**上海大学“区块链”课程论文考试**

**Polygon (MATIC) 项目分析**

姓名：徐哲渊 学号：21122916

**字数：3583**

**摘要：**Polygon（以前称为Matic Network）是第一个结构良好，易于使用的以太坊扩展和基础设施开发的平台。它是一种框架，可用于创建与以太坊兼容的区块链网络和扩展解决方案。Polygon目前已有效降低交易费用并持续推出多个解决方案以增强速度、安全性与隐私性。本文将聚焦于Polygon相较于其它区块链项目的不同与创新点——解决方案与可扩展性。

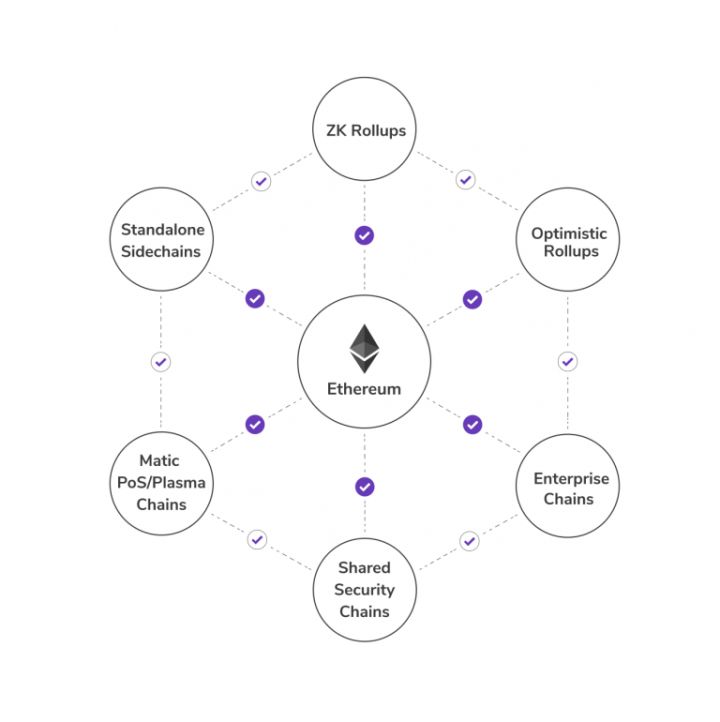
**关键字：**解决方案; 可扩展性；框架；以太坊

**论文评语：**

成绩： 任课教师：吴建刚

1. 经济模型分析
   1. 项目、创始人及团队简介

Polygon（以前称为Matic Network）是第一个结构良好，易于使用的以太坊扩展和基础设施开发的平台。和以太坊相比，Polygon的速度、可扩展性和可用性都更加有优势。Polygon采取了一种受plasma影响的独特的第二层（L2）扩展方法，创建一个树状的 "子区块链"，将以太坊区块链作为信任和仲裁层。子区块链通过允许许多交易在被发送到以太坊区块链之前被分批处理，帮助降低交易成本。



图表 1 Polygon框架示意图

Polygon于2017年10月推出，由Jaynti Kanani，Sandeep Nailwal和Anurag Arjun共同创立，他们分别是两位区块链开发人员和一位商业顾问。

Jaynti是一名全栈开发人员和区块链工程师，目前担任Polygon的首席执行官。他在以太坊上实现Web3，Plasma和WalletConnect协议方面发挥了不可或缺的作用。在参与区块链之前，Jaynti曾在 Housing.com 担任数据科学家。

Polygon的联合创始人兼首席运营官Sandeep Nailwal是一位区块链程序员和企业家，曾担任Scopeweaver的首席执行官和Welspun Group的首席技术官。

Anurag Arjun是Polygon唯一的非编程联合创始人。作为产品经理，他曾在IRIS Business，SNL Financial，Dexter Consulting和Cognizant Technologies工作过。

* 1. 项目想要实现什么

Polygon试图提供一个通用框架，允许开发人员利用以太坊安全性创建定制的，专注应用程序的链，并提供一个可互操作的网络，将各种不同的扩展解决方案链接在一起，并主要致力于找出以下解决方案：

·解决以太坊出块慢，网络拥堵，交易费用高的问题

·解决区块链平台的可扩展性有限的问题

* 1. 为什么需要分布式记账

分布式账本避免了传统中心化信息管理所带来的信任和安全风险，使信息纂改成本大幅提高，从而保证了信息的权威性。

* 1. 代币机制

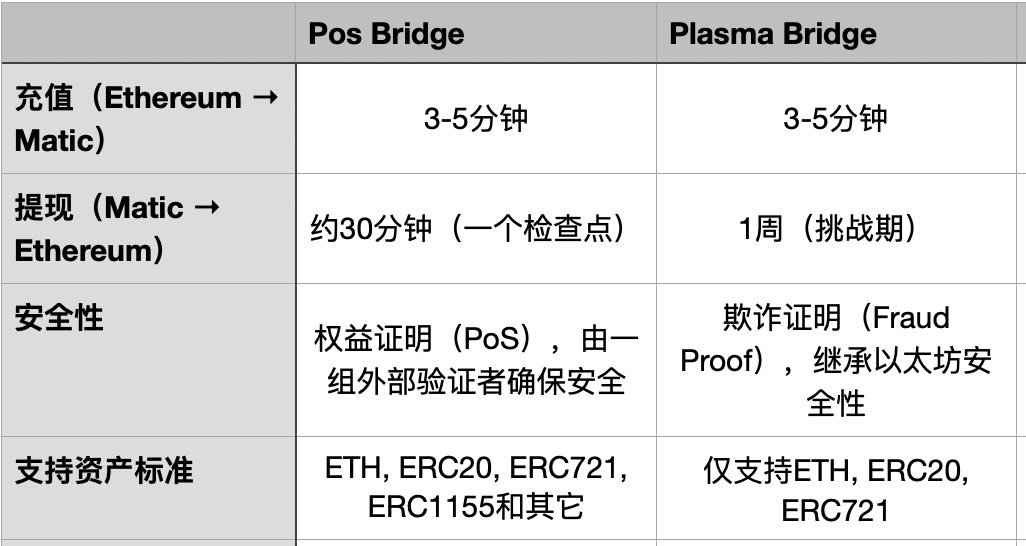
MATIC是Polygon中的实用程序代币。MATIC代币用于在Polygon网络中的参与者之间进行付款和交换。MATIC代币在以太坊上为ERC-20，并且在主网时无需更改为Matic Network的本地代币。

1. 技术模型分析
   1. 共识机制

Polygon通过PoS权益证明共识机制确保安全，在该机制中，验证者将MATIC代币质押至以太坊主链托管的智能合约中。在这种挖矿方式中，区块链系统中的节点不需要太高的算力，而只需要质押一定数量的代币，运行一段时间后就可以产生新的货币，而产生的新货币就是通过质押得到的收益。

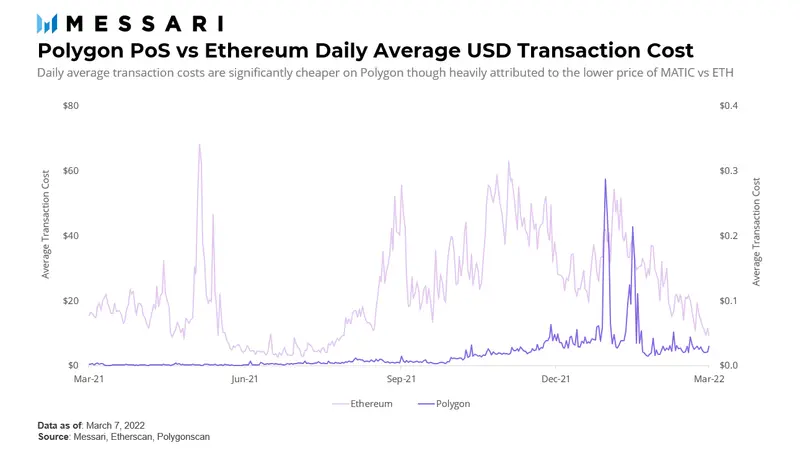
* 1. 帐户机制及智能合约

要将资金从以太坊转到Polygon，必须经过桥（Bridge）。当用户将资金存入桥时，它们实际上被保存在以太坊合约中，然后在Polygon上被重新创建。当赎回资金时，用户需要回到桥。用户通过桥发送的代币在Polygon上被销毁后，以太坊合约中的资金将被解锁。在Polygon上，用户可以选择使用两个桥：Plasma Bridge和PoS Bridge。



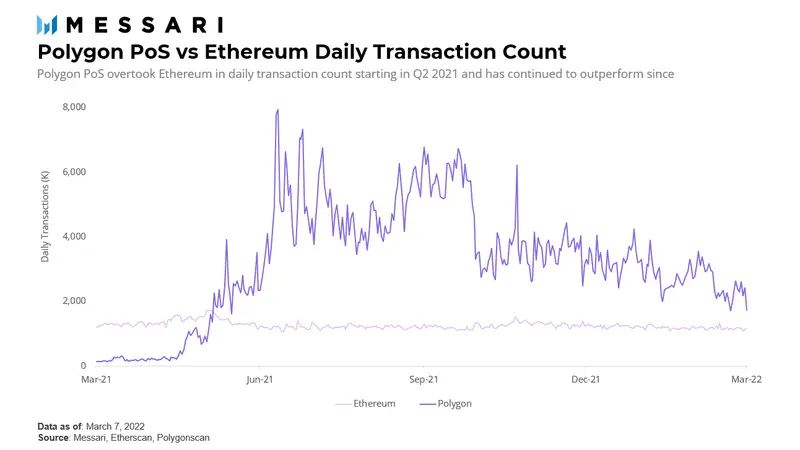
图表 2 PoS Bridge与Plasma Bridge对比

PoS Bridge是官方推荐使用的桥，它具有更快的提款时间，支持更多的以太坊资产标准；而Plasma Bridge提款时需要等待7天的挑战期，但是它在安全级别上会更高。



图表 3 Polygon PoS与以太坊的平均交易费用对比

上图反映了Polygon PoS和以太坊之间平均交易成本的差异。Polygon PoS 的平均成本极低，通常远低于0.1美元，而用户需要在以太坊上支付至少20 美元。假设过去一年PoS 链上完成全部交易都在以太坊上进行的，那么用户将多支付近 150 亿美元的总交易成本。这一巨大优势也使Polygon网络拥有超过1.3亿个独立地址数以及16亿笔交易记录。



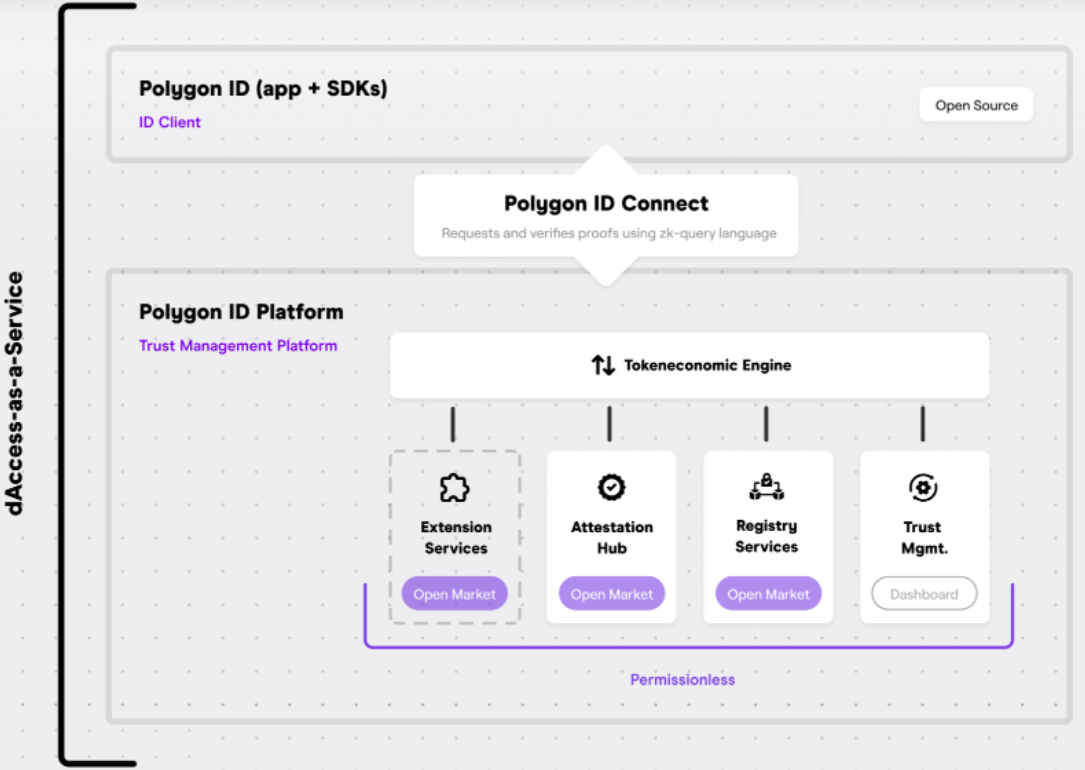
图表 4 Polygon PoS与以太坊的日交易量对比

* 1. 数据库、隐私保护、身份验证等

Polygon ID是区块链原生地身份系统，这也是一种新的以个人隐私为核心的身份解决方案，它应用零知识（Zero-Knowledge）证明为用户建立数据身份，利用安全性层作为维护私人信息的一种方式。Polygon认为，ZK证明是解决以太坊区块链上围绕隐私问题的答案。

Zero-Knowledge（ZK）证明是一种用于证明声明的技术，该声明保护了交易双方的隐私。这使得发件人、收件人、金额和交易内容可以被屏蔽，同时仍然允许交易被验证。ZK专注于只提供处理交易的必要信息，而不披露任何其他细节。它能够通过一个自动验证器发挥作用，该验证器作为两方之间的加密中介。为了验证信息，甲方等待验证器的确认来评估乙方信息的准确性，而不是直接验证信息。这使得双方的隐私得到保护，双方只获得必要的信息，而不获得完整的钱包历史。

根据Polygon团队表示，这类解决方案容许用户操纵它们的数据身份，这也是Web3为其互联网颠覆式创新的关键标准。用户不用递交敏感的私人信息，如身份证件或驾驶执照，就可以通过 Polygon ID 在链上证明他们的身份。



图表 5 Polygon ID结构示意图

Polygon Nightfall则是一个面向企业的以隐私为中心的汇总（Rollup），旨在降低ERC20，ERC721和ERC1155令牌私人转账的交易成本。它使用乐观汇总（Optimistic Rollup）来降低成本，并通过利用ZK证明来获得隐私。乐观汇总合约部署在以太坊第1层上。提议者将交易汇总成区块，并将其提交给乐观合约。挑战者将向相同的合同提交任何无效区块的欺诈证明。执行私人转账所需的所有信息都存在于客户中，并且不依赖于任何链下第三方。 通常使用Optimistic rollup方案的用户不得不等待7天的挑战期，但Nightfall通过为用户提供“即时退出”的选项从而改善这一点。其运作方式是，由流动性提供者与用户该笔交易交换位置，先为用户垫付即时提款所需的资金，并在7天的等待期内占据该位置。

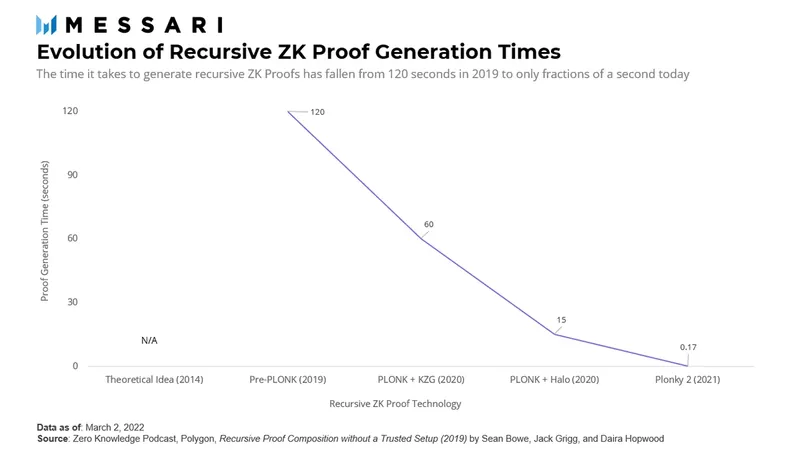
* 1. 现有技术文档及代码评价

Polygon目前已公布了多个解决方案，包括Polygon PoS, Polygon Hermez, Polygon Avail, Polygon Edge, Polygon Nightfall, Polygon Miden, Polygon Zero等。

Polygon Hermez每秒能处理多达2000笔交易，预计这一数字还会更高。并且与一般主网gas费相比，该产品降低了90%以上的交易成本。同时，Hermez也是唯一一个不需要中心化运营商的第二层解决方案。

而另一个解决方案Polygon Zero的目标是速度。迄今为止发现的最佳解决方案是通过可扩展的 ZK-SNARK，也称为递归证明。递归ZK证明通过增加任何时候可以处理的交易数量来加快速度。高效的递归ZK证明允许将处理分配到更易于管理的并发工作块中。一旦每笔交易都经过验证，递归算法就会遍历并聚合所有证明，直到它们最终形成一个证明。最终证明可以以比当前替代方案更快、更具成本效益的速度发送到主网。

Polygon Zero能够通过Plonky2做到这一点。Plonky是一个递归ZK证明生成器，能够每0.17秒生成一个SNARK证明，这使Plonky2成为世界上最快的递归ZK证明器。



图表 6 ZK Proof生成速度

Polygon Miden是一个基于STARK的zk-rollup，旨在解决rollup很难支持任意逻辑和交易的问题。Rollup通过打包交易来减少链上数据存储，可以减少拥塞并降低交易费用，但很难支持交易包中的某个任意交易的验证，这影响了它验证所有链下交易的能力。一旦开发完成，任何项目都可以在这个zk-rollup之上部署智能合约。

与其他项目不同之处在于，Miden生成STARK证明。尽管使用STARK证明更贵，但它相对要更安全。Miden创始人还计划进一步研究递归STARK证明，来降低其价格。Miden具体的运行步骤如下：

·交易首先会分发送给Miden的执行节点；

·这些执行节点一次将5000笔交易捆绑到区块中，并生成一个 STARK 证明；

·每200笔交易捆绑的区块生成一个STARK证明，证明交易的有效性；

·最后将最终STARK证明结果是上传到 L1 以太坊来达成共识和确定性。

1. 项目未来
   1. 未来规划及激励机制

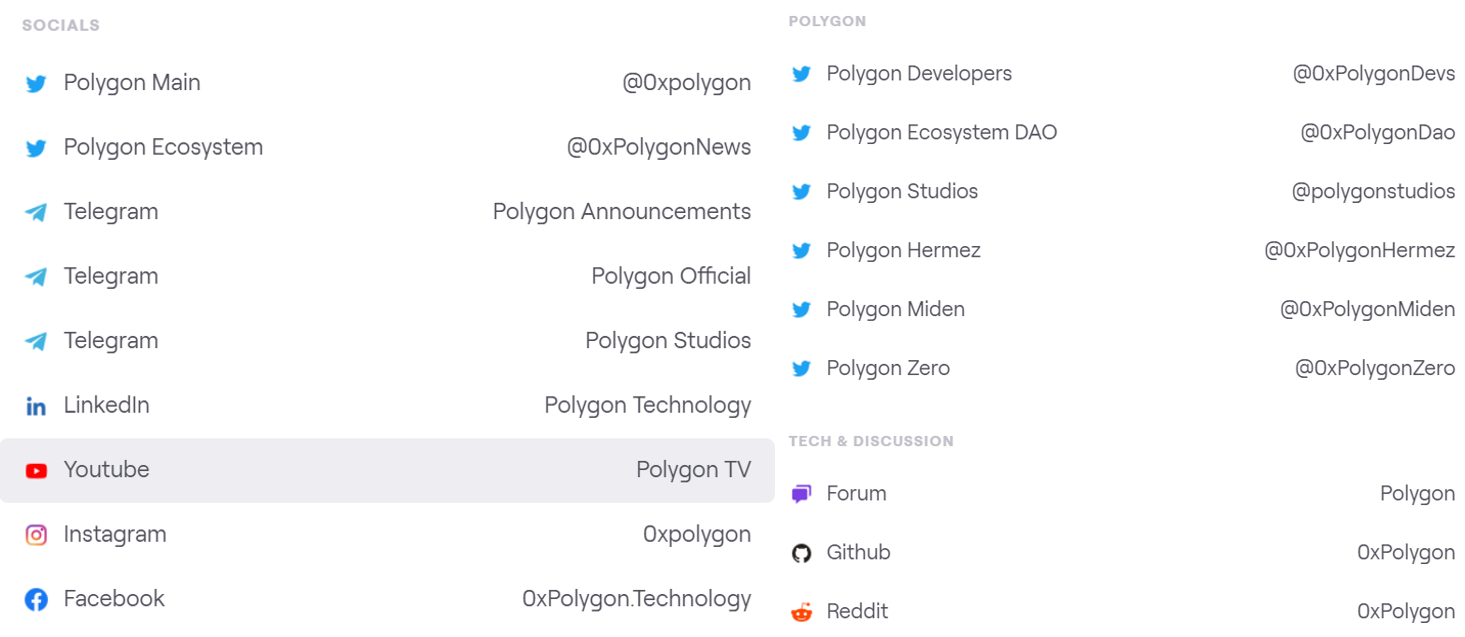
目前，四个方案（Polygon Miden, Polygon Avail, Polygon Zero, Polygon Nightfall）处于开发和测试阶段。在未来继续研发解决方案的同时，Polygon也将未来的重点放在了企业合作方面。随着每种产品继续研究、测试或推出自己的扩展解决方案，Polygon将更加重视寻找合适的合作伙伴和协议以集成到 Polygon 的产品网络中。

预计在2022年内，Matic代币将完成重新设计，这意味着Polygon的激励机制可能会有重大改革。Matic代币是Matic Network遗留的产物。未来的代币将有一个新的代码，并适用于所有Polygon产品。据称，新代币对用户不是强制性的，即不需要购买、质押或持有。这意味着对于大部分用户来说，它可能只是后台的东西。

同时，Polygon承诺在2022年内使用两千万美元抵消Polygon碳足迹，并购买额外的信用额度以成为负碳，为环境保护做出贡献。

* 1. 现有社区及应用评价

截至今年4月，已经有超过19000个dApps在Polygon网络上运作，比起半年前的2021年10月增长了六倍。数据显示，包括在主网和测试网上的dApps在内，65%的团队完全集成在Polygon上，而35%的团队部署在以太坊上。



图表 7 Polygon社区

Polygon社区拥有较高的活跃度，主要集中在Twitter以及Telegram上。Polygon的主要推特账号Polygon – Matic拥有150万追随者，发推频率维持在较高水准，几乎每日都会发送多条动态，使Polygon最新的目标与合作消息保持公开透明。这意味着关注Polygon的进程是较为容易的。

* 1. 项目投资分析

目前来看，Polygon是相当具有潜力的。包括测试与研发中的项目，Polygon至今已公布了总计9个解决方案，分别注重于交易过程中的不同方面。它在有效地兼顾安全性的同时，解决了以太坊交易费用高，交易速度慢的问题，至今仍保持着高交易量。这一成功证明了Polygon的价值。

作为一个框架，Polygon是否能够持续性地取得成功，取决于是否能够如它所言将不同解决方案链接在一起，并最终将以太坊转变为一个成熟的多链结构。如果这一诺言得以兑现，将会极大增加不同系统间的交互性与可操作性，让互联网真正连接起来。要做到这一点还是有一定技术难度，不过鉴于Polygon之前的成功经历与积极的合作研发，我认为可以对此持乐观态度。