瑞波（$XRP）研究报告

Myles Snider, Kyle Samani 和 Tushar Jain
2017 年 8 月 31 号

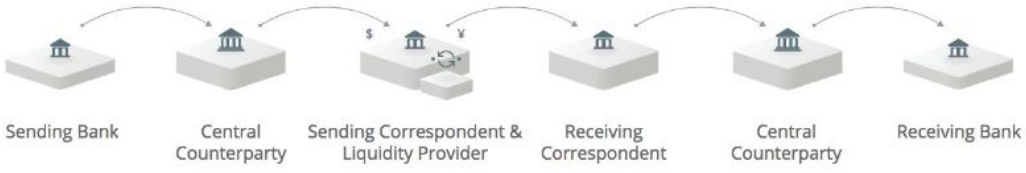
简介

请注意：在本报告中，我们将在多个语境中提到“瑞波（Ripple）”：
瑞波公司（Ripple Inc.）——一家总部位于加利佛尼亚州，由风险投资支持的 C 类股份公司
瑞波协议/网络（Ripple protocol/network）——银行内部通信的设计规范
瑞波币（XRP）——瑞波协议的原生，但非排他的货币
我们将在本报告中对它们进行区分。
瑞波是一个用于银行结算的区块链协议。不像很多其他的区块链，瑞波旨在与现有机构合作，以实现在全球快速交易*任何资产*。瑞波协议的原生货币 XRP 仅仅用于支付瑞波网络的交易费。它也可以用在别的场景，但银行可以选择办理任何资产的借据，包括美元、欧元和其它法定货币。瑞波公司则负责开发促进银行之间资产的去中心化交易的基础设施协议。
瑞波协议使用了一种叫做“瑞波协议共识算法”（简称 RPCA）的独特的共识机制。该算法与比特币的工作量证明或以太坊未来的权益证明共识模型不同。RPCA 的既定目标是提供更高的可扩展性和更快的确认时间。
瑞波协议是由瑞波公司开发和维护的，该公司是一家位于美国，筹集了超过 9,300 万美元风险资金的 C 类公司。目前，瑞波公司单方面控制着瑞波网络。这个安排以及瑞波公司计划逐渐实施平民化控制，会在下文进行讨论。
我们意识到瑞波协议有机会替代传统的银行间网络，但是我们必须分清一个区块链的好用途和一个好的投资机会之间的区别。我们认为瑞波协议满足前者，但 XRP 代币却不满足后者。瑞波协议能够影响价值万亿的经济活动，但是它的商业价值不太可能被 XRP 所捕获。XRP 代币除了用作微不足道的交易费用以外，没有其它的核心用途，因此它的价值不太可能随着瑞波网络使用的增加成比例增长。我们不会进行对 XRP 进行定量的估值，因为我们不认为 XRP 在定性方面是一个有吸引力的投资。

摘要

背景

原始的瑞波设计是古老的借据（IOU）网络的现代化、数字化实现。为了深入了解瑞波的机制，我们必须首先了解现代银行系统的一些基础知识。
在现代银行系统中，当我把钱存入我的银行账户时，实际上我是将该笔存款借贷给银行。银行就产生了一笔负债：它欠我的钱，而我可以在任何时候取回所有或一部分存款。我每存一次钱，本质上就是延伸了对银行的信用——我相信银行有能力偿还我的所有存款。
我很容易把 100 美元转账给使用同一个银行的朋友。银行内部将负债从一个债权人转移到另一个债权人。具体来说，银行将它对我的负债减少 100 美元，然后将它对我朋友的负债增加 100 美元。
该系统能发挥作用是由于我和我的朋友对银行都扩展了银行的信用，并且我们都相信当我们需要提款时，银行有能力偿还我们的存款。这笔交易体现为银行内部账本的改变，该账本记录了它欠每个客户的金额。
但是当我想转账给使用不同银行的朋友时，这个过程会变得更加复杂。在某些情况下，这两个银行可能存在信任关系，因此接收方银行愿意接受我的银行的借据，但很多时候情况不是这样的。如果我使用大通银行而我的朋友使用美国银行，那么我们之间的交易就不是一家银行更新它的内部账本那么简单了；相反，这些银行必须（在某个时间点）实际地交换货币。因为这类银行间的交易频繁发生，因此银行通常交换的是借据，然后再定期用实际的货币转移进行结算。这个借据系统使得交易更快速地进行。
然而，这个系统能够正常工作是因为银行之间（在我们的例子中是大通银行和美国银行）相互信任，能够履行兑现彼此的借据的责任。如果我们的银行没有这个信任关系，那么我们必须等到某笔账款实际上转移完成，或者该笔交易必须通过相互信任的第三方进行。这两种方式都比简单的借据发行更慢，成本也更高。并且这些交易在跨境情况下更加复杂，因为不同国家之间的银行不太可能建立可信的关系。
大通银行和釜山银行（一家韩国银行）可能就没有建立可信的关系。如果我想把钱从大通账户转到我朋友的釜山账户，这笔交易必须经过多方才能完成。而每一笔交易都需要成本和时间。因此国际支付非常缓慢和昂贵。



图片来源

瑞波账本的解决方案

瑞波网络通过用区块链替代上述系统——来消除摩擦、加快交易速度和结算时间，并大大降低成本。在很多方面，这是区块链技术完美的一个使用场景。传统系统速度慢、成本高并且容易出错；银行必须相互协作以实现不同内部数据之间的价值转移，使得快速结算交易极其困难。银行通常必须在国外银行开户，并用当地货币作为储备资金（这种银行被称为“我行在他行开的账户”）。
账户中的这些资金平常处于闲置状态，直到银行需要用这种货币进行支付，从而造成周转资金的效率低下。而没有资金支撑开设多个“我行在他行开的账户”的银行，或者需要用他们账户里面没有的货币币种支付的银行，必须依赖第三方流动性提供商来提供这些资金。这个过程不仅让银行面临交易对手风险，它们的资产往往进行一次转移需要冻结好几天。

瑞波允许银行从一个脱节、基于信任的数据库移植到一个单一的分布式数据库——瑞波账本。这一点使得交易获得传统系统无法取得的流动性和速度，并极大地释放了周转资金。瑞波解决了银行遇到的切实困难。
瑞波网络本质上是信任连线的映射。当双方需要交换价值，但他们相互之间没有建立直接的信任关系，瑞波通过最快速和最短的可能路径处理这些交易，使全球各方在无需建立新的信任关系情况下，能够即时进行交易。该网络提供了一个记录所有这些交易的分布式账本。
可能银行间的瑞波协议最有趣的特性是，这些交易不一定需要通过该网络的原生代币 XRP 计价。瑞波网络能够以任何资产计价，处理银行之间的借据。一个“美元对美元”借据的例子如下。
该例子比较复杂，所以先介绍一些快速入门的术语：

- 银行X—美元，指银行X 在瑞波协议上发行的美元资产
- 银行Y—美元，指银行Y 在瑞波协议上发行的美元资产
- 虽然这两种资产名义上是相同的（都是美元），但是它们的价值可能不一样，因为每一种资产都面临不同的交易对手风险；例如，如果银行X 是 2008 年 8 月的雷曼兄弟，而银行Y 是摩根大通银行呢？一般来说，在瑞波网络上，信用更高的实体发行的资产，其价值会稍微高一些，尽管它们名义上是等价的。

某个消费者（用户A）可以通过像银行X 这样的网关存入 100 美元。如果该用户希望发送其中的 50 美元给另一个国家的用户B，那么银行X 就会瑞波平台发行价值 50 美元的“银行X—美元”。这只是银行X 发行的另一种形式的借据，该“银行X—美元”是另一方所持有或接受的；现在这种借据不仅仅存在于某个银行的内部数据库，它还可以在瑞波账本上进行交易。
虽然用户B 没有银行X 的账户，但他可能有银行Y 的账户，而银行Y 可以在瑞波网络上发行自己的“银行Y—美元”。
用户A 可以发起一笔交易，把 50 美元发送到银行Y 的用户B 账户。银行 X 会自动提交一笔交易，在订单簿上把价值为 50 的“银行X—美元”兑换成同等价值的“银行Y—美元”，这个订单可以被任何一个做市商满足。然后同时持有“银行X—美元”和“银行Y—美元”的做市商把 50 银行X—美元转换成 50 银行Y—美元，然后发送到银行Y 的用户B 账户。交易完成。
通过这种方法，瑞波网络也可以充当一个去中心化交易所。由于银行X 的信用可能比银行Y 好，所以银行X—美元的价值可能略微高于银行Y—美元。因此做市商有机会在交易所赚取少量利润，通过这样为做市商提供激励。
这个转移能够以另一种方式进行：不使用借据，而是用 XRP。如果银行X 和银行Y 同时接受用美元兑换 XRP，这个机会就会存在。在用户A 发起一笔交易后，银行X 会把美元转换成 XRP，然后把 XRP 发送到银行Y，银行Y 收到 XRP 后把它换成美元。最后用户B 把美元从银行Y 提现出来。
我们发现很重要的一点是，上述的第二中方法不是 XRP 所独有的。银行和金融机构可以使用 BTC、ETH、DASH 和其它任何加密资产作为中介货币，完成同样的转账。在这些情况下，这些转账会发生在各自的区块链，而不是瑞波账本。

瑞波协议价值主张

瑞波共识协议（被称作 RPCA）依靠一个独特的算法来确定瑞波网络中所有节点都认同的某个事实。像其它所有的分布式加密共识机制，RPCA 是一个涉及很多不同的参与者和交互的复杂系统。以下为概述：
RPCA 的核心是一组节点运营商，其中每个运营商维护各自的特殊节点列表（UNL）。一个 UNL 就是某个运营商扩展了信任关系的其它节点的一个列表。该运营商仅仅考虑它的 UNL 的共享账本状态的提议。运营商交换“候选集”，这些

候选集是可能被添加到最终账本的交易集合。共识达成的过程需要节点不断地交换候选集，直到超过 80% 的运营商 UNL 中验证节点确认了同一个集合和交易顺序。只有达到这个阈值，某个验证集才能被添加到瑞波账本。
给定 UNL 中的节点会持续交换验证集，直到达到 80% 的阈值。但是，除非整个网络所有 UNL 的重叠程度足够高，否者不同的 UNL 通过不同的交易集就可以单独达成 80% 的共识。这也意味着整个网络账本（它包含了所有的 UNL）不会达成一个统一的共识，从而造成网络分叉。因此为了达成整个网络的共识，瑞波协议要依赖 UNL 足够的重合度（至少 40%）。

RPCA 的问题

正如前文所述，这个共识达成过程的主要挑战在于不同的运营商的 UNL 不相同。除非网络上所有的 UNL 具有足够的重合度，否则会导致网络分叉。虽然运营商存在理论上的动机去添加不同的 UNL（为了实现去中心化），但他们也有动机集中 UNL 来防止硬分叉。
还有一点导致该问题更加复杂，就是存在着一个由瑞波公司制定的默认 UNL，它会自动被新进入网络的服务商订阅。每个服务商可以在任何时间选择退订该 UNL，然后选择一个新的，但这样又产生了两个问题。第一，关于哪些服务商是值得信任的公开数据很少，所以新的服务商很难决定把哪一些运营商包含到自己的 UNL 当中。第二，UNL 之间差异的增大会导致分叉的概率增加，因此企业客户端有动机选择把分叉概率降到最低的 UNL。这两个因素都意味着新的节点很有可能会选择瑞波公司推荐的 UNL。
瑞波公司已经采取了一些缓解这些问题的措施。首先，瑞波公司会逐渐把更多的第三方验证节点到它的默认 UNL，取代那些由瑞波公司运营的节点。其次，瑞波公司宣传瑞波网络上有 55 个独特的验证节点（截止至 2017 年 7 月），其中大部分是由瑞波公司以外的企业和机构运营。但是，这些验证节点似乎还没有被添加到默认的 UNL 当中。
RPCA 最后的一个问题在于，似乎没有足够的动机让别人实际运行一个验证节点。节点不会因为他们执行的工作而获得补偿。根据瑞波公司的说法，机构参与者为了网络的健康而运行节点。

> “如果瑞波网络取得成功，并被广泛用于银行间的结算，参与者就有动机保护网络的可靠性和稳定性。如果它发生了，机构将会运行瑞波服务参与到网络中。一旦运行了服务器，运营一个验证节点的额外成功和工作量基本上为零——只需要将软件的开关从‘关’切换到‘开’。正是验证节点决定了瑞波网络的发展，所以运行一个验证节点最主要的激励是维护和保护网络的稳定运行和合理发展。”

我们认为这一点是潜在的危险假设，和影响瑞波网络长期稳定点的因素。
这些担忧之前已经被研究过了，并且有详细的解释。

- 比特币开发者 Peter Todd 关于 RPCA 的技术问题。
- 微软的 Jo Lang 关于瑞波的潜在风险。
- 这份指出 RPCA 漏洞并对瑞波公司白皮书中提出的观点进行抨击的研究报告，促使瑞波公司做出了回应/更正。

XRP 代币

XRP 是瑞波协议的原生代币。以下为该代币的一些事实：

- XRP 的总量为 1,000 亿。所有代币均已预挖，意味着它们在协议上线时就全部被创造出来了。
- 瑞波公司已经把一部分 XRP 分发给企业客户端。目前，瑞波公司持有大约 620 亿 XRP。
- XRP 被用作支付瑞波平台的交易费用（防止网络受到垃圾攻击）。

- 被用作交易费用的 XRP 会被销毁；XRP 费用不会支付给验证节点。XRP 是一种通货紧缩货币。
- 瑞波公司持有 550 亿 XRP，它们会在 2017 年年底之前被锁定在一个托管合同；该合同每个月会释放 10 亿 XRP，为期 55 个月，它们的用途由瑞波公司自行决定。

XRP 价值主张

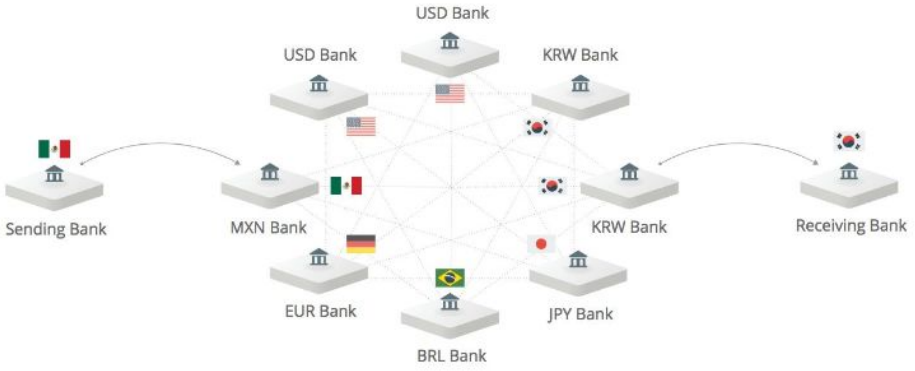
XRP 是一种自由流通的加密货币，它可以在多个加密交易所进行交易。如果 XRP 要创造长期的价值，它必须有效用。我们会在下文探究它的效用。

XRP 提出的第一个价值主张是：它必须用来调用瑞波协议。用户的钱包中至少有 20 XRP（本文发表时价值为 4 美元）才能参与到网络中。XRP 是支付网络交易费用的唯一手段，所以为了处理交易，各方必须持有一定数量的 XRP。这个功能用于防止网络上的垃圾攻击，因为每笔交易都有成本。

虽然这两个应用场景意味着只要瑞波网络一直存在，XRP 就会存储某些价值，但是它并不意味着随着网络的增长，代币的价格也会上涨。据瑞波公司的说法，XRP 的价值主张在于它作为结算货币的效用。

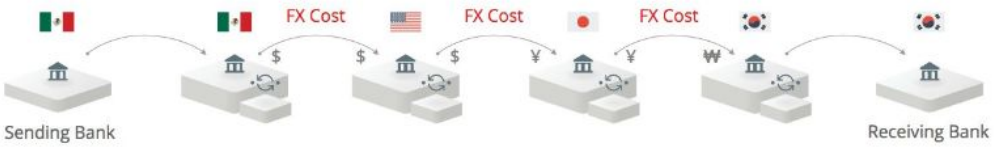
虽然银行可以在瑞波网络自由地交换借据，但最终这些借据必须结算。如果通过法币，这些结算依然受制于瑞波旨在取代的传统银行系统的低效。

在下文举例的结算借据过程中，为了能够处理所有的订单簿，流动性提供者或做市商必须提供高达 28 种不同的货币交易对。做市商必须在每一家机构和他们提供交易的每种资产都有账户和余额。在某些情况下，这些交易还必须通过好几家不同的流动性提供者或做市商，这增加了总交易成本，降低了交易速度。



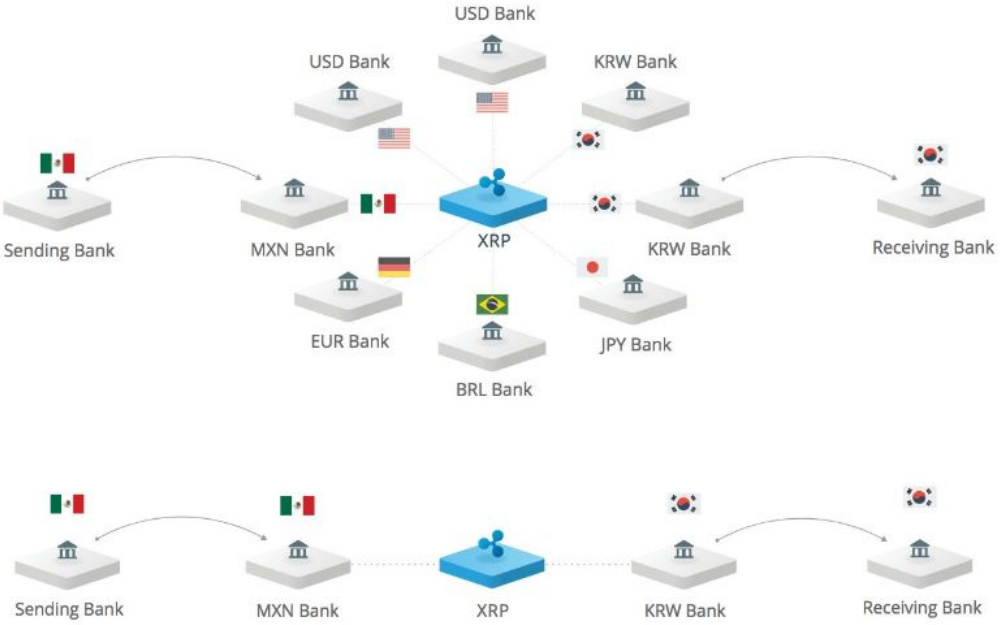
图片来源

需要注意的是，该过程反映了目前银行系统已经在使用的过程。然而，由于瑞波把这些清算迁移到一个区块链上，因此即使通过多个不同的参与方，该过程也比传统的银行系统更加快速和廉价。



图片来源

另一方面，交易可以通过 XRP 计价，这样减少了处理交易的网络参与者的数量。如下图所示。



图片来源

瑞波公司期望 XRP 将会用作多种资产和/或法币对的连接货币。他们还期望银行和金融机构会选择用 XRP 处理交易，而不是借据，因为这样的清算更加快速。我们对这两个言论都持怀疑态度。

如上文所述，XRP 的结算功能并不是瑞波协议独有的。这些国际结算可以通过比特币、以太坊或其它任何加密货币。我们发现，银行很有可能会转向使用全球储备加密货币，它可能是比特币或在区块链上发行的一种法定货币（例如中国人民银行，就讨论过可能将法定货币上链）。而那些希望使用 XRP 进行结算的银行，则需要在它们的账户持有大量的 XRP，这将带来巨大的价格风险。相对于这个风险，它们更倾向于在 XRP 还没打开市场的地方，仍然使用传统系统进行支付。

我们没有找到一个令人信服的理由去投资一种专门用于银行间结算的数字货币。虽然 XRP 目前的交易确认比 BTC 或 ETH 更快，但长期看这不一定都是这个情况。XRP 极不可能用于银行间结算系统之外（除了银行间结算系统，基本上也没有支持它的基础设施），因此它可能不会像比特币或以太坊那样成为一种全球储备货币。任何一种处于全球储备地位的加密货币都可能相对稳定。相对于 XRP，银行更偏向于使用全球储备来结算借据。当政府最终在区块链上发行法定货币时，银行能够立即采用它们青睐的本地货币结算。金融机构可以继续使用瑞波协议来处理借据，但是我们认为 XRP 作为一种结算货币，它不太可能被广泛使用。

如果 XRP 不被用作结算货币，则它无法维持目前价值 85 亿美元的隐性网络价值。以当前的价格投资 XRP 就是赌 XRP 将会成为全球银行间结算的货币。该结果很可能是二元的，并且我们不认为 XRP 会成为全球结算货币。

风险

下文列举了与瑞波协议和 XRP 代币相关的主要风险，因此我们认为以目前的价格投资 XRP 是一项不明智的投资。

- 瑞波网络目前面临主要的中心化风险：

    - 瑞波公司控制着绝大部分代币，并且对这些代币有着绝对的控制权。随着瑞波公司抛售这些代币，XRP 对美元的价格会面临着重大的下行压力。
    - 瑞波公司通过默认 UNL，对协议有着重大的影响力。
    - 瑞波公司目前运营着大多数的验证节点运营商。
- 关于 RPCA 的不确定性：
    - 由于瑞波公司保持了对网络极大的控制权，而瑞波协议还未在大量不诚实节点的条件下进行测试。
    - 多份研究报告质疑了它的共识协议机制，包括安全性的不确定性。
    - 网络参与者运行一个完整的验证节点的激励不明确。这一点会导致网络的不稳定性和/或更高程度的中心化。
- 冗余的风险：
    - XRP（作为一种桥接/结算货币）的主要价值主张是 BTC、ETH、DASH 或其它二层网络（例如闪电、雷电网络）能够轻易做到的。相对于这些替代者，XRP 最多只能提供边际效益。
    - 随着比特币和以太坊网络的发展，目前瑞波相对于 BTC 和 ETH 的速度和扩展性优势会逐渐消失。
    - 由于 XRP 是一种银行间结算货币，它在瑞波网络之外几乎没有用途。银行更倾向使用它们顾客存入的资产进行银行间结算，这些资产可能是 BTC、ETH 或链上的法定货币。为了结算目的引入一种单独的货币会适得其反。
- XRP 转账 vs. 借据转账
    - 为了将运营资金要求降到最低，银行和金融机构很有可能倾向于在瑞波区块链通过借据直接发行资产。
    - 银行发行的这些资产可以在瑞波去中心化交易所进行交易，在多个参与方流通，意味着至少存在一种方式使得资产能够在国际上流通。多方借据流通的费用可能稍微高于使用 XRP 作为一种全球桥接货币，但这些费用仍然是传统系统的一个摩擦。
- 使用瑞波的生态经济
    - 为了进行交易而持有 XRP 的银行需要持有足够的代币，以满足最大的预期支付义务——无论 XRP 价格涨跌，这都是一个大问题。

结论

XRP 目前的网络价值大约为 85 亿美元，该价值还不包括瑞波公司持有的 620 亿枚 XRP 代币。我们认为这个价值的大部分来自于合作伙伴的投机和瑞波公司发布的客户公告。该公司在多个方面取得了重大进展，并持续与全球各地的银行和其它金融机构签署重要的合作伙伴关系。我们意识到瑞波公司提供的服务的伟大价值，也认为银行间结算是区块链技术最合适的使用场景之一。

然而，更加重要的是要意识到，一个很好的区块链技术用途不一定能为这个区块链的原生代币带来价值。在 XRP 的场景中，我们认为该代币除了用作微不足道的交易费用以外，几乎没有任何效用，因此从长远看来，它不太可能维持和创造价值。虽然我们预计随着瑞波公司发布更多的公告，XRP 代币的价格会继续上涨，但我们不认为瑞波协议的设计能为 XRP 带来持续的价值。瑞波公司的确为银行提供了有效的服务，但 XRP 的价值可能有限。基于以上原因，我们对 XRP 目前的价格持看跌态度。

如有任何意见或疑问，请发送邮件到 research@multicoin.capital。