# 产品概述

xCurrent 的技术概述

2017年10月

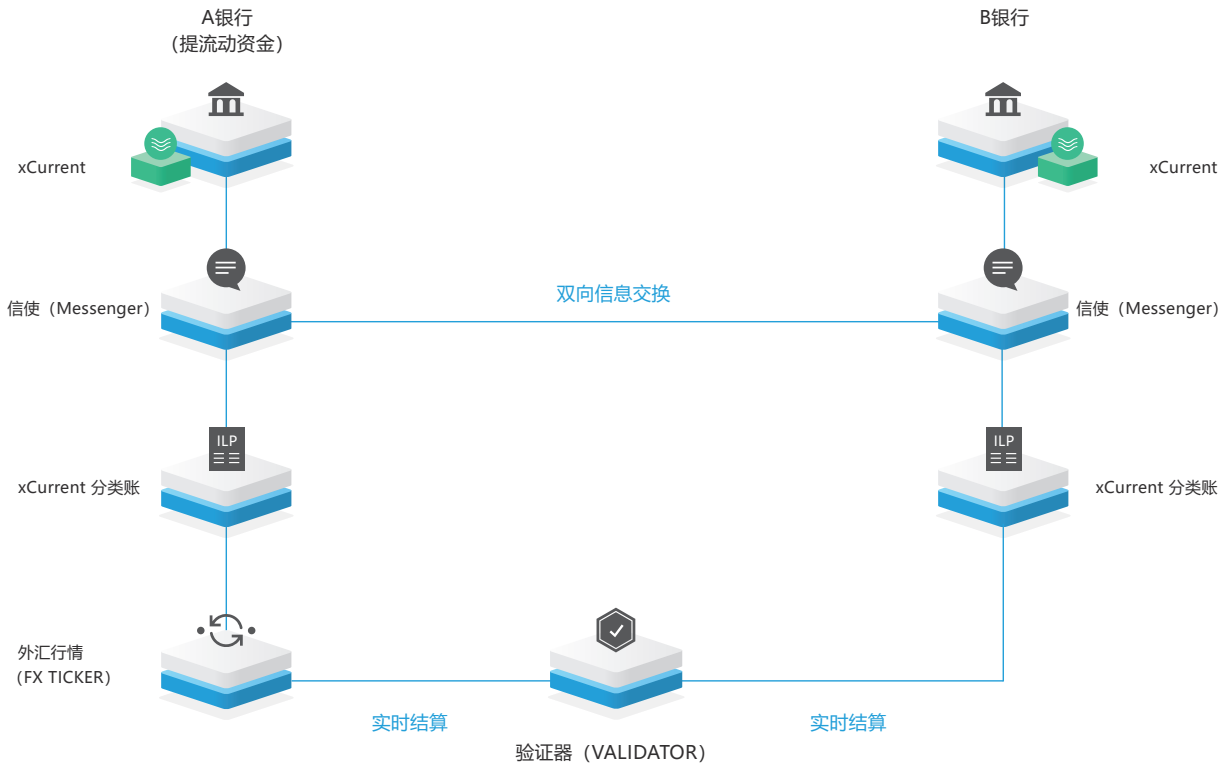
ripple

# 流畅的全球支付体验

一项贯通全球金融机构网络的统一技术

# 产品概述

作为一项 Ripple 针对银行推出的解决方案，xCurrent 是围绕一个开放式中立跨账本协议 Interledger Protocol、 即 ILP 而建立的，旨在实现不同分类账和网络之间的交互操作。它提供一个加密安全的终端到终端支付流程，它的设计旨在支持每个银行各自的风险、隐私和合规要求。它的设计目的是遵从每个银行的风险、隐私和合规要求。该软件的架构适合于银行现有的基础设施，可以最大限度地减少整合开销和业务中断。




### 信使（MESSENGER）

信使 (Messenger) 是基于 API 的 xCurrent 双向消息传递组件。它可以连接到收款银行的实时信使 (Messenger)，就交易信息、支付费用、外汇汇率(如果适用)、支付细节和预期的资金交付时间进行相互交换。它将这些信息打包，并将整个成本构成提交给发款银行，为交易的总成本提供了前所未有的可见性。如果信息不正确或缺少，交易参与方会在启动交易之前发现，从而大大增加直通处理的成功率。此外，银行可以用信使 (Messenger) 为付款设置费用和外汇汇率。外汇汇率在外汇行情 (FX TICKER) 中设置，并在报价过程中使用 信使 (Messenger) 查询。

每一笔付款都有一个付款 ID，可用于在付款执行的任何时间查询付款状态，包括资金结算进行中或之后，从而对失败的或延迟的付款进行更有效的故障排除。利用信使 (Messenger) 交换的付款数据可用于满足司法管辖区内特定的监管需求和其他增强服务。信使 (Messenger) 利用传输层安全性（TLS）v1.2，以便与现有的银行系统、合作伙伴信使 (Messenger)和 xCurrent 的 ILP 组件进行安全通讯。

### 验证器（VALIDATOR）

验证器 (Validator) 是以加密方式确认付款成功或失败的组件。它以消除所有结算风险和实现最小化结算延迟的方式，协调各交易方 xCurrent 分类账上的资金流动。验证器 (Validator) 为交易对手提供唯一的真相来源，同时保护银行客户可识别性付款信息的隐私。银行可以选择将自己的验证器 (Validator) 应用于所有交易中，或者依赖于交易对方运行的验证器 (Validator)。

### XCURRENT 分类账

xCurrent 分类账是每个交易银行总账本的分类账本。xCurrent 的这一组件被用来追踪交易各方的信贷、借记和流动资金。xCurrent 分类账使交易各方能够以原子方式结算资金，这意味着无论涉及多少参与方，整个交易要么即时结算，要么全部不结算。

xCurrent 分类账以毫秒为单位完成资金结算。此外，因为付款或完全处理好，或在结算之前就已失败，所以结算风险被消除。xCurrent 分类账旨在 7 天 24 小时为银行提供按需服务。这些功能综合起来能够使银行提供小额、按需的国际汇款产品和业务，并从中获利。

### 外汇行情（FX TICKER）

外汇行情 (FX Ticker) 是xCurrent 的组成部分，通过流动资金提供商发布外汇汇率，来促成 xCurrent 分类账之间的往来。此组件提供它所设置的任何一对分类账之间的汇率。此外，它还追踪每个已设置的 xCurrent 分类账的账户、货币和账户拥有方验证凭据。在交易过程中，它为结算而协调 xCurrent 分类账上的转账，确保外汇报价的有效性，并将付款金额转账到收款银行的 xCurrent 分类账。

# 工作原理

## 资金流动

本节将使用示例付款来演示如何通过 xCurrent 实现资金流动。在这个例子中，Alpha 公司（美国）需要支付 Beta 公司（欧元区）共计 100 欧元。Alpha 公司在美国的美元银行开有一个账户，Beta 公司在欧盟的欧元银行开有一个账户。两家银行都整合了 Ripple 的软件 xCurrent。


### 设置

为了使跨货币汇款通过 xCurrent 流通，银行可以利用其现有的与其他银行的往来账户关系，通过其外汇交 易部门提供流动资金，或使用外部流动资金做市商为稀有货币渠道提供外汇流动资金。此示例将该功能作为流动资金提供商，无论是银行的外汇部门还是外部流动资金做市商。

作为设置过程的一部分，流动资金提供商确保收款银行账户已有预付的本地货币资金。

美元银行的分类账

| 账户 | 借 | 贷 | 余额 |
|---|---|---|---|
| 发款方 | | | $10,000 |
| 流动资金提供商 | | | |
| 费用 | | | |
| Ripple 的独立账户 | | | |

欧元银行的分类账

| 账户 | 借 | 贷 | 余额 |
|---|---|---|---|
| 收款方 | | | €3,000 |
| 流动资金提供商 | | €200,000 | €200,000 |
| 费用 | | | |
| Ripple 的独立账户 | | | |

美元银行的 Ripple xCurrent 分类账

| 账户 | 借 | 贷 | 余额 |
|---|---|---|---|
| 搁置 | | | |
| 流动资金提供商 | | | |

欧元银行的Ripple xCurrent 分类账

| 账户 | 借 | 贷 | 余额 |
|---|---|---|---|
| 搁置 | | | |
| 流动资金提供商 | | | |

每家银行设立一个独立账户，其余额反映在 xCurrent 分类账上（一种追踪流动资金提供商资金状况的子分类账）。流动资金提供商对该独立账户所作出的任何资金投入都反映在流动资金提供商的 xCurrent 分类账上。

在此示例中，流动资金提供商将提供 4 万欧元可用资金用作 Ripple 交易的支付款。对于双向流动，流动资金提供商也将在他们的美元账户预先放入资金并将部分流动资金转移至独立账户。这个例子中只显示从美元银行到欧元银行的付款。

美元银行的分类账

| 账户 | 借 | 贷 | 余额 |
|---|---|---|---|
| 发款方 | | | $10,000 |
| 流动资金提供商 | | | |
| 费用 | | | |
| Ripple 的独立账户 | | | |

欧元银行的分类账

| 账户 | 借 | 贷 | 余额 |
|---|---|---|---|
| 收款方 | | | €3,000 |
| 流动资金提供商 | | €200,000 | €200,000 |
| | €40,000 | | €160,000 |
| 费用 | | | |
| Ripple 的独立账户 | | €40,000 | €40,000 |

美元银行的 Ripple into xCurrent 分类账

| 账户 | 借 | 贷 | 余额 |
|---|---|---|---|
| 搁置 | | | |
| 流动资金提供商 | | | |

欧元银行的 Ripple into xCurrent 分类账

| 账户 | 借 | 贷 | 余额 |
|---|---|---|---|
| 搁置 | | | |
| 流动资金提供商 | | €40,000 | €40,000 |

一旦独立账户获得资金，流动资金提供商就针对发款银行向外汇行情 (FX Ticker) 发布外汇汇率报价。在这个例子中，欧元/美元的汇率为1.1429。

**付款流程：整合汇款报文处理和结算**

如果一笔付款由 Alpha 公司发起，两家银行的信使 (Messenger) 会交换有关 Alpha 公司和 Beta 公司的信息，以便进行了解客户（KYC）/反洗钱（AML）的核实与制裁审查。这些客户信息以及私密信息完全由两家银行进行设置。发款方的信使 (Messenger) 也会询问欧元银行有关交付 Beta 公司付款的处理费用。它同时也从流动资金提供商（可以是银行的外汇部门）获得兑换率。

美元银行的信使 (Messenger) 编辑此信息，并加上他们的处理费用，向银行呈现交易的全部费用。假设美元银行的费用为 5 美元，欧元银行的费用为 5 欧元，而欧元/美元的汇率为 1.1429，向 Beta 公司汇出 100 欧元的总成本为 125 美元。一旦 Alpha 公司接受了要价，付款就开始了。美元银行扣除 Alpha公司的账户金额 125 美元，收取 5 美元的费用，并贷记 120 美元至独立账户。

这些资金尚未贷记给流动资金提供商。它们会被搁置，直到欧元银行为验证器 (Validator) 提供证明，证实它也把资金搁置并能转到 Beta 公司。

美元银行的分类账

| 账户 | 借 | 贷 | 余额 |
|---|---|---|---|
| 发款方 | | | $10,000 |
| | $125 | | $9,875 |
| 流动资金提供商 | | | |
| | | | |
| 费用 | | $5 | $5 |
| | | | |
| Ripple 的独立账户 | | $120 | $120 |
| | | | |

欧元银行的分类账

| 账户 | 借 | 贷 | 余额 |
|---|---|---|---|
| 收款方 | | | €3,000 |
| | | | |
| 流动资金提供商 | | €200,000 | €200,000 |
| | €40,000 | | €160,000 |
| 费用 | | | |
| | | | |
| Ripple 的独立账户 | | €40,000 | €40,000 |
| | | | |

美元银行的 Ripple xCurrent 分类账

| 账户 | 借 | 贷 | 余额 |
|---|---|---|---|
| 搁置 | | $120 | $120 |
| | | | |
| 流动资金提供商 | | | |
| | | | |

欧元银行的 Ripple xCurrent 分类账

| 账户 | 借 | 贷 | 余额 |
|---|---|---|---|
| 搁置 | | | |
| | | | |
| 流动资金提供商 | | €40,000 | €40,000 |
| | | | |

欧元银行也将 105 欧元搁置，并向验证器 (Validator) 提供加密收据，证明该条件已经满足。这将启动验证器 (Validator) 指示美元银行将来自 Alpha 公司的资金搁置，并提供搁置的加密收据。这些收据包含资金搁置的密码证明，但不包含关于银行、交易方或付款细节的任何信息。

| 美元银行的分类账 | | | |
|---|---|---|---|
| 账户 | 借 | 贷 | 余额 |
| 发款方 | | | $10,000 |
| | $125 | | $9,875 |
| 流动资金提供商 | | | |
| | | | |
| 费用 | | $5 | $5 |
| | | | |
| Ripple 的独立账户 | | $120 | $120 |
| | | | |

| 欧元银行的分类账 | | | |
|---|---|---|---|
| 账户 | 借 | 贷 | 余额 |
| 收款方 | | | €3,000 |
| | | | |
| 流动资金提供商 | | €200,000 | €200,000 |
| | €40,000 | | €160,000 |
| 费用 | | | |
| | | | |
| Ripple 的独立账户 | | €40,000 | €40,000 |
| | | | |

| 美元银行的 Ripple xCurrent 分类账 | | | |
|---|---|---|---|
| 账户 | 借 | 贷 | 余额 |
| 搁置 | | $120 | $120 |
| | | | |
| 流动资金提供商 | | | |
| | | | |

| 欧元银行的 Ripple xCurrent 分类账 | | | |
|---|---|---|---|
| 账户 | 借 | 贷 | 余额 |
| 搁置 | | €105 | €105 |
| | | | |
| 流动资金提供商 | | €40,000 | €40,000 |
| | €105 | | €39,895 |

一旦验证器 (Validator) 收到证据证明两家银行都将资金搁置，它就会启动资金结算，指示两个分类账释放并转移搁置的资金。这是一个原子过程，意味着两个异地银行结算的交易同时发生， 从而消除了结算的风险。

**关于第三方验证者的注意事项：**从理论上讲，第三方可以运行一个验证器 (Validator) 的网络，通过拜占庭式容错 (BFT) 的共识算法达到共识，不存在将受保护的敏感数据传递给第三方或将其发布到公共分布式分类账中的风险。交易细节保密，只对交易银行公开，而验证器 (Validator) 只用于验证是否已满足某些加密条件（如：是否有可用的资金用于交付）。

美元银行的分类账

| 账户 | 借 | 贷 | 余额 |
|---|---|---|---|
| 发款方 | | | $10,000 |
| | $125 | | $9,875 |
| 流动资金提供商 | | | |
| | | | |
| 费用 | | $5 | $5 |
| | | | |
| Ripple 的独立账户 | | $120 | $120 |
| | | | |

欧元银行的分类账

| 账户 | 借 | 贷 | 余额 |
|---|---|---|---|
| 收款方 | | | €3,000 |
| | | €100 | €3,100 |
| 流动资金提供商 | | €200,000 | €200,000 |
| | €40,000 | | €160,000 |
| 费用 | | €5 | €5 |
| | | | |
| Ripple 的独立账户 | | €40,000 | €40,000 |
| | €105 | | €39,895 |

美元银行的 Ripple xCurrent 分类账

| 账户 | 借 | 贷 | 余额 |
|---|---|---|---|
| 搁置 | | $120 | $120 |
| | $120 | | $0 |
| 流动资金提供商 | | $120 | $120 |
| | | | |

欧元银行的 Ripple xCurrent 分类账

| 账户 | 借 | 贷 | 余额 |
|---|---|---|---|
| 搁置 | | €105 | €105 |
| | €105 | | €0 |
| 流动资金提供商 | | €40,000 | €40,000 |
| | €105 | | €39,895 |

一旦交易在两个 xCurrent 分类账上结算，欧元银行将收取 5 欧元的费用，并将 100 欧元交付至 Beta 公司的账户。

一旦资金到达 Beta 公司的账户，美元银行会接到通知，可以立刻向 Alpha 公司提供付款确认信息。

## API 操作流程

执行“资金流动”部分中描述的付款，须涉及下列对信使 (Messenger) 的 API 请求。

### 报价流程

1. 发款方通过在银行客户端应用程序（可能是现有网上银行系统的一部分）提供有关付款的信息来启动流程。此信息必须至少包括以下内容：
   a. **付款人：** 发款方。
   **b. 收款人：** 付款收款方。
   c. 支付**金额**和**货币**，及其是否为“付款人”或“收款人”金额：
      - **付款人金额：** 指定金额从付款人账户中扣除。信使 (Messenger) 可以计算费用和外汇成本，并从付款人的账户中扣除。剩余的金额贷记入收款人的账户。
      - **收款人金额：** 指定的金额贷记入收款人的账户。该金额根据付款人的币种从付款人账户中扣除。信使 (Messenger) 计算费用和外汇成本 — 将它们添加到从付款人账户中扣除的金额。发款银行使用发款方提供的信息对其自己的信使 (Messenger) 进行询价请求。

2. 发款银行的信使 (Messenger) 将询价请求发给收款银行的信使 (Messenger)，以接收其付款中属于它的部分，其中包括其费用（在示例中为 5 欧元）和空字段，指示收款银行处理付款所需的任何附加信息。
3. 位于发款银行的信使 (Messenger) 获取由流动资金提供商自外汇行情 (FX Ticker) 发布的外汇汇率。
4. 发款银行得出付款中它的部分，包括它的费用（在示例中为 5 美元）。


5. 发款银行收到对其询价请求的响应，并将报价单传递给初始付款人，以确定付款条件（包括收款银行和发款银行的费用以及外汇兑换率）是可以接受的。如果条款是可接受的，则发款银行将做出接受报价请求。如果收款银行信使 (Messenger) 的设置对付款要求有更多信息，则发款银行将在接受报价请求中提供所要求的信息（虽然在技术上不需要额外的付款信息，但出于监管上的原因，金融机构通常需要与 pacs.008 或 MT 103 报文相类似的信息来处理付款）。 信使 (Messenger) 生成一个付款 ID，它包含在接受报价回复中。收款银行审查报价并执行合规检查，以确保：
   a. 付款条件是可以接受的。
   b. 要求发款银行提供的额外付款信息被提供了，并足以处理付款。

6. 如果条款和额外付款信息是可接受的，则收款银行将发出锁定报价请求。锁定报价表示双方打算处理付款，并按照付款合同字段中所描述的方式交付资金。在报价单锁定后，合同字段是无法更改的。
7. 发款银行的信使 (Messenger) 接收到付款现在已锁定的通知，并在其数据库中更新付款状态，以反映新状态。


两个机构现在有一个相同的付款都处于锁定状态，含有两个机构需要执行付款的所有信息。

**付款流程**

在两家银行接受报价后，发款银行可以启动端对端支付，该付款由三个子付款组成：

- **发送付款:** 发款银行的内部账面移交。发款银行在发款方的账户中扣除款项，并存入其自己的独立账户。在此次转账中，发款银行收取的任何费用均从发款方的账户中扣除。
- **结算付款：** 通过跨账本协议执行转账资金从发款银行的交易账户（其 xCurrent 分类账上）转移到收款银行的交易账户（在其 xCurrent 分类账上）。当发款银行发出提交子付款请求时，转账会被自动启动。执行结算付款不需要发款银行这边采取任何其他行动。
- **接收付款：** 收款银行的内部账面移交。收款银行借出自己的独立账户并贷记收款方的账户。在此次转账中，收款银行收取的任何费用均从收款方账户中扣除。

执行端到端支付包括以下步骤：

1. 发款银行进行内部账面移交，扣除付款人账户的资金。在上面的例子中，扣除了 125 美元：120 美元为付款，5 美元为发款银行的费用。
2. 发款银行向信使 (Messenger) 发出提交发送付款请求，以承认这些资金已从该银行内部系统中的发款方账户中扣除。对信使 (Messenger) 的请求不影响银行的内部系统。通常，整合逻辑通过执行提交发送付款请求来协调内部系统中的（内部账面）移交。
3. 发款银行的信使 (Messenger) 通知收款银行的信使 (Messenger)，这些资金已从付款人的账户中扣除。
4. 提交发送付款请求启动结算付款，通过跨账本协议 (ILP) 将资金从发款银行的 xCurrent 分类账转移到收款银行的 xCurrent 分类账。
5. 发款银行的信使 (Messenger) 通知收款银行的信使 (Messenger) 结算付款已发送。
6. 收款银行发现 xCurrent 转账已经通过验证器 (Validator) 进行了验证，并进行了内部账面移交，将资金交付给收款方账户。
7. 收款银行对其信使 (Messenger) 执行提交接收付款请求，从而将付款的状态在其数据库内更改为成功。

8. 收款银行的信使 (Messenger) 通知发款银行的信使 (Messenger) 资金已经被交付到收款方的账户。
9. 收到通知后，发款银行的信使 (Messenger) 组件会将付款的状态在其数据库中更改为成功。

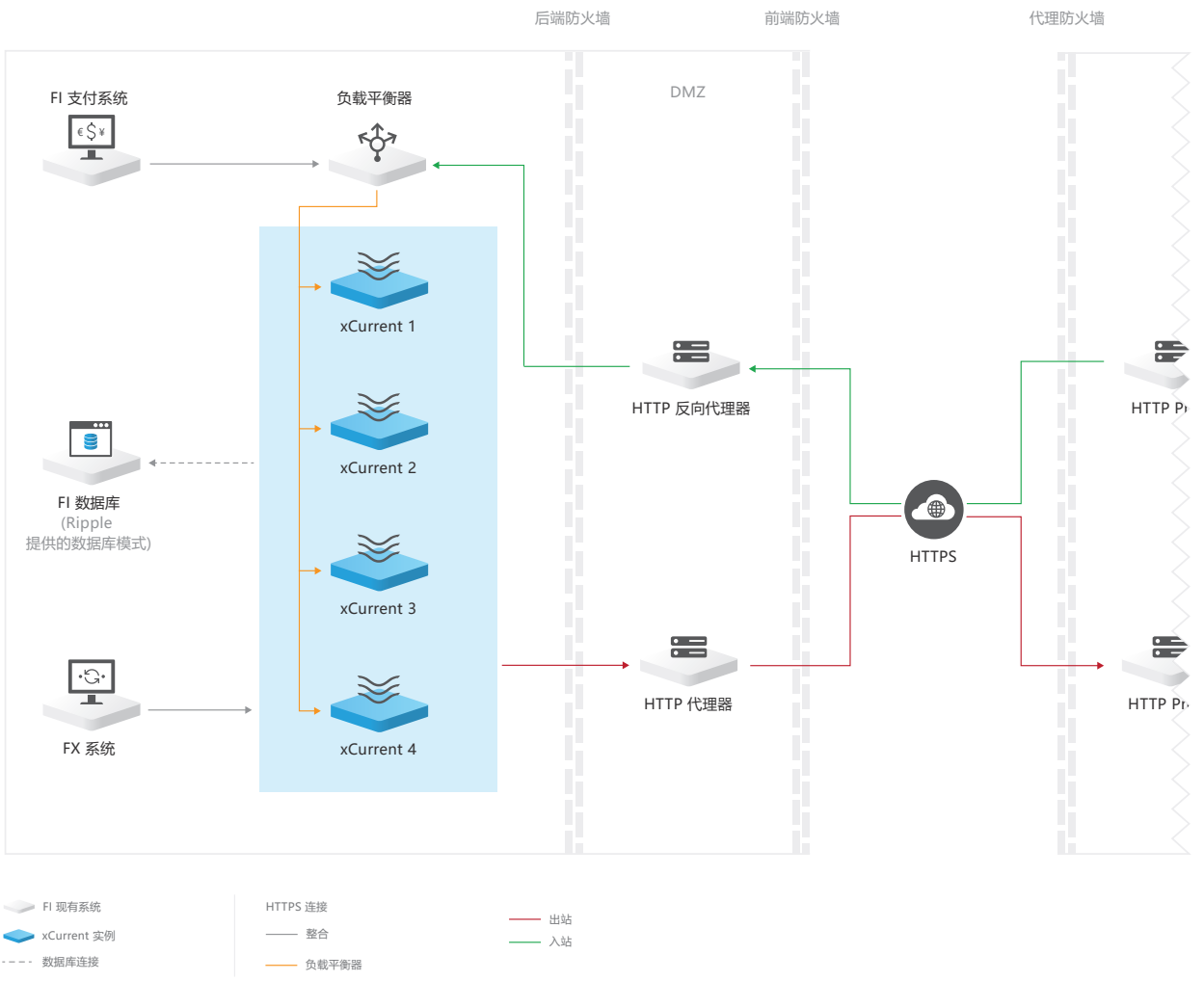
这时，双方认为付款完成。


付款现已完成。Alpha 公司汇出 125 美元，同时 100 欧元被汇入 Beta 公司的账户。

# 参考架构

xCurrent 通常安装在银行的公司防火墙后面的环境中，并使用负载均衡器来处理信使 (Messenger) 的入站连接，并使用代理服务器来处理所有 xCurrent 组件的入站和出站连接。银行可以在负载均衡器后面部署多个运行xCurrent 的服务器，以扩展其处理能力来支持相应的（增加的）付款量。下面的示例描述了 xCurrent 在银行的典型生产部署：

**启用 Ripple 的机构** **启用 Ripple 的机构**




备注：如果银行不提供流动资金，则只需设置信使 (Messenger) 和 xCurrent 分类账。

上面的关系图具有以下特点：

- 两个启用了 Ripple 的机构都可以通过 xCurrent 汇出和接收付款。
- 发款或收款机构均可提供流动资金。
- xCurrent 部署在安全可靠的网络区域中，位于公司防火墙和 DMZ 之后（xCurrent 不应部署在 DMZ 中）。
- xCurrent 的所有组件都应在单个应用程序服务器上共存，并通过 HTTPS 进行通讯，并使用 TLS 证书进行身份验证。
- xCurrent 部署应通过 HTTPS 与合作伙伴的 xCurrent 部署进行通讯，并使用 TLS 证书进行身份验证。
- xCurrent 支持所有服务的负载均衡和水平扩展，从而建立主动高可用 (HA) 部署。
- 用于信使 (Messenger)、xCurrent 分类账、验证器 (Validator) 和外汇行情 (FX Ticker) 的数据库是利用所提供的数据库模式创建的，并部署在同一数据库服务器上。
- 每个 xCurrent 组件（信使 (Messenger)、xCurrent 分类账、验证器 (Validator) 和外汇行情 (FX Ticker)）实例都需要访问数据库。它可以获得支持，每个组件可用各自单独的数据库，或所有 xCurrent 组件共用同一个数据库。
  Ripple 推荐第二种选择。

## 技术要求

| | |
|---|---|
| 操作系统 | Red Hat Enterprise Linux（RHEL）6.7 和 7.2 |
| 架构 | x86 （64 位） |
| 内存 | 8 GB |
| 中央处理器 | 4 核 |
| 磁盘存储 | 100 GB |
| 支持的数据库连接 | PostgreSQL 9.4<br>microsoft SQL Server®2012<br>microsoft SQL Server®2014 |
| 部署选项 | RPM |
| RPM 依赖关系 | Node. js v6.9.0 或更高版本 |

# 关于 Ripple

Ripple 利用区块链技术为全球支付提供了统一的流畅的体验。通过加入日益增长的 Ripple 全球网络，金融机构可以在世界任何地方即时、可靠和成本有效地处理客户付款。银行和支付服务供应商可以利用数字资产 XRP 进一步降低成本和进入新市场。

Ripple 在旧金山、纽约、伦敦、卢森堡、孟买、新加坡和悉尼设有办事处，有超过 100 家的客户遍布全球。

**联系我们**

欲了解加入 RippleNet 和利用 xCurrent 跨境付款的详细情况，
请通过 ripple.com/contact 联系我们。


ripple