上海大学“区块链”课程论文考试

XRP 项目分析

姓名：李睿欣　　学号：21726043

字　数：6412 字

摘　要：本文介绍了 Ripple 项目产生的经历，共识机制的作用机理，账户设置，代币机制等信息。并根据 XRP 白皮书中提到的三大问题，从 Ripple 的技术层面回答了这三大问题的解决情况。对比分析了 ripple 与其离职高管单干的 Stellar 项目的代码更新及社区运营情况，均优于对家。最后结合 SEC 状告 Ripple 的背景，本文认为 Ripple 是一家值得投资的公司，但就现阶段而言，XRP 并不是一个值得投资的项目；然而，倘若 Ripple 可以使得 XRP 具备真正的应用价值，则 XRP 项目也将具有投资价值，且未来潜力很大。

关键字：Ripple、XRP、RPCA.

论文评语：

成绩：　　任课教师：吴建刚

1 经济模型分析

1.1 项目产生历程

XRP 是由 Ripple Labs 瑞波实验室创造的一种数字资产，用于表示 Ripple 网络上的价值转移。Ripple 旨在连接银行、付款提供商以及数字资产交易所，提供一个实时高效的全球汇款解决方案。

瑞波公司是由 Ryan Fugger 于 2004 年创立，创立初衷是替代银行结算系统，建立一个去中心化的点对点支付系统，每个人成为自己的银行。

从那时至今，外汇支付体系依然还是 SWIFT 体系（国际资金清算系统），外汇交易中间依赖大量的中间方，整体效率非常低下、通常需要 3-5 天的到账时间；费用又比较高昂，一般要 20-70 美元的费用。

Fugger 当初也是是看到了跨境转账服务中存在的痛点，才开始了对跨境转账点对点交易体系的创建。早期的系统是只在相互信任的熟人间进行转账，囿于熟人关系，瑞波网络初期只是小众的支付平台，迟迟没有取得进一步发展。

直到 2011 年，Jed McCaleb 和 Chris Larsen[1]两位区块链领域的大神一起加入瑞波社区。他俩改变策略，系统节点从个人转向银行机构，以银行为客户，并将区块链概念引入 Ripple。

2012 年两人从 Ryan Fugger 手里接过 Ripple 社区控制权，并发行 XRP。他们认为，需要有一种受信任的、可流转的加密数字货币作为法币间的桥梁，以解决流动性问题。Ripple 项目也就是从这里开始被发扬光大。

1.2 项目想要实现什么

Ripple 项目的初衷就是要建立一个分布式的 P2P 清算网络：每个人都是自己的银行，可以签发、接受借贷，同时又可以作为借贷通道。该项目最初几乎是依靠 Ryan Fugger 一个人的力量支撑下来，并获得了一定范围内的成功。

但 Ripple 的用户一直不多，仅流行于若干个孤立的小圈子，原因很简单：Ripple 的设计思路基于熟人关系和信任链，一个人要使用 Ripple 网络进行汇款或借贷，前提是在网络中已经存在他的朋友，否则无法在该用户与其它用户之间建立信任链。

[1]♦杰德•迈克卡勒伯（Jed McCaleb）则是全球最大的比特币交易平台 Mt.Gox 同时也是著名 P2P 网络 eDonkey——电驴的开发者
♦克里斯•拉森（Chris Larsen）在网络金融领域已经摸爬滚打十多年，是著名互联网银行 E-Loan 和 P2P 信贷公司 Prosper 的创始人。

1.3 为什么需要分布式记账

上文提到过，Ripple 项目的创立初衷是创始人希望可以取代银行，使得个体之间可以点对点的实现转账，清算等业务，提高效率，降低中间费用。最初，这个项目是通过信任链来实现的，这使得他们的项目一直囿于熟人关系，影响范围有限。

后来 Jed McCaleb 和 Chris Larsen 将区块链的技术带入到这个项目中，区块链的去中心化思维完美契合了这个项目的初衷，同时依靠计算机来进行数据处理，免除了原有信任链的认识沟通所花费的时间成本，弥补了熟人网络的缺陷，使得该项目走向了成功。

1.4 代币机制

瑞波币的发行总数是固定的，初始设定为 1000 亿个。目前可精确到 6 位小数，最小的单位称为一滴（drop），1,000,000 滴等于 1XRP。

初始供应量的 1000 亿枚中，创始人保留 20%，Ripple 公司拥有 80%。XRP 未进行公开发售，经过空投和减持后，Ripple 公司仍然持有 60%左右的 XRP，分布非常集中。初始阶段创始团队保留 20%的行为在当时就引发了极大的争议，创始团队被批评获得了太多利益。经过长期的演化，现阶段已有 48%的 XRP 通过各种形式进入了流通，而 Ripple 公司直接或间接控制了余下的 52%。为了缓解市场关于项目方持有比例过高而造成中心化问题的担心，Ripple 公司将持有的大部分 XRP 转入了三方托管账户，每个月最多向市场出售 10 亿枚。

图 1 关于 XRP 的流通情况的图

图片来源：CoinMarketCap

由于 Ripple 协议的开源性，恶意攻击者可以制造大量的“垃圾账目”，导致网络瘫痪，为了避免这种情况，Ripple Labs 要求每个 Ripple 账户都至少有 20 个瑞波币，每进行一次交易，就会销毁十万分之一个瑞波币。这一费用对于正常交易者来说，成本几乎可以忽略不计，但对于恶意攻击、制造海量的虚假账户和交易信息者，所销毁的瑞波币会呈几何数级增长，成本将是巨大的。

另外，瑞波币与其他虚拟货币最大的不同就是它不能进行挖矿，除了一些特殊情况

被赠送的，一般都只能通过购买获得。

2 技术模型分析

2.1 共识机制

xRapid 是瑞波公司提供的一项跨境转账支付方案。在金融机构进行跨境支付时，只要使用 Ripple Net 的 XRP 资产作为货币交换的桥梁，便可在几乎不划手续费的情况下，于 4 秒内完成转账。而瑞波币能够实现这种便捷高效的全球回款方案，则依赖于 Ripple 共识算法（Ripple Protocol Consensus Algorithm，简称 RPCA）。

RPCA 算法中，通过子网络内部互相信任，由这些内部信任的子网络构成大的网络的方案来解决拜占庭将军问题。

Ripple 账户及 XRP 交易的所有信息都存储在一个分布式记账的账本中，即：XRP Ledger。

瑞波币账本是由诸多独立的验证节点来进行网络化管理，这些节点持续地对比各自的交易记录。

在具体说明共识过程之前，我们先来学习几个瑞波网络里的专有名词：

服务节点，就是可以接收交易的区块链节点，包括验证节点与非验证节点两种，验证节点是指被其它节点加入到信任列表中的节点，可参与共识过程，非验证节点不参与共识过程。

区块，区块记录交易，在 RPCA 中有两种区块比较关键，一个是最新关闭的区块，也就是最新被共识过的区块，另一个是开放区块，开放区块是指当前正被共识的区块，当开放区块被共识过，也就成了新的最新关闭的区块。

UNL（Unique Node List）信任节点列表，每个服务节点都会维护一个信任节点列表，这里的信任并不是我们通常理解的信任[2]，而是指我信任这个列表中的节点不会联合起来作弊。在共识过程中，我们只接受来自信任节点列表中节点的投票。在 Ripple 中，我们用在配置文件中加入其它验证节点的公钥的方式来指定 UNL。本文以为 UNL 这种与传统区块链项目截然不同共识方式的出现，正是受到了 Ripple 项目初期，熟人网络的影响，这与其早期发展经历密切相关，是难以复制的模式。

Ripple 网络每隔几秒就会产生一个新的区块，这个区块的产生过程就是所有网络节点共识的过程。假设共识过程是成功的，并且网络中没有分叉产生，那么新生成的区块就是全网唯一的。

[2] UNL 的信任与其原有的信任链中的信任天差地别，UNL 中的信任是彼此越陌生才越可信，而原有信任链中的信任则是彼此越熟悉才越可信，这两种信任分别蕴含着人本性恶与人本性善的底层思维。

RPCA 对交易分两个阶段完成，第一阶段是达成交易集的共识，第二阶段是对新生成的区块进行提议，最终形成被共识过的区块。

达成交易集的共识分轮进行，在每一轮中进行下面的操作：

第一步，交易共识，形成交易集。

1．每个节点在共识开始时尽可能多的收集所能收集到的需要共识的交易，并放到“候选集”里面；

2．每个节点对它信任节点列表中的“候选集”做一个并集，并对每一个交易进行投票；

3．UNL 中的服务节点交流交易的投票结果，达到一定投票比例的交易会进入到下一轮，达不到比例的交易要么被丢弃，要么进入到下一次共识过程的候选集中；

在最终轮中，所有投票超过 80%的交易会被放到共识过的交易集中，这里的交易集与比特币类似，也是 Merkle 树的数据结构。

第二步，区块打包，再共识。

形成交易集后，每个节点开始打包新的区块，打包区块的过程如下：

把当前区块号、共识交易集的 Merkle 树根 Hash、父区块 Hash、当前时间戳等内容放到一起，计算一个区块哈希

每个节点广播自己得出的区块哈希到它可见的节点，这里的可见节点不仅仅指可信列表中的节点，而是通过节点发现过程能发现的节点

节点收集到它所有可信列表中节点广播过来的区块哈希后，结合自己生成的区块哈希，对每个区块哈希计算一个比例，如果某一哈希的比例超过一个阈值（一般是 80%），则认识这个哈希是共识通过的区块哈希。如果自己的哈希与之相同，则说明自己打包的区块得到了确认，是新的被共识过的区块，直接存到本地，并且更新状态。如果自己的哈希与共识通过的哈希不同，那就需要去某个区块哈希正确的节点索要新的区块信息，要到之后存储到本地并且更新当前状态。

如果上面没有对某一区块哈希超过设定的 80%阈值，那么重新开始共识过程，直到满足条件。

至此，一个区块的共识过程结束，开启下一轮共识过程。

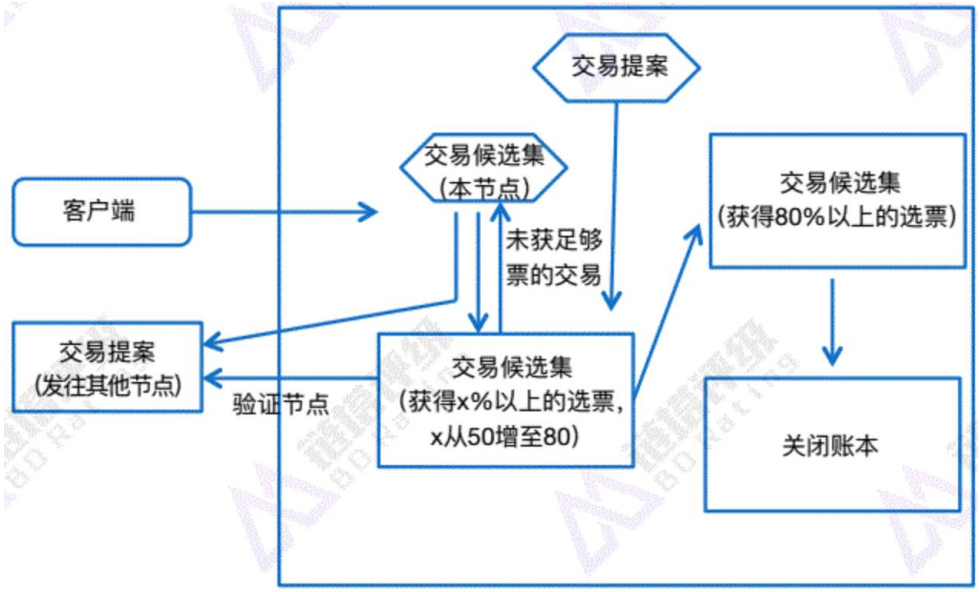


图 2　关于 RPCA 的运作机理的图

图片来源：链塔数据平台

2.2　账户机制

XRP Ledger 中的“账户”代表 XRP 的持有者和交易的发送者。账户的核心要素是：

1.标识地址，例如 rf1BiGeXwwQoi8Z2ueFYTEXSwuJYfV2Jpn

2.XRP 余额。其中一些 XRP 被预留给储备金。

3.一个序列号，有助于确保此账户发送的任何交易都按正确的顺序应用，并且每个交易只能应用一次。要执行事务，事务的序列号与其发送方的序列号必须匹配。然后，作为应用交易记录的一部分，账户的序列号将增加 1.

4.影响此账户及其余额的交易历史记录。

5.一种或多种授权交易的方式，可能包括：账户固有的主密钥对，这可以禁用，但不能更改；可以轮换的“常规”密钥对；用于多重签名的签名者列表，与账户的核心数据分开存储。

创建账户没有专用于“创建账户”的交易。如果付款将 XRP 等于或大于账户预留发送到尚无账户的数学上有效的地址，则付款事务会自动创建新账户，这称为为账户注资，并在账本中创建一个 Account Root。

目前 XRP Ledger 可以删除账户，但必须满足一些要求，例如，删除账户需要付出 2XRP 的交易成本。删除账户后，可以通过正常的账户创建方法在账目中重新创建账目。已删除并重新创建的账户与首次创建的账户没有什么不同。

2.3 三大核心问题

从 XRP 的白皮书中，我们可知，分布式记账技术想要组建一种高性能、低费用，同时去中心化的交易平台，就要解决三大核心问题：正确性、一致性以及可用性问题。

正确性，指的是分布式系统要能识别正常交易与欺诈交易。

RPCA 中正确性的验证方式很简单，因为共识需要 80%的阈值，那么只要 UNL 中有 80%的诚实节点，就能达成共识，另外即使有超过 20%的欺诈节点，也不能破坏正确性，因为欺诈节点也必须达到 80%以上才能达成共识。无论欺诈节点还是诚实节点，达不到 80%，都无法通过共识。

一致性，指的是要在去中心化系统中保证能达成全局唯一的共识。

RPCA 中一致性是通过子网络与其它子网络的连通性来保证的，要保证区块链不分叉，必须确保每个子网络必须至少与整个网络节点中的 20%保持连通性。达到 20%连通性的前提下，如果一个子网络中得出的共识区块哈希与整个网络得出的不一致，也就无法达成 80%的共识要求，也就无法产生分叉。

可用性，指的是去中心化的分布式记账系统的性能问题，具体表现为平衡以上两个需求后所需的算力水平及防欺诈的算力复杂程度。

在每一轮投票过程中，节点会搜集它 UNL 中每个节点的响应时间，一直响应时间慢的节点将会被剔除出去，这样 UNL 就能保持一个较高的沟通效率。在高效沟通的前提下，RPCA 算法能保证每 3 秒左右就能产生一个区块，Ripple 官方给出的 TPS 数据是 1500。这样的性能基本能满足一般的生产需求。

2.4 现有技术文档及代码评价

以子网络共识取代全体共识，降低了同步沟通成本，提高了共识效率。在 RPCA 协议下，内部互相信任的子网络形成的共识取代了全网共识，而组成这些网络的验证节点往往具有较好的资质和硬件性能，能够在保证共识具有一定程度可靠性的基础上提高分布式网络的效率，适合 Ripple 网络跨境支付服务提供商的定位。目前，Ripple 的 TPS 可以达到 1500 以上，但实际发生的 TPS 要远低于这个数字，交易确认时间在 3.8 秒左右。

要求节点间有较高的连接度和 UNL 一致性。Ripple 网络的性能取决于形成共识的子网络的性能，也就是说，对验证节点之间的连接效率有较高要求。同时，RPCA 是一种验证节点间相互信任的网络，子网络信任度越高，主网速度越快。组成子网络的验证节点的信任度体现为节点 UNL 的一致性，一致性越高，共识速度越快。Ripple 如果想进一步提高效率，就需要在这两个方面继续改进。

Ripple 的代码更新频率和开发者社区关注度在业内属于头部水平，领先于竞争对手 Stellar[3]。Ripple 的 Github 有 rippled 和 ripple-lib 两个项目，共 3894 个 Star、1253 个 Fork、128 位 Contributors（可能有重叠），以及 14752 个 Commits。Ripple 的主要竞争对手 Stellar 有 6 个项目，我们选取其中主要的 core 和 go，统计出下表中的数据。可以看出，Ripple 在这方面对 Stellar 有一定优势，但二者基本处于同一档次，均为行业头部水平。

表 1　关于 Ripple 与 Stellar 代码更新对比的表

项目	Ripple	Stellar
Star	3894	2398
Fork	1253	823
Contributors	128	109
Commits	14752	5519

数据来源：Github，通证研究院

3　项目未来

3.1　现有社区评价

Ripple 拥有数量庞大且行业分布广泛的合作伙伴。Ripple 的合作伙伴包括银行、支付服务提供商和交易所等，官网披露数目在 200 家以上。Ripple 的合作伙伴不仅数量较多，而且质量在区块链行业也拥有很大优势，其中很多是传统金融机构，包括世界第二大汇款公司 MoneyGram。同时，Ripple 的合作伙伴可以得到验证，信息比较可靠。

图 3　关于 Ripple 的部分合作伙伴的图

图片来源：Ripple 官网

Ripple 的社区热度相对较高，群众基础广泛。2019 年 Ripple 的 Facebook 主页有 130626 个赞、141920 个关注；Twitter 账户有 91.2 万关注、4571 个喜欢；Reddit 有 197k 关注。整体来看，Ripple 在社交媒体的关注度处于行业头部，并显著高于竞争对手 Stellar。

[3]Stellar 由 Ripple 的离职高管 Jed McCaleb 创立，代码和商业模式都与 Ripple 比较相似，二者存在直接竞争关系。Stellar 起步较晚，各方面资源支持也不如 Ripple，所以在合作伙伴和规模上存在一定劣势。

表 2　关于 Ripple 与 Stellar 关注度对比

社交媒体关注数	Ripple	Stellar
Facebook	141920	22487
Twitter	91.2 万	21.6 万
Reddit	197K	98.8K

数据来源：通证研究院

3.2　未来规划

2020 年 12 月 23 日，SEC（美国证券交易委员会）发推特表示，已以“进行了 13 亿美元（瑞波公司发行的 XRP）的未经注册的证券出售”罪名起诉 Ripple 公司及其两名高管。而 ripple 公司则强烈抗击这 SEC 的提出的罪名，认为这是美国证券交易所对于加密行业的一次打压。两者的交锋之处在于“XRP 是否为证券”。

尽管 Ripple 公司以种种理由对其进行了抗辩，该公司首席执行官 Brad Garlinghouse 公开说明：“SEC 在事实和法律认定上均发生了错误，瑞波币是一种货币而非证券，原因在于：第一，瑞波币不是投资合同。瑞波币的投资者们不参与公司分红也未获得投票或其他公司权利。代币购买者不会从瑞波币中获得任何收益，持有者与公司没有任何关系；第二，瑞波公司有自己的股东，如果欲投资公司，投资者需购买公司股份而不是瑞波币；第三，不同于证券，瑞波币的市值与瑞波公司毫无关系，相反，币值波动与其他虚拟货币相关。”

但正如邓建鹏（2022 年）学者分析的那样，瑞波公司的抗辩理由大多都难以立足。使得 Ripple 公司陷入如此被动的境地，核心问题还是它的“去中心化问题”，而从它的共识机制与代币机制上，瑞波公司并没有做到“充分去中心化”。

目前，已有多家交易所主动下架 XRP，瑞波公司正在试图与 SEC 取得和解。

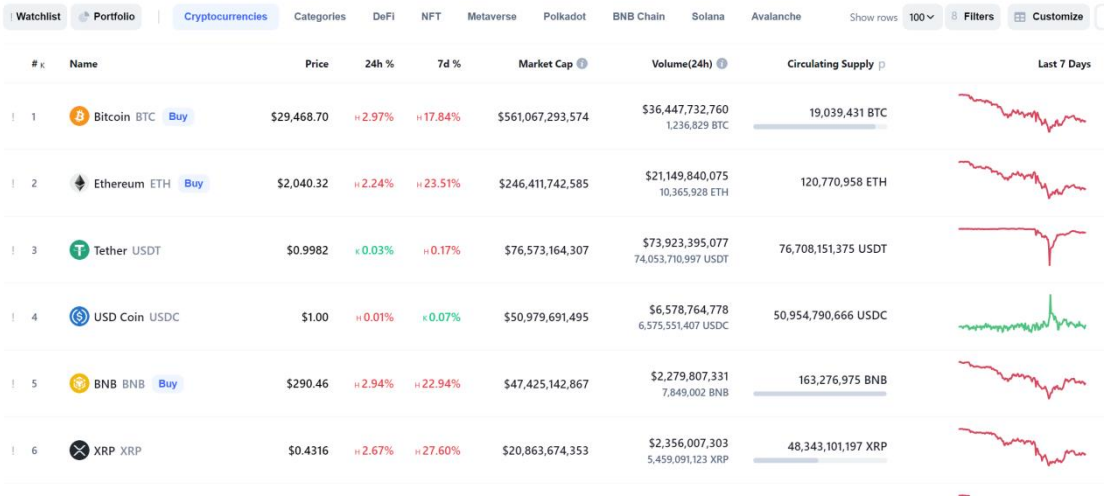
对于 Ripple 公司的未来，XRP 的现状不容乐观，而公司也正在向新的方向发展。

在 Ripple 官网上，可以看到：中央银行数字货币（CBDC）无疑将在区块链技术支撑新型现代全球金融基础设施中发挥关键作用。Ripple 正在为 XRP 积极寻找落地应用场景，并且很可能是协助各国央行发行数字货币。而且 Ripple 目前也确实正在聘请“央行技术合伙人经理”这一职务，计划在旧金山、纽约和伦敦的每个办事处各一名。而担任新职位的人员将负责设计和部署央行数字货币（CBDC）项目。

Ripple 公司表示，各国央行可以在 XRP 的区块链网络上发行稳定币。这说明 Ripple 迫切希望将 XRP Ledger 引入其合作伙伴——各国的中央银行，并且不会因正在进行的诉讼而脱轨。如果项目落到实地，XRP 也将具有实际的应用价值，而不再像之前那样脱

离公司主业。

3.3 项目投资分析



#	Name	Price	24h %	7d %	Market Cap	Volume(24h)	Circulating Supply	Last 7 Days
1	Bitcoin BTC Buy	$29,468.70	2.97%	17.84%	$561,067,293,574	$36,447,732,760 1,236,829 BTC	19,039,431 BTC	
2	Ethereum ETH Buy	$2,040.32	2.24%	23.51%	$246,411,742,585	$21,149,840,075 10,365,928 ETH	120,770,958 ETH	
3	Tether USDT	$0.9982	0.03%	0.17%	$76,573,164,307	$73,923,395,077 74,053,710,997 USDT	76,708,151,375 USDT	
4	USD Coin USDC	$1.00	0.01%	0.07%	$50,979,691,495	$6,578,764,778 6,575,551,407 USDC	50,954,790,666 USDC	
5	BNB BNB Buy	$290.46	2.94%	22.94%	$47,425,142,867	$2,279,807,331 7,849,002 BNB	163,276,975 BNB	
6	XRP XRP	$0.4316	2.67%	27.60%	$20,863,674,353	$2,356,007,303 5,459,091,123 XRP	48,343,101,197 XRP	

图 4 关于区块链项目前六名的市值情况的图

数据来源：CoinMarketCap

2022 年 5 月 14 日，CoinMarketCap 平台的总市值为 1,270,470,283,586 美元，XRP 排行第 6 位，市值为 20,863,674,353 美元，约占总市值 2%。2018 年，XPR 也曾位列过第三名的好成绩，但在 2020 年经历 SEC 的诉讼后，其市值增速远远落后于其他同类区块链项目。

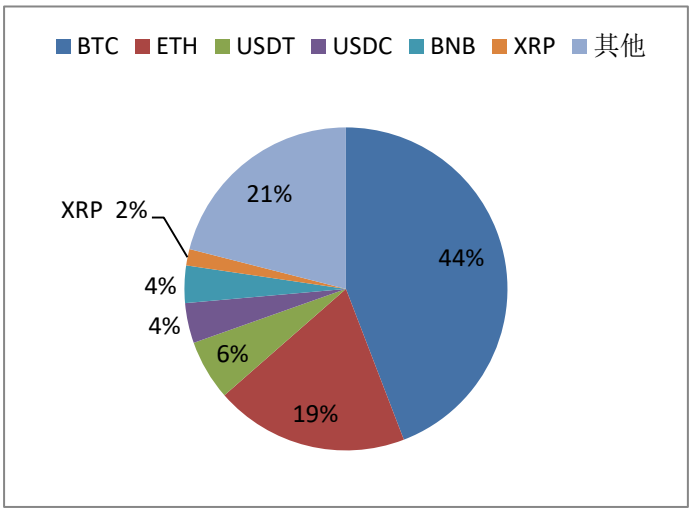


图 5 关于区块链项目的市值占比的图

从总体上说，Ripple 是家好公司，其项目团队专业，行业经验丰富，社区运营情况好，具备一定的影响力。产品定位精准，能够提供比对标组织 SWIFT 更优秀的服务。但是，XRP 并不是一个好项目。

Ripple 与其他老牌区块链项目有着根本性的不同，传统项目，例如：BTH、ETH 基

本上可以说是先有的技术后有的市场定位，所以都是“区块链+”项目。而 Ripple 的项目却是现有的市场定位，其早期目标就是为了提供更便捷的 P2P 跨境转账平台，最开始用的方法也不是区块链技术。只是后期由于区块链大神的加入发现区块链技术是达成原有目标更好的解决方案，所以，这是一个“+区块链”的项目，所以这个项目并没有那么去中心化。所以其旗下产品除了要通过 XRP 来进行跨境转账的 xRapid，还有通过银行来实现转账的 xCurrent 以及通过添加可信任的网关来进行转账的 xVia。从其产品市场反馈来看，xCurrent 反而是其最受欢迎的产品。因此，XRP 就显得比较被动，Ripple 的客户可以不使用 XRP 来转换价值就可以在 Ripple 网络上实现跨境转账业务。那么，XRP 又怎么能够反应 Ripple 项目的未来发展情况，XRP 除了每笔交易固定被销毁的那些，几乎不存在其他的使用价值，甚至于可以与公司主营业务相分离，这使得 XRP 成了一个可有可无，非常可笑的虚拟货币。

所以，Ripple 收到 SEC 的状告也就不奇怪了。就现阶段而言，XRP 并不具备良好的投资前景，但是如果 Ripple 公司真正开始着眼于 XRP 的实际使用途径，例如目前 CBDC 项目，真正可以使 XRP 具备一定的应用价值，其未来还是非常可观的。

4 参考文献

[1]. 邓建鹏，李铖瑜.美国对虚拟货币证券性质的认定思路及启示——以 SEC 诉瑞波币为视角 [J]. 新疆师范大学学报(哲学社会科学版)，2022，43(01):139-148.DOI:10.14100/j.cnki.65-1039/g4.20211201.001.

[2]. 王朝阳，郑步高.互联网金融中的 RIPPLE:原理、模式与挑战[J].上海金融，2015(03):46-52.DOI:10.13910/j.cnki.shjr.2015.03.008.

[3]. 何洪亮.瑞波币与瑞波系统的运行机制[J].时代金融，2016(29):267+278.

[4]. 付闵笑聪.区块链下数字货币的理论与实践[D].上海交通大学，2019.DOI:10.27307/d.cnki.gsjtu.2019.000414.

[5]. 邓青.基于区块链的跨境支付应用研究[D].江西师范大学，2020.DOI:10.27178/d.cnki.gjxsu.2020.000873.

附 1：

1、请说明发起比特币交易到交易确认的整个过程。（说明中请包含：交易者如何产生地址、如何对交易签名、如何发出交易、矿工如何接受交易、如何选出记账人、为何会使用矿池挖矿、矿池挖矿的过程、为何可能会有软分叉、为何限制区块大小、如何控制区块出块时间、区块中包含的内容，并讨论为什么使用 UTXO 设计）

交易者通过随机字串，得到私钥，再由私钥得到公钥，再通过哈希算法，得到一组固定长度的字串，这组字串就是交易地址。

交易者用私钥对交易信息进行加密，交易信息的哈希值被记账人打包成区块，再广播出去，接收方用公钥解密成功，即可验证交易者对该交易签名，表明此交易未发生变动。

交易者编写关于交易的脚本就可以发出交易。

每隔 10 分钟，上一个区块的哈希加一个随机数产生新哈希，矿工们拼算力，第一个算出新哈希的被确定记账人，会被奖励若干比特币，记录好交易产生新的区块，将新哈希广播全场，完成记账。

矿池挖矿是因为目前比特币社区挖矿体量巨大，全网算力使得单台机器挖到矿的可能性比过去低了很多，既然一人之力不够，顺其自然就出现了团队挖矿，这种将多台机器算力整合在一起，按一定方式分配挖矿利益的团体就是矿池。

一般来说，同一时间只会产生一个区块，但如果出现同一时间出现两个除矿工签名外其他都一致的区块，就出现了分叉。而一般这种情况会出现在涉及共识层面的变化，如果这个变化使得适用新共识与采用旧共识都可以兼容验证新的区块，仍然保证单链的就是软分叉，而不可兼容，出现多链的就是硬分叉。

BTC 限制区块大小为 1M 是为了应对交易垃圾邮件堵塞网络的威胁以及潜在的分布式拒绝服务（DDoS）的攻击。

BTC 的出块时间为每 10 分钟一个，这里要考虑的是 POW 算力比拼的时间以及广播传遍全网的时间，因此中本聪基于当时的算力水平给出了 10 分钟这个保证区块链安全的出块时间。但随着全网计算机算力水平的提升，这个时间是可以被缩短的。目前的实际出块时间其实也有小于 10 分钟的。

区块中包含区块头部信息，有版本号、本区块哈希值、本区块高度、上一区块哈希值、本区块打包交易数据的哈希值、时间戳、交易数量统计、本区块大小、本区块总交易额以及难度。

UTXO 也可以说是比特币世界的灵魂所在，在这里要讨论一下货币的的本质，货币如果不在交易中衡量价值转移，其本质上并不具备价值（暂不考虑收藏价值），我们无法真正将它拥有，像一项资产一样拥有，因为它只有在流转中才对我们有价值，很多时候它只是一种第三方担保我们所拥有资产的凭证，当存在了第三方担保，也就慢慢出现了中心化。而区块链的本质是去中心化，因此就需要消除这个第三方，使得 BTC 网络的节点可以进行点对点的交易，所以就存在 UTXO。不是你拥有第三方担保的资产，而是全网共识你有未使用过的过去交易的他方输出，所以这个 UTXO 就可以像货币一样作为价值尺度，来证明交易双方的价值转移。

2、请说明如果签名正确、余额足够的情况下，发出的交易迟迟没能出块，应该是什么原因，应该采取什么措施，分别说明不同措施的后果。

手续费比较低，遇到交易高峰，没有被纳入记账范围。

措施 1：等，错过高峰，总能被记账。缺点，等待时间不确定，不适于有时间限制的交易。

措施 2：去矿池填单，让算力强的矿池，帮忙记账。缺点，需要支付额外的费用，成本较高。

3、请说明以太坊项目的目标，它与比特币不同的技术设计及其原因。

以太坊是一个开源可编程的提供智能合约的平台，其目标是通过专有加密货币，即以太币，在其去中心化虚拟机中智能处理点对点合约。

以太坊与比特币的关系类似于原材料与初级加工品，比特币作为区块链 1.0 的产品既可以作为虚拟货币也可以处理智能合约等多方面发展，就好比牛奶可以用来直接饮用，也可以加工成面包、蛋糕来食用，甚至可以沐浴美容；而以太坊作为区块链 2.0 的产品，主打智能合约，在这个领域专精成更便利高效的产品，为潜在客户提供更好的体验感，就好比由牛奶加工的奶酪，主要服务于食用途径，在味道上提供更丰富的口感。从这个角度也可说明为什么以太坊要舍弃 POW 转向 POS，POS 更加高效也更安全，对于智能合约而言，可以使用更少的资源达成共识，为其客户提供更好的服务。

4、请说明以太坊智能合约的运行原理以及合约的整个生命周期。

以太坊的运行原理与比特币类似，区别在于以太坊记录的交易是智能合约，记录节点是虚拟机，共识机制由 POW 转变为 POS；而比特币记录的交易是支付行为，节点是计算机设备，共识机制仍然是 POW。

智能合约是一段写在区块链上的代码，一旦触发合约中的条款就会被自动执行，人为因素无法左右其执行。智能合约的三个阶段：构建、存储及执行。构建，区块链内的

多个用户根据实际需求、合约双方的权利义务以及执行的评判标准，预先在以太坊虚拟机上设定好各个程序。存储，当编码被完成，消耗一定以太币就会被记录在区块链上并被广播给全社区。执行，一旦被记录在区块链上，智能合约就会定时评判各个合约执行的条件，一旦满足条件，且对比用户签名也都验证生效，合约会自动执行，成功执行的合约也会自动移出区块。

一、评估要求

1、按时交稿、内容要求完整（即按本提纲内容进行）；20%

2、格式是否正确及语言是否规范（补充一下，图表都要编号和命名，如：“图 1 关于什么的图”、“表 3 关于什么的表”等，表命名在表上方，图的命名放图下面）；10%

3、内容是否充实（总的要求 3000 字-5000 字左右，每一部分分析是否充实，加入了**自己的分析和思考**，数据和图表精确引用，**如果拷贝太多则是负面评价**）；30%

4、逻辑及分析是否正确（每一部分分析是否合理并准确）；20%

5、**是否有新意**（是否有独特的视角或超过课堂讲的内容的自学的东西的突破）；20%

二、文献要求

请在文章中用作者加年代的方式表示参考文献，比如：张某某（2009）提出什么什么。双比如，某理论（张某某，2009）提出什么什么。

请将文章中参考的文献用脚注标出。

参考文献的格式请百度“参考文献”。

三、“附 1”要求

附 1 占整个论文 30%的分数，请根据课程内容、根据自己查找的资料进行回答，回答要简洁，不要有废话和无关的话，尽量采用罗列的方式。