. Within the scheme, providers integrate Ripple and adopt the scheme’s framework to enable interoperability with other providers participating in the scheme.

While the assessment of the Ripple proposal was conducted against the same Effectiveness Criteria applied to all other proposals, the QIAT acknowledges the differences in starting points between cross-border and domestic payments that impact certain criteria, such as user experience.

EXECUTIVE SUMMARY OF THE PROPOSAL

■ Major strengths

– If the originating and beneficiary provider are both on the Ripple Network, then the solution processes and settles payment within five seconds, plus the time of the provider’s compliance processes.

– The solution bolsters the certainty of the cross-border payment experience by providing end-to-end transaction visibility to banks, as well as settlement confirmation. Ripple enables more transparency in the total cost of a payment to the payee prior to authorization, if participating banks are willing to provide this transparency. However, effective transparency will depend on how participating banks deploy the solution to end-users.

– The solution facilitates additional liquidity options, as banks can use their own liquidity to fund payments but can also access liquidity through a competitive marketplace, wherein Ripple would select the authorized provider with the lowest-cost FX.

– The solution is flexible enough to be integrated directly into an FI’s payment hub, or it may be integrated into a third-party provider’s platforms to which FIs are already connected.

■ Areas for improvement and enhancement

– The solution does not address common standards and processes across FIs. This will present a challenge to the solution’s ability to achieve the user experience and speed of payments outlined in the proposal, particularly as FIs have control over many elements of the end-to-end payment process (e.g., authentication, availability of good funds, notification to end-users).
However, the new provider-run governance body should now help solve this challenge through a commercial rule set, though further details are not yet available.

- More detail is needed on how the solution will address cross-border differences in messaging formats, processing rules, regulatory issues, and conflicts across countries. These variations include differences in consumer protection and data privacy regulations.

- Ripple cannot access transaction data, which promotes privacy but prevents network-wide fraud monitoring unless the FIs choose to participate. In addition, the proposal does not specify dispute-handling rules, although it does refer to a participation agreement and commercial framework that would govern the relationship between Ripple and participating FIs.

■ Use cases addressed

- The proposal focuses on the cross-border payment use case, including low-value remittance payments (P2P), international corporate payments, international transaction-banking payments services, and cross-border intra-bank currency transfers.

■ Proposer’s overall ability to deliver proposed solution

- Ripple has 30 pilots at FIs globally, with access to over 60 currencies through channel partners. However, no deployment at scale has been completed to date.
Ubiquity

U.1 Accessibility

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

Rationale:
Ripple facilitates payments to/from all types of payment accounts in the FIs that are part of the network (U.1.1). Ripple supports payments from both banks and Regulated Non-bank Account providers (e.g., Western Union). Payments through the solution can reach any and all payees, as long as there is one Ripple-integrated FI in the payer’s country (other FIs first send to the Ripple-integrated FI through existing domestic payment systems) and one in the payee’s country (the Ripple-integrated FI sends funds over the existing domestic payment systems to the payee) (U.1.2). While Ripple does not facilitate domestic payments to/from all accounts for the cross-border use case addressed in the proposal, by focusing on cross-border, the solution supports multi-currency payments (U.1.3). Ripple outlines a plan for widespread adoption by starting with an indirect-access model (with only one FI integrated with Ripple), moving to a direct-access model over time (FIs access Ripple directly through their own integration or use of a payment service that becomes Ripple-enabled), and then moving to the use of multi-hop payments to scale and reach FIs that do not have common connectors (U.1.5).

The solution demonstrates technical feasibility for providers to adopt it through examples of FIs that are live; providers are motivated to participate by the benefits of improved transparency and speed in cross-border payments. Integration will require providers to change processes and operating systems in order to build new functionalities (e.g., escrow accounts) (U.1.5).

U.2 Usability

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

Rationale:
Ripple’s technology enables FIs to provide cross-border payment services to customers. An FI can use Ripple to provide a straightforward, simple end-user experience using a variety of access across channels, devices, and platforms as decided by the FI (U.2.1). Ripple operates and processes payments 24x7x365 (U.2.3).

Ripple does not provide the above functionalities and capabilities to End Users itself; rather, it relies on providers to do so (U.2.1, U.2.3). FIs have a great deal of flexibility in how they provide Ripple to customers and determine how to provide a user-friendly experience to customers. This flexibility for FIs is intentional in order to accommodate each country’s regulatory requirements for cross-border payments. Although Ripple is available 24x7x365, the provider FI can establish its own operating hours for sending and receiving payments. The FI also controls the availability to End Users through a variety of channels, devices and platforms, as well as how well varying levels of end-user technological proficiency and usability needs are addressed (U.2.4).

Ripple can enable payment with limited information, however, the need for information is defined by participating FIs. No standard set of information defined and no directory is provided as part of the solution (U.2.2).
## U.3 Predictability

<table>
<thead>
<tr>
<th>Rating</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very Effective</td>
<td>☐</td>
</tr>
<tr>
<td>Effective</td>
<td>☑</td>
</tr>
<tr>
<td>Somewhat Effective</td>
<td></td>
</tr>
<tr>
<td>Not Effective</td>
<td></td>
</tr>
</tbody>
</table>

**Rationale:**

Ripple provides predictability to the FI for how payments are processed in its baseline core features (U.3.1). The solution’s design ensures delivery of the baseline features and communication of those features to providers (e.g., cost of payment prior to payer authorization); providers are then responsible for delivering baseline features to end-users (U.3.2). Standard communication protocols through the Interledger protocol are used and a consistent message format is determined by the provider-run governance body established to ensure consistent, interoperable use of the solution (U.3.3). Since the FI is responsible for the end-user’s experience, Ripple itself cannot ensure reliability or standardization in that experience; however, the commercial rule set provides a way to do so through provider agreement (U.3.4).

The solution does not define error resolution protections, rights, and liabilities, instead indicating that the commercial rule set may do so (U.3.5). The solution also does not provide a generic, brand-agnostic term to distinguish the solution from other payment systems (U.3.6).

## U.4 Contextual data capability

<table>
<thead>
<tr>
<th>Rating</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very Effective</td>
<td>☐</td>
</tr>
<tr>
<td>Effective</td>
<td>☑</td>
</tr>
<tr>
<td>Somewhat Effective</td>
<td></td>
</tr>
<tr>
<td>Not Effective</td>
<td></td>
</tr>
</tbody>
</table>

**Rationale:**

Ripple supports the transfer of information to end-users by enabling messaging functionality to share contextual payment data, fees, and confirmations of acceptance and delivery (U.4.1). Ripple has helped to establish a provider-run governance body to maintain a scheme that includes technical standards for the execution of interbank payment transactions over Ripple technology. This body defines the message format based on standards defined by international standard-setting bodies (U.4.3).

The proposal would benefit from providing more detail on the integration of contextual data with interfacing business and personal finance systems (U.4.2).

## U.5 Cross-border functionality

<table>
<thead>
<tr>
<th>Rating</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very Effective</td>
<td>☑</td>
</tr>
<tr>
<td>Effective</td>
<td></td>
</tr>
<tr>
<td>Somewhat Effective</td>
<td></td>
</tr>
<tr>
<td>Not Effective</td>
<td></td>
</tr>
</tbody>
</table>

**Rationale:**

Ripple enables FIs to execute cross-border payments faster than the two to four days that are common today, if the originating and beneficiary providers are both connected to Ripple (U.5.1). The solution enables interoperability with real-time payment systems in other countries by using domestic networks when the originating and/or beneficiary provider is not on the Ripple network (U.5.2). Ripple enables visibility into the fees and FX cost before the payer authorizes the transaction (U.5.3) and relies on the commercial rule set to ensure that FIs make the required advance disclosure. Ripple provides an FX quote and fees through an FX Connector (third-party FX providers) or an FI’s own liquidity (nosto and vosto accounts) for conversion from one currency to another (U.5.4).
U.6 Applicability to multiple use cases

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

Rationale:
The solution focuses on the targeted use case of cross-border payments, initially on low to mid-value P2P and B2B payments, although the solution can be extended to cross-border P2B or B2P. The solution may also be extensible to domestic payments, though the proposal does not focus on this use case.

Efficiency

E.1 Enables competition

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

Rationale:
Ripple allows users to have a choice of providers just as they do today (E.1.). End-users who switch providers can continue to use Ripple if the FI participates in the network. The commercial rule set requires disclosures (E.1.3). All providers are allowed to provide services as long as they meet participation requirements (E.1.4).

The proposal would benefit from providing more detail on how the solution allows entities to easily switch providers or use multiple providers (e.g., receive money using the Ripple network to payment accounts at different FIs) (E.1.2).

E.2 Capability to enable value-added services

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

Rationale:
Providers integrate with the solution using RESTful APIs. Providers, regardless of size or incumbency, can offer value-added services as long as they meet participation requirements (E.2.1-2). Future value-added services may include a liquidity sourcing and management service, or customizable risk-monitoring tools. The solution enables providers to disclose to customers that value-added services are optional (E.2.3).

E.3 Implementation timeline

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

Rationale:
To achieve faster cross-border payments, Ripple must connect to a network of banks, with at least one FI in each country. Ripple has completed 30 pilots at FIs globally and has 90 active customers in the pipeline, 10 commercial deals underway, and channel partners’ enabling
access to over 60 currencies. However, there has not yet been a commercial deployment at scale. In addition, further details are needed on funding, hurdles, which entities are expected to adopt the solution first, market share, and growth projections (E.3.1).

E.4 Payment format standards

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
Ripple supports a variety of messaging standards but does not set a particular standard for use (E.4.1). The provider-run governing body will define the messaging format, based on standards defined by international standard-setting bodies (E.4.5).

More clarity would be helpful on the exact message format the governing body intends to use. In addition, the proposal does not describe the mechanism for updates to message formats to facilitate innovation (E.4.4).

E.5 Comprehensive

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The solution focuses on clearing and settlement. In concert with FIs, which are responsible for the other aspects of the end-to-end payment process, Ripple is able to deliver an end-to-end payment process from initiation to reconciliation (E.5.1). The solution’s technical design supports all of its features (E.5.2).

E.6 Scalability and adaptability

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The technical design supports the projected use cases focused on cross-border payments (E.6.1). Ripple governs the closed network and can provide updates to adapt technical design to ongoing developments through quarterly upgrades to the Ripple Connect software, with backwards compatibility (E.6.3).

Further detail would be helpful on the solution’s projected transaction volumes and how the solution supports those volumes and values at peak times or periods of stress (E.6.2).

E.7 Exceptions and investigations process

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
Ripple provides transaction data to FIs with each payment for full visibility. Its messaging function includes flexible, open-ended fields that enable a two-way conversation between banks that could be used to help identify and potentially resolve fraud or other issues.
The solution does not, however, provide any other tools, messages, alerts, or notifications to help address exceptions (E.7.1). Each FI must each handle its own investigation and exception-handling processes and find ways to resolve disputes with other FIs (E.7.1, E.7.2). Since Ripple does not see the transaction data, it does not record or retain this information or aggregate exceptions data to spot patterns (E.7.2, E.7.3).

Safety and Security

S.1 Risk management

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The proposal refers to a participation agreement and commercial rules that include a risk framework. The participation agreement and commercial framework cover commercial matters (including roles, responsibilities, rights and obligations, including FI rights and liabilities, when using Ripple).

Ripple’s commercial rules outline obligations of participants in terms of systemic, replacement and principal risk, and provides a base for updating and amending rules when needed. Monitoring of compliance will reside with the participating FIs, which can also define which other parties then can safely interact with.

The risk management framework described does not go into detail around operational risks (S.1.3) and the risk of authorized, fraudulent, and erroneous payments (S.1.4).

S.2 Payer authorization

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
Payers authorize to their FI with each payment initiation (S.2.1). Payment authorization occurs in the same channel in which the payer initiates the transaction. Ripple enables visibility into the fees and FX cost before the payer authorizes the transaction, although whether this user experience is enforced by operating rules is not clear. The solution does not address pre-authorization of payments (S.2.2-3).

S.3 Payment finality

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
Instead of the FI, a notary confirms good funds by confirming the accuracy of the cryptographic signatures indicating that the payment is fully funded in each escrow account. The payment becomes irrevocable once the notary approves and the commercial rules document how funds will be released after approval. Following approval, the FIs will receive Interledger instructions to release funds from their respective escrow accounts (S.3.1-2).
No mechanisms or processes are defined for protecting or compensating the payer in the event that the payment is disputed, beyond compliance with consumer laws (S.3.3)

S.4 Settlement approach

**Rationale:**
The Ripple solution settles in commercial bank money (S.4.3) using synchronized transactions on the books of the originating and beneficiary FIs through the Interledger protocol. Within the Ripple system and using the same liquidity provider, this real-time gross settlement can occur in less than one second. It is up to the FIs or the governing body to use real-time gross settlement or deferred net settlement to exchange value with the Ripple liquidity providers; it is also up to the FIs to define terms, risk limits, and settlement periods and operating hours (S.4.1, S.4.3).

The commercial rules provide a common understanding of how payments are settled, but more clarity would be helpful as to how the solution manages credit and liquidity risk arising from the use of commercial bank money in settlement and in cases of deferred net settlement that causes a lag between transaction finality and settlement (S.4.3).

S.5 Handling disputed payments

**Rationale:**
The proposal refers to a participation agreement and commercial framework that define the process, rights, and obligations for addressing disputed payments between FIs. The proposal does not describe mechanisms for any party to the transaction to request prompt voluntary return of funds from the payee (S.5.3), but leaves the approach to these transactions to participating FIs. If needed, rules can be established in the commercial agreement for the solution. In addition, more detail is needed on the rules around requirements, processes and timeframes for addressing disputed payments (S.5.1). While the commercial framework is said to include key provisions around loss allocation and indicates that the liability for unauthorized transfers arising from the result of provider negligence is on the provider, further detail is needed on the approach to support the reasonable protection of consumers, businesses and governments against losses related to errors (S.5.4, S.5.5).

S.6 Fraud information-sharing

**Rationale:**
Ripple reduces the likelihood of some common fraud techniques and provides greater transparency to investigate fraud. The solution facilitates information-sharing that supports the management and monitoring of fraud through Ripple Connect, which consolidates payment information in a user-friendly format to allow FIs to share contextual and fraud information if they so choose (S.6.1).
However, Ripple does not see transaction data and does not require providers to share information in order to manage and monitor fraud (S.6.1). Ripple does not aggregate, manage or protect data owned by entities other than providers for purposes of fraud information-sharing (S.6.2). Ripple does not provide timely updates and alerts for fraud (S.6.3). In the solution, FIs are responsible for fraud detection, reporting, and resolution of the transactions they process. Ripple does not have information-sharing mechanisms through a central, authoritative, trusted source to support differential access to content or to aggregate fraud information to spot patterns (S.6.5-7). The provider-run governance body could choose to aggregate fraud information among participants to spot patterns (S.6.7).

### S.7 Security controls

<table>
<thead>
<tr>
<th></th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Rationale:</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The traffic between Ripple Connect and FIs is encrypted and occurs over secure HTTPS (S.7.1). Much of the security, such as data retention and disposal controls, relies on FIs (S.7.2). The commercial rules for the solution contractually obligate providers to take “commercially reasonable security measures” to detect fraud. In addition, providers are motivated to improve the security of each transaction since the commercial rules allocate liability to providers in cases where an unauthorized transfer is a result of provider negligence (S.7.3). Additional detail would be helpful on the other sub-criteria, including technical access components and controls – e.g., data breach prevention and detection, layered security controls, and operational and procedural components and controls. More information is likewise needed on the solution’s physical security, operations security and monitoring, Ripple’s managerial policies and oversight, and the solution’s adaptability to enterprise-level security architectures (S.7.1-3).</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### S.8 Resiliency

<table>
<thead>
<tr>
<th></th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Rationale:</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The solution uses distributed financial technology, which means that there is not a central operator or single point of failure in the solution. If one participant goes offline, that does not affect other institutions’ ability to transact (S.8.3). The proposal response indicates work completed around business continuity and disaster recovery plans, audits, availability metrics, incident severity system and user support expectations. The proposal would benefit from more detail in each of these areas (S.8.1-5).</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### S.9 End-user data protection

<table>
<thead>
<tr>
<th></th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Rationale:</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The solution describes a commercial ruleset that defines expectations for data protection. Data transferred by Ripple Connect between the FIs is encrypted and occurs over secure HTTPS</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
connections using OAuth 2.0 for authentication. The commercial ruleset requires participating FIs to protect confidential information, including data information at rest and the sensitive information needed for account set-up, transaction set-up and to process and complete a payment (S.9.1-3).

Detail is not provided on the types of controls and mechanisms to protect the sensitive information. While Ripple technology allows providers to provide services that let Payers and Payees initiate or receive without knowing each other's Account numbers, Ripple does not define these requirements (S.9.2-3).

S.10 End-user/provider authentication

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
FIs are responsible for end-user authentication and for due diligence on other FIs to which it wants to send money without any Ripple-imposed minimum requirements (S.10.1). This due diligence includes assessing the onboarding and compliance policies of the counterparty. The payment scheme run by the governing body is likely to develop authentication requirements, but further details would be helpful.

The proposal does not describe mechanisms to ensure that a payment reaches the intended payee account (S.10.2), nor mechanisms to apply strong authentication procedures based on the risk-weighting of a transaction (this is up to the FI) (S.10.4-5). The proposal does not explain how new authentication models would be adopted and old models decommissioned (S.10.6).

S.11 Participation requirements

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale**
A commercial rule set governs commercial matters pertaining to the solution, including roles, responsibilities, rights, and obligations (S.11.1-2).

The proposal would benefit from detailing the process for monitoring and ensuring providers’ compliance with participation requirements (S.11.3).

**Speed (Fast)**

F.1 Fast approval

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The Ripple technology supports approval within two seconds when both the originating and beneficiary providers are using the Ripple solution, since the originating FI can use Ripple Connect to find the FX Connector with sufficient liquidity within milliseconds. However, Ripple does not describe operating rules to enforce fast approval, nor to ensure 24x7x365 operations.
F.2 Fast clearing

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The Ripple technology supports clearing within five seconds when both the originating and beneficiary providers are using the Ripple solution. The clearing process occurs between the FIs through Ripple Connect over HTTPS, typically within five seconds. The two FIs share payment information and determine fees, FX rates, and delivery times. However, Ripple does not describe operating rules to enforce fast clearing; such rules fall under the purview of the governing body.

F.3 Fast availability of good funds to payee

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The Ripple technology enables immediate availability of good funds when both the originating and beneficiary providers are using the Ripple solution, but it allows FIs to delay funds’ release (hold the funds after settlement for a period of time) to the payee to protect against unauthorized, erroneous, or fraudulent payment. Ripple does not describe operating rules to enforce fast availability of good funds to the payee; such rules would fall under the purview of the governing body.

F.4 Fast settlement among depository institutions and regulated non-bank account providers

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The Ripple technology enables real-time gross settlement or deferred settlement in commercial bank money within five seconds—plus the time of the provider’s compliance processes—when both the originating and beneficiary providers are using the Ripple solution. Ripple does not describe operating rules to enforce fast settlement; such rules would fall under the purview of the governing body.

F.5 Prompt visibility of payment status

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The Ripple technology supports tracking of the payment at various stages of the payment process, with visibility of status within five seconds. FIs use Ripple Connect and the payment ID to track the payment’s status in real time and to update the payer and payee as to that status.
Ripple does not describe operating rules to enforce prompt visibility of payment status to the payer and payee; such rules would fall under the purview of the governing body.

Legal

L.1 Legal framework

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The solution relies on a set of commercial rules established by a Global Payments Steering Group, consisting of major participating FIs. These commercial rules establish the legal framework for all participants.

Detail on legal framework, the applicable legal sources, the gaps in legal sources, and unique legal provisions are not yet provided (L.1.1-2, L.1.5).

L.2 Payment system rules

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The solution relies on a set of commercial rules established by a Global Payments Steering Group, consisting of major participating FIs. Key features of the payment system rules—such as payment finality or error resolution—will be defined by these commercial rules. They will also govern how rules can be amended and non-compliance can be sanctioned.

While the proposal references the commercial rules and describes high-level features, more detail is not provided such as on error resolution (L.2.1, L.2.5) and the amendment process (L.2.2).

L.3 Consumer protections

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The solution generally relies on FIs’ legal framework. As the consumer payer and payee remain customers of the FI, the consumer laws that apply to FIs remain applicable. The proposal does not provide details on the solution’s commercial rule set as they pertain to consumer protections. The solution does not detail how consumer protection laws can be met across borders, particularly when regulations and requirements differ by country, though the commercial ruleset can address

L.4 Data privacy

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>
Rationale:

FIs determine the payer and payee information they require to ensure compliance with their own procedures and their jurisdiction’s laws (L.4.1). The Ripple commercial rules defines ‘confidential information’ and determines when information is protected, as well as defining the obligations of all parties to protect data. It defines the permissible and restricted uses of personal data shared during the payment cycle. FIs are bound by this agreement (L.4.1). Data shared between FIs over Ripple Connect is encrypted (L.4.2).

The proposal does not address how end-users can view the data that is collected on them (L.4.4), but leaves that to the discretion of the FIs. It also does not describe its approach to data breaches of the payment system, the end-user, or the provider (L.4.5). In addition, the proposal does not address how to manage and reconcile the diversity of data privacy rules by country. These aspects can however be included in the commercial rules.

L.5 Intellectual property

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale:

The solution has taken a due diligence review of intellectual property (IP) rights and is establishing procedures for third parties to bring any IP concerns to Ripple’s attention. Interledger, the open protocol used by Ripple, is an open-source standard and thus should remain free for everyone to use.

Governance

G.1 Effective governance

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale:

Ripple’s governance is defined by participation agreements and its commercial framework. The Global Payments Steering Group (GPSG) provides a good basis for governance to ensure consistent, interoperable use of the solution; however, details of the governing body’s structure and terms are not yet shared.

The QIAT has interpreted the Effectiveness Criteria such that solutions at this stage of development earn a rating of “Somewhat Effective.”

G.2 Inclusive governance

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale:

Ripple’s governance is defined by participation agreements and its commercial framework. The Interledger protocol’s governance is provided through the World Wide Web Consortium, which includes a broad set of participants. The GPSG is a provider-run governance body to ensure consistent, interoperable use of the solution; however, details of the governance body’s
structure and terms are not yet shared, in particular, how input and influence from stakeholders beyond the GPSG members will be enabled

The QIAT has interpreted the Effectiveness Criteria such that solutions at this stage of development earn a rating of “Somewhat Effective.”