**上海大学“区块链”课程论文考试**

**Axie Infinity项目分析**

姓名：**张娜** 学号： **21726017**

**字数：4060**

**摘 要：**

区块链是一种带时间戳不可篡改的数据库，其最大的特点是去中心化，Axie Infinity便是基于区块链技术的游戏，是一款去中心化回合制策略游戏。Axie Infinity是以太坊上的热门游戏，允许玩家收集、繁殖、饲养、战斗和交易基于代币的生物，称为 Axies。目前它拥有14万Axies，每个Axie都有独特的特征，这些特征决定Axie在战场上的行为，每个Axie都是具有不同属性和优势的不可替代的代币 (NFT)。

本文通过对Axie Infinity创建过程的探索，分析了其经济模型、技术模型以及未来发展，旨在对区块链游戏有更加深入的研究。

**关键字：区块链游戏 去中心化 代币**

**论文评语：**

成绩： 任课教师：吴建刚

目 录

[目 录 1](#_Toc104494197)

[第一章 项目概况 1](#_Toc104494198)

[1.1 创始团队 1](#_Toc104494199)

[1.2 项目简介 1](#_Toc104494200)

[1.3 创意点 2](#_Toc104494201)

[第二章 经济模型 4](#_Toc104494202)

[2.1 代币 4](#_Toc104494203)

[2.2 PVE：人机对战 6](#_Toc104494204)

[2.3 PVP：网络对战 6](#_Toc104494205)

[第三章 技术模型 1](#_Toc104494206)

[3.1 加密货币 1](#_Toc104494207)

[3.2 Ronin侧链 1](#_Toc104494208)

[3.3 共识机制 2](#_Toc104494209)

[3.4 智能合约 3](#_Toc104494210)

[第四章 未来发展 4](#_Toc104494211)

[4.1 未来规划及激励机制 4](#_Toc104494212)

[4.2 现有社区即应用评价 4](#_Toc104494213)

[4.3 项目投资分析 4](#_Toc104494214)

[附1： 7](#_Toc104494215)

第一章 项目概况

## 创始团队

2017年12月，Sky Mavis创始人兼CEO Trung Thanh Nguyen想到了Axie Infinity的想法：如何把口袋妖怪玩法与NFT和云养猫结合起来？

Trung自2017年12月开始打造这款游戏。到了2018年1月份的时候，以太币价格达到了峰值1300美元，随后Tu Doan担任艺术总监和游戏策划。3月，Jeffrey加入负责游戏增长；5月份，Aleksander Leonard Larsen也进入公司担任COO；7月份，Andy Ho加入成为了CTO，最终形成了五人初创团队。

1. Trung Thanh Nguyen – CEO
2. Aleksander Leonard Larsen – COO
3. Tu Doan – 艺术总监及游戏设计
4. Andy Ho – CTO
5. Jeffrey Zirlin – 游戏增长

## 项目简介

1. Axie Infinity创建过程

2017年12月：概念形成-开发起步

2018年2月：初版Axie预售开启-售得900ETH

2018年3月：内部Axie- NFT市场发布

2018年5月：喂养游戏发布

2018年10月：战斗游戏发布

2019年1月：土地买卖开启-售得3200ETH

2019年5月：ETH 2层（僵尸网络）内部土地/商品- NFT市场发布

2019年12月：土地与Axie联合市场起步

2019年12月：社区alpha（纸牌战斗游戏） 发布

2020年5月：Mavis Hub发布

2020年5月：第一季度土地售罄-售得4600+ETH

2020年6月：Axie Infinity进入育碧创业实验室

2020年6月：Ronin侧链测试网

2020年8月：土地游戏性内部alpha

2021年2月：Ronin主网起步

2021年4月：Axies转移至Ronin

2021年5月：Ronin添加菲亚特入口匝道

2021年9月：AXS股票发行

2021年11月：Katana去中心化交易起步

1. 游戏操作流程

第一步，下载“OKEx链上钱包”和“Ronin Wallet”，分别在两个钱包插件内创建自己的链上钱包；RONIN钱包是Axie Infinity的官方钱包，是一款基于ERC20（以太坊主链）的侧链钱包，将ETH存入MetaMask钱包，再将MetaMask钱包中的ETH转入Axie Infinity的官方钱包Ronin；

第二步，在官方市场点击跨链桥，将OKEx链上钱包中的ETH跨链到Ronin Wallet并在市场中购买3只AXIE宠物；

第三步，通过宠物繁殖、PVP(玩家对战)、PVE(人机对战)以及完成日常任务获得SLP代币，再使用SLP喂养新的Axie；

最后，所有者可进行交换变现。AXS（Axie Infinity Shards）和SLP（Smooth Love Potion）目前都可以在大多数的去中心化交易平台（简称DEX，比如Uniswap）进行交易，然后换成现金用于日程开销。

## 创意点

1. Play to Earn

在Axie Infinity中，玩家可以通过做任务、PVE模式和PVP模式赚取SLP，Axie游戏中的物品均由NFT来进行标识，这些独特的加密令牌可以与数字内容衔接，每一个小Axie都有一个NFT代码。每一只Axie都非同质化且具有独特性。NFT赋予了买家对Axie的所有权（ownership）；玩家可以在NFT市场上用Axie NFT来换取真金白银，有的Axie NFT售价甚至超过了60万美元。

1. 土地销售

Lunacia在游戏中是Axie的家园，被划分成一块一块代币化的土地，土地所有者可以在土地上找到AXS代币。Lunacia包括90,601块土地，每一块土地都有NFT代码，玩家可自由交易。土地上可产出各种资源，这个资源对提升用户参与游戏的获得感及提升属性，如各种Axie 升级都，会大有帮助。

1. 游戏生态

区块链最大的特征是去中心化，这使得游戏开发商与玩家的关系发生了变化。游戏规则并不完全由开发商制定，开发商跟游戏玩家有可能形成一种共识，并形成一个社区。玩家会自发地去维护游戏的平衡性，帮助开发商获取用户，延长游戏的生命周期，共建整个社区。

第二章 经济模型

## 代币

2022年，魏丽婷等人提出非同质化代币应用场景，其中就包括区块链游戏与娱乐领域。在加密猫游戏之后，加密游戏领域井喷式活跃起来，体育游戏以及模拟经营类游戏都吸引了数量庞大的游戏爱好者和数字投资者。这些在以太坊上开发的游戏通过 EＲC-721 标准提供了具有创造性和可玩性的沉浸式社交平台，以其操作透明、去中心化、流动性稳定的独特产品属性，为参与者提供了真实数字所有权，这种游戏和数字资产的双重融合和体验，带来了虚拟游戏世界新的产业发展方向。[[1]](#footnote-1)

Axie Infinity便是区块链游戏之一，其使用的代币主要有三种：

1. ETH

ETH是整个游戏生态内和外部经济体系唯一的交互点。游戏之初，玩家需要使用ETH购买至少3个Axie；此外，成功卖出Axie的卖家将承担4.25%的ETH作为交易手续费。

1. SLP

SLP即Smooth Love Potion，玩家可以通过宠物繁殖、PVP(玩家对战)、PVE(人机对战)以及完成日常任务获得SLP代币。

表1 宠物繁殖过程及SLP消耗数量



1. AXS

AXS即Axie Infinity Shards，是游戏平台发行的治理代币，是Axie游戏系统的ERC20代币（即可替代Token），供应总量27,000万，主要有Staking、治理和支付三种使用场景。AXS 持有者可以通过玩游戏、参与关键的治理投票来赚取 AXS 代币。



图1 AXS使用场景

## PVE：人机对战

PVE模式中玩家的宠物根据成功通过的关卡而获得经验值，随着经验值的增加玩家的宠物会在PVE模式中增强，增强后的宠物更容易通过更高等级的关卡，同时也能更快拿到更多的PVE奖励，从而更有效率地完成PVE每日指定的任务上限。

## PVP：网络对战

游戏内每个月进行一次赛季，玩家将自动参与游戏赛季。同时，根据玩家战斗的胜利次数进行排名，每个赛季的前1000名官方会给与AXS代币奖励。

第三章 技术模型

## 加密货币

2020年，曾诗钦等人提出：加密货币（cryptocurrency）是一类数字货币（digital currency）技术，它利用多种密码学方法处理货币数据，保证用户的匿名性、价值的有效性；利用可信设施发放和核对货币数据，保证货币数量的可控性、资产记录的可审核性，从而使货币数据成为具备流通属性的价值交换媒介，同时保护使用者的隐私。[[2]](#footnote-2)

Axie Infinity 使用的是双通证结构，有两种支付系统，一种为玩家奖励SLP，另一种为AXS。AXS 作为 Axie Infinity 协议的治理代币，还充当从 Axie 市场购买游戏内不可替代代币(NFT) 的法定货币。与治理代币AXS不同，SLP是通过游戏玩法铸造的，是通过战斗或冒险模式对玩家的激励或奖励。目前，币安交易所已经上线了SLP的出售功能，玩家可以将SLP从Ronin侧链转移到币安交易所，再把SLP兑换为法定货币。

## Ronin侧链

2013 年 5 月，NoLan 在 BitcoinTalk 论坛提出了原子转移( atomic transfers) [[3]](#footnote-3)思路，是实现原子式跨链数字资产交易的最初基础技术方案。比特币核心开发者加入的Blockstream 公司于 2014 年 10 月发布的白皮书中提出了楔入式侧链( pegged side chains) [[4]](#footnote-4)的概念，目的是实现不同区块链资产的跨链转移及在不影响主链的情况下实施更多的技术创新。

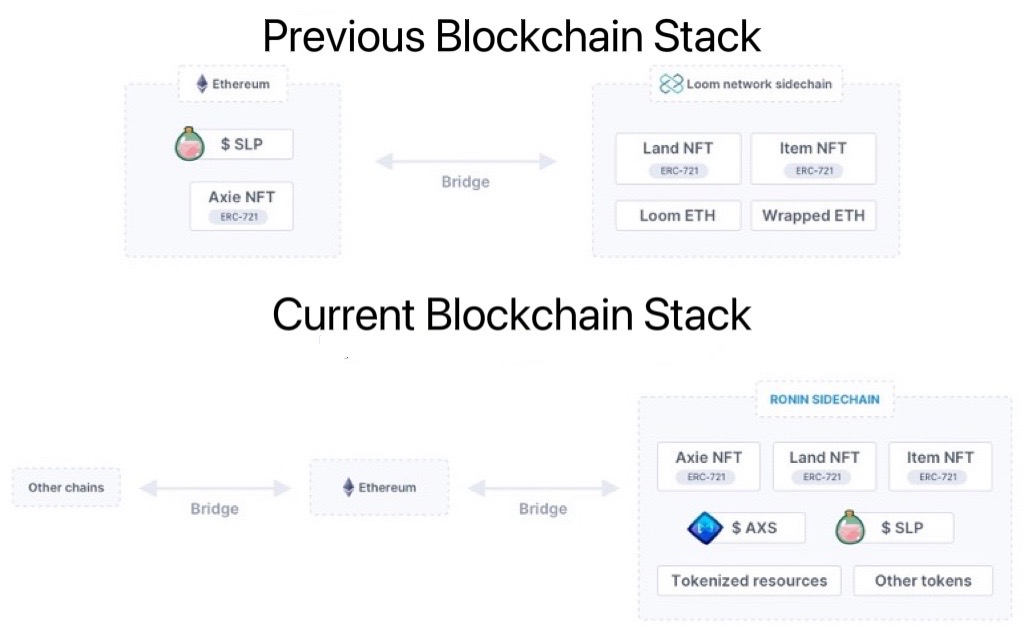
为了使参与 Axie 游戏和经济体系变得快速且顺畅，Sky Mavis创建了Ronin侧链。目前的Axie游戏已经转移到了Ronin侧链上，玩家需要同时拥有Ronin钱包和以太坊钱包。设置了Ronin钱包之后，可以使用Ronin桥将ETH转移到Ronin上，等ETH变成加密状态（Wrapped ETH），就可以用它来购买Axie NFT。

图2 Axie Infinity区块链栈

## 共识机制

2020年，王群等人提出：共识机制是分布式系统中实现去中心化信任的核心，它通过在互不信任的节点之间建立一套共同遵守的预设规则，实现节点之间的协作与配合，最终达到不同节点数据的一致性。[[5]](#footnote-5)

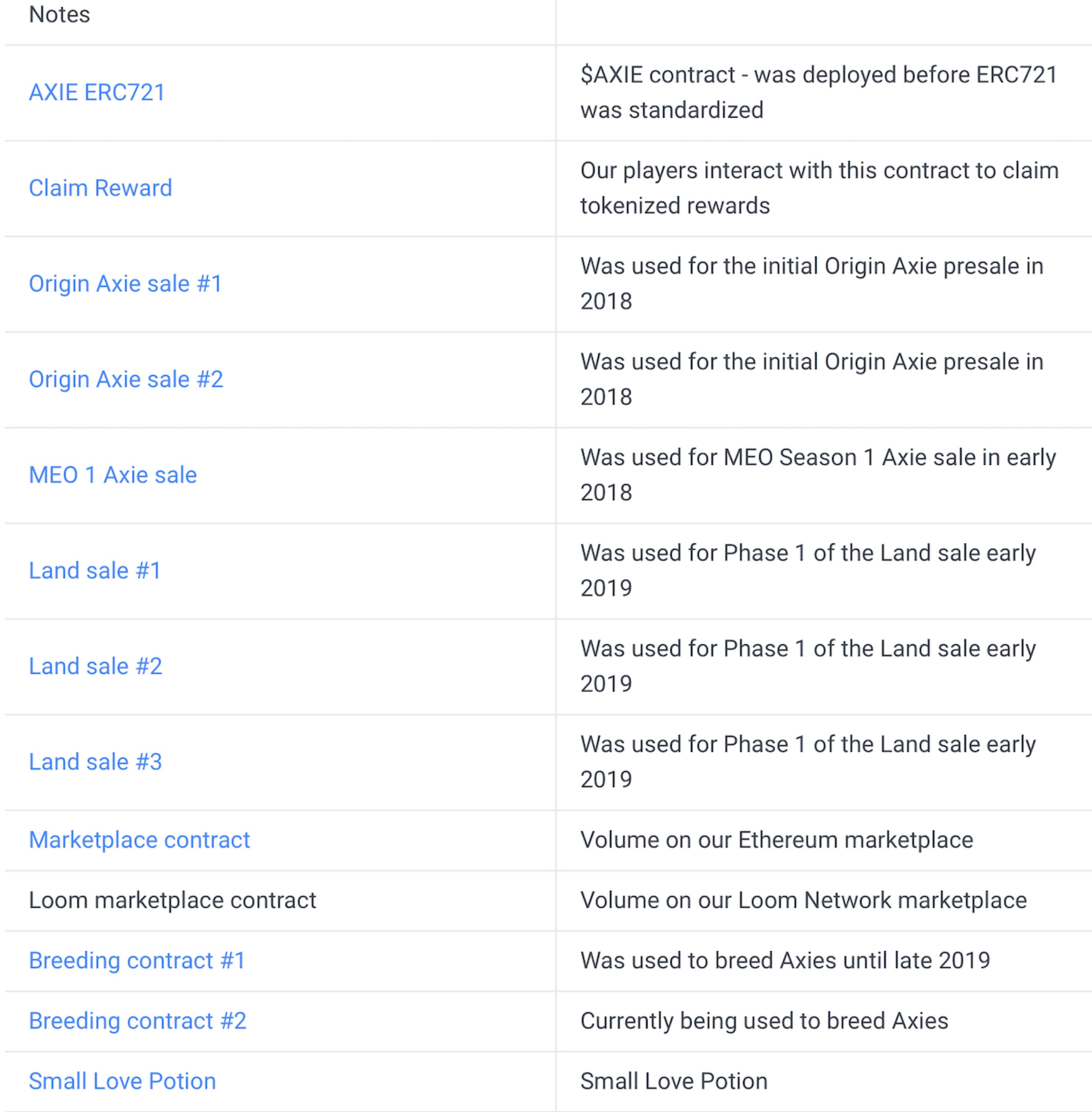
Axie Infinity使用的是 PoA (Proof of Authority) 的共识机制。换言之，他采用了更少的验证节点（目前是 7 个），获得了更快的转账速度。目前 Ronin 网络的验证节点包括：Binance、育碧（Ubisoft）和 Animoca。每当有了交易，大家不再互相发了，而是统一发送到 Authority 手中，由它来验证交易。POA 网络中的 validator 验证人，就是大家选举出来的 Authority。Validator 验证并签署交易之后，普通节点都从 validator 那里同步数据。

## 智能合约

智能合约是部署在区块链上的可执行代码，可不依赖中心机构自动化地代表各签署方执行合约。在金融区块链中，智能合约可以被认为是一种系统，一旦预先定义的规则得到满足，它就向所有或部分相关方发布数字资产。[[6]](#footnote-6)

在Axie Infinity中，一方放入游戏资产，该游戏资产存储在智能合约中，其他人就可以从智能合约中购买它。双方都能够无信任地获得想要的东西。

表2 Axie Infinity智能合约



第四章 未来发展

## 未来规划及激励机制

Axie Infinity在打造自己的世界Lunacia，并于2019年开始拍卖“土地”，同年将Axie Infinity和土地市场合并。土地游戏将为 Axie Infinity游戏添加一个新可玩性和变现维度。

Axie Infinity中有三种代币：ETH、SLP、AXS。玩家玩游戏通过赚取代币令牌获得奖励，通过PVP和PVE模式赢得比赛，通过游戏赚取Token。开发者可通过赚取代币获得奖励，赌注者通过赚取代币来获得奖励。

## 现有社区即应用评价

Axie Infinity是一款新型游戏，用户和核心开发团队都聚集在这里，为其发展共同努力。Axie拥有76万成员Discord服务器，被认为是NFT游戏中最大最强的社区，社区共建是Axie Infinity生态系统的原则，这将成为促进价值增长的根本性动力。2022年1月，第一个Axie创建者项目正式发布。

目前Sky Mavis只拥有Axie infinity的20%，其他80%左右归他们的社区所有。在这种模式下，用户是所有者，当用户是所有者时，他们会进行自主营销，并在产品之上构建事物。它是去中心化的，不仅仅是人们谈论数据存储的去中心化，而且也适用于项目的所有权。

## 项目投资分析

作为区块链游戏，Axie Infinity有一定的投资价值：

首先，在疫情背景之下，网络游戏成为了最火热的娱乐项目之一，Axie Infinity作为区块链游戏又具有其独特的优势，用户数量不断增加；

其次，作为区块链游戏，其业务本身是数字化的；游戏中的NFT代币，拥有较强的实用性和纪念属性，对于年轻的受众群体非常有吸引力；

再次，区块链游戏最大的特点是去中心化，用户是所有者，不仅可以玩游戏，还可以参与社区的建设和游戏的构建；

最后，目前Axie Infinity已转移到专属以太坊侧链 Ronin，由于 Ronin 的 Gas 费用与以太坊相比可以忽略不计，使得更多用户更容易进行繁殖，从而推动了Axie数量、繁殖费用和市场成交额的增长。

参考文献

【1】魏丽婷,郭艳 ,贺梦蛟.非同质化代币(NFT):逻辑、应用与趋势展望[J].经济研究参考,2022(04)

【2】曾诗钦,霍如,黄韬,刘江,汪硕,冯伟.区块链技术研究综述：原理、进展与应用[J].通信学报,2020,41(01):134-151.

【3】SCHULTE S，SIGWAＲT M，FＲAUENTHALEＲ P，et al． Towards blockchain interoperability ［C ］/ /International conference on business process management． Vienna， Austria: Springer，2019: 3－10．

【4】BACK A，MAXWELL G，COＲALLOM，et al．Transferring ledger assets between blockchains via pegged sidechains: U.S．10812274［P］．2020－10－20．

【5】王群,李馥娟,倪雪莉,夏玲玲,王振力,梁广俊.区块链共识算法及应用研究[J/OL].计算机科学与探索:1-34[2022-05-28]

【6】BUTERIN V. A Next-generation Smart Contract and Decentralized Application Platform[EB/OL]. https://github.com/ethereum/wiki/wiki/White-Paper, 2018-5-11.

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）
2. 发起者通过自己的钱包软件创建一笔包含一定数量比特币的交易输出，并用自己的私钥进行加密签名。
3. 接收者的公开地址就是其公钥的哈希值，发起者在转账的时候，用接收者的公钥对交易进行加密等操作，以此保证这笔交易只有接收者才能验证，从而使得比特币可以安全地转到接收者的钱包中。
4. 发起者创建的交易输出包含一段程序代码，谁能拿出一个签名和接收者的公开地址匹配上，就支付给谁。
5. 未经使用的一个交易输出，简称UTXO，每一笔账单就是一个UTXO。被交易消耗的UTXO被称为交易输入，由交易创建的UTXO被称为交易输出。
6. 发起人的这笔交易将被广播到整个比特币网络中。挖矿即对交易数据的打包和确认。首先根据区块的数据结构，将交易打包进区块，再采用 Merkle Tree 算法生成区块体中所有交易的Merkle Root（哈希值），然后根据区块头部的元数据，采用相应的共识算法（如 PoW、PoS 等）获取新区块的记账权。
7. 矿工将生成的新区块广播到区块链网络中，任意一个节点在接收到新区块后，对其进行验证，验证通过后将该区块链接到本地区块链上。同时，不同的区块链系统还将采用相应的算法防止分叉的产生，维护主链的唯一性和稳定性。
8. 发起者的钱包软件会用一段程序将交易输出锁定到接收者的地址上，同时还会在交易输入上绑定一段解锁的程序。当一笔比特币交易被发送到任意一个连接至比特币网络的节点，这笔交易就会被该节点独立验证。如果交易被验证有效，该节点会将这笔交易传播到这个节点所连接的其他节点。如果被验证为无效，这个节点会拒绝接受这笔交易。
9. 如果接收者的钱包软件完成了验证，这些UTXO便属于接收者了。
10. 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。
11. 原因：算力不足，网络拥堵
12. 措施及后果
13. 提高交易费：可能导致交易费不断攀升
14. 扩容：成本高、消耗大
15. 替代交易平台：成本高

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。

目标：

1. 可持续性
2. 安全性
3. 去中心化
4. 强韧性
5. 安全性
6. 简洁性
7. 持久性

不同技术设计：

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 平台 | 共识机制 | 状态 | 合约模式 | 交易 | 执行环境 | 出块时间 | 账户设计 |
| 比特币 | 工作量证明 | 未花输出 | 纯函数 | 支付 | 内置脚本 | 10分钟 | UTXO |
| 以太坊 | 工作量/权益 | 账户 | 图灵完备 | 智能合约 | EVM | 15秒 | 余额 |

原因：

1. 比特币出块时间长；
2. 工作量证明过于昂贵和浪费；
3. 比特币支付系统缺乏扩增能力；
4. 余额机制更加直观：每个账户有一个状态，状态中直接记录了账户当前的余额，转账的逻辑就是从一个账户中减去一部分余额，并在另一个账户中加上相应的余额，减去的部分和加上的部分必须相等；
5. 以太坊构建了较完整的、开源的生态系统。

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。

运行原理：

1. 创建与运行：智能合约运行在EVM（Ethereum Virtual Machine）上，以太坊是一个交易驱动的状态机，调用智能合约的交易发布到区块链上后，每个矿工都会执行这个交易，从当前状态确定性地转移到下一个状态。
2. 汽油费：以太坊中使用汽油费机制，防止出现死循环。合约中的指令在执行时要收取汽油费，由发起交易的人来支付。
3. 错误处理：智能合约的执行具有原子性，一旦遇到异常，除特殊情况外，执行操作全部回滚，不会只执行一部分。智能合约中不存在自定义的try-catch结构，不可以捕获异常。
4. 嵌套调用：嵌套调用是指一个合约调用另一个合约中的函数。如果被调用的合约执行过程中发生异常，有些调用方法会导致发起调用的这个合约也跟着一起回滚，而call()函数调用则不会连环回滚，只会使得当前调用失败，得到false返回值。

生命周期：

1. 开发：开发人员使用不同的高级语言来编写智能合约
2. 编译：将各种高级语言编写的智能合约源代码编译为能够在以太坊虚拟机上运行的字节码（bytecode），同时生成相应的合约调用接口ABI，该接口定义了合约所有可以被调用的外部函数和参数列表。
3. 部署：编译之后的智能合约字节码需要被部署在以太坊区块链平台中。合约的部署通常由一笔合约部署交易来完成, 其中交易的数据字段将被设置为合约部署字节码, 而交易的接收方被设置为空。矿工在进行交易打包时, 将会按照交易发送者的地址和交易序列号信息来生成一个新的地址, 并将合约的字节码部署到该地址。这个新生成的地址就是合约地址, 是合约的唯一识别, 之后对于该合约的所有操作都将使用这个地址进行。
4. 调用

a.交易调用，由普通账户发起一笔合约调用交易。

b.消息调用，由某个合约发起对另一个合约中函数的调用，合约之间的调用参数不会留在区块链数据中。

1. 销毁：以太坊允许合约进行“自我销毁”, 不过并不是所有的合约都可以销毁, 而是需要开发者在进行合约编写时加入该功能。

1. [1]魏丽婷,郭艳 ,贺梦蛟.非同质化代币(NFT):逻辑、应用与趋势展望[J].经济研究参考,2022(04) [↑](#footnote-ref-1)
2. [1]曾诗钦,霍如,黄韬,刘江,汪硕,冯伟.区块链技术研究综述：原理、进展与应用[J].通信学报,2020,41(01):134-151. [↑](#footnote-ref-2)
3. SCHULTE S，SIGWAＲT M，FＲAUENTHALEＲ P，et al． Towards blockchain interoperability ［C ］/ /International conference on business process management． Vienna， Austria: Springer，2019: 3－10． [↑](#footnote-ref-3)
4. BACK A，MAXWELL G，COＲALLO M，et al．Transferring ledger assets between blockchains via pegged sidechains: U.S．，10812274［P］．2020－10－20． [↑](#footnote-ref-4)
5. [1]王群,李馥娟,倪雪莉,夏玲玲,王振力,梁广俊.区块链共识算法及应用研究[J/OL].计算机科学与探索:1-34[2022-05-28] [↑](#footnote-ref-5)
6. [1] BUTERIN V. A Next-generation Smart Contract and Decentralized Application Platform[EB/OL]. https://github.com/ethereum/wiki/wiki/White-Paper, 2018-5-11. [↑](#footnote-ref-6)