清华大学金融科技研究院
INSTITUTE FOR FINTECH RESEARCH,TSINGHUA UNIVERSITY

研究报告

2018 年 第 5 期 （总第 5 期） 2018 年 5 月 10 日

基于区块链的支付交易模式研究

寻朔

（鑫苑房地产金融科技研究中心）

【摘要】支付是资金流通的基础环节。在国际跨境转账和清算领域，交易存在着高成本、耗时、对账环节复杂等问题。随着区块链技术的发展，底层技术开发者和传统金融机构都在关注，区块链能否在降低结算风险、提高支付效率和节省银行资源等方面发挥优势，从而改善现有的跨境支付模式。本文介绍了基于区块链的转账支付原理，涵盖两个案例分析，分别为：比特币转账和 Ripple 支付模式（第一个基于区块链的支付网络），探讨区块链技术应用于传统行业的可行性和优势以及潜在问题。

清华大学金融科技研究院
INSTITUTE FOR FINTECH RESEARCH,TSINGHUA UNIVERSITY

Research Report

2018- edition 5 May 10th 2018

Payment systems: Transactions in a Blockchain environment

Xun Shuo
XIN Real Estate Fintech Research Center

Abstract：Payment is the basis part of fund flow. Especially in the fields of international cross-border payments, clearing and settlement, fund transactions have many problems, such as high cost, time consuming and complicated intermediate reconciliations. With the development of blockchain, both the underlying technology developers and financial institutions have considered whether this technology can provide new ideas to reduce settlement risk, increase efficiency and save bank resources, which aims at improving the existing cross-border payment system. Based on the cryptocurrency payment principle, this paper involves two case study, one is bitcoin transfer and the other is Ripple payment model. In addition, we give briefly discussions on the feasibility, advantages and potential problems of blockchain when it applied to traditional industry.

目录

基于区块链的支付交易模式研究

寻朔

（鑫苑房地产金融科技研究中心）

当前，区块链无疑是整个互联网金融行业的最大风口。区块链创业公司如雨后春笋般出现，学术界对区块链的研究和应用逐渐走向深入，同时各国政府和中央银行对基于区块链技术开发的数字货币或虚拟代币也给与高度关注。不可否认，“区块链+”的浪潮已经涌来。

区块链本质上是一个对等网络 P2P 的分布式账本数据库，由中本聪（Satoshi Nakamoto）在《Bitcoin: A Peer-to-Peer Electronic Cash System》论文中首次提出。一个完整的区块链系统包含了基于密码学、数学、计算机科学等在内的很多技术，其中有存储数据的数据账本及用于验证加密的数字签名、时间戳等，有作为基础支撑的 P2P 网络和维护系统的共识算法，有挖矿和工作量证明机制，有匿名交易机制和比特币钱包，还有哈希函数、Merkle 树等相关概念。正是这些技术，保障了区块链在无中心的网络上可以实现交易、验证、追溯和链接等功能。

如今，随着互联网经济的发展，全球金融流通速度空前加快，作为资金流通基础环节的支付，尤其是国际间的跨境支付和清算，在降低资金往来成本、提升运转效率等方面提出了更高的要求。那么在“区块链+”的时代，能否发挥分布式记账技术特点，在降低结算风险、提高支付效率和节省银行资源等方面发挥技术优势，改善现有的跨境支付模式，

不仅是技术提供商关注的区块链商业应用场景，同时也是传统金融机构不断探索的新型商业模式。日前，22 家银行加入被 SWIFT 视为“跨国支付新标准”的区块链概念验证测试，招商银行完成了全球首笔基于区块链技术的同业跨境人民币清算业务。

鉴于此，本文从区块链交易支付原理出发，在技术的角度，以较有代表性的比特币区块链转账为例，介绍交易规则和确认验证过程，探讨区块链技术应用于传统跨境支付业务模式的落脚点，并选择全球第一家基于区块链的跨境支付网络 Ripple 为例进行分析。

一、比特币区块链支付交易规则---UTXO 交易模式

区块链（或称 “分布式账本数据库”）在安全性、公开性、透明性、不可篡改和追溯性方面相较传统中心化数据库有独特的优势[①]，同时，区块链平台还能够提供编程环境让用户编写智能合约，降低合约建立、执行和仲裁中所涉及的中间机构成本。

由于目前大多数区块链技术的应用与比特币类似，并且大部分是比特币架构的扩展。所以，介绍区块链上的交易和转账，本文以比特币转账为例，说明区块链上交易的重要概念---UTXO（Unspent Transaction Output）交易模式。

我们首先回顾一下传统的基于账户的支付系统交易模式,此模式在银行、信用卡、证券交易系统、互联网第三方支付平台广泛使用，由关系数据库支撑，交易记录简单直观。

[①] 区块链工作原理及核心技术与特点参看《区块链的技术原理、应用与监管》研究报告（寻朔、柯岩）

在基于账户的支付系统，张三有一个账户，余额 100 元，李四有一个账户，余额 50 元。当张三要付给李四 20 元时，支付系统会做以下操作：首先，检查张三账余额，如果不足 20 元，交易终止，向张三回复“余额不足”；第二，在不收取交易手续费情况下，张三账户里扣除 20 元；第三，李四账户里增加 20 元，最后交易完成。

而对于没有中心处理机构的区块链比特币交易，则采用 UTXO（未花费的交易输出，Unspent Transaction Output）方案。需要说明：

第一，比特币的区块链账本里记录的不是账户余额，而是每一笔交易（转账记录），即：记录每一笔交易的付款人、收款人和付款金额。

第二，除了创世区块外，所有区块中的交易有若干输入（资金来源）和若干输出（资金去向），所产生的输出就是“未花费过的交易输出”。输入需要上一笔输出地址所对应的私钥进行签名。

第三，当前整个区块链网络中的 UTXO 会被储存在每个节点中，只有满足了来源于 UTXO 和数字签名条件的交易才是合法的。

我们引入如下比特币交易的例子去具体说明。假设场景：张三挖到 12.5 枚比特币。过几天，他把其中 2.5 枚比特币支付给李四，又过几天，他和李四各出资 2.5 比特币凑成 5 比特币付给王五。那么这个过程是如何通过 UTXO 实现呢？如图 1 所示。

图 1 UTXO 交易过程

从记账角度看交易规则（区块内部）：

（1）除了 coinbase 交易，即：矿工挖矿奖励，所有资金来源都必须来自前面某一个或几个交易的 UTXO。

比特币是矿工挖出来的，矿机进行类似猜数字游戏，耗费大量算力寻找“幸运数字”，找到一个合格区块后，便获得一个特权，即:创造一个 coinbase 交易写入区块，交易输出地址写上矿工自己的收款地址。矿工的区块奖励金额从 2009 年的 50 个比特币，如今已经减至 12.5 个。这个 coinbase 交易随着张三挖出来的区块被各个节点接受，交易不可更改（基于工作量证明的共识机制，一般认为一个区块在最长链上后面

链接五个区块，就不可能被分叉，后面细讲）。

图 2 所示的是创世区块，即：比特币区块链中的 Block#1，该区块内记录的所有交易就是奖励矿工构建区块的 50 个比特币，这是区块链系统默认的奖励，并没有交易输入地址。

图 2 比特币区块链创世区块 Block#1 中交易信息

（2）一笔交易的输入量和输出量必须是相等的。

图 1 的第一个交易#001 号交易是 coinbase 交易。过了几天，张三打算付给李四 2.5 个比特币，张三发起#002 号交易，这个交易的资金来源写着#001（1），也就是#001 号交易的 ID 号（1）的 UTXO，然后将本交易的交易输出 UTXO 中，即：将 2.5 个比特币收款人的地址设为李四的地址。

这里需要注意的是，这一笔交易必须将前面产生的第一项 12.5 个比特币的输出项全部消耗，因为给张三给李四只有 2.5 个比特币，所以为消耗剩下的 10 个比特币，张三将自己的地址写到交易输出中，这样完成输入与输出的配平规则。

再过几天，张三和李四打算各出一半，给王五付 5 个比特币。那么张三或李四发起#003 号交易，在交易输入部分有两个资金来源，分别是#002（1）和#002（2），代表第#002 号交易的第（1）和（2）UTXO。交易输出，张三重复前面的过程，给王五 2.5 个比特币，将 7.5 个比特币发

还给自己的地址，李四直接发送 2.5 个比特币王五。以后王五若再需要支付 5 个比特币，就可以在他的交易里注明资金的来源是#003（1）和#003（2）。

所以，所谓的王五拥有 5 个比特币，实际上是说，当前区块链账本中，有若干笔交易的 UTXO 收款人写的是王五的地址，而这些 UTXO 的数额总和为 5。比特币系统里，一个人可以拥有多个地址，要计算一大堆地址一共收了多少 UTXO，一般借助比特币钱包代为跟踪计算。

以上我们讲述了比特币实际上是以 UTXO 转账记录的形式存在，coinbase 交易是区块链系统默认的对矿工建立有效区块的奖励，所以，只要账本的初始状态确定，每一笔交易记录可靠且有时序，交易就可以被追溯。

二、比特币区块链交易确认和有效性验证

两个核心问题：相互没有信任基础的个体之间如何就交易的合法性达成共识，也就是说，为什么我们可以相信转账的真实性？没有中央处理人的存在，谁来负责记账和确认每笔转账交易的有效性？以上问题也是中本聪论文中的核心。

解决以上两个问题，我们要引入工作量证明的共识算法和矿工小组（或称区块创造者 block creator）的概念。我们依然用张三、李四和王五转账的例子说明。

首先，生成有效交易。比特币所有者张三利用他的私钥对比特币输出地址为下一位所有者李四的交易签署一个数字签名，并将这个签名附

加在转账记录末尾，制作成交易单，付款人签名后交易记录才有效。若没有张三利用私钥签名该笔交易，那么一个公开的账本，每个人都将资金输入地址写“张三的地址”，那张三岂不是要倾家荡产。

第二，传播交易。交易的发起人张三不但要将交易单广播给收款人李四，还要同时复制若干份一模一样的交易单广播到全网的矿工小组。矿工小组定期将收集到的信息打包，成为一个区块。

第三，工作量证明。中本聪核心想法是信任工作量最大的账本，这一点是比特币和其他很多数字货币的核心与关键，也是在无中心的系统里全网节点保持账本一致的关键。

那么什么是工作量证明？对收集到的交易列表打包为区块后，矿工小组需要在区块内补充一个特殊数字，使得整个区块交易列表用加密哈希函数 SHA256[②]求值，得到 0 和 1 字符串前 30 位全是 0（比特币协议定期更换 0 的个数，使得发现新区块的时间控制在 10 分钟左右）。

寻找这个特殊数字的难度有多大呢？对于一组交易信息，哈希值前 30 位全是 0 的概率是$1/2^{30}$（约 10 亿分之一），而找这个特殊数字的方法只有试错法（guess and check）！一旦猜到了这个特殊数字，验证起来就非常快，只要将整个交易列表计算哈希值，检查前 30 位是不是 0 就可以。换言之，这个特殊数字证明了该矿工小组做了海量计算，其他组无需再做等量计算，称这个特殊数字为“工作量证明(Proof of Work)”。区块有了工作量证明才是有效的！

[②] 哈希函数 SHA256 的输入值可以是任意信息或文件，它的输出值是固定长度的 0 和 1 字符串或称比特串，例如 256 比特，称之为“哈希值”

为奖励该挖矿小组试错猜测特殊数字的工作，允许他们得到一个特权，即：在该区块的首行写入一条 coinbase 交易，比特币输出地址为本矿工小组地址，没有输入地址。图 3 展示的是 2018 年 4 月 18 日 8 点 11 分链入比特币区块链主链的 Block #518750（518750 代表这是主链上第 518750 个区块），矿工为 btc.com。区块内在第一行我们可以看到，该矿工获得 12.5 个比特币的 coinbase 交易。第二行以后为该矿工小组打包的其他交易。

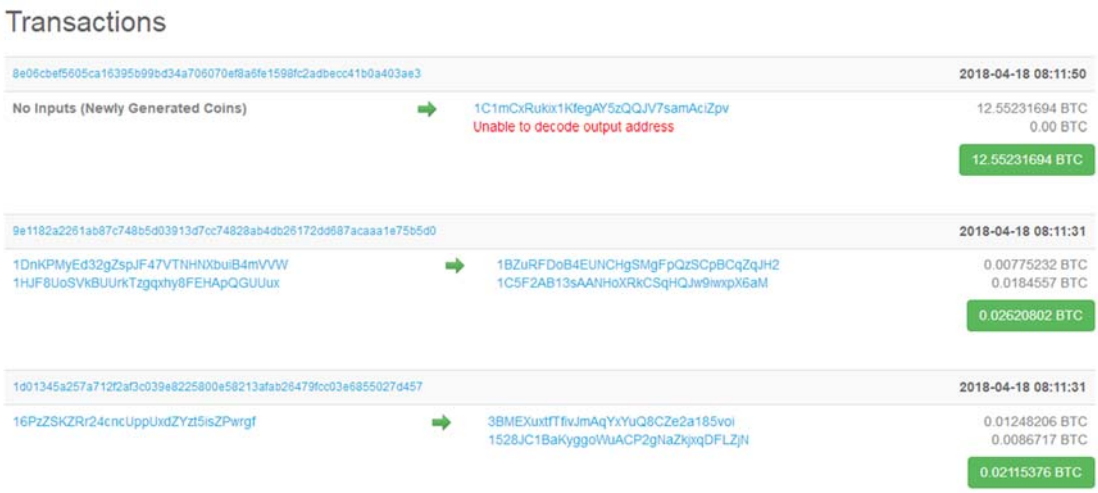


图 3 Block #518750 部分交易信息

第四，区块验证。当某挖矿小组给区块赋予工作量证明后，为了得到奖励，必须立刻请其他矿工组确认自己的工作，因此该小组将有效区块广播至其他矿工组。中本聪规定，当某个矿工接到其他矿工送来的有效区块后，必须立即停下挖矿工作进行区块确认。确认的信息有三个：

1. 本区块哈希：SHA256 计算区块哈希值，是否满足 256 比特串前 30 位为 0；

2. 本区块的前一区块哈希：区块哈希依赖其链接的前一区块哈希，保证区块先后顺序；

3. 交易输入的 UTXO 来源。例如，李四给王五 2.5 个比特币，并注明了这 2.5 个比特币来自之前张三支付给李四的一笔交易，确认时要确认之前交易是否存在，同时还要检查李四之前没有将 2.5 个比特币支付给别人。其实，第一笔交易是张三作为矿工获得奖励的 12.5 个比特币，这笔交易是默认的，根据地址追溯就可以确认李四的 UTXO 是否能支付王五 2.5 个比特币。

第五，有效区块链到主链。如果完成了上述所有验证并全部通过，那么这个矿工小组就认可接受到的区块有效，并将这个区块链入矿工小组原本的区块链中，舍弃目前正在进行的工作，后面的挖矿工作基于这本更新后的主链进行。

最后，确认反馈。对于挖矿小组来说，当把带有工作量证明的区块广播出去后，如果后面收到其他小组播送的区块，其“前一区块哈希”为自己之前广播的区块哈希，那么就表示他们的工作被其他小组认可，因为已经有其他小组基于他们的区块进行工作。

那对于交易的双方来说，收款人只要发现交易被多个（目前默认是至少 6 个）挖矿小组认可，就可以确认自己收到了这笔钱，并且是全网共识有效的，后面他就可以在付款时将交易输入指向这笔交易的输出地址了。

可矿工为什么愿意贡献出算力，付出成本去猜特殊数字呢？从图 4 可以看到，矿工 btc.com 除了可以获得挖矿奖励的 12.5 个比特币之外，

还能收入付款人给出的 0.00224774 比特币手续费。挖矿奖励和手续费是矿工的收益来源也是矿工挖矿的动力，一般矿工小组也会优先选择手续费高的交易单优先确认。

由此，我们把比特币从流入区块链系统到验证流通整个过程介绍完了。那么，为什么有效区块的转账交易需要至少 6 个确认才能认为是可信且不可逆转的？

目前来说，比特币网络大约需要 10 分钟产生一个区块， 60 分钟确认一笔交易,也就是 6 个区块确认。这意味着，收款人在主链（拥有算力最大的的区块链/最长的区块链）上看到交易汇款记录被一个区块包含时不可马上相信,付款人可能制造双花交易[③](double-spending attack),而是应该等待各个挖矿小组在挂出 6 个确认区块,才可以确认转账成功。

除非伪造人拥有全网超过 51%的算力，在落后 6 个区块的情况下从另一个分支赶超当前主链，使拥有伪造交易的分支拥有最多计算量，才能一直圆谎（若有这么卓越的算力，不如直接挖矿获得收益），否则伪造交易所在的区块不会在全网信任的主链上，换言之，不会在计算量最大的区块链上。

图 4，以 Block #518750 的第一笔交易为例，两个交易输入地址（资金来源地址）给两个输出地址转账，该笔交易已经获得 4 个区块确认，再获两个区块的确认，收款人可以相信其真实性。

[③] 双花交易:收款人确认收款后，欺诈人将区块链主链分支，从分支上建立另外的交易单，取消之前的付款，而将同一笔钱再次付款给另一个人.

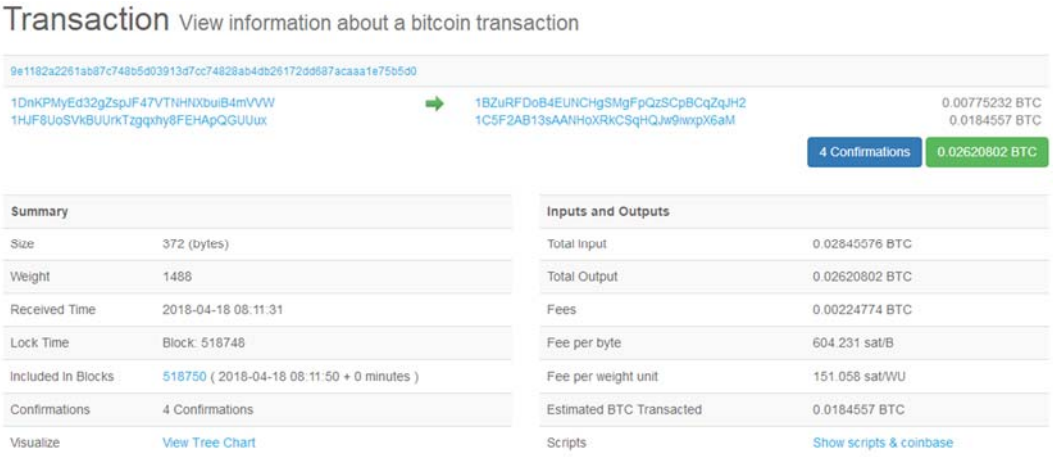


图 4　Block #518750 内的交易记录

三、基于区块链的跨境支付业务模式

3.1 传统跨境支付模式

目前全球多数国家大多数银行使用 SWIFT 系统（环球同业银行金融电讯协会），它运营着世界级的金融电文网络，银行和其他金融机构通过该网络，与同业交换电文，完成金融交易。目前，全世界已有超过 200 个国家的 7000 多个银行在使用 SWIFT 协议。

虽然 SWIFT 系统为大多数金融机构接受,但其也有一些不足。例如，利用该网络进行国际转账支付手续费相当高，达 7%左右；电汇支付需要经过汇出行、中央银行、代理银行、收款行等多个机构，每一个机构都有自己的账务系统和清算系统，资金到账时间需要一周以上。从中国的工商银行打款给美国的汇丰银行，其采用的仍然是较古老的发电报的方式等。表 1 简要列举了传统跨境支付流程以及存在的商业痛点：

表 1 传统跨境支付模式流程及痛点问题

	支付发起	资金转移	资金交付	交易后
涉及主体	付款人、汇款行	SWIFT/代理行	收款行、收款人	银行、监管机构
传统流程	1.付款人通过汇款行向另一国家/地区收款人发起转账汇款； 2.汇款行履行KYC/AML相关流程； 3.汇款行收取资金和服务费，确认并支持后续查询和争议处理	银行通过SWIFT网络或代理行模式（汇款行不是SWIFT会员机构）向收款行发起跨境转账	1.收款人通过收款行接受通知； 2.由收款行履行KYC/AML流程； 3.再以当地货币形式支付给收款人相应款项	根据监管法规要求，银行需要定期向监管机构报送跨境支付业务信息，包括收付款人身份信息、币种信息、汇款金融和时间等
痛点问题	1.收/付款人信息通过人工和重复性的业务流程收集，效率较低； 2.在KYC流程中，银行对客户信息材料真实可信度控制有限，不同机构之间KYC水平有差异。	1.金融机构的基础设施架构和业务流程有差异,清算参与方多、体系复杂,只能通过服务器代码和交易数据报送的方式，成本高，耗时长； 2.通过代理行模式需逐行逐笔进行信息验证,效率低且拒绝率高； 3.银行需在往来账户中预存外币，交易成本高。	与支付发起阶段类似，不同银行KYC/AML审核水平有差异且能力有限。	银行监管合规成本较大，由于跨境转账流程复杂，涉及数据信息和转移渠道多样，需要较高技术水平和业务流程支持。

3.2 基于区块链的跨境支付

波士顿咨询的一份研究报告显示，欧洲银行的 IT 成本支出平均占据银行整体运行成本的 16%。一个重要原因就是，传统银行在账本维护、支付交易结算和清算方面的架构过于复杂，维护成本过高。同时，交易费、手续费居高不下问题也是跨境支付行业的集中痛点，根据麦肯锡报

告[④]，2016 年全球跨境支付交易量占不到全球支付的 20%，但其所带来的交易费占到了全球支付交易费的 40%！那么，基于区块链的跨境支付新模式能否发挥技术优势呢？图 5 是基于区块链的支付模式示意图。

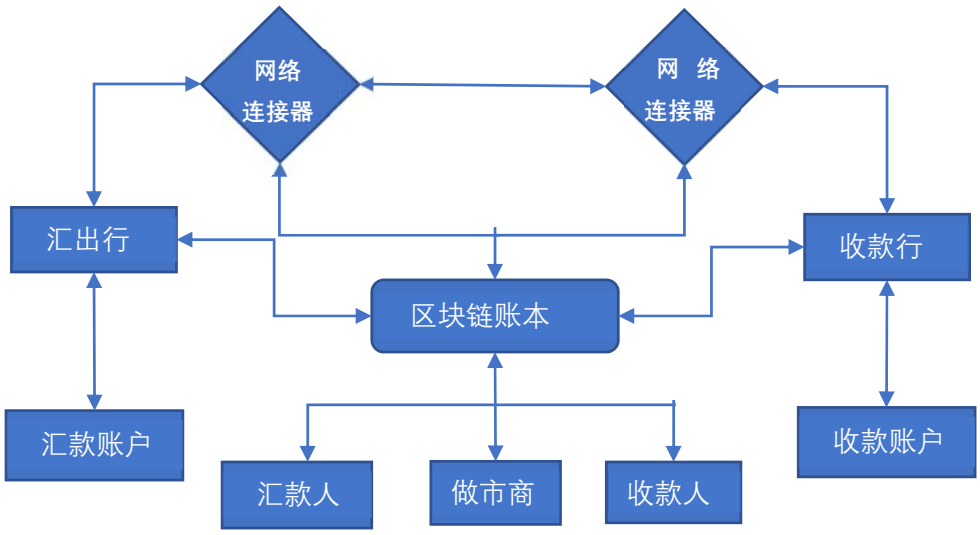


图 5 区块链跨境支付模式图

基于区块链技术的转账，首先需要将传统金融机构、外汇做市商/流动性提供商等加入区块链支付网络，构建支付网关。这样可以满足所有参与支付结算的网关节点共同维护交易记录，参与一致性校验的需要，从而省去银行或金融机构间繁琐的对账流程，节省银行资源。

在交易前，通过对收付款人建立“数字身份”，将收付款人关键信息上链，建立付款人、银行、转账服务商和收款人之间的信任，完善传统身份验证和 KYC 服务流程。通过智能合约[⑤]记录收付款人之间转账行为的权利与义务关系，将原有人工操作和流程审批等过程做自动化处理。

---

④ 《Global Payments 2016: Strong Fundamentals Despite Uncertain Times》

⑤ 基于区块链技术的智能合约，可增强链上交易的可控性和一致性，参与方可按照事前约定的规则，在满足特定条件后共同执行。

在资金交付阶段，通过嵌入区块链的智能合约增强交易可控性，条件满足时自动将资金自动存入收款人账户，或者收款行执行 KYC 流程之后允许收款人提取资金。交易完成后，相关交易记录密文存储在分布式账本中，监管机构根据需要进行数据的提取解密与审查，为 KYC 流程和反洗钱监管提供新的解决思路。

目前，国际上基于区块链的技术解决方案常采用以下尝试：或者用数字货币作为外汇兑换媒介，或者向银行提供技术支持与低层协议，建设多中心化的全球汇款系统，代替传统成本较高的 swift 通道。采用第一种方式，支付网关可以将区块链上数字资产流动与现实中的法定货币相连接，实现法定货币可以转换为区块链上的数字资产，便于后续的支付转账。有些国际公司已经进行了类似尝试，Ripple 公司使用的其原生代币 XRP， OKlink 选择 OKD，SnapCard 和 Circle 使用的是比特币。采用第二种方式，则是技术提出较高的要求，需要优化银行基础账本体系，构建完备的底层协议。

3.3 案例研究：世界第一个开放的支付网络 Ripple

（1）Ripple 公司简介

Ripple 成立于 2012 年，创造了世界上第一个开放的支付网络，本质上是一种分布式共享化的支付协议，可以实现基于区块链技术的货币兑换和实时支付与结算功能，由 Ripple Labs 开发、运行和维护。Ripple 的目标是为银行和金融机构打造可以更快速、更廉价地进行交易和结算的网络。

目前，Ripple 网络接入金融机构数量已经超过了 100 家，其中包括瑞银集团、西班牙国家银行等等，英格兰银行（Bank of England）和沙特阿拉伯金融管理局都是 Ripple 的付费客户。值得一提的是，2016 年，加拿大的 ATB 银行和德国 Reisebank 银行利用 Ripple 网络完成全球第一笔基于区块链技术的银行间跨境汇款，ATB 在 8 秒之内将 1000 美元支付给了 Reisebank（传统模式需 2 到 6 个工作日）。日前，全球第二大汇款公司速汇金(MoneyGram）宣布将在其支付网络中将 XRP 作为降低汇款成本和结算次数的工具进行测试。

Ripple 网络主要基于跨账本协议（Interledger Protocol，ILP）、共识总账和原生的货币 XRP，其交易方案有以下两种：

第一种，使用 Ripple 系统原生代币 XRP[⑥]交易（XRapid），XRP 是媒介货币，可以充当各种货币兑换之中的一个中间物；同时，XRP 可用于支付交易费，即：每产生一笔交易就会消耗一定 XRP（消耗十万分之一的 XRP），进而起到保护网络安全性的作用。

第二种，通过 XCurrent 插件优化银行基础账户，打通银行基础记账模块，通过跨账本协议，将银行账户与分布式账本建立关联和映射，无需实际资金搬运的情况下，通过信息处理实现资金交割（目前银行多选择测试此种方案）。

（2）Ripple 的核心部件

Ripple 方案中最主要有两个核心部件，Xvia 和 Ripple Net，如图

[⑥]Ripple 币 XRP 总量 1000 亿，无需也不能挖矿，数量递减。XRP 担任桥梁货币和燃料消耗两个作用。

6 所示。

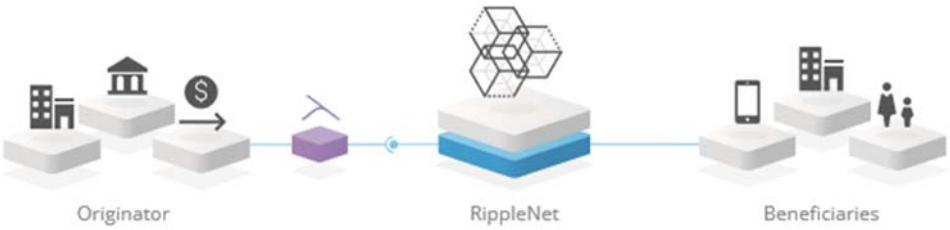


图 6 Ripple 系统示意图

XVia：帮助各类机构接入 Ripple 支付网络成为网关的工具，为流动性做市商、汇出行和汇入行点对点交易创造基础。网关是允许用户将资金转入或转出 Ripple 网络的节点。在 Ripple 分布式网络中，任何一个用户都可以在网关挂出买单和卖单来交易货币，流动性做市商既挂出卖单也挂出买单，在为市场提供流动性的同时赚取差价。图 7 展示了资金在网关和做市商流动转换过程，我们以欧元账户支付日元为例。

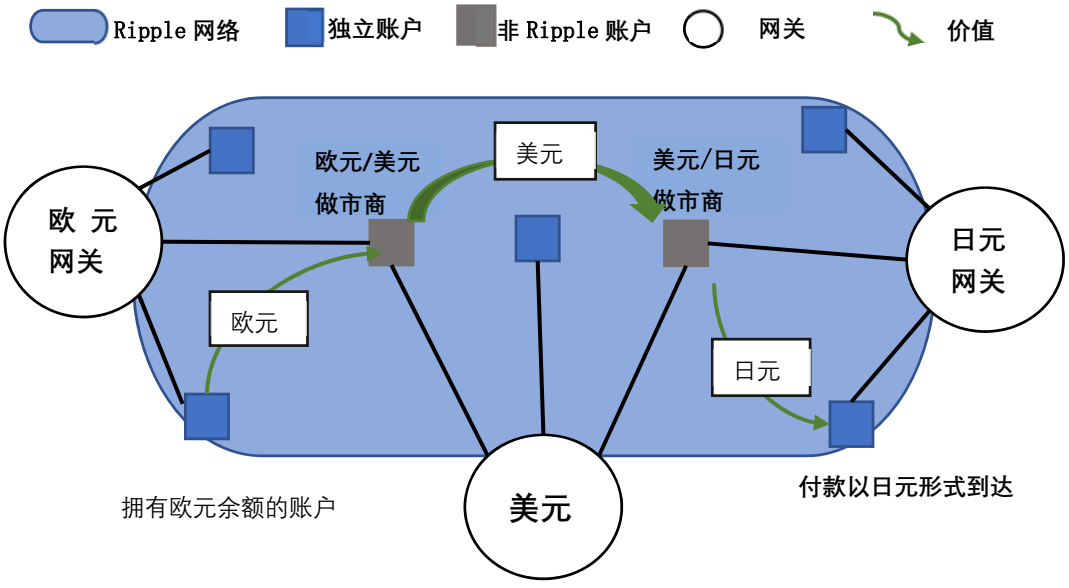


图 7 资金流动过程

Ripple Net:没有中心处理机器，为保证交易的隐私性，网络中所有

的关键信息都是加密的。另外，Ripple 网络是权限链或联盟链，并非公有链，节点不具备匿名性。

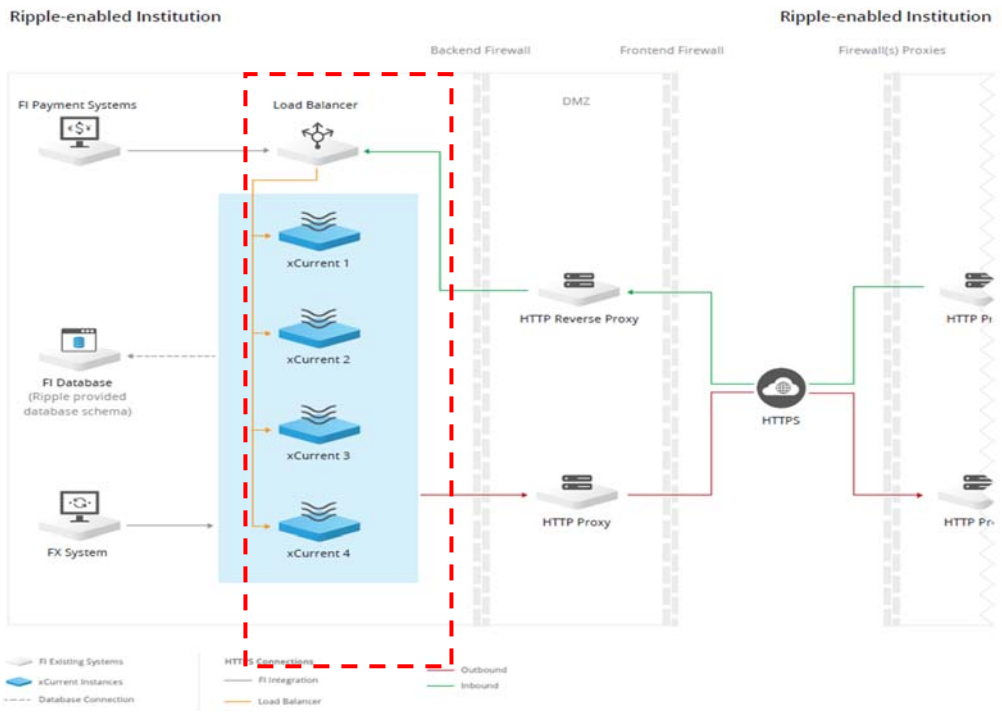


图 8 Xcurrent 模块安装位置

集成功能插件 Xcurrent 是在银行系统中处理 ripple 支付交易的一个插件模块，安装在银行后端防火墙内（图 8）。Xcurrent 包括四个功能模块：Messenger、ILP Ledger、 FX Ticker 和 Validator（图 9 所示）。

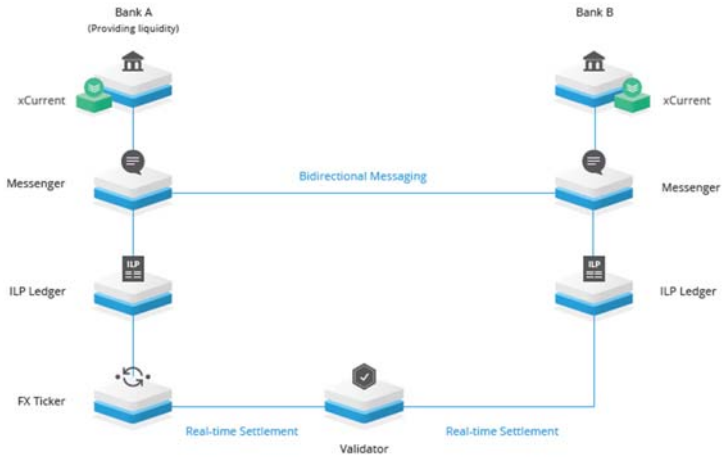


图 9 Xcurrent 内部插件

Messenger:在银行系统中处理 Ripple 支付交易的一个应用程序接口。Messenger 为汇款行和收款行间提供一个信息通道，用于交换 KYC/AML、风控信息、手续费、汇率和其他支付相关信息。在交易发起之前，Messenger 把这些信息送到交易对手方，需要检查这些信息是否正确，只有通过确认，才能执行交易和清算资金。

ILP Ledger: 跨帐本协议 Interledger Protocol 是交易银行总账本的分账，它记录了交易各方银行账户的借贷情况以及资金流动性提供商（Liquidity Provider）或称做市商[⑦]的资金变动。银行接入 Ripple Net 一定要遵循这个规范，它把不同帐本之间即时地连接起来，使不同帐本之间有互操作性。利用 ILP Ledger 进行资金结算是原子级别的，即：结算过程不可再分割，要么结算完成，要么失败，降低交易风险。

FX Ticker: 做市商通过 FX ticker 向 Ripple 网络提交外汇报价，银行内部的外汇交易平台也可以通过该模块集成到区块链支付网络，起到做市商功能。Ripple 会自动选择网络中众多做市商中报价最低者，实现资金转换成本的最小化。

Validator:是交易双方信任的来源，用于确认交易是否成功并触发记账过程。参与区块链支付交易的相关各方参与共识过程，满足拜占庭容错要求，Validator 触发区块记账，并保持账本一致性。

（3）跨境支付案例

假设美国的 Alpha 公司向欧洲的 Beta 公司支付 100 欧元，并假设由外部做市商提供资金流动性。

⑦ 做市商通过在收/付款行开设的账户，提供跨境转账的货币兑换服务。

- 支付准备阶段

Alpha 公司（Originator）和 Beta 公司(Beneficiary)在对应银行 Dollar 银行和 Euro 银行完成开户并存有相应币种的资金（图 10）。Dollar Bank 账本和 Euro Bank 账本是银行系统内部的记账账本，银行拥有记账权。

另外，每个银行账户需要扩展一个 Ripple 外挂独立账户（Ripple Segregated Account），这个账户余额与外部的 Ripple ILP Ledge（用来跟踪做市商的资金状态）关联，有映射关系[⑧]。

Dollar Bank's Ledger

Account	Debit	Credit	Balance
Originator			$10,000
Liquidity Provider			
Fees			
Ripple Segregated Account			

Euro Bank's Ledger

Account	Debit	Credit	Balance
Beneficiary			€3,000
Liquidity Provider		€200,000	€200,000
Fees			
Ripple Segregated Account			

Dollar Bank's Ripple ILP Ledger

Account	Debit	Credit	Balance
Hold			
Liquidity Provider			

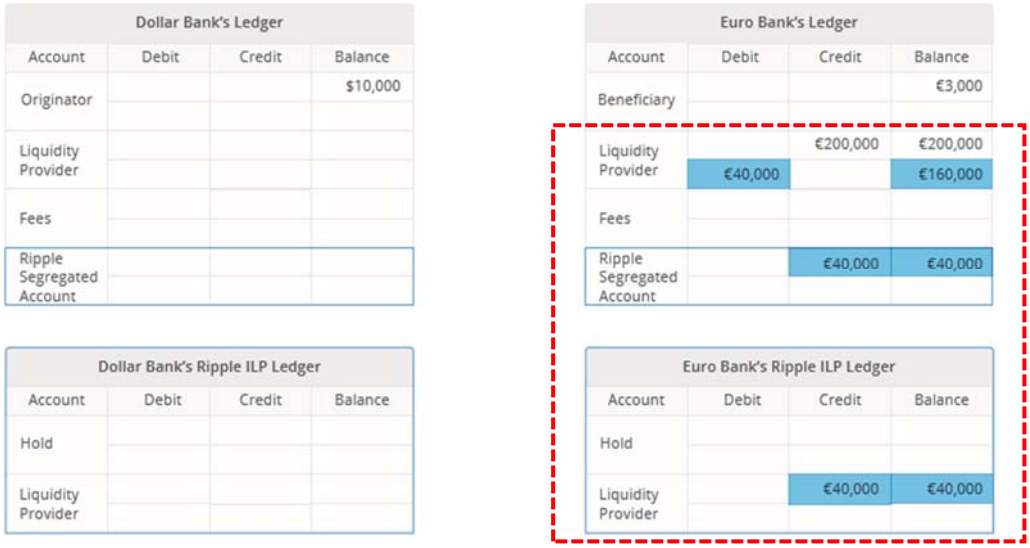
Euro Bank's Ripple ILP Ledger

Account	Debit	Credit	Balance
Hold			
Liquidity Provider			

图 10 dollar 银行账户和 Euro 银行账户

做市商通过本地清算系统向 Euro 银行注入初始资金 200,000 欧元，并将其中的 40000 欧元注入其 Ripple 外挂账户，用于这笔交易的流动性支出（图 11）。这个案例中，只有单向资金支出，所以做市商单向做市即可。

⑧ Ripple Segregated Account 和 Ripple ILP Ledger 的映射关系是由跨账本传输协议（Inter Ledger Protocol）规范的



Dollar Bank's Ledger

Account	Debit	Credit	Balance
Originator			$10,000
Liquidity Provider			
Fees			
Ripple Segregated Account			

Euro Bank's Ledger

Account	Debit	Credit	Balance
Beneficiary			€3,000
Liquidity Provider		€200,000	€200,000
	€40,000		€160,000
Fees			
Ripple Segregated Account		€40,000	€40,000

Dollar Bank's Ripple ILP Ledger

Account	Debit	Credit	Balance
Hold			
Liquidity Provider			

Euro Bank's Ripple ILP Ledger

Account	Debit	Credit	Balance
Hold			
Liquidity Provider		€40,000	€40,000

图 11 做市商向 Euro 银行做市并向外挂账户注入资金

一旦 Ripple Segregated Account 有了资金，流动性提供商通过 FX ticker 将外汇报价提供给 Dollar 银行（Ripple 网络自动选择众多流动性提供商中报价最低者/最优换汇路径）。在这个案例中，我们假设 offer 价格为 EUR/USD =1.1429。

- **支付（整合业务流和资金流）**

图 12 支付流和资金流

如图 12 所示：

① Alpha 公司通过 Dollar 银行发起给 Beta 公司支付 100 欧元的汇款请求；

② Dollar 银行通过 Messenger 连接到 Euro 银行，提交相关汇款信息、订单信息等；

③ Euro 银行根据 Dollar 银行的提交的请求检查：Beta 公司此笔订单是否满足当地 KYC/AML 监管要求，是否还需向 Dollar 银行申请进一步的 Alpha 公司信息；检查通过，Euro 银行返回相应的手续费。

④ Dollar 银行收到 Euro 银行的应答后，通过 FX Ticker 获得欧元对美元汇（EUR/USD=1.1429）。Dollar 银行最后呈现出来的是这笔交易的总成本（all-in cost）。假定美元银行手续费为 5 美元，欧元银行手续费为 5 欧元，EUR/USD 为 1.1429，那么总的成本差不多为 125 美元（100 欧元*1.1429+5 美元+5 欧元*1.1429）。

⑤ 一旦 Alpha 公司接受了这个费用，这笔支付即被发起。Dollar 银行借记了 Alpha 公司-125 美元，收下了 5 美元的手续费，贷记 Segregated Account +120 美元，ILP 账本也同时更新（见图 13）。

Dollar Bank's Ledger

Account	Debit	Credit	Balance
Originator			$10,000
	$125		$9,875
Liquidity Provider			
Fees		$5	$5
Ripple Segregated Account		$120	$120

Euro Bank's Ledger

Account	Debit	Credit	Balance
Beneficiary			€3,000
Liquidity Provider		€200,000	€200,000
	€40,000		€160,000
Fees			
Ripple Segregated Account		€40,000	€40,000

Dollar Bank's Ripple ILP Ledger

Account	Debit	Credit	Balance
Hold		$120	$120
Liquidity Provider			

Euro Bank's Ripple ILP Ledger

Account	Debit	Credit	Balance
Hold			
Liquidity Provider		€40,000	€40,000

图 13 Dollar 银行记账

这 120 美元还没有真正贷记到流动性提供方的账户上，而是在 Hold 账户中，直到 Euro 银行向 Validator 提供了足够 post 给 Beta 公司资金的证明（例如：Beta 公司冻结某部分资金或 beta 公司提供可验证的发货信息等方式）。

发起共识的过程，Ripple 给出的方案是 Consensus+Validation 的验证结构（见附录）。简而言之，Validator 组成的网关节点能够基于特殊节点列表（UNL，unique node list）投票达成满足拜占庭容错的账本共识。需要说明的一点是，参与投票节点的身份是事先相互知道（不具备匿名性），因此算法的效率比 PoW 等匿名共识算法要高效，3-5 秒内就能够完成交易的验证和确认，该共识算法只适合于权限链（Permissioned chain）。

此案例中，Beta 公司提供给 Validator 的保证是通过 Euro 银行冻结一部分资金。流动性提供方将用于流动性支出的 40000 欧元中的 105 欧元放入 Hold 账户，并发送一个加密的收据（receipt）给 Validator（图 14）。

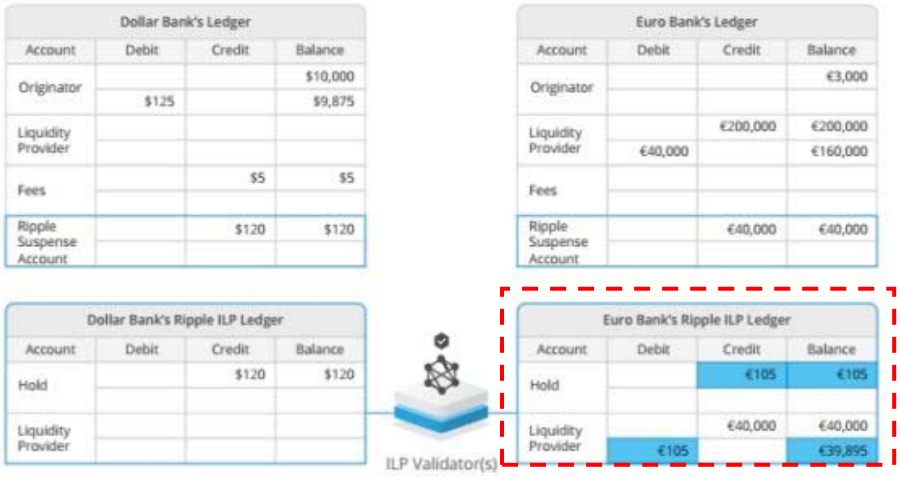


图 14 流动性提供方资金处于 Hold 账户

一旦 Validator 收到两边银行的资金存入 Hold 账户的证明，共识通过，它就触发双方资金清算，自动记录两边账本：释放 Dollar 银行 ILP ledger Hold 账户资金给流动性提供方账户，同时转移 Euro 银行 ILP ledger 中流动性提供方 Hold 账户资金给 Euro 银行，100 欧元记入 Beta 公司，5 欧元手续费记入银行账户，支付结束（图 15）。

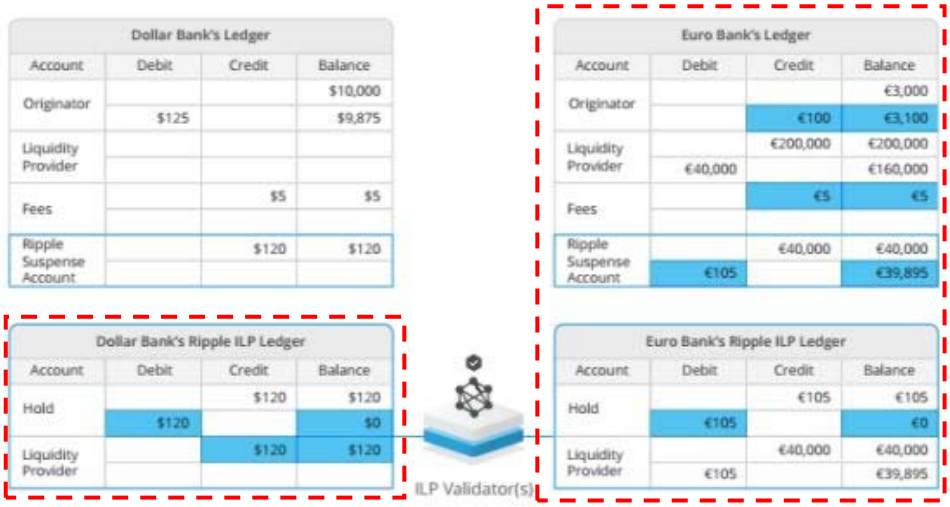


图 15 Dollar 银行释放资金、Euro 银行记账

需要强调的一点，Ripple Segregated Account 主要作用是体现流动性提供方的账户情况，这是非常关键的设计。RippleNet 通过债务关系的转换，使得无需实际资金的搬运，在短短几分钟内通过信息处理，最终实现资金的交割。上述详细的资金流和业务流细节过程有些复杂，但是由于通过区块链网络进行电子化操作，执行时间是短暂的，支付成本远低于传统的跨境支付模式。

(4) Ripple 面临的问题

通过上面的分析，我们可以看出 Ripple 这样的互联网协议进行金融交易，在支付费用、效率、金融服务互联性等方面的优势，但同时

Ripple 面临的问题也是不可忽视的。

首先,Ripple 的快速跨境兑汇可能会造成洗钱、背离外汇监管条例,甚至可能支持恐怖活动货币转移的活动。目前,世界各国均在加强洗钱和反恐的监控,而现在技术的条件下,ripple 网络体系自身不能良好进行洗钱监控。2015 年,美国财政部下属机构金融犯罪调查合作局(FinCEN)就对 Ripple 提出指控,认定其违反了银行保密法,该公司在出售 XRP 时并未注册成为货币服务提供商,且没有建立起系统的反洗钱程序。

其次,目前各国对于数字货币的监管态度有较大分歧,Ripple 面临监管合规风险。以美国为例,虚拟货币交易所交易的数字资产属于证券范畴,数字货币交易所需在 SEC 注册备案或获得牌照后可从事盈利活动。那么,若监管层将 XRP 看作一种证券,Ripple labs 未来是否能够取得直接交易外汇或者证券相应资质法律文件仍是未知数。即使 Ripple 公司可以获得许可,那 Ripple 网络中各个网关节点又当如何确认资质依旧是较大的问题。

再次,Ripple 网关的安全性问题。虽然 Ripple 国际商业自律组织 International Ripple Business Association(IRBA)对于开展公众服务的网关提供了一定的准入门槛,并且符合这些条件的网关可以获得 IRBA 认证标志。但是加入了 IRBA,但并不意味着这些网关就一定是安全的,Ripple 公司并不对网关的质量把关。这意味着,用户在某网关充 USD,没用完,该网关跑路,那么网关交易平台就没了,用户在该网关的 USD 余额凭证就成废纸,并且 Ripple 公司并不对此损失直接负责。

最后,推广认可的问题。区块链去分布式架构和点对点的交易不经

过中心监管，对现有的网络架构形成了挑战，但缺少的是被广泛使用的完善程序，接受程度受制于用户和网络参与者。从银行的角度看，目前银行对于区块链的应用还是比较谨慎，尚未出现杀手级的应用，与区块链技术结合的尝试基本处于 PoC（原型验证）测试阶段。那么，Ripple 在积极寻求和银行合作的过程中，实现从理论技术到成熟商业模式的转换，并经得住成本考验是一个亟待解决的问题。

四、总结

“区块链+”概念在近几年被炒的火热，但从实际发展来看，真正能够在技术层面有实质性说服力的区块链公司其实很少，除了谈概念，更多的就在已有的应用场景中，与区块链技术相结合，出现“区块链+产业”的应用落地模式。

以交易支付场景为例，传统金融机构更愿意通过联盟链/权限链的方式加入区块链网络，节约业务成本、提高效率。基于区块链的跨境支付实现可靠、安全、不间断服务，减少了人工处理环节，缩短了清结算时间，将明显提高交易速度。同时，由于传统跨境支付模式中存在支付处理、接收、财务运营和对账等成本，通过分布式记账，将削弱交易流程中的中介机构作用，提高了资金的流动性，实现了实时确认和监控，能够有效降低交易环节中的直接成本和间接成本。

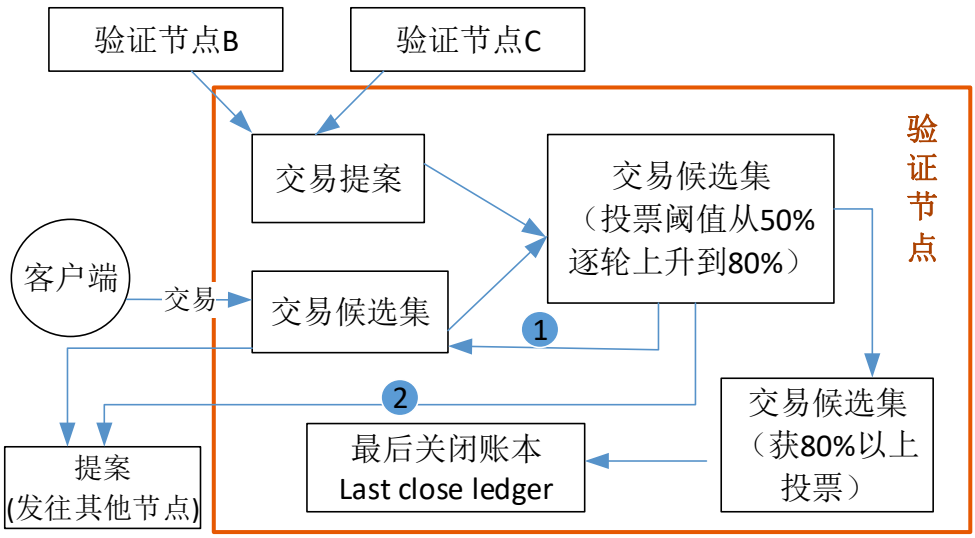
以上区块链带来的优势是显而易见的，但我们也应当看到其面临的问题，例如，区块链的应用依赖于底层的设计，如今底层平台的不完善是限制区块链应用发展的重要因素。因此，区块链应用未来发展首先需

要做好算法和法律合规的双重优化，其次，区块链和数字货币未来发展必须要有一套全新的支付清算管理模式与之相配套，以更好地提升支付清算效率，防范可能存在的风险。

附录：Ripple Net 共识过程

在 Ripple 的网络中，交易由客户端发起，经过追踪节点（tracking node）或验证节点（validating node）把交易广播到整个网络中。追踪节点主要负责响应客户端的账本请求以及分发交易信息，只起广播的作用。而验证节点除包含追踪节点的所有功能外，还能够通过共识协议，在账本中增加新的交易数据，即：验证节点有投票权，参与共识过程并记账。每个验证节点预先配置一份可信任节点列表 UNL（Unique Node List），如果不是来自该验证节点的 UNL，则忽略收到的提案。

每 隔



几秒，

Ripple 网络将进行如下共识过程：

① 在一定时间内，没有超过 50%的交易，将留待交易候选集，下一次共识过程去确认；
② 获得超过 50%投票的交易，作为提案发给其他节点，同时提高阈值到 60%，如此重复直到阈值达 80%；
③ 经过 80%UNL 节点确认的交易正式写入本地的账本数据中。

(i) 每个验证节点会不断收到从网络发送过来的交易，通过与本地账

本数据验证后，不合法的交易直接忽略，合法的交易将汇总成交易候选集（candidate set）。交易候选集里面还包括之前共识过程无法确认而遗留下来的交易。每个验证节点把自己的交易候选集作为提案发送给其他验证节点。

(ii) 验证节点在收到其他节点发来的提案后，如果不是来自 UNL 上的节点，则忽略该提案；如果是来自 UNL 上的节点，就会对比提案中的交易和本地的交易候选集，如果有相同的交易，该交易就获得一票。

(iii) 在一定时间内，没有超过 50%的交易，将留待下一次共识过程去确认。当交易获得超过 50%的票数时，则该交易进入下一轮。

(iv) 验证节点把超过 50%票数的交易作为提案发给其他节点，同时提高所需票数的阈值到 60%，重复步骤 3）步骤 4），直到阈值达到 80%。

(v) 验证节点把经过 80%UNL 节点确认的交易正式写入本地的账本数据中，称为最后关闭账本（Last Closed Ledger），即账本最新状态。

参考文献

[1]. Bitcoin:A Peer-to-Peer Electronic Cash System.Satoshi Nakamoto.

[2]. Ripple Product Overview: A technical overview of Xcurrent.

[3]. Ripple Solution Overview: A comprehensive business overview for financial institutions on RippleNet.

[4]. Ripple Set-up Models: Liquidity and infrastructure Provisioning.

[5]. Distributed ledger technology in payments, clearing, and settlement. Working papers in the Finance and Economics Discussion Series (FEDS).

[6]. 区块链技术的特点和未来发展趋势，姚前.

[7]. 区块链在跨境支付上的颠覆创新可能，腾讯研究院.

[8]. 中国区块链技术和应用发展白皮书，工信部.

[9]. 2016 年全球支付报告，麦肯锡

联系人: 邮 箱: