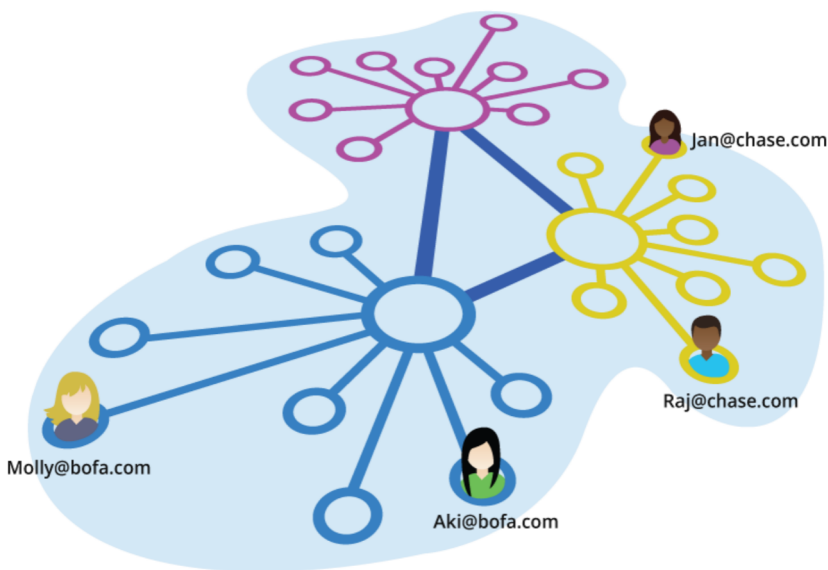




**world's open payment network**

created by  
**Ripple Labs Inc**  
[www.ripple.com](http://www.ripple.com)



*the first book about ripple  
begin your brilliant new payment experience  
right here, right now!*

written by **ming peng**

# RIPPLE 开放式全球支付网络

超越比特币的新金融革命

ming peng

This book is for sale at <http://leanpub.com/ripple>

This version was published on 2014-01-14



This is a [Leanpub](#) book. Leanpub empowers authors and publishers with the Lean Publishing process. [Lean Publishing](#) is the act of publishing an in-progress ebook using lightweight tools and many iterations to get reader feedback, pivot until you have the right book and build traction once you do.

©2013 - 2014 ming peng

从前，*HTTP* 协议将孤立的站点连接起来创造了互联网，然后有了新浪，谷歌，淘宝，腾讯等互联网企业，影响了我们生活的方方面面。

现在，*RIPPLE* 协议将各种货币和金融机构连接起来，形成全球化的去中心的准实时金融系统，这将成就怎样的未来？

# Contents

货币概述 . . . . .	1
货币作用 . . . . .	1
货币简史 . . . . .	3
现有货币的不足 . . . . .	8
货币的未来 . . . . .	9
不得不说的比特币 . . . . .	10
比特币是什么 . . . . .	11
比特币大事记 . . . . .	14
大洋对岸的比特币故事 . . . . .	16
比特币原理 . . . . .	20
比特币的优势与不足 . . . . .	23
<b>RIPPLE . . . . .</b>	<b>25</b>
为什么会有 ripple . . . . .	25
原理概述 . . . . .	28
ripple 币，比特币 2.0? . . . . .	30
理解 ripple . . . . .	33
简介 . . . . .	33

## CONTENTS

理解瑞波账簿 . . . . .	34
理解瑞波生态系统 . . . . .	37
商业集成 . . . . .	39
瑞波关系网 . . . . .	40
多重交易 . . . . .	41
使用 <b>ripple</b> . . . . .	42
用户使用场景 . . . . .	42
瑞波钱包 . . . . .	45

## 货币概述

金子，黄黄的，发光的，宝贵的金子！只要一点点儿，就可以使黑的，变成白的，卑贱的变成尊贵的，老人变成少年，懦夫变成勇士。。。。

-- 莎士比亚

随着人类文明的发展，社会活动出现分工，逐渐有了物品交换的需求，于是出现来商品，其中分离出来固定地充当一般等价物的特殊商品，就是货币；货币是商品交换发展到一定阶段的产物。货币的出现大大降低了人们物品交换的难度，加快了资源配置的速度，成为商品生产分配过程中不可缺少的特殊道具，在人类文明的发展中起了非常重要的作用。

## 货币作用

由于货币属于商品，因此他同所有商品一样也具有使用价值和交换价值。当处在不同形式的价值运动中时，货币所表现出来的作用也不尽相同：价值尺度、流通手段、支付手段、贮藏手段和世界货币。其中，价值尺度和流通手段是货币的基本职能。另外三种职能则是在两者的基础上形成的派生职能。

价值尺度 价值尺度是货币作为社会劳动的直接体现。货币本身作为一种商品，可以以自己为标准，与其

他商品进行量的比较，而此时商品的价值形式就转化为价格形式，商品通过货币进行表达的价值形式即为价格。当货币执行价值尺度这一职能时，货币只需要以想像中的或是观念上的形式存在就可以了，然而他的单位则必须依赖于现实中流通的货币。正是由于货币的价值尺度功能，使得人们可以将不同形式的商品先转化为货币的价格形式，然后再与其他商品进行交换。货币本身作为商品也存在不同货币之间量的差别，因此人们为货币也制定了一个量的标准，即规定价格标准（有时亦称价格标度）。

**流通手段** 流通手段的职能是货币作为商品交换的媒介，即购买手段的职能。其主要特点是在商品买卖中，商品的让渡和货币的让渡在同一时间内完成，通俗地说是一手交钱、一手交货。因此，从价值运动的角度观察，货币执行流通手段职能时，在同一时间内，价值的运动是双向的。即卖方在得到价值的同时出让使用价值，买方在让渡价值的同时获得使用价值。货币作为流通手段时，称为通货。

**贮藏手段** 贮藏手段的职能，指的是当货币退出流通领域，被当作社会财富的代表被保存起来时货币所发挥的作用。一般来说，货币用作价值储藏风险是最低的。但是，通胀会削减购买力，而且货币并无利息收入，因此，长期来说，价值储存的功能并不及其余的能力重要。

**支付手段** 货币执行支付手段的职能是随着商品赊账买卖的产生而出现的。在赊销赊购中，货币被用来偿还债务。后来，它又被用来支付地租、利息、税款、工资等。

世界货币 当货币跃出国内市场，在世界市场上购买外国商品，支付国际收支差额，作为社会财富的代表在国家与国家之间转移时，它就具有了世界货币的职能。

货币的本质是一般等价物，正是它使得商品交易与服务贸易等活动更加方便、高效。<sup>1</sup>

## 货币简史

历史上不同地区曾有过不同的商品交换充当过货币，后来货币商品逐渐过渡为金银等贵金属。随着商品生产的发展和交换的扩大，商品货币（金银）的供应越来越不能满足对货币日益增长的需求，又逐渐出现了代用货币、信用货币，以弥补流通手段的不足。进入20世纪，金银慢慢地退出货币舞台，不兑现纸币和银行支票成为各国主要的流通手段和支付手续。

物物交换 在原始社会，人们使用以物易物的方式，交换自己所需要的物资，比如一头羊换一把石斧。但是有时候受到用于交换的物资种类的限制，不得不寻找一种能够为交换双方都能够接受的物品。这种物品就是最原始的货币。牲畜、盐、稀有的贝壳、珍稀鸟类羽毛、宝石、沙金、石头等不容易大量获取的物品都曾经作为货币使用过。

金属货币 经过长年的自然淘汰，在绝大多数社会里，作为货币使用的物品逐渐被金属所取代。使用金属货币的好处是它的制造需要人工，无法从自然界大量获取，同时还易储存。数量稀少的金、银和冶炼困难的

---

<sup>1</sup>中文维基百科 - 货币 <http://zh.wikipedia.org/wiki/货币>



铜逐渐成为主要的货币金属。某些国家和地区使用过铁质货币。



中国古钱币

早期的金属货币是块状的，使用时需要先用试金石测试其成色，同时还要秤量重量。随着人类文明的发展，逐渐建立了更加复杂而先进的货币制度。古代希腊、罗马和波斯的人们铸造重量、成色统一的硬币。这样，在使用货币的时候，既不需要秤量重量，也不需要测试成色，无疑方便得多。这些硬币上面带有国王或皇帝的头像、复杂的纹章和印玺图案，以免伪造。

中国最早的金属货币是商朝的铜贝。商代在我国历史上也称青铜器时代，当时相当发达的青铜冶炼业促进了生产的发展和交易活动的增加。于是，在当时最广泛流通的贝币由于来源的不稳定而使交易发生不便，人们便寻找更适宜的货币材料，自然而然集中到青铜上，青铜币应运而生。但这种用青铜制作的金属货币在制作上很粗糙，设计简单，形状不固定，没有使用单位，在市场上也未达到广泛使用的程度。由于其

外形很像作为货币的贝币，因此人们大都将其称为铜贝。

据考古材料分析，铜贝产生以后，是与贝币同时流通的，铜贝发展到春秋中期，又出现了新的货币形式，即包金铜贝，它是在普通铜币的外表包一层薄金，既华贵又耐磨。铜贝不仅是我国最早的金属货币，也是世界上最早的金属货币。

金银等贵金属 西方国家的主币为金币和银币，辅币以铜、铜合金制造。随着欧洲社会经济的发展，商品交易量逐渐增大，到 15 世纪时，经济发达的佛兰德斯和意大利北部各邦国出现了通货紧缩的恐慌。从 16 世纪开始，大量来自美洲的黄金和白银通过西班牙流入欧洲，挽救了欧洲的货币制度，并为其后欧洲的资本主义经济发展创造了起步的条件。



黄金货币

纸币 随着经济的进一步发展，金属货币同样显示上使用上的不便。在大额交易中需要使用大量的金属硬币，其重量和体积都令人感到烦恼。金属货币使用中还会出现磨损的问题，据不完全的统计，自从人类使用黄金作为货币以来，已经有超过两万吨的黄金在铸币厂里、或者在人们的手中、钱袋中和衣物口袋中磨损掉。于是作为金属货币的象征符号的纸币出现了。世界上最早的纸币在宋朝年间于中国四川地区出现的交子。最初的纸币是以黄金为基础的，与黄金可以自由兑换，两者可以同时流通，纸币的发行量也比较少。到 19 世纪末，资本主义经济出现了速度空前的膨胀与发展，于是纸币逐渐成为主要的流通货币，但是它们仍然有黄金作为发行的保障。这种货币制度称为“金本位”。

纸币本位制，亦称“自由本位制”。以国家发行的纸币作为本位货币的一种货币制度。其特点是国家不规定纸币的含金量，也不允许纸币与金（银）兑换，纸币作为主币流通，具有无限法偿能力；同时，国家也发行少量金属铸币作为辅币流通，但辅币价值与用以铸造它的金属商品价值无关。由于发行纸币是国家的特权，在中央银行国有化之后，国家便委托中央银行发行纸币。中央银行发行纸币的方式是通过信贷程序进行的，所以纸币实际上是一种信用货币。由于该种货币制度不与黄金挂钩，纸币发行量一般由国家根据经济发展的需要来决定，国家要对其实行严格的管理，所以也叫“有管理的通货制度”。当今世界各国的货币制度，几乎都是纸币本位制。



### 小思考

只要国家担保并指定为法定货币，货币的表现形式很多，有比纸币更好的表现形式吗？

数字化货币 随着信息技术的发展，各类纸制文档逐渐电子化，货币也跟随这种趋势。当货币作为存储手段时，银行只需要知道储户在它这里存有多少钱，而并不一定时时刻刻都为其保存该数量的货币。当货币作为流通手段，当储户张三从其账户中转账一定量货币到李四账户时，银行并不需要将张三的那份货币挪动到属于李四的那份，而只需在他们的账户中分别做增减操作即可。

存在银行中的纸币逐渐从一本存折变成一张卡，再变成连卡也可以省略了，是网上银行或手机银行中的一

条条记录，人们不再需要纸币也能实现支付和结算，无论作为何种用途，纸币均逐渐数字化。人们只需准备很少的一些纸币零用，大多数使用场景均可用数字化货币取代。

## 现有货币的不足

运输和存储时，纸币仍然不够方便；水火自然磨损等也容易让纸币损坏；纸币容易被伪造，仅仅靠技术防伪手段难以杜绝，还需国家采取强力手段打击伪造等犯罪行为。

数字化货币是现有货币的最高级形态，作为主要形态纸币的补充，它解决了货币使用过程中的很多问题。但是其发行与纸币挂钩，所以它无法克服纸币的一些固有问题。其中争议最多的，就是货币的超发，世界上主要国家历史上几乎都经历过货币超发带来的灾难性后果。

第一次世界大战后，法国采取纸币通货膨胀的政策，法郎发生贬值，到 1922 年时，其购买力已跌至 1915 年的 43%，同英镑的比价从 1914 年的 25.22:1 跌到 1926 年的 240.2:1。法国不得不终止金本位的实行。1928 年法国制订新货币法，规定法郎含金量为 0.065 克，仅相当于一战前的 1/5。

第二次世界大战后，法国再度发生恶性通货膨胀，同英镑比价跌至接近 1:1000。1960

年发行新法郎 (Nouveau Franc)，确定其币值为旧法郎的 100 倍，相当于 0.1802 克黄金。

其次，随着经济的发展，新的需求出现了。

跨国贸易大量增加，币种的兑换需求越来越大，对兑换速度兑换效率有了更高的要求；电子商务的迅速发展，催生了远程交易的需求，人们仍然希望一手交钱一手交货，但并不希望跑老远的去面对交易。

数字化货币从银行流向第三方支付，催生新的金融服务行业，数字货币的使用形式也更加灵活。但其仍然仅限国家范围内使用，汇率的存在和变动使得国家甚至可以通过强力手段发动对其它国家的货币战争，货币之间的对抗造成额外的风险。

成本高昂，大型的中心化的清算中心分别维护各自的账单，增加的冗余和中间环节，增加了整个系统的使用成本，降低了效率。

## 货币的未来

人们在寻找一种国际化的货币，方便快捷，使用成本低，安全，不能超发，然而进展缓慢。世界上到底有没有这么一种更完美的货币？没人知道答案，然而在人们孜孜不倦的探寻之下，有一种货币渐渐浮出水面，给我们带来一些曙光。

# 不得不说的比特币

没有根基也许可以建一座小屋但绝对不能造一座坚固的大厦。

-- Eng.Isidor Goldreich

一切秘密都在密钥之中。

-- 匿名

在国家金融体系之外，大型企业及社区等民间集体的广义“货币”也遍地开花，虚拟币，游戏币，会员卡等层出不穷，由于电子货币实际上只是一条条有意义的记录，简单快捷低成本，几乎所有的此类货币都以电子货币的形式发行（国家也不允许民间发行纸币）。

他们在各自的领域内发挥了积极的作用，但也仅限于它们各自的领域内流通：

- 它们只能购买特定的商品，一般为非实物商品。一首歌，一本电子书，或者游戏中的道具等。可谓专币专用。
- 货币使用价值为发行方信用担保，在其领域内流通有效，外界并不认可。游戏玩家会认为游戏币可以买顶级装备有较高的价值，但对不玩游戏的大多数人来说游戏币没有意义。
- 货币本身一般无价值，只是一些数字或者一张卡片，也无法保证不会被超发。

- 国家对货币的严格管理，企业没有意愿也不能发行通用货币。

上述所有特性决定它们不可能成为一般意义上的货币，它们只能偏安一隅，像一粒粒沙子看着国家法定货币这个高楼大厦。

直到一个叫中本聪（Satoshi Nakamoto，可能是化名）的人出现。

2008 年 11 月 1 日，一个自称中本聪的人在一个隐秘的密码学讨论组上贴出了一篇研究报告，报告阐述了他(她)对电子货币的新构想，比特币就此问世。2009 年 1 月 3 日，中本聪开创了比特币 P2P 开源用户群节点和散列函数系统，从此，其对等网络和它的第一个区块链开始运行，他发行了有史以来的 50 个比特币。一年后，在比特币论坛上，用户群自发交易中，产生了第一个比特币公允汇率。该交易是一名用户发送 10,000 比特币，购买了一个披萨饼。随后比特币开始在全球快速发展。

## 比特币是什么

如前所述，比特币是一种用开源的 P2P 软件技术产生的电子货币，也是根据该开源软件以及建构其上的整个 P2P 网络的总称。

与大多数现行货币不同的是，比特币货币系统是独立存在的，其运行不依赖于中央银行、政府、大型企业的支持或者信用担保。比特币使用遍布整个 P2P 网络



节点的分布式数据库来管理货币的发行、交易和账户余额信息。比特币采用密码学的原理，确保各个比特币节点按照既定的协议达成共识，从而确保货币流通各个环节的安全性。例如，比特币只能被它的真实拥有者使用，而且仅仅能使用一次，支付完成之后原主人即失去对该份额比特币的所有权。



比特币

比特币货币总量按照设计预定的速率逐步增加，增加速度逐步放缓，并最终在 2140 年达到 2100 万个的极限。P2P 的分布式特性与去中心化的设计结构，确保了理论上任何机构都不可能操控比特币的货币总量，或者制造通货膨胀。在全球范围内，比特币可以通过多个线上的交易所和服务商进行兑换交易，也可以在线下找到兑换点，兑换为现钞或金币。

## 中本聪身份之谜

当人们对比特币津津乐道时，比特党也在试图揭开中本聪的神秘身份。讨论组的老手们从未听说过中本聪这个人，有关他(她)的信息也寥寥无几，还都隐晦不明甚至自相矛盾。网上简介显示他(她)在日本居住，但他(她)的电子邮箱地址却是来自德国的一个免费服务站点，谷歌上也没有他(她)的任何信息，显然，“中本聪”是个假名。

在一个比特币聊天频道里，有人自负地认为“Satoshi”在日语中是“智慧”的意思，其他人则怀疑这是4家科技公司名字的“拼盘”三星(Samsung)、东芝(Toshiba)、中道(Nakamichi)和摩托罗拉(Motorola)。甚至连他(她)的国籍也受到质疑，因为他(她)的英语太地道了，简直毫无瑕疵。

有人暗示，或许中本聪不是一个人，他(她)代表一个有着未知目的的神秘组织谷歌的一个团队或是国家安全局。豪涅茨说：“我和这家伙通过几封电邮。”豪涅茨有一段时间是比特币核心开发成员。“我总认为他不是真实存在的人，我大概每两周收一次回信，就像有人偶尔检查邮箱一样。比特币的设计非常棒，不像是靠一个人就能完成的。”

中本聪很少透露自己的信息，他(她)在网上谈论的话题只限于源代码技术讨论。2010年12月5日，在比特币使用者开始要求维基解密接受比特币捐赠后，原本言谈简洁只聊业务的中本聪以前所未有的热情参与到讨论中。“不，不要这样做。”他(她)在比特币论坛里发帖说，“这个项目需要逐步成长，这样软件才能在这个过程中不断增强。我呼吁维基解密不要接受比特币，它还是一个萌芽阶段的小型测试社区。在这个阶段，如果不能妥善处理，只会毁了比特币。”

在此之后，就像他(她)的神秘出现一样，神龙见首不见尾的中本聪又消失了。格林威治时间2010年12月12日6点22分，就在他(她)发帖争辩给维基解密捐赠比特币7天后，中本聪在论坛发了最后一个帖子，帖中谈到软件最新版本几个无关紧要的细节，他(她)的电邮回复也变得更加不稳定，最后完全终止了。比特党对他(她)的离开感到悲伤和不解。但不管怎样，他(她)的发明已焕发出勃勃生机。

## 比特币大事记

2011年6月，在维基解密创始人阿桑奇和谷歌总裁Eric Schmidt秘密会晤时，阿桑奇向他介绍并解释了

“无国度”的比特币。维基解密、自由网、Singularity Institute、互联网档案馆、自由软件基金会以及其他的一些组织，开始接受比特币的捐赠。一些小型的企业也开始接受比特币，LaCie 公司是一间上市公司，接受比特币作为其 Wuala 服务的付款方式。

2012 年 10 月，BitPay 发布报告说，超过 1000 家商户通过他们的支付系统来接收比特币的付款。

2012 年 11 月，WordPress 宣布接受比特币付款。声明说肯尼亚、海地和古巴等地区遭受国际支付系统的封锁，比特币可以帮助这一地区的互联网用户购买服务。

2013 年 3 月，美国财政部金融犯罪执法系统 FinCEN 发布了虚拟货币个人管理《条例》。

2013 年 4 月，海盗湾, EZTV, 开始接受比特币捐款。中国四川省雅安地震后，公募基金壹基金宣布接受比特币作为地震捐款。

2013 年 5 月，电子前哨基金会宣布，在研究美国财政部金融犯罪执法系统发布的虚拟货币个人管理《条例》后，把比特币和汽车一样，当作礼物重新接受捐赠。

8 月 8 日，比特币被美国德州联邦法官 Hirsh 裁为合法货币，受《联邦证券法》监管。

8 月 19 日，德国政府认可了比特币的法律和税收地位，成为全球第一个正式认可比特币合法身份的国家

10 月 29 日，全球第一部比特币自动提款机于加拿大温哥华激活，但交易额限额每天 3000 加元。

11月20日美国司法部和美国证交会的代表在北京时间周一晚间出席美国参议院的一个听证会时称，比特币是一种合法的金融工具，这一说法预计将会推进比特币合法化的进程。据听证会上公布的文件，美联储主席伯南克认为，比特币“或具有长期的承诺”，也能够某一天“促进更快速、更安全和更高效的支付体系”。目前还没有必要对虚拟货币进行直接干预和监管。

11月20日，中国人民银行副行长易纲在一场论坛上表示，从人民银行角度，近期不可能承认比特币的合法性。但他同时认为，比特币交易作为一种互联网上的买卖行为，普通民众拥有参与的自由。此外，易纲还指出比特币“很有特点”，具有“启发性”，个人会保持长期关注。<sup>2</sup>

比特币散发出无穷的魅力，这个诞生在互联网上的新生事物，似乎天生就没有国界，迅速在世界范围流行起来。

## 大洋对岸的比特币故事

### Rockxie 的致富路

Rockxie 的家乡位于湖南省和江西省的交界处，由于家境贫寒，小时候家里常常连学费都缴不起，但是 Rockxie 读书很用功，并以优异的成绩考上了合肥工业大学计

---

<sup>2</sup>维基百科比特币发展史

算机系。钻研于计算机领域的 Rockxie 从 2006 年大三开始，在起点中文网上连载第一部网络小说《黑客传说》，小说以“计算机”、“黑客”为主要元素，融入了推理和玄幻的风格，在网上广受好评，累计点击量超过 400 万，而 Rockxie 也由此挖到了第一桶金。

他将这数万元稿费全部用来补贴家用，自己投身于第二部小说《超级系统》的创作。毕业后，Rockxie 在上海一家软件公司从事软件开发。但是习惯了自己支配时间、自由撰写网络小说的他，对朝九晚五的生活很不适应。不多久，他就离开了公司，专心投身于写作。期间，他还和朋友合伙创业，主要从事传统工业电器方面的销售，不过由于市场、管理，以及个人兴趣等方面的原因，三年之后他最终还是选择退出。

故事发展到这里好像也没什么大不了，就在他准备撰写新小说《超脑黑客》时，“比特币”这个神秘的概念，跃入了他的视野。当时比特币交易所遭到黑客袭击，价格从 29 美元跌到了 3 美元左右，大家都很消沉，纷纷探讨比特币的泡沫，也有一些人想寻找下家，抛售手中的比特币。而 Rockxie 在论坛里泡久了，对这种新型的电子货币渐渐产生了兴趣。一开始他并没有想到投

资，只是想把这个元素融入小说，于是广泛地收集一些比特币的资料，其中包括许多国外的技术性文章。通过不断地学习，他发现比特币的泡沫并没有想象中那么大，而当时他创业项目不太景气，在股票市场也频频受挫，于是开始购入比特币投资。第一次购买比特币是通过淘宝网的卖家，大约 40 元人民币一个，其中还包括几元手续费。随后比特币价格慢慢回升，Rockxie 也越买越多，并开始登录专业的交易网站，他陆陆续续购买了 1000 个，平均成本约 60 多元，共动用了六七万元资金。

就在 Rockxie 不断购买比特币的同时，他从一位比特币圈内的朋友处得到消息，一家名为“bitfountain”（烤猫）的公司正在比特币社区中面向全世界发起众筹项目。烤猫公司虽然在国内名不见经传，但是在比特币世界里却赫赫有名，它是比特币世界中最大的矿机供应商之一（挖矿机是一种软件，可通过连续计算产生比特币），当时谋求在互联网虚拟 IPO 上市。虚拟 IPO 是和现实资本市场平行的世界。在这个世界中，人们可以通过特定的交易系统，用比特币买卖公司的股票，上市公司会根据每年的业绩情况，以比特币的形式，给股东分红。”在烤猫公司上市之前，其原始股为 0.1 比特币一股，买 5000 股以上可以

额外赠送 10% 股，Rockxie 将其 1000 个比特币全部买入了烤猫股份，共持有 11000 股。随着比特币热度持续上升，烤猫公司成功地虚拟上市，其股价从 0.1 比特币上升到目前的 5 比特币，Rockxie 的资产又翻了 50 倍。经过几次减持后，Rockxie 目前仍然持有公司超过 5000 股的股份，并持有 6000 多枚比特币，总市值超过千万人民币。

就这样，Rockxie 成了像其书中主角《超脑黑客》主人公那样传奇一般的人物。当被问及面对一个新生事物，他怎么会有勇气一次下这么大注码时，Rockxie 答道：起初我和很多人一样，也认为比特币是泡沫，所以只是想把它作为一个素材写进小说。但正是因为写作的缘故，我才对比特币进行了深入研究。我是读计算机的，随着对比特币算法、体系的了解程度越深，我对它的信任度越强，所以才敢于做这样的投资。当比特币被越来越多的人认同，使用范围越来越广时，它的价格会不断上升。在国外，已经有很多支持比特币支付的商店和旅馆；在国内，也有很多淘宝卖家支持比特币，不论外界评论怎样，比特币仍然会沿着自己的轨道发展。<sup>3</sup>



### 小思考

为什么大洋西岸产生的一个新兴事物短短时间即能在大洋东岸催生一个千千万富翁？

---

<sup>3</sup>IT 时报网络作家上演比特币投资神话



目前，比特币最为主要的参考汇率是 Mtgox 交易所内比特币与美元的成交汇率。2013 年 11 月，比特币的交易价格创下 1242 美元的历史新高，同期黄金价格为每盎司 1241.98 美元，比特币价格首次超过黄金。短短两年时间，比特币的价格涨了成千上万倍。它为什么有如此大的魅力？



比特币市值

## 比特币原理

中本聪在其论文<sup>4</sup>中对比特币网络的原理有详细的描述。该论文论述严谨，涉及大量数学，密码学及计算机知识，质量很高，也让常人难以理解。理解有助于信任和使用，这里尝试用浅显的语言对该论文做一个通俗易懂的解读。

我们可以把比特币理解为很复杂的方程组的有限个（约 2100 万）解，每一个解都能解开方程并且是唯一的。如果把它想象成人民币的序列号，每个比特币就相对于一张人民币。挖矿的过程就是通过庞大的计算量不断的去寻求这个方程组解的过程。由于这个方程

---

<sup>4</sup>比特币论文 <http://bitcoin.org/bitcoin.pdf>

组被设计成了只有 2100 万个解，所以比特币的上限就是 2100 万。

那如何把钱花出去呢，编号为 1 的比特币的持有人都知道有这么一个比特币，那它不是可以永远使用它？答案是不行。比特币网络是一个在线系统，比特币本身作为一串数（方程组的解）离开了比特币网络一点用处也没有，这些数只有放进比特币网络里才能正常运作。

比特币网络被设计成了一种分布式系统，我们可以把它想象为一个账本，它上面记满了各类明细。这个账本并不存在某个中心的服务器里而是面向所有人公开，每一个比特币钱包都是一个节点。这些节点用类似于 BT 下载的 P2P 网络相连。



### 小知识

比特币钱包记录着全世界所有人的数据，现在的数据大约为 7G，如果以后钱包继续增大可以抛弃一些陈旧且无意义的交易细节。

怎么能保证比特币在同一时刻只会拥有一个合法的主人呢？答案来了，每当你发起一次交易的时候，都会向整个比特币网发出广播，内容如下：

“我是钱包 A，有编号为 123 的比特币，现在要转账给钱包 B，请你们更新你们的账本”比特币网络里的其他钱包收到这个信息纷纷与自己的账本比对，并回应：“我

带入方程算了下，编号为 123 的比特币存在。我看到了钱包 A 和 B 也存在，且该 123 号比特币确实为 A 所有，我承认这笔交易并将修改我的账本。”

当确认的节点数达到一定量的时候（取决于收款方想要有多稳妥），交易就成功发生了。接下来，越来越多的节点收到了这个消息，并且没有人提出异议，这个交易记录就被整个比特币网络所接受，从此比特 123 成为了 B 钱包里的所有物。

如果你在交易结束之后，欺骗本地客户端，又让 A 钱包发出信息：

“我是钱包 A，有比特币 123，现在要转账给钱包 C，请你们更新你们的账本”（和之前一样的过程）。其他节点收到信息与本地数据库一对比：“不对，我这写着比特币 123 在 B 手里，不承认交易。”

越来越多的节点拒绝了交易，于是你的交易就失败了。挖矿也是同样的原理，利用大量的计算力去计算方程组特解，而你的矿机程序会先与本地的账本进行对比，发现自己这里从来没有这个特解，于是向全网广播：

“我是 A，我这有个新比特币，叫 234，你们要没见过我可就收下了？”

之后的原理与交易就相同了。你可能注意到，交易的成功需要有大多数节点接受才能成功，也就是说，只要系统中诚实的节点数量多于欺诈的节点数量，整个系统就是安全的。比特币网络的这种容错机制，可以保证即便是有一定的欺诈者（一直发布虚假信息）和捣乱者（一直拒绝承认别人的交易）也不会影响到整个网络的运转。

## 比特币的优势与不足

**去中心化** 比特币是第一个真正意义上的分布式的虚拟货币，整个网络由用户构成，没有中央银行。去中心化是比特币安全与自由的保证。

**全世界流通** 比特币可以在任意一台接入互联网的电脑上管理。不管身处何方，任何人都可以挖掘、购买、出售或收取比特币。

**专属所有权** 操控你的比特币需要你的私钥，它可以被隔离保存在任何存储介质。除了你之外无人可以获取。

**低交易费用** 目前可以免费汇出比特币，但最终对每笔交易将收取约 1 比特分的交易费以确保交易更快执行。关于交易费的详情。

**无隐藏成本** 作为由 A 到 B 的支付手段，比特币没有繁琐的额度与手续限制。知道对方比特币地址就可以进行支付。

**很酷的技术** 比特币是技术人士的挚爱！你可以在众多

平台上发掘不同硬件的计算能力。这本身已构成一种乐趣。

比特币是第一个被公众广泛接触和认可的电子货币，作为电子货币大军的排头兵，它冲在了最前面也出尽了风头。但它也有不足和风险。

**隐私和安全** 由于比特币的方便易用及没有监管，一些违法犯罪分子选择比特币作为脏款转移工具；所有的比特币交易都公开且永久地存储在网络中，这就意味着任何人都可以查看到任何一个比特币地址中的余额和交易记录。

**资源浪费** 其次随着比特币渐渐流行，越来越多的人投身到挖矿的行列中，很多计算资源和电力消耗在挖矿行为中，这看上去像浪费。比特币的交易确认时间较长，一般需要 10 分钟，所以如果对时效性有较高要求，比特币不适用。

**仍需兑换** 比特币无法超发，作为一种货币为人们提供了很大的信心，但它无法解决和其它货币的协作问题。短时间内产生一种世界货币的可能性很小，多币种共存的现象将继续下去，所以货币对抗及货币兑换问题也依然存在。

**比特币仍有实验性** 比特币是一个正处于积极发展中的实验性新货币。尽管它的实验性正随着它不断增长的使用率而在逐渐减小，但是要记住比特币是一个全新的发明，它正探索以往从未被尝试过的理念，因此，没有人可以预测比特币的未来。

**政府的态度** 比特币还不是正式的货币，政府对其的态度也将极大影响其发展。

# RIPPLE

Send money to anyone, anytime anywhere in any currency °

-- 瑞波指南

当 http 被发明时，没人会想到会诞生谷歌或者 youtube 这样的网站类似，也没人能预测 ripple 的无限潜能。

-- 瑞波指南

## 为什么会有 ripple

虽然比特币名气更胜，实际 Ripple 系统的历史早于比特币。2004 年工程师 Ryan Fugger 的推出了第一版 Ripple；后来 Mt.Gox 的创始人 Jed McCaleb，加上曾经在网络金融领域有多年创业经验 Chris Larsen，两者共同成立了 OpenCoin 来接管 Ripple，负责运行和维护 Ripple 的平台。Ripple 致力于打造一个分布式的点对点的支付和交换系统，且支持任意的币种，无论美元，人民币，比特币都没问题。



Ripple Labs 的前称是 Opencoin，在 2013 年 4 月份获得了来自谷歌和 IDG 的投资之后备受关注。

现在很多公司都在基于现有互联网支付的基础设施进行一些创新，但是在这个过程中遇到很多问题，进而发现现有的基础设施不够用。比如现在的各种独立支付网络相互之间是隔离的，你用支付宝给另一个支付宝转钱很简单，但是如果用另一个支付工具比如财付通就比较困难了。但真正的互联网不是这样的，访问网站可以用任何一个浏览器，但是现在的支付系统不是这样的。



#### **currency\_symbol**

现在的支付和 70 年代电子邮件的景象类似，如果多家支付系统进行合作，就可以实现跨网络进行支付，但是目前没有一种协议可以让网络之间的支付变得很平常。在邮件的发展过程中有过许多尝试，比如说建立一个超级服务器，让任何东西都通过他们的服务器来解决，但是没有公司成功。而成功的是现在这套开放协议 SMTP，它允许大家都介入，从而让跨网络的电子邮件沟通成为了可能。正是这些开放协议的出现，使邮件服务从早期的割据到现在通过一个协议将不同的邮件连接起来，成为一个非常通用的服务。

从 IT 技术的角度看，支付相对邮件更加困难，因为支付有先后顺序的问题。比方说如果你用你帐户里的钱开了一张支票，又开了另一张支票，但是帐户里的钱只够支付一张支票，就必须要有了一张作废，这种情况下需要一个中间机构来决定。比特币的出现解决了这个双重出现问题，Ripple 用一个类似的方案也解决了

这个问题。Ripple 希望能连接各个支付网络，大家可以从一个支付网络给另一个支付网络进行交互，而你的顾客或者你的接受方愿意用什么支付网络都没有关系。

在日常生活中，比方说一个人想给另一个人发钱，愿意支付这一方只有一个支付宝帐户，另一方有一个美国银行的帐户，这是一个很常见行不通的情形，钱没法过去，中间有一个障碍。通常，大家会进行一个操作，找一个中间人，然后这个中间人可以既有美元、美国银行帐户，也有支付宝帐户。他愿意帮你把美元付出去，也愿意支付宝结算。

如果你用 Ripple 完成上面所描述的支付过程，很重要一点就是你不需要相信中间人，它不仅能帮你把美元发出去，也能接受人民币。Ripple 这个网络就会让你的两笔转帐同时发生，中间人可以是陌生人，也可以就是做事的机构，但是你完全不需要信任它。另外由于 Ripple 的中间人省去了谈价格这个过程，并且这个网络是一套协议，它会自动给你找最优的价格。比方说用人民币兑换美元，它有可能基于现在的网络情况，用人民币换成比特币，再换成美元。这样得到的价格比较合理，这个网络自动帮你执行这样一个过程。然后有很多很复杂的路径，这些都是网络自动选取的。

总体来看，Ripple 省略了找中间人这一个步骤。而跨国支付的问题，Ripple 并不是不需要中间人，而是中间人隐藏在网络这套协议当中，而且它解决了信用问题。



## 原理概述

Ripple 系统的核心是一个共享的公共的数据库，它包含一个总帐簿存着所有账户的收支信息，所有人都可以查看这个帐簿，任意账户的每一笔帐目往来。此外，帐簿还存有买卖信息，你可以买卖某种货币或资产，从而实现了一个分布式的兑换系统。每一个该网络的使用者都必须通过某种方式达成共识，最后一致同意对总帐簿进行修改，我们把这种过程叫做共识 (consensus)。共识每 2 至 5 秒钟就进行一次，这样我们不需要集中化的清算系统，也可以进行交易。



### ledger

现代的货币体系都是基于信用的，如现金和债券都有国家信用担保。对存在银行中的钱来说更是如此，你有 100 元存在银行意味着只要你需要，你就可以取出这 100 元，国家信用担保。Ripple 使用类似的信用体系，只是信用不是来自国家，而是一个全球的公共的分布式在线帐簿（以及你自己对特定网关的信任），该帐簿由一个运行 ripple 服务器软件的点对点网络共同维护。为了使每个节点的帐簿保持一致，之前描述的共识过程会持续进行。总帐簿包含每一笔借贷记录：谁借了另一个人多少钱，是什么币种，什么时候发生的。法定货币在 ripple 系统中是以虚拟货币 (IOU) 的形式记录的，所有每一个账户的虚拟货币结余由账户所有的借贷交易共同决定。

Ripple 系统有一个重要的概念叫网关，它的作用有点像银行，接受用户现实中的法定货币并转化其 ripple 的账户中的虚拟货币 (IOU)。例如你在网关中存一万元人民币，网关会在 ripple 系统中给你发行等量的虚拟人民币，表示你在网关中有一万块人民币，你可以提取，兑换或支付给别人。与银行不同的是，该账簿不是银行私有的会计帐本，而是全球共享的一个在线总帐。这样，ripple 网络就和外部世界连接起来了。虽然网关这个概念一般用来称呼往 ripple 系统中存取钱的商业机构，实际上它和别的 ripple 账户没有什么不同，只要别人愿意信任你，任何人都可以作为一个网关。



#### consensus



选择网关时一定要非常谨慎，因为不像瑞波币是整个 ripple 网络通用的，某网关发行的虚拟货币一般只能在该网关交易和提现，建议只信任 ripple 官方推荐的网关。

当支付行为在 ripple 中发生时，不同账户间的虚拟货币余额会自动调整，来体现这笔交易。但记住，ripple 系统只负责帐簿的记录，它并不能强制网关（或其他参与者）履行提现义务，所以 ripple 用户必须十分小心，你只有真正信任另一个用户时，才告诉系统你只信任哪个账户，信任的币种是什么，额度是多少。这

中 ripple 系统中叫信任链。当付款人和收款人直接没有直接相连的信任链时，ripple 会查找有没有连通的间接信任链，撮合交易使其成功。一个交易会像波纹一样沿着信任链扩散出去，直到到达接收者。最后，总帐簿显示的是所有货币余额，你就可以按需中网关那里体取现金或还款。



六度空间理论表明，一个人通过社交链找到世界上的另一个人，中间人个数不超过六个。Ripple 信任链的工作原理和六度空间类似。

除了借助系统中的信任链，Ripple 也允许外部的交易商交易不同网关发行的货币借贷，这样，即使某笔支付找不到一条信任链促成交易，也可以在外部交易商的帮助下完成交易。

为了防止单点故障及有人试图控制 ripple 币，ripple 被设计成一个分布式的系统，任何人，包括 Ripple Labs 都不能控制系统，除非征得大多数节点的一致同意。

## ripple 币，比特币 2.0?

除了分布式的支付和交换系统，ripple 也有自己的货币，瑞波币。Ripple 网络的使用者并不一定需要使用瑞波币，系统支持任意的货币。作为 ripple 系统的内置货币，瑞波币与其他货币有一些不同。它限量发行 1000 亿个，每一个 ripple 网络的参与者都支持瑞波币，这就避免了交易对手风险。而其它货币在 ripple 中表

现为虚拟货币，你可以使用虚拟货币在 **ripple** 系统中交易，但你需要提防交易对手违约或者欺诈的风险(主要是网关)。瑞波币还有一些额外的作用。

## 防止 **ripple** 网络被滥用

防止交易泛滥。为防止系统受到分布式拒绝服务攻击(DDOS), 对每一笔交易，系统都会收取很少量的，正常情况下可以忽略的瑞波币作为交易费用。但如果系统负载太高，比如受到攻击，这个费用会被临时提高，使得攻击者负担不了高额的交易费用而不得不停止攻击。

防止总帐增长太快。系统会跟踪系统中账户的状态，账户每使用一次系统资源，必须保留一定的 **ripple** 币作为保证金，交易成功时保证金退回。这样就防止某些账户无节制的提交很多交易，滥用系统资源造成总帐簿过膨胀。

## 作为中间货币

如果没有中间货币，你可能要将人民币换成日元，再换成欧元，再换成目标货币美元，甚至中间还会有更多的链条。瑞波币的存在使得任意两种货币的兑换都至多只经过一次转换即可。下面几个因素让 **ripple** 币成为理想的中间货币：最高的流动性。没有中间环节，没有交易费用，你可以直接将货币付给另一个账户。

没有交易对手风险。瑞波币是 **ripple** 系统内置的货币，在系统内可以全流通而不需要信任链。

不能超发。Ripple 网络创建时，1000 亿瑞波币即创建好了，创始人保留了一部分，其余 800 亿瑞波币被授权给 ripple labs 公司用来发展 ripple 系统。



货币只有流通和使用才有价值，故 Ripple Labs 会通过慈善，赠送等有意义的渠道分发瑞波币。

### 最小单位一滴

瑞波币的最小单位是滴，一个瑞波币等于一百万滴瑞波币。现在系统会对每次交易收取 10 滴瑞波币作为交易费用，这 10 滴瑞波币会被摧毁掉。一个瑞波币就够一个账户做 10 万个交易了，所以这个设置看上去不错。如果瑞波币升值了，也可以通过共识过程降低交易费用。

# 理解 ripple

多币种，快结算，好方便，省费用。“多快好省”的支付解决方案。  
-- 瑞波指南

## 简介

ripple 是一个应用于金融事务的互联网协议。它维护了一个公共帐簿，包含所有参与者的账户信息，从而相隔多远交易都成为可能。原本需要数天才能完成的支付和清算，现在只需几秒就可以了，更快捷。它也让跨币种支付变的异常简单。  
![A101](https://ripple.com/wiki/images/f/fc/A101.png)

上图是 ripple 系统的简单示意图。最上面的 RTXP 即 ripple 协议，它运行在整个瑞波网络上，也就是全世界的瑞波 p2p 节点，所有的节点通过该协议从总帐上获得信息，写入信息。

第二层代表 ripple 的总帐簿，可以把它理解为一个分布式的数据系统，存储着所有的账户和交易信息。它的存在使得大家可以像平常银行里查询转帐付款一样，进行各种操作。

第三层为和用户紧密相关的一些概念。

- 地址。每个用户都有一个 ripple 地址，系统要求所有和该地址相关的操作，都需要用该用户的私钥加密。
- 信任链。每个用户可以信任另一个用户，这样另一用户就可以和你共享你的货币。
- 兑换申请。每个用户可以向 ripple 系统提交申请，将一种货币的资金换成另一种。

在线总账可以说是 ripple 的核心，让我们来看看用户是如何和它交互的。

## 理解瑞波账簿

账簿本身由三个组件组成，即上图的地址，信任连，兑换申请。看上去很简单，它们具体都有什么作用呢？

地址。地址是账簿最基本的组件，它唯一的标致了你在 ripple 系统中的身份。每个 ripple 账户都有一个唯一的地址，其中保存了账户什么币种有多少结余等信息。这有两个意思。一是别人可以通过该地址给你付款。二是由于瑞波账本是共享的，所以别人也能查询到该地址的一些信息，包括余额。

![A102](https://ripple.com/wiki/images/d/d4/A102.png)



### 小思考

余额等算隐私吗？公开的话是利大于弊还是弊大于利？至少中国大陆民众官员财产公开的呼声挺高的，而这在 ripple 中根本不是问题，只需知道他的地址即可。

信任链。信任链是瑞波中用来管理两个账户之间结余的机制。信任链可以连接任意两个地址，也可以随时建立和取消。信任方 **alice** 建立一条信任链到受信任方 **bob**，意味着 **alice** 允许 **bob** 替她保管她的钱。建立信任链时，还需要指定币种和数量，意味着 **bob** 只能为 **alice** 保管特定的币种，且数量不超过设定的上限。



为方便起见，信任双方的结余记录在受信任的一方。这是因为信任链表示的是 **alice** 的账户中 **bob** 保管的部分是多少。每个账户可以有多条信任链，ripple 客户端自动计算每个账户的资产净值。在下图中，**bob** 欠 **alice** 125 元而 **alice** 欠 **charlie** 50 元，所以 **alice** 的资产净值是 75 元。





交换申请。瑞波中第三个重要概念是交易申请。只要账户中有余额就可以发起交换申请，从而将手中资产从一种货币兑换成另一种。申请时需要设置您期望的汇率。在下图中，alice 发起申请希望将手中的美元换成欧元。



事务。瑞波系统自动调节信任链的结余，有三种方式。下图中我们用红色圆圈表示事务发生前的结余，红色箭头表示事务发生后的结余。- 被信任方从信任方借入一定资金。通过这种方式，bob 声称他欠有alice 一笔资金。



- 信任方从被信任方赎回被借走资金。通过这种方式，alice 声称 bob 不再欠有她资金。



- 结余可以在信任同一个网关的不同账户之间转移。通过这种方式，alice 声称 bob 不再欠她钱而是欠 charlie 等量的钱。



不同币种间的交换申请可以由第三方撮合，用两个同步的事务。**alice** 的 200 美元转出给第三方，同时第三方转让 150 欧元给她。



这些最基本的概念支撑起了整个瑞波帐簿：地址，交易链，交易申请和事务。通过合理使用这些基本组件，用户可以在瑞波中很简单的完成他们的支付任务。

## 理解瑞波生态系统

瑞波生态系统由四种角色组成，客户，商业机构，网关和做市商。任意的瑞波用户都可以作为任意角色使用，不需要特殊的地址或权限。判断某个用户扮演的是什么角色，主要看它和其他地址是什么关系，交易时起什么作用。下面我们依次讨论每个角色在瑞波系统中分别起什么作用。

用户。**alice**，以及其他用户，使用瑞波并信任一个本地网关。如下图绿色所示。大多数用户只有一条对本地网关的信任链用来交易他们的本地货币。

商人。**bob**，以及其他商人，也使用并信任一个本地网关。如下图蓝色所示。和他们的客户一样，大多数商人也只有一条对本地网关的信任链用来接收本地货币。

网关。网关作为一个中间机构，被交易双方信任，所以可以代为保管双方的资金，这让快速的支付成为可能，即使交易双方不见面。由于用户和商人信任网关而网关可以不信任任何人，网关就成了一个知名的枢纽和交易中心。每一个集群代表了一个本地的商业社区。



这样的社区遍布世界，每一个都以各自的本地网关为中心，形成一个以本地货币为交易媒介的商业社区。



做市商。瑞波做市商连接这些分散各地的商业社区使它们成为一个整体。做市商信任多个网关，从一个网关中买余额然后在另一个网关中卖出。做市商的出现，建立了一条通路，让 `alice` 可以使用瑞波网络从任意的商人那购买商品而不需关心商人信任的是哪个网关，使用的是哪种货币。



一旦找到一条买家和卖家间的通路，瑞波会自动调节信任链两方的余额。如下图所示，`mark` 接收 `alice` 的美金，同时支付给 `bernard` 欧元，`mark` 和 `bernard` 均可以从各自的网关处取现，`alice` 的钱成功支付给了 `bernard`。



## 商业集成

在现代商业社会，商人们已经通过不同支付网络的接收支付，著名的支付网络包括 ACH，SWIFT 或者卡系统。瑞波提供了简单的 JSON 接口让使用者可以方便的将他们现有业务接入到瑞波系统。通过接入瑞波系统，您可以监控自己的瑞波地址，所有的收入和支付都一目了然。



商人。商人可以创建自己的瑞波帐号然后信任一个本地网关。利用瑞波接口商人 bob 可以实时的结算 alice 的购物清单。



商人支付流程。对于服务于商人们的支付处理商来说，它们可以使用一个瑞波账户处理来自瑞波网络的支付就可以了。商人们不需要做任何流程上的变化。



客户支付流程。对于服务于最终客户的商家而言，无论其是否提供了消费卡或会员体系，均可使用瑞波简化他们客户的支付行为。如果使用瑞波联合协议，托管的客户能像发电子邮件一样完成支付，甚至不需要其是基于瑞波系统完成支付。



## 瑞波关系网

瑞波系统中的交易双方总是互相信任且愿意做交易的，通过信任链及信任链的传递将大家连在一起使得关系网任意两人间的支付都成为可能。

客户。大多数瑞波用户只和本地网关打交道。这一条信任链就足以让他们能和瑞波中的任意用户做交易，在他们看来，网关处理了所有的支付细节。



商人。同样，瑞波中的商人也只需和本地网关打交道。他们只需要订好商品价格并接受本地网关支持的货币付款即可。借助瑞波网络，商品可以销往全世界。



网关。网关处理的事务总是本地的，所有的交易都发生在信任它的客户之间，这就让网关知道它所有的用户。同样，这也方便监控瑞波网络上的一些交易使得交易满足本地法律的要求。



做市商。做市商和不同的网关做交易从而提供额外的流动性。如果需要不同币种间的结算，他们需要满足本地法律要求。做市商信任多个网关，通常也意味着这些网关都是值得信任的，这就保证了每一个支付都由值得信任的客户组成。



## 多重交易

由于使用共享的总帐，即使 4 个角色同时参与交易，瑞波系统也能保证交易的原子性。每一个交易者只需知道和相信它的直接交易对手，但通过信任链您可以和世界上的任意瑞波用户交易。



# 使用 ripple

给我一个支点我能撬动地球。

-- 阿基米德

## 用户使用场景

让我们看看到底如何使用 ripple 系统。假设 alice 想网上付款给 bob。![[A202]](<https://ripple.com/wiki/images/b/be/A202.png>)

alice 只有现金，bob 需要的也是现金，但是他俩隔了很远，甚至可能在不同的国家用着不同的货币。alice 打算借助 ripple 的本地网关完成转帐。![[A203]](<https://ripple.com/wiki/images/9/9e/A203.png>)

- 她建立一条到网关的信任链，从而可以借助该网关完成转账。
- 她“存款”100 美元到网关。
- 相应的，网关通过信任链发送 100 美元给 alice 的账户。

同时，bob 也信任了一个他所在地的网关。要让转账顺利进行，首先瑞波系统需要找到一条从 alice 到 bob 的信任链通路。这条通路可能由一个或多个瑞波机构组成，但 alice 和 bob 不需要知道，也不需要操心。然

后，当 alice 转账给 bob 时，瑞波处理所有的细节，调节参与者的账户余额，完成交易。

- alice 的转账的资金被转移到某个参与者的账户。
- 某个参与者将 alice 那边的转过来的钱再转给 bob。

这一波接一波传递的转账过程有点像水波运动，这也是瑞波（ripple）系统名字的由来。由于各个参与者的转账过程是同时进行的，瑞波系统不会像现有金融系统那样有多余的延迟和负载。现在，bob 可以保留 alice 转给他的那 100 美元，用它和别人做交易，或者将他从本地网关中取出来。

### 和银行的不同

粗略一看瑞波和现在银行系统很相似，但是 ripple 系统的业务范围远远超过了传统银行。

假设 alice 每个星期给每个小孩 20 美元零花钱。alice 可以为她小孩开通瑞波账户，并且都建立到她自己账户的信任链。这样 alice 就可以给小孩零花钱，alice 就像一个孩子们的网关。

![A301](https://ripple.com/wiki/images/a/ab/A301.png)

每个星期 alice 发给每个小孩 20 美元花。由于没人和网关做交易，所以 alice 和网关间的信任链余额没有任何变化。但由于 alice 给了 20 美元给每个小孩，所以她自己账户净值只有 40 美元来了。



小孩之间可以方便的赠送零花钱。比如 carol 可以把自己的一些零花钱给 dave。

小孩们也可以自由的在瑞波系统里面消费，不需要他们母亲的介入，就像手握现金一样。它们不需要信任任何网关或第三方，只需要信任他们的妈妈，就可以在妈妈设置的限额内自由消费了。

![A306](https://ripple.com/wiki/images/a/a7/A306.png)

通过以 alice 的帐号作为中介，孩子们方便的在外部 ripple 系统消费。

### 家庭内的借贷

如果 alice 的某个小孩，比如 edward 想买一些稍微贵点的东西，超出了他账户余额，怎么办呢？alice 可以建立一条道 edward 的信任链，这样 edward 就可以从 alice 那里额外借用一定数量的钱，就像信用卡一样。

![A305](https://ripple.com/wiki/images/2/2a/A305.png)

当 edward 支付那件贵重物品时，瑞波会从 edward 账户划走 30 美元支付给 bob（其中 10 美元是 edward 向 alice 借的），这样 edward 账户净资产为负 10 美元，alice 净资产仍为 40 美元（其中 10 美元借给 edward 了）。

![A304](https://ripple.com/wiki/images/6/66/A304.png)

### 账户可移动性

瑞波一个强大之处在于 alice 可以自由切换网关而她现有的 ripple 信任链不受影响。她公开的瑞波地址还

是一样，所以对别人没有影响，就是只要手机号码不变无论你切换到哪个电话公司别人都可以通过这个电话号码找到你一样。alice 的家人甚至都不需要知道 alice 的网关地址变过了。

## 多币种

如果 alice 要出远门，她可以信任访问地网关的本地货币。这样她的 ripple 账户可以持有多种货币，就像物理钱包一样。出门之前，alice 可以讲她的持有货币美元转换成欧元，她只需选定合适的汇率，在瑞波系统里卖出美元即可。当然她也可以选择市场中已有的欧元卖单，用美元买入即可。这两种方式，瑞波都会自动找到交易对象，alice 甚至连个电话都不需要打。

![A313](https://ripple.com/wiki/images/2/25/A313.png)

但是即使没有外币，alice 和她的孩子们仍然能支付欧元。瑞币自动取得最佳汇率然后告诉 alice 她将支付多少美元。

## 瑞波钱包

迫不及待想使用瑞波系统？很简单，你只需要注册一个瑞波钱包，激活你的瑞波钱包，最后信任一个网关开始交易。这一切都需要借助瑞波网页版钱包，让我们来看看如何使用吧。



瑞波仍然是一个快速发展的系统，现阶段仅网页版钱包，桌面版钱包和手机版钱包尚在紧张开发中。详情请关注 [ripple](https://ripple.com) 官方网站。

瑞波支付网络让人们在网上快速付款和收款成为可能。此外，瑞波有内置的市场允许用户以最佳汇率兑换货币。瑞波网络是一种点到点的网络，由瑞波公司创建和开发。

网页版钱包是当前唯一可用的钱包，它是一个 javascript 程序语言编写网页应用程序，以后也可能会打包成浏览器插件。你可以访问[网页版钱包<sup>5</sup>](https://ripple.com/client)，然后就可以使用钱包的各种功能了。

---

<sup>5</sup><https://ripple.com/client>