**上海大学“区块链分布式记账技术”课程论文考试**

Algorand**项目分析**

姓名：卢思颖 学号： 21122702

**字数：4715**

**摘 要：**

在区块链这一新兴技术中，Algorand项目以环保绿色以及解决区块链三元悖论而在第一次荷兰式拍卖中强势出圈。在algorand项目发布的三年内，该公链上的社区和应用也十分广泛，其打造的全球化合规化区块链也受到应用方好评。本文从algorand项目创始人团队、纯粹权益证明的共识机制、智能合约以及激励机制、项目投资分析等技术模型和经济模型视角展开分析，将algorand该金融公链的特点展示并浅显分析其未来发展。

**关键字：**Algorand；区块链；共识机制；智能合约

**论文评语：**

成绩： 任课教师：吴建刚

**1经济模型分析**

**1.1项目、创始人及团队简介**

**1.1.1项目**

Algorand是一个全新的金融区块链系统平台，根据创新理念研发而成，同时实现真正的去中心化、可扩展性和安全性。[1]

**1.1.2创始人**

Algorand公司创始人为西尔维奥·米卡利，是图灵奖，哥德尔奖和RSA奖的获得者。同时，他是美国国家科学院，美国国家工程院，美国艺术与科学院和Accademia dei Lincei的成员。他拥有罗马大学数学Laurea学位和加州大学伯克利分校计算机科学博士学位。

在Algorand，Silvio负责监督所有研究，包括理论，安全和加密金融。[2]

**1.1.3团队简介**

除了创始人西尔维奥·米卡利，algorand团队中还有许多其他密码学和创业者。

首席执行官史蒂夫·科基诺斯是一位连续创业者，他领导的Fuze公司改变了企业将协作视为业务可见性、流程改进和结果的关键驱动因素的方式。[2]

首席运营官肖恩·福特负责上市执行和运营，包括产品管理、工程、营销和全球社区开发。在他担任algorand首席运营官前，他曾在LogMeIn，Avid Technology，Monitor Group等多个公司担任过重要职位。

此外该项目团队的计算机人才也有着强大的学术和理论背景。系统安全领域的世界级专家Nickolai Zeldovich也是白皮书联名作者，首席科学家陈婧曾获得美国自然基金会Career Award，而CTO Yossi Gllad在2017年则获得IETF/IRTF网络研究应用奖。[3]

**1.2项目想要实现什么**

Algorand项目想要创造一个每个人都能高效、透明、安全地创造和交换价值的世界，通过技术力量实现无摩擦金融。[4]该项目希望通过权利下放实现全球信任，创造推动数十亿人采用的简单设计，消除所有人繁荣的障碍。

**1.3为什么需要分布式记账**

分布式账本是一种在网络成员间共享、复制和同步的数据库或记录系统。这种共享账本消除了调解不同账本的时间和开支，且没有中心管理员和集中数据存储。[5]而algorand项目为了实现全球信任，需要利用透明公开强大的分布式账本算法以权利下放的方式来消除需要时间来建立的主体信任。同时，分布式记账的去中心化的门槛更低，可以吸引更多的用户参与。另外，分布式记账能有更高的市场效率，降低成本。

**1.4代币机制**

ALGO是algorand项目的原生代币。它的最大供应量为100亿代币，Algorand项目将使用ALGO代币参与共识并协助保护网络，且ALGO代币永远不会超过流通供应量的49%。ALGO代币定期在节点之间重新分配。同时，将使用ALGO代币通过代币授权、竞赛和投资，为贡献者和应用程序开发人员提供激励，并且协助金融生态系统的发展。[6]

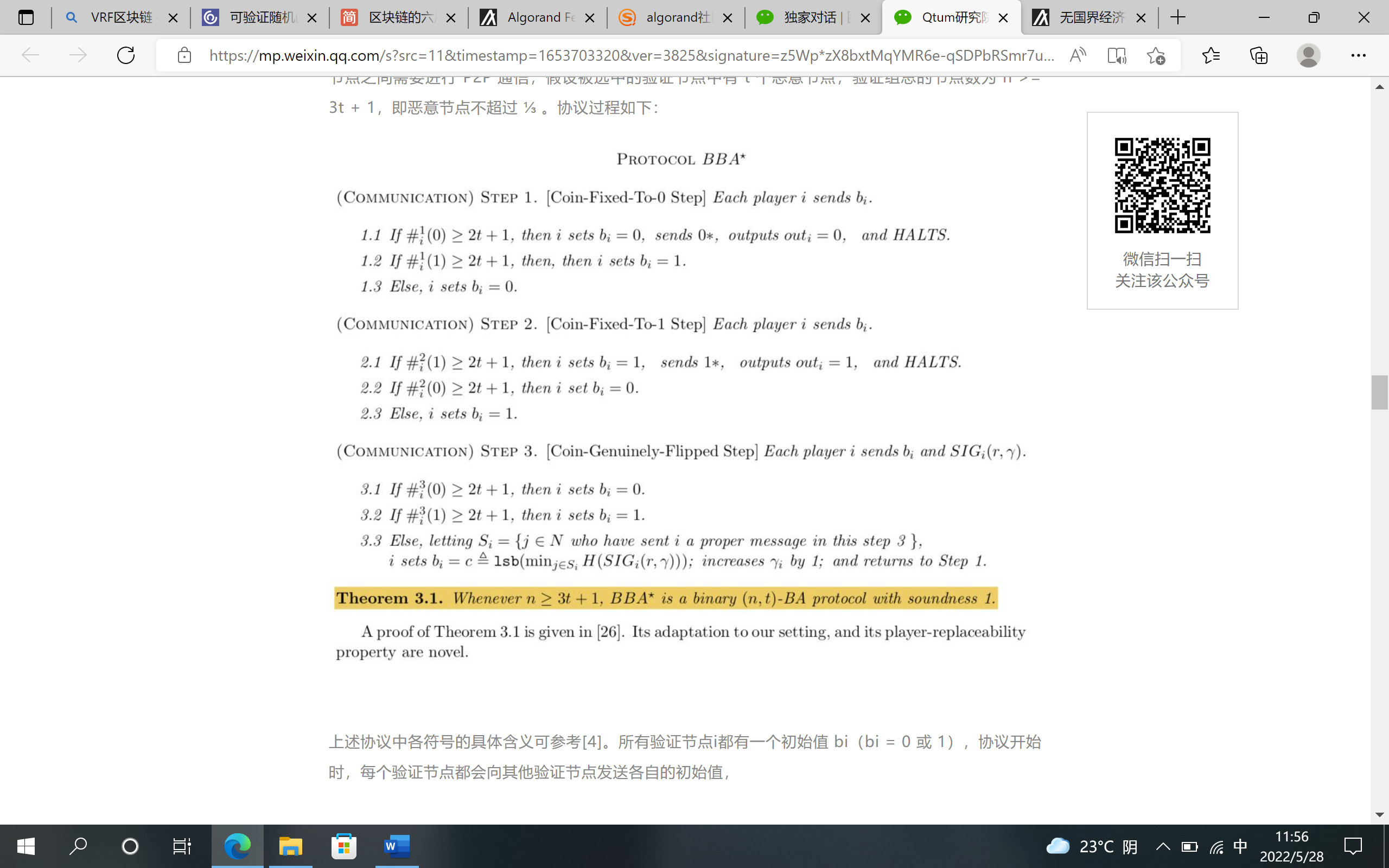
**2技术模型分析**

**2.1共识机制**

**2.1.1共识机制的过程**

区块链技术由分布式存储、密码学、共识机制、智能合约等技术构成。共识机制是指选择区块并将其计入区块的方式。共识机制的作用旨在可容错的网络环境下实现状态机复制排序的一致性。[7]

Algorand的共识机制是基于纯粹权益证明（PPoS）的分散式拜占庭协议协议。[8] 它可以容忍任意数量的恶意用户，只要诚实的用户（遵循协议指令的用户）持有系统中总股份的三分之二以上。相较于比特币的PoW工作量证明，Algorand的共识机制可以解决确认时间长、易分叉和扩展性差的问题。



**图1：二元拜占庭协议（BA\*）具体内容**

Algorand的共识机制主要有两个基本过程，第一步在每轮共识开始之前，选出潜在的领导者各自生成新区块，对新区块进行签名和广播。第二步，随机选出验证组，对领导者广播的新区块进行验证，达成共识后广播确认新区块，进入下一轮。而在验证组投票的过程中包括软投票和认证投票。

在第一步中，每位参与的账户通过可验证随机函数（VRF）的运行来确定是否选择该账户来建议块。选择帐户后，每个节点都会将其建议的块与VRF输出一起传播，这证明该帐户是有效的提议者。网络中的每个节点都将从其他节点获取区块建议，然后验证这些建议的 VRF 输出。[8]

接下来，每个节点将为运行每个账户的VRF，以查看他们是否被选中参加软投票委员会。如果选择了一个帐户，将根据其拥有的算法数量进行加权投票。所选的每个帐户通过投票确认阻止来过滤提案。这些投票将针对超时时计算的最低VRF块提案，并将与VRF证明一起发送到其他节点。每个节点将在添加到投票计数之前验证委员会成员VRF证明。达到软投票的法定人数后，该过程将进入认证投票步骤。

然后选择一个新的委员会来检查在软投票阶段投票的区块提案，以了解超支，双重支出或任何其他问题。如果有效，委员会再次投票以证明该区块。这以类似于软投票的方式完成，其中每个节点都通过其管理帐户进行迭代以选择委员会并发送投票。这些投票由每个节点收集和验证，直到达到仲裁，触发回合结束，并提示节点为区块创建证书并将其写入分类帐。此时，将启动新一轮，并重新开始该过程。[8]

**2.1.2共识机制如何解决不可能三角**

区块链技术中有广泛讨论的三元悖论，即可扩展性、安全性和去中心化。在米卡利的演讲中他着重分析了Algorand项目是如何解决区块链三元悖论的。

在可扩展性方面，由于用户运行其可验证随机函数（VRF）只需要大约1微妙，无论该用户拥有的令牌数量，因此十分快速。一旦选定新的区块，每个成员都将向网络传播一条简短的即时计算的消息。因此只要被选中参与认证投票的委员会成员数量一定，则消息的传播时可扩展的。

在安全性方面，由于选出新区块的委员会成员说秘密运行个人可验证随机函数（VRF）所挑选出的，因此只有当成员通过网络传播各自广播其VRF和区块意见时，攻击者才能知道委员会成员。又由于信息的快速传播，仅1微秒，攻击者此时的攻击失去了意义，因此algorand具有安全性。

在去中心化方面，由于每一次委员会的秘密随机选出，相较于比特币由于PoW工作量证明导致目前仅几个矿池进行挖矿，形成新的“中心化”，algorand项目中每一个人都有机会参与到下一个新区块建设的可能。

**2.2账户机制及智能合约**

**2.2.1账户机制**

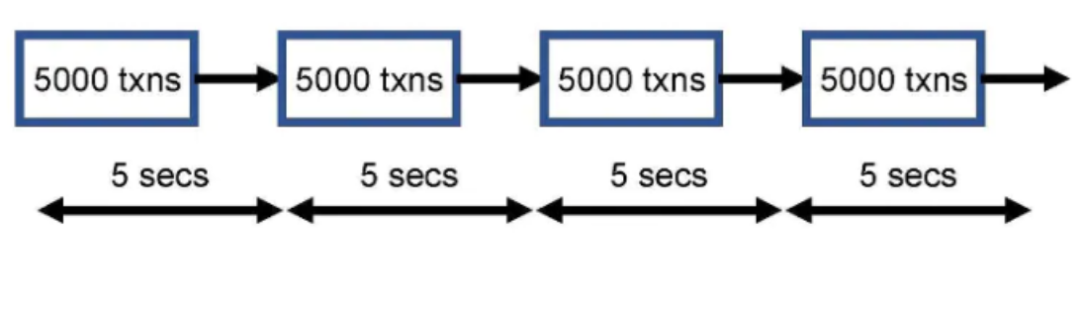
公共地址和专用支出密钥组合用于保护帐户。公共地址是公开的，用于标识帐户，其中私有支出密钥用于安全目的，并用于能够从该帐户发送事务所需的公共地址的身份验证和加密。

Algorand项目重新密钥通过允许用户更改其私有支出密钥而无需更改其公共地址。而algorand重新加密的技术能够快速地保持公共广播的持久性，降低运营开销，灵活地维护单个公共地址。[9]

**2.2.2智能合约**

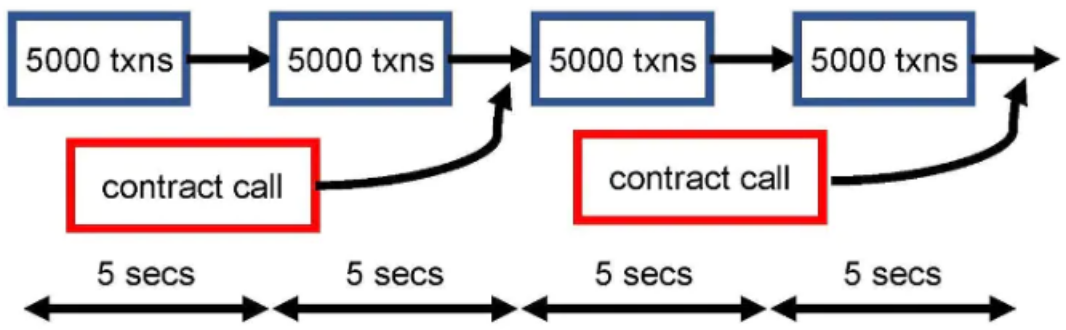
智能合约是一种自动执行的合约，双方之间的协议条款直接写入代码行。代码和协议存在于分布式，分散的区块链网络中。[10]为了满足日常需求，algorand提供了layer-1智能合约以及链下合约。

Algorand项目第一层智能合约用于执行许多常见的交易。第一层智能合约通过TEAL程序编写，同时Algorand Layer-1合约还为常见的“售后”交易，证券化贷款，众筹，仅授权交易，多签名钱包以及其他简单的重复交易提供直接支持类型。



**图2：使用第1层智能合约的正常Algorand执行**

Algorand项目第二层智能合约为链下合约，用于处理较为复杂或者过大的合约。链下合约代码以高级语言编写，并由虚拟机（VM）执行。链下合约具有其自身的长期状态，称为合约存储。为了保护隐私，合约存储本身未出现在区块链上。为了安全起见，每个合约调用都会发布一个承诺到最新的合约存储。链下合约可以读取账户余额和其他链上信息，并且可以发出交易（例如付款）来修改区块链状态。与传统的以太坊式合约不同，这些“效果交易”不是直接执行的。取而代之的是，该请求的效果由合约执行委员会验证者的法定人数来验证。通话效果交易被打包为第1层“全有或全无”交易，保证一起成功或失败。



**图3：使用Algorand链下合约执行**

**2.3数据库和隐私保护**

Algorand项目的数据库于其他区块链项目一样，在数据结构中存储信息。

在隐私保护方面，algorand项目不会直接使用用户的消费密钥来进行共识，而是产生一个参与密钥。因此在参与密钥被破坏时，用户权益和隐私仍然能被保护。

**2.4算法网络结构**

Algorand网络有两种类型的节点来同时优化去中心化和高交易吞吐量：中继节点和参与节点。

中继节点充当中央网络集线器，并保持与许多其他节点的连接。中继节点具有高带宽网络连接，可实现高效的通信路径，最终减少通信中的跃点数。它们通过累积来自参与节点和连接到它们的其他中继节点的协议消息，执行重复数据删除、签名检查和其他验证步骤，然后重新传播有效消息来实现此目的。中继节点也通常位于互联网交换点，以减少传播时间。任何人都可以（并鼓励）运行中继节点。[11]

参与节点代表地址的赌注，并持有参与密钥，用于在共识算法中对区块进行提案和投票。任何人都可以主持参与节点。

**2.5现有技术文档及代码评价**

现有的75页白皮书以及其智能合约虚拟机等技术文档都非常成熟。但是美国北卡罗来纳大学夏洛特分校的计算机与信息学院王永革教授认为algorand项目存在分叉的可能，而非项目所提出的零分叉。此外，“大部分节点是诚实节点”这种假设不切合实际，同时，algorand的拜占庭协议存在优化空间。因此，我认为algorand在其创新的共识机制中仍有改进的空间。

**3项目未来**

**3.1未来规划及激励机制**

**3.1.1激励机制**

Algorand项目并没有激励机制。Micali教授曾回应”Algorand协议只需要进行平凡的计算，因此不需要激励”。 Algorand的共识协议由于不基于PoW，用户参与共识协议的代价非常小。这使得激励机制对共识协议本身不像对PoW系统那样有决定性的作用。但是，陈婧表示，在基于algorand blockchain上的生态系统会设定一定的激励机制，并希望这样的激励机制可以促进社区建设，保持社区关注度。

**3.1.2未来规划**

Algorand作为一个专注地球可持续发展的绿色项目，承诺成为现在和未来具有负碳网络的最环保的区块链。并计划在algorand公链上构造可互操作的生态系统。

**3.2现有社区及应用评价**

在algorand公链上目前已出现许多应用。比如TOP网络，AssetBlock，欧泰公司等。目前已经创建大使社区，AlgoGrant计划服务于做应用的专业团队，还有Algorand Accelerate计划为团队提供孵化支出。目前algorand项目有一些潜在应用，包括DeFi合规应用潜力，房地产等实体资产通证化应用，国际服务商业、支付等应用，股票、债券、衍生品等金融产品链上发行以及稳定币公司Tether在Algorand网络集成和开发稳定币USDT。

对于Algorand现有社区和应用，当下技术社区尝试过整体公链性能的人均反馈较为积极，速度体验性较好。同时，目前社区相关应用和项目的更新，更多为干货和技术更新。因此，我认为现有社区及应用在构建整个algorand生态系统中的进展较为稳定和快速，在可持续发展方面和促进无国界经济方面进行了相关项目推进和改善。

**3.3项目投资分析**

Algorand项目本身的团队实力、项目创新性、社区和合作方的情况以及潜在应用的前景都是世界顶尖水平。未来国际区块链产业的方向是合规化，而algorand的安全性保障了其合规化和法律化。因此长期来看，algorand项目是具有可期待的潜力价值的。但是，在algorand整个区块链中存在部分对生态有危害的节点，公司需要警告并收回部分权利，来防止再次遇到二级市场剧烈波动的问题。

同时，马绍尔群岛主权数字货币，将使用algorand技术建造世界上第一个国家数字货币。Algorand成为ISDA成员，通过与ISDA合作和区块链上实现公共领域模型(CDM)。Algorand通过符合伊斯兰教法的融资认证伊斯兰机构现在可以开始使用Algorand区块链进行经济交易。并且，algorand的区块链平台仅通过手机，帮助非洲4亿人记录数字身份。这些已经在进行的国际化数字货币和数字身份项目，让我认为algorand项目会走向全球并引领金融公链的不断发展。

**参考文献**

[1]希尔维奥·米卡利,卿苏德.理论计算、密码学和区块链[J].互联网天地,2019(09):2-11.

[2] 阿尔戈兰德.我们的团队[EB/OL]. www.algorand.com/about/our-team,2022-5-30

[3] 杨浩峰.专题研究九：区块链项目Algorand[EB/OL].[zhuanlan.zhihu.com/p/149445885](https://zhuanlan.zhihu.com/p/149445885),2022-5-30

[4] 阿尔戈兰德.关于我们[EB/OL].[www.algorand.com/about](https://www.algorand.com/about),2022-5-30

[5][百度百科.分布式账本[EB/OL]baike.baidu.com/item/%E5%88%86%E5%B8%83%E5%BC%8F%E8%B4%A6%E6%9C%AC/22352185](https://baike.baidu.com/item/%E5%88%86%E5%B8%83%E5%BC%8F%E8%B4%A6%E6%9C%AC/22352185),2022-5-30

[6] 阿尔戈兰德.我们对透明度的承诺[EB/OL].[www.algorand.com/transparency](http://www.algorand.com/transparency),2022-5-30

[7]王波,任英琦,黄冬艳.H-Algorand：基于多块输出的公有链共识机制[J].计算机应用,2020,40(07):2150-2154.

[8] 阿尔戈兰德.算法协议概述[EB/OL].[www.algorand.com/technology/protocol-overview](https://www.algorand.com/technology/protocol-overview)，2022-5-30

[9] 阿尔戈兰德.ALGORAND在第一层中的特性和功能[EB/OL].[www.algorand.com/technology#REKEYING](https://www.algorand.com/technology#REKEYING)，2022-5-30

[10] 阿尔戈兰德.常见问题[EB/OL].[www.algorand.com/technology/faq](http://www.algorand.com/technology/faq),2022-5-30

[11] 阿尔戈兰德.算法网络结构概述[EB/OL].[www.algorand.com/technology/algorand-network-architecture](https://www.algorand.com/technology/algorand-network-architecture),2022-5-30