1项目简介

瑞波（Ripple）是世界上第一个开放的支付网络，通过这个支付网络可以转账任意一种货币，包括美元、欧元、人民币、日元或者比特币，简便易行快捷，交易确认在几秒以内完成，交易费用几乎是零，没有所谓的跨行异地以及跨国支付费用。 Ripple是开放源码的点到点支付网络，它可以使你轻松、廉价并安全的把你的金钱转账到互联网上的任何一个人，无论他在世界的哪个地方。因为Ripple是p2p软件，没有任何个人、公司，或政府操控，任何人可以创建一个Ripple账户。

瑞波币是Ripple网络的基础货币，它可以在整个Ripple网络中流通，瑞波币的运营公司为ripple labs（其前身为opencoin）。瑞波币是Ripple系统中唯一的通用货币，其不同于Ripple系统中的其他货币，瑞波币在Ripple系统内是通用的。

2工作原理

以网关或瑞波币XRP为桥梁，用户甲将任意类别的货币或虚拟货币兑换为瑞波币XRP，然后发送给其它任何地区的用户乙，用户乙可将收到的资金兑换成自己需要的任意货币币种；

还有另一种模式，用户甲将资金存放在乙信任的网关，经过网关转给乙。

瑞波(Ripple)系统还允许用户在本系统内发行“私人货币”。假如某个瑞波(Ripple)用户甲信誉很好，甲就可以拿自己发行的“私人货币”与信任他用户乙兑换成美元或比特币等其它币种；用户乙可根据需要赎回兑换给甲的货币。这实际上是个借贷过程，用户甲具有了向其他人借贷的融资权力。

瑞波(Ripple)协议维护着一个全网络公共的分布式总账本。该协议有“共识机制”与“验证机制”，通过这两个机制将交易记录及时添加进入总账本中。瑞波(Ripple)系统每几秒钟会生成一个新的分账实例，在这几秒钟的时间内产生的新交易记录，根据共识和验证机制迅速被验证。这样的一个个分账按照时间顺序排列并链接起来就构成了瑞波系统的总账本。瑞波的“共识机制”让系统中所有节点在几秒钟内，自动接收对总账本交易记录的更新，这个过程不需要经过中央数据处理中心。

3应用场景

1、现实与虚拟货币的双向流通；

2、多币种的P2P兑换与支付；

3、P2P网络信贷；

4、个人网络清算。

4瑞波共识算法

瑞波协议共识算法（RPCA）每隔几秒钟由所有节点应用，以保持网络的正确性和一致性。 一旦达成共识，当前分类账被视为“封闭”，并成为最后封闭的分类帐。

4.1RPCA轮流定义

最初，每个服务器在合意轮开始之前已经看到所有尚未应用的有效事务，并以被称为“候选集合”的列表的形式公布它们；

然后，每台服务器合并UNL（唯一节点列表）上所有服务器的候选集，并对所有事务的真实性进行投票；

如果收到超过最低百分比的“1”票的交易被传递到下一轮（如果有的话），而没有获得足够票数的交易将被丢弃或被包括在候选组中以用于下一个分类账的共识流程；

最后一轮共识要求服务器UNL的80%的最低百分比同意交易。

4.2如何保证正确性

1、保证拜占庭故障的数量f≥（n-1）/5，确认错误交易需要满足（4n+1）/5；

2、下图概率表示恶意卡特尔的大小将保持在拜占庭失败的最大阈值以下的可能性；

例如，考虑A有$ 100的情况，并将其全部发送给B。如果应用程序首先提交该支付交易，则在检查A的余额后立即返回$ 0。该值基于候选交易的暂定结果。有些情况下，付款失败，A的余额仍为100美元（或者由于其他交易，成为其他金额）。确切知道A向B支付成功的唯一方法是检查事务的状态，直到它处于验证账本中且结果代码为
tesSUCCESS。如果交易与任何其他结果代码一起处于验证账本中，则付款失败。

5瑞波币的运行模式

瑞波币的起始数量为1000亿，并且不会再增加，这一点也与比特币类似。但二者存在本质上的区别，即瑞波币不会像比特币那样可以“挖矿”。Ripple的创始人之一曾经就职于比特币交易平台，他对用来生成比特币的挖矿程序颇有微辞，因此就在设计Ripple系统时舍弃了它。Ripple
Labs拥有资金的25%，全部在了Ripple系统的运作上。

Ripple客户端不需要下载区块链，它在普通节点上舍弃掉已经验证过的总帐本链，只保留最近的已验证总帐本和一个指向历史总帐本的链接，因而同步和下载总帐本的工作量很小。

5.1发币方式

1、对社区用户的免费赠送

2、WCG挖矿（目前已经停止）

3、大户批发

4、对内部员工以工资形式发放

5、对合作机构的免费赠送

5.2转账方式

发送者在带有签名的消息中指定一个支付地址。每个交易都有一个哈希，从而通过它去那些具有足够多总账历史的节点查阅交易。总账有足够多的信息核实交易符合支付条款。Ripple的交易费用非常的低，每次交易只有1/1000美分的交易费（交易费不发给任何人仅会凭空消失）。这个交易费是用来防止有人通过大量的交易破坏系统的行为，一般正常交易时间在3s-5s左右。

5.3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。