**上海大学“区块链”课程论文考试**

**STEPN项目分析**

姓名：**顾亚亚** 学号： **21726061**

**字数：3269**

**摘 要：**

STEPN是Solana链上一款跑步游戏，玩家可以通过在户外运动（跑步或是走路）来赚取奖励，将区块链项目与现实生活链接起来，让非币圈也能体验区块链的发展。

本文主要基于Solana链对STEPN这款游戏的经济模型及技术模型进行分析，并对游戏机制及项目未来进行一定的说明和预测。

**关键字：**Solana，STEPN，跑步

**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

一、项目

STEPN是世界上第一个移动设备上的Move-2-Earn的NFT游戏，它致力于通过碳抵消来对抗全球变暖，项目方来自澳大利亚。STEPN是一个Game-Fi项目，玩家可以通过现实生活中的步行、慢跑或跑步来获取奖励（游戏代币），并且可以燃烧游戏代币来升级他们的运动鞋、制造更多运动鞋、升级游戏内宝石、支付维修费用以及支付在线马拉松参与费用。在最高级别，玩家可以获得治理代币，能够决定游戏的利润分配。

M2E这个概念很早就被提出来，但STEPN却是最快将这个想法“兑现”的，仅用了120天就完成了产品交付。从2021年11月3日起就一直在进行Beta测试，邀请了来自43个国家的1000多名玩家参与，更实现了每周超过70%的玩家留存率。STEPN在推出的仅3个月时间里面，它就拥有了超过180多个国家的用户，日留存率是高达80%。截止到4月，STEPN活跃用户已经超过了80000。

二、创始人及团队

STEPN是一家澳大利亚的游戏开发商开发的，两位创始人Jerry Huang和Yawn Rong均为华人，前者在2008年就进入了游戏圈。Yawn在接受采访时曾提到，团队是看到Axie Infinity后才开始思考新的方向，这才有了STEPN。

## 1.2项目想要实现什么

* 创造了一种链上世界和现实世界结合在一起的体系
* 推动Web3.0走向大众化
* 通过碳抵消来对抗全球变暖

## 1.3为什么需要分布式记账

因为STEPN是Solana链的一款游戏，核心就是分布式记账技术，当然，这种跑步获得奖励的手游，不利用区块链技术也可以开发出来，但是这样的话，游戏中的代币和装备就基本不具备任何价值，运用分布式记账技术，用户就会投资和运动想办法获得NFT，进而通过游戏中搭建起来的经济系统进行交易，也可以直接在游戏中换成稳定币USDC，不用区块链技术的话，是难以实现的。

## 1.4代币机制

双代币系统：一种是GST，一种是叫GMT。

GST：游戏代币，无限增发，客观来讲没有这个时代的价值，来升级运动鞋、制造运动鞋、升级宝石、支付维修费用以及在线马拉松参与费用。

GMT：治理代币，已经上到了交易所，可以在各大主流的交易所买到，所以它是有真实的价值的，它的总量就是60亿枚。

无论赚取的是GST还是GMT，都可以在这个游戏当中直接换成稳定币USDC。

## 1.5游戏机制

一、你要买STEPN的一双鞋，当然它不是说实体的给你一双有运动鞋，它是给你一个NFT，NFT现在的价格大约10SOL币（Solana生态的代币）左右，差不多1500美金。那如果你不买这双鞋，你也可以玩这个游戏，但是你是不能靠运动来赚钱的。

二、通过在现实世界跑步即可赚取代币收益，所得收益可以用来升级、修复运动鞋以提高“赚币”效率，也可以直接卖出。

# 2.技术模型分析

由于STEPN是基于Solana 公链的NFT游戏，所以接下来会针对Solana 公链进行相关技术模型的分析。

Solana是采用了PoH（Proof of History历史证明)审批算法的专为DeFi（去中心化金融）开发的区块链。Solana就是区块链里面的类似iOS平台的系统，用户可以使用基于该平台开发出的各种APP。

目前对比BTC和ETH来看，Solana公链还是有一些优势的：

* 处理速度快, 交易成本低
* 可以获得持有虚拟货币的“利息”报酬
* 未来可以和其他的区块链互通

## 2.1共识机制

Solana采用混合共识机制（历史证明PoH与权益证明PoS相结合）。

PoS（权益证明机制）：是Solana的基础共识机制，一方面，验证者是根据节点在网络中的SOL持有量来选择的，SOL越多，被选为验证者的机会就越大，验证者在批准交易并将其添加到区块链时获得奖励。另一方面，根据用户持有货币的多少和时间（币龄）来决定发放的利息额度。

PoH（历史证明机制）：是Solana一个巧妙又实用性极高的创新，证明一个事件在特定的时间点上发生过。通过VDF（可验证延迟函数）为网络上的所有节点建立一个全局可用的时钟，有规范的顺序，不是区块生产者任意确定的顺序。Solana将基于哈希的时间链和状态分离，不是将每个区块的哈希链接在一起，而是网络中的验证者对区块内的哈希本身进行哈希，这种机制就是PoH（Proof of history）。

时间对于区块链技术至关重要，因为我们不能花没有收到的钱，也不能花已经花了的钱（避免双花问题）。传统的PoW（工作量证明机制），可以看成是一个大型去中心化的时钟，节点会将多笔交易打包成区块，并将区块分发给网络中的其他节点，当网络中所有节点都接受并更新了区块链，打包的交易就正式得到了确认。由于区块中存在时间戳，每更新一次区块，这个时钟就会“滴答”一次，时间也会全局更新一次。虽然这种机制十分安全，但等待节点确认以更新全局状态需要消耗大量的时间。Solana有了全局可用的时钟，这样每个节点既有了时间概念，又可以了解网络上发生事件的先后顺序。这样就无需等待所有区块链节点同步更新数据和状态，整体的效率得到大幅提升。

## 2.2帐户机制及智能合约

Solana链属于无许可区块链，所以账户机制也是生成公钥和私钥，同时创建Solana钱包，即可正常参与验证、质押等。

Solana提供了一种不同于传统的基于EVM的区块链的智能合约模型。在传统的基于EVM的链中，合约代码和状态都存储在链上的合约。Solana中智能合约（或程序）是只读或无状态的，并且只包含程序逻辑。一旦部署后，智能合约就可以通过外部账户进行交互。Solana中与程序交互的账户会存储与程序交互相关的数据。这是Solana和基于EVM的智能合约之间的关键区别。以太坊上的账户与Solana上的账户不同，Solana账户可以存储数据（包括钱包信息），而以太坊账户并不存储数据。

## 2.3数据库、隐私保护、身份验证等

Solana链上的数据储存在节点上，去中心化的存储方式，确保了安全性。隐私保护、身份验证、质押交易等都是通过密钥对来实现的。并且Solana有一个质押者价格保障机制，一定程度上对散户虚拟资产提供了保障。

## 2.4现有技术文档及代码评价

除有关资讯外，暂查询不到Solana公链相关的技术文档。

关于Solana公链的代码解析，查询到一份相关资料，会上传到参考资料中，由于非计算机专业，对代码只有浅层次的理解，评价难度较大。Solana公链代码相对比于以太坊，明显多了一些时间戳代码的调用。

# 3.项目未来

## 3.1未来规划及激励机制

一、未来规划

为了延续APP的生命周期，STEPN未来会逐渐从游戏APP向运动APP转型，运动软件的生命周期和游戏是截然相反的，用户使用时间越长，则越不会离开。STEPN未来规划就是从一款游戏类Gamefi项目向Web 3.0运动APP转型，调整游戏属性和社交属性的权重，未来会吸引更多不怎么喜欢玩游戏、不会使用去中心化钱包的大量跑步爱好者。

二、激励机制

目前STEPN依然会维持现有的加密代币激励机制，根据NFT跑鞋的等级及运动量给予奖励。

## 3.2现有社区及应用评价

一、现有社区：

表1 关于STEPN近期用户总数变化图

图表, 直方图

描述已自动生成

截止到 2022-05-12，STEPN链上总统计用户高达423,296，总三月份开始该数据就呈现指数型函数增长，增速反而越来越快，新用户增长数峰值环比增长率达到每两周35%，但是该种局面在四月底到五月初打破，随着市场行情的变动，参与STEPN的每日新用户以有眼可见的速度减少，五月的第一周，新用户增长速率下降刚好也为35%左右。

二、应用评价：

现阶段项目口碑整体向好，一定程度上改变了一些玩家的生活作息，也搭建了自有的经济体系，不过依然存在漏洞：

* 赚钱效应会吸引更多投机者和打金工作室，加速游戏生命周期的终结
* 新玩家入局减缓可能会导致币价下跌，陷入死亡螺旋

## 3.3项目投资分析

不建议投资，项目依然存在较为严重的风险点：

一、反作弊机制不能保证长期有效

作为一款运动 APP，其需要的是真实用户而非投机者，但是赚钱效应势必会引来打金工作室或是部分投机用户通过各类作弊方式来进场，因此保证反作弊机制能够长期有效是该项目发展的关键因素，依赖于团队的开发能力。

二、新玩家的进场速率影响较大

如果STEPN的新用户进场速率变慢或者停滞，有可能会出现GST抛压过大币价下跌陷入死亡螺旋的情况。虽然就目前而言，STEPN内代币的产出和消耗保持着较为平衡的状态，GST目前的应用场景集中在游戏内的升级、合成宝石、加速开宝箱与繁殖的机制，而用户在回本后，其产出其实是大于消耗的。

或许STEPN不会带来什么暴富的机会，但STEPN至少可以说是一个能改变生活方式，带领大家进入Web 3.0的划时代产品。

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、如何选出记帐人、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）

* 交易者接入比特币网络便会生成随机的公钥和私钥；
* 实践中会对交易信息进行哈希，然后把私钥和交易信息的哈希值作为输入，通过一定的算法便可以生成签名；
* 交易信息会由节点向比特币网络进行广播，节点自动收取交易并被记录进区块，因为一个区块的产生时间是10分钟，所以所以10分钟内的一些交易会被打包，由矿工节点进行封装；
* 交易的输入金额会略微大于输出，多出来的便是给矿工的手续费，矿工会根据交易手续费的高低优先选择手续费较高的打包进区块；
* 区块中主要包括三个部分：上一个区块的哈希值、随机数、所有交易信息的梅克尔根值；
* 选择记账人类似于做一道数学题，打包好的区块头中会有随机数字段Nonce值，矿工只能通过穷举的方式来不断调整Nonce值，使得计算出来的哈希值小于某个固定值，最先满足要求的哈希值的矿工会被选为记账人并获得奖励，由于只能不断的穷举、哈希，考验各个节点的服务器算力；
* 由于固定值是系统提前确认好的，所以可以通过调节这个固定值来改变难度，这样就可以控制出块时间；
* 由于个人的服务器数量有限，算力也有限，能被选为记账人的几率很小，因此可以大家将算力集合到一起，形成矿池，增加挖到矿的几率，这样矿池中所有的服务器都可以拿到相应的收益分成；
* 因为区块链中的每个节点都可以参与记账，当两个节点几乎在同一时间挖到矿并同时发布区块，此时原本一条的区块链上就有可能出现软分叉；
* 中本聪为了应对交易垃圾邮件堵塞网络的威胁和潜在的分布式拒绝服务(DDoS)攻击，2010年将区块的大小限制在1MB以内；
* UTXO设计的目的主要就是为了对区块信息进行溯源，比特币规定每一笔新的交易的输入一定要是某笔交易未花费的输出，每一笔输入的时候也要有上一笔输出所对应的私钥进行签名，并且每个比特币的节点都会存储当前整个区块链上的UTXO，整个网络上的节点通过UTXO及签名算法来验证新交易的合法性。这样一来，节点不用追溯历史就能验证新交易的合法性。

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。

交易手续费太低，交易排序靠后，导致矿工迟迟没有把交易打包出块。可以采取以下措施：

一、等：等待时间不确定，也无法确认预期内一定能出块；

二、手动设置交易费用：导致高昂的经济成本，也无法确认多高的手续费可以达到怎样的预期效果；

三、选择流量低谷时进行交易：一定程度上可以提高出块几率和速率，但具体也无法确定；

四、重新发起一笔交易：万一之前的交易出块了，目前来讲是不可撤回的。

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。

以太坊的目标是搭建一个去中心化的应用平台，类似于苹果的APP Store，提供一个底层的架构给开发者，具有智能合约功能，可以进行各种各样区块链项目的开发。

区别于比特币的技术设计有以下几点：

一、以太坊支持基于solidity语言的智能合约，主要是为了解决现实生活中合同交易的痛点，智能合约是完全按照编程执行的应用程序，没有任何欺诈，审查，停机或第三方干扰的可能性；

二、实现了智能合约能落地执行的EVM（以太坊虚拟机），原因在于通过以太坊虚拟机，可以实现solidity这样的代码在区块链上的执行；

三、每一次合约或交易都会收取固定的gas（取决于代码的大小及复杂程度），维持以太坊基本的经济运行；

四、以太坊构建的是一个完整、开源的生态系统，比特币作为“货币”的意义更大一些，仅仅具备一些交易、储存价值的功能，这样就可以满足区块链项目开发的需求。

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。

一、运行原理

智能合约本质上是运行在以太坊上的一段代码，代码的逻辑定义了合约的内容，开发者可以自己编译智能合约或是“自治代理”，因为这种语言是“图灵完备”的，除了基本的转账、存储，还支持范围更广泛的计算指令集。

当满足时间或其他智能合约规定的条件时，代码会自动运行，执行指令。

二、生命周期

智能合约的生命周期大概包含以下几个环节：

（1）合约存储：创建一个合约账户，以太坊智能合约有两种类型的账户：外部个人账户和合约账户；

（2）合约创建：使用 solidity 等语言创建一份合约代码；

（3）合约部署：在账户空间中部署合约；

（4）合约执行：通过EVM在本地计算机上运行智能合约；

（5）合约升级：由于区块链上的代码是不可更改的，所以要实现升级，需要部署一个具有调用转发功能的合约，指向新的合约地址；

（6）合约销毁：合约发起者可以调用“自毁程序”即可销毁合约。

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”。

1. “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。