

PiGMC 白皮书

全球化的区块链社群应用

PiGMC 基金会

二〇一八年七月

C 目录 Contents

| | |
|--------------------|----|
| 第一章 项目背景..... | 1 |
| 一、 行业背景..... | 1 |
| 二、 市场痛点..... | 4 |
| 三、 解决思路..... | 5 |
| 第二章 项目阐述..... | 8 |
| 一、 项目应用..... | 8 |
| 二、 应用内容..... | 9 |
| 第三章 技术实现..... | 17 |
| 一、 技术架构..... | 17 |
| 二、 网络节点架构..... | 20 |
| 三、 技术特色与优势..... | 22 |
| 第四章 治理结构..... | 26 |
| 第五章 发行说明..... | 27 |
| 第六章 团队介绍..... | 29 |
| 第七章 风险提示及免责说明..... | 31 |

第一章 项目背景

一、 行业背景

(一) 游戏市场

市场分析公司 Newzoo 发布了最新的《全球游戏市场报告》，数据显示，2017 年全球游戏业收入规模达到 1089 亿美元，这意味着比 2016 年增长了 7.8%，其中数字游戏收入为 944 亿美元，占全球市场总规模的 87%。手游是最大的部分，智能机和平板游戏收入将同比增长 19%至 461 亿美元，占市场总收入的 42%。到 2020 年，该公司预计手游收入将占全球游戏市场总规模的一半以上。

亚太地区是全球最大的游戏市场，中国地区的游戏业收入将达到 275 亿美元(折合人民币 1890 亿元)，占全球市场规模的四分之一。Newzoo 预计全球游戏市场未来将继续保持 6.2%以上的年复合增长率，到 2020 年达到 1285 亿美元。基于对全球 70 多家上市公司的最终财报结果统计，Newzoo 表示 2017 年全球游戏市场总规模为 1089 亿美元，手游表现比预期更好，尤其是中国区，不过该地区的 PC 游戏收入低于此前的预测。

【手游市场】：2017 年全球手游市场达到 461 亿美元规模，同比增幅 42%。其中四分之三以上，也就是 353 亿美元都是来自于智能机游戏收入，平板游戏收入占 108 亿美元。过去几年来平板设备的销量一直在下滑，但仍有 2.8 亿活跃用户，这部分收入对于手游整体规模的贡献是不容忽视的。

【主机游戏市场】：随着主机制造商、发行商和消费者们越来越倾向于不同形式的数字业务模式，主机游戏的收入表现也好于 2016 年。微软和索尼两家公司

从自研游戏、第三方游戏分成和付费订阅收入模式获得的收入超过了 140 亿美元。在 2017 年, Newzoo 测算全球主机游戏收入达到 335 亿美元, 其中 65.8% 都来自数字游戏。

【PC 游戏市场】: 全球 PC 游戏收入在未来几年都将持续出现轻微下滑, 由于休闲游戏转向了移动设备, 网页游戏收入自从 2015 年就已经出现了下滑。在 2016 年, Facebook 从游戏当中获得的收入达到了 2011 年以来的最低点, Zynga 的 PC 游戏收入同比下滑了 30% 以上。Newzoo 测算全球页游市场规模在 2017 年降低到 45 亿美元, 同比降幅 9.3%。

PC 游戏的下滑主要是欧美和亚洲市场去年出现了下降, 而新兴市场则出现了比较低的增长, 由于 2017 年的表现比预期更差, Newzoo 调整了对该市场的长期预测, 目前该公司预计全球 PC 游戏市场收入将在 2019 年达到 245 亿美元, 比之前的 290 亿美元预期有了很大幅度的降低。。

(二) 网络社群市场

根据 iiMedia Research(艾媒咨询)发布的《2017 年全球移动社交市场研究报告》中的数据显示: 2012—2016 年全球总人口规模及使用网络人口比例呈稳步上升状态, 2016 年世界总人口达 74.4 亿人, 其中使用网络的人口占比达 45.9%。世界人口稳步增长, 互联网渗透率也逐年提升, 互联网浪潮在全球范围的蔓延, 为人们使用社交网络提供条件, 满足人与人之间交流和情感表达的需求。

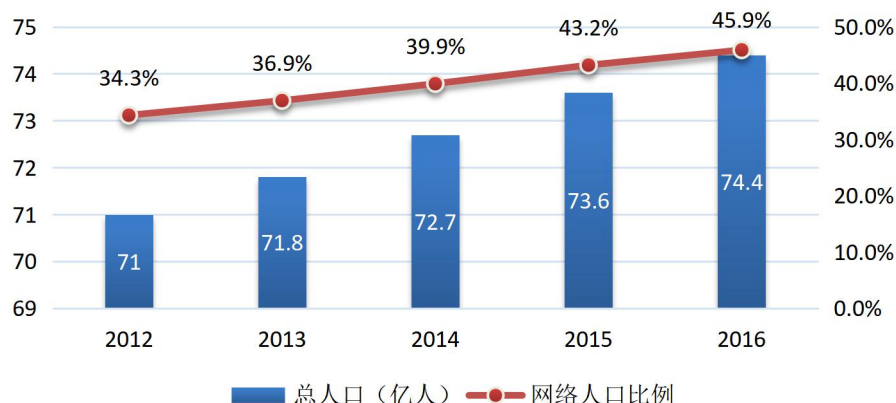


图 1-1：2012-2016 全球总人口和网络人口比例

数据显示：2017 上半年 Facebook 活跃用户达 21.0 亿人，位于各社交软件之首，而同属 Facebook 系的社交产品 WhatsApp、Messenger 则分列二、三位。中国互联网巨头腾讯旗下社交软件微信、QQ 则分别以 9.6 亿及 8.8 亿活跃用户位列四、五位。

网络社交的快速发展，带动了网络社群经济的同步提升，广义的网络社群是指随着互联网的出现而实现的用户基于网络平台的聚合与交流。互联网的出现是网络社群产生的基础，网络交往平台的更迭、社群成员需求变化、新的商业模式，三者共同推动网络社群发展，可以大致分为三个阶段。

- 社交阶段：以熟人社交为主，是现实交往的延伸，主要交流内容是信息传递和情感交流；
- 社区阶段：以陌生人社交为主，交流平台一般都是社区型的平台，主要交流内容变成基于共同兴趣的内容，工具性更强；
- 社群阶段：以信任感社交为主，以某一个共同点链接一切，通过标签聚合用户，社交内容更加精细化；

人和内容是网络社群形成发展并产生商业价值的两个要素，社群长期健康发展的核心是信任感。



图 1-1：社群信任感构成

二、 市场痛点

社群市场虽然发展十分迅猛，但是在传统的技术架构下，也暴露了很多痛点问题，包括：

（一） 用户隐私泄露

目前的社群平台都是中心化结构，用户的数据都存放在网站的服务器上，一旦服务器遇到问题或被人恶意使用，用户的信息就会被大量泄露（Facebook 泄露用户信息事件就是一个典型的例子）。

（二） 内容版权无法保护

社群中有大量用户自制内容，很多都是优秀的文化作品，比如歌曲、小说、音乐等，但在目前的互联网大环境下，这些文化作品盗版相对容易，盗版情况十分严重，而且侵权人的盗版惩罚成本很低，更进一步加剧了盗版的情况。

（三） 中心化架构

目前大多数社群虽然号称是自组织结构，但实际上基本都是由中心化架构来主导的，都有主导者和管理者（比如百度贴吧的吧主），而且权力极大，用户的

知情权和管理权都受到了极大的制约，导致内部腐败情况层出不穷。

（四） 缺少横向联系

大多数社群是基于共同兴趣和信任感而建立的，其内部一般比较稳定，交流比较频繁。但是社群之间往往缺乏横向联系，资源整合和规模效应的优势完全没有发挥出来。很多用户只能在相互隔绝的社群中来回切换，完全无法体验到互联网的便捷性。

现在全球以每天新增加 3-5 个区块链机构的速度在发展，区块链用户的增长速度、区块链社群建设和运营严重滞后于区块链机构的发展速度。 区块链社群建设已成为各个区块链机构和社群用户共同面临的最重要和最棘手问题。 目前大多数区块链机构和社群用户都在基于 Telegram、Twitter、Reddit 、Facebook、微信、微博、论坛等来建设社群，各平台存在的局限性和单一性已远远不能满足日趋发展迅猛的区块链生态对社群载体的需求。未来的区块链发展需要更好的社群生态，社群生态的建设需要更全面的解决方案。

三、 解决思路

上述的问题看起来牵涉到各个方面，似乎纷繁复杂，难以解决，但是我们究其根本就可以看到，问题的根源在于：中心化结构带来的低效和行业不透明。在中心化的组织架构下，点对点的交易难以进行，交易的效率比较低。而且中心化组织缺乏外部的监督，必然会不断膨胀，获取最大化的利益，不断侵害（无论是主观还是客观）用户的利益。

想要解决这些问题，就必须打破中心化的结构，让交易主体直接对接，提高效率，并提高行业的透明度。但是这样以来又会带来更为严重的问题——在没有中心组织的制约下，人类的现有技术条件难以维持交易互信。交易互信的问题

从人类诞生以来就伴随着社会的发展而一直存在，人类为了实现交易互信建立了大量法律和技术方面的约束条件，却一直无法杜绝交易欺诈的现象。而去中心化或弱中心化会让交易更加混乱——这就把通过传统的技术力量或模式改造解决问题的道路堵死了。所以需要我们引入新的技术概念——区块链。

区块链是一种按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构，并以密码学方式保证的不可篡改和不可伪造的分布式账本。它具备去中心、安全性、信息透明、智能合约等特点，对于解决当前社群行业的问题有决定性的意义。因此，我们认为区块链社群将是未来社群经济的主流方向。区块链和社群的完美结合，将表现在以下一些方面：

(1) 去中心化，将数据知情权和经济支配权从集中的组织者还给用户

一方面，没有中心服务器的好处在于广大社群用户群体对数据的知情权是相同的，保证了社群足够的信任感。另一方面，区块链技术去中心化的特性也能将社群内经济的支配权从集中的组织者还给广大的用户，让用户的自组织权力发挥到最大限度。

(2) 安全系数极高，隐私泄露情况无处遁形

区块链技术是一种分布式记账方式，所有人都可参与记账，且所有人都会拿到一本完全相同的账本，这意味着所有的数据都是公开透明的，每一个人可以看到每一个账户上到底有什么数据变化，而且，其中的所有数据都几乎无法被修改，这意味着它非常安全，任何玩家想要搞什么小动作都会永久记录在案。区块链只会在一种情况下不安全：某人或某个组织篡改了该区块链 50% 以上的数据。但是联系到现实，一个成规模的区块链的节点数往往数以万计，且各节点分布不均，想要篡改难如登天，在这种安全机制下，隐私泄露情况一旦出现将会被立即发现。

(3) 重塑信用体系：由信任人到信任机器

有了智能合约，玩家可以利用区块链创作社群内容。信任不再是问题，因为区块链系统是去中心化的，创作内容直接存储在区块链上，任何人都可以看到，用户创作的内容一旦发布会自动确权。任何关于内容的交易都要通过智能合约来进行，用户创作内容的版权可以得到充分的保障。

(4) 保障社群内容的虚拟价值

在现有的社群框架体系中，用户的虚拟财产随时可能失去。归根结底的原因在于：社群平台管理数字虚拟财产的载体是自家服务器，服务器的存在对玩家产生了制约——玩家所拥有的只是虚拟财产的使用权，而非所有权。针对这问题，区块链提出了完美的解决方案，区块链协议的不可破坏性使得链上的财产权明确，不会因为社群平台服务器的停止运营而凭空消失。

【结语】：

一个新事物的出现，褒贬不一是难免的，但我们更应看到的是区块链存在的积极意义，不能固步自封。社群在区块链领域中，拥有非常特殊的先锋地位，原因在于社群领域的试错成本低。完全的去中心化、去人为干预化，一旦出现危机，谁也掌控不了，后果是不堪设想的。但是社群作为一种虚拟空间，无论成败，对现实的都不会产生直接的影响，且社群本身就是对现实的模拟，我们可以将社群作为区块链大规模应用的试点，以图找寻一种最佳的区块链运用模式，从而造福社会。

第二章 项目阐述

一、项目应用

根据上述的思路，PiGMC 团队基于区块链技术开发了一系列 DAPP 生态，项目以游戏社群为切入点，逐步建设一个全球化的多元社群生态体系。为何以游戏社群为切入点呢？以中国市场为例，目前中国网络社群用户中，有 43.2% 的用户参与过游戏社群，仅次于明星社群，由此可见，游戏爱好者在社群参与方面有较强的行动力，而且从商业价值来看，游戏社群的变现也是较为容易的，游戏社群的规模化和盈利前景在整个社群经济中都是比较看好的。因此，PiGMC 以游戏社群为切入点，逐步打开区块链社群的市场。

PiGMC 将以加密社交聊天工具为基础工具，以实现完全去中心化社群的价值为导向，让用户可以放心地在社群中交流，不用担心隐私被泄露，每个人都自主地参与到社群的管理和运营中，社群的信息和数据完全公开透明，用户自创的内容也将具备全网唯一的版权，内容盗版将被杜绝。PiGMC 将让各类社群具备内在的价值，实现入口——粘性——价值——吸引更多流量的良性循环。

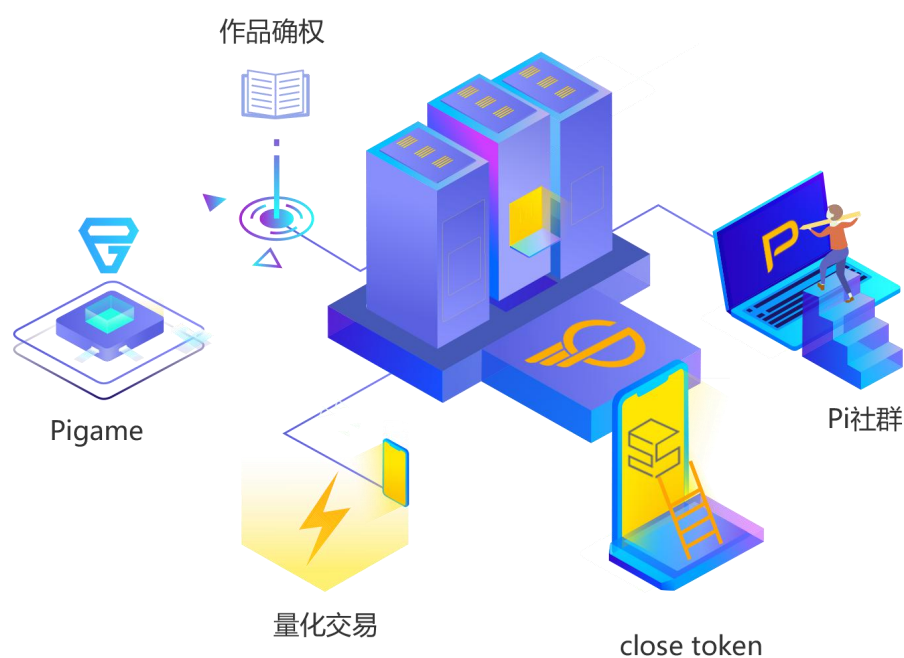


图 2-1：项目应用

二、应用内容

(一) Pi 社群

自 2008 年一个化名为中本聪的神秘密码学极客发布了比特币的白皮书，比特币的出现标志着区块链 1.0 时代的开启。比特币作为区块链的第一个应用，为区块链的发展奠定了坚实的基础。以太坊开创的智能合约技术，把区块链带入了 2.0 时代，使得区块链技术在更广泛的领域得到了应用。随着区块链技术的不断研发创新，我们相信不久的将来区块链技术将改变我们的生活，“区块链+”将是继“互联网+”之后又一个技术引领时代的领域。伴随区块链技术的发展，区块链知识也得到了不断地普及，越来越多的人开始关注区块链，了解区块链，参与区块链。区块链作为一个新生事物，用户基数和互联网用户相比而言存在着巨大的差距。个人如何参与区块链，如何培养更多的区块链用户，区块链机构如何获得用户的关注，于是“社群”这个传统的概念慢慢在区块链生态中被越来越

越多的人提及和重视，社群建设也开始成为各区块链机构兵家必争之地。

PiGMC 中的社交 DAPP 应用 Pi 社群，通过应用区块链技术的底层加密算法为通讯信息进行加密，以从未被破解的区块链加密算法为支撑，确保信息无法破译，只有通信双方能够解密通讯内容。加密用的私钥由用户自己使用的客户端生成，除了用户自己其他人无法获知。

通过点对点的信息传送，确保信号不被中间服务商（即使社群 DAPP 也不能）截留破解。由私钥生成的通讯地址，在客户端显示的只是一串唯一的字符代码，用于识别不同用户的通讯地址，而不记载任何的用户信息，因此不会泄露或绑定联系人身份。

用户的历史聊天记录经过私钥加密保存在本地，可以将之移动至其他地方存储。如果用户私钥被窃取，除非黑客知道聊天记录的保存地址，或可以复制调用聊天记录，否则不会泄露用户任何历史信息。

在社群建设和管理工具应用体验层面，Pi 社群的设计思路是，底层利用区块链去中心化账本记录社群的权属信息、AOD 贡献度激励算法信息 以及任务信息，用智能合约解决社群贡献度激励和任务奖励问题，保障社群生态经济的公开透明。而应用层则采用高效的多中心开发架构，充分保证各种读写操作的高性能，有效避免了区块链目前交易合约确认时间长、费用高、易拥堵等问题，最大程度保证社群产品的流畅互动体验。社群建设和运营工具已经在开发和未来陆续开发的功能有：创建社群功能、投票功能、直播学习、手机挖矿、任务发布、日常任务、资产钱包、资讯发布、游戏等。

社群生态架构：

在 Pi 社群生态架构中有 3 种角色：个人、社群、区块链机构

个人：

区块链和数字货币用户，可以加入或创建社群。每个ID且只能创建一个社群。

社群：

社群是PiGmc生态中的基层组织单位，简单理解就是每个群。我们把社群的创建者成为社群节点人，也叫管理员。管理员将有共同的需求和爱好者聚集在一起，通过高效的即时通讯群组形式的载体实现。组织社群的成员在即时通讯群组中互动。社群的管理员可以选择入驻某个生态社群，其社群成员在生态内产生贡献或完成任务获取PiGmc Token奖励时，社群的群主也相应会得到PiGmc Token奖励。

区块链机构：

生态社群是PiGmc生态的核心结构，由若干个小社群组成，多个小社群达成共识就可以申请成立生态社群，由投票决定是否成立。通过Timeline、直播学习、互动交流、任务中心等工具组成的载体实现。社群创建人可以去任务中心领取由区块链机构发布的任务，将社群内的注意力和活跃度价值转化为完成任务的价值，通过获取任务奖励分成而获利。社群创建者可以在社群广告栏中添加广告，为优质区块链项目提供路演机会，从而通过流量变现和生态消费实现商业回报。

区块链机构发布任务需要预先储备一定的PiGmc Token,设置社群贡献度奖励项目和参数，通过AOD算法（全称：Algorithm of Devote，中文：贡献度算法）计算社群成员的贡献度，并使用智能合约，奖励PiGmc Token激励社群成员对社群做出贡献，从而促进自我社群的壮大并提升与社群用户粘性和活跃度。社群奖励池系统 每24小时进行一次激励分配计算，并根据计算结果，将奖励PiGmc Token自动分发到社群成员及其做隶属的社群节点人的个人钱包中。

（二）Close Token

Close Token 钱包分为物理冷钱包和在线轻钱包两个应用。物理冷钱包无 WIFI、无 SIM 卡，内置安全系统可生成各种钱包地址和私钥。Close Token 轻钱包负责与外网通信建立信道打造点对点资产转出、转入，并加入余额宝、媒体等功能。物理冷钱包与轻钱包之间通过二维码实现加密离线支付。Close Token 钱包绝非简单的数字资产存储和交易工具，它最重要的作用在于支付，把加密数字资产和实际经济的通道打通。Close Token 钱包设计和实现了闪付系统，并联合商家的企业社群成立线下支付场景，使得社群用户可以快速安全地使用数字资产进行支付。Close Token 钱包将应用于全球贸易、消费、金融、游戏、旅游等领域的支付，依托区块链的技术特点为全球的商家、消费者提供快速便捷的结算支付及相关服务。

（三）作品确权

社群用户中创作者可以通过 DAPP 应用中独有区块链技术进行确权，用户在作品出炉的第一时间，上传自己的作品。由于每个区块会加盖时间戳，且数据全网开放可查询，这样就可以对作品进行全球的公证。免除了需要向不同国家递交不同资料的繁琐流程，降低了创作者登记版权的经济成本与时间成本。经过确权公证的 IP 可以在 PiGMC 上自由交易，用户使用 PiGMC 发行的数字资产进行 IP 的购买，交易过程透明公证，PiGMC 全程跟踪，保证交易过程的保护。

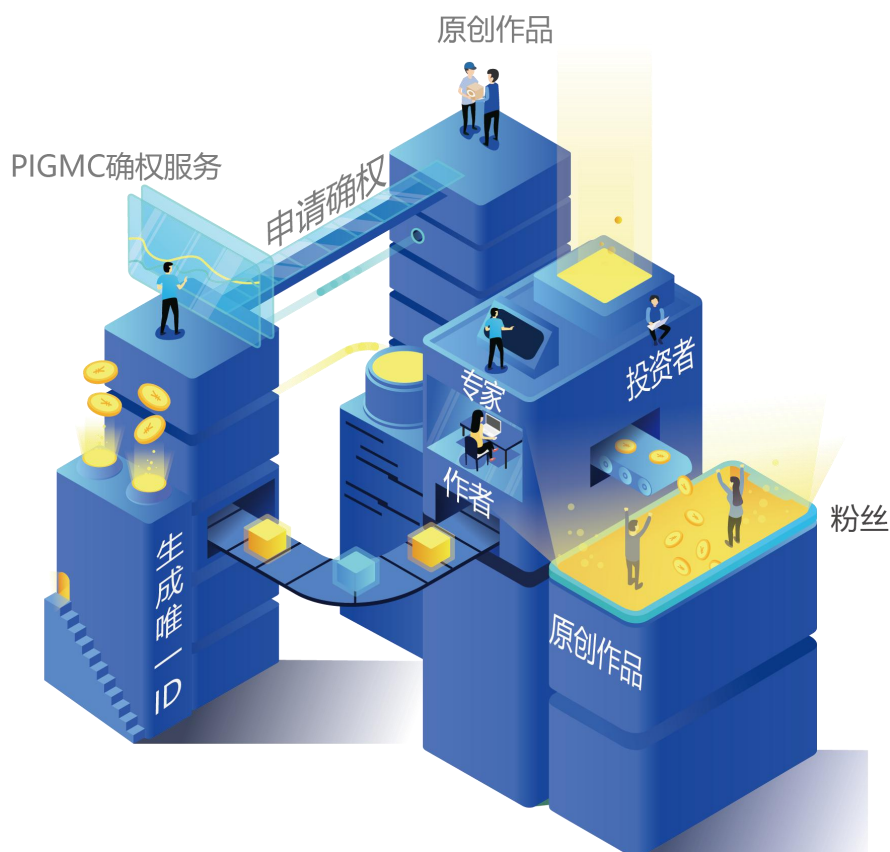


图 2-3：作品确权

(四) 资产交易系统

近年来随着比特币、以太坊和诸多数字资产的兴起，投资数字资产成为大多数普通人获取财富自由的最佳途径。但是奈何人工操作肯定会受情绪影响，而且手动操作很慢，从输入价格，到点击下单按钮，至少也要 2 秒钟。在这两秒钟内，价格可能发生很大的变化。

PiGMC 推出一套符合市场规律的交易系统，并不会让用户在交易上投入大量的精力和时间，也可以取得挺不错的收益。

量化交易，是指以数学统计和数学建模为基础，利用计算机技术，从海量的历史和当前数据中，发掘出能够大概率带来超额收益的交易方式，避免人工交易过程中由于投资者情绪波动带来的非理性决策导致的负面影响。一个合格的量化

交易模型，必须基于有明确的经济含义的趋势判断或者套利原理，进行进一步的系统化和程序化抽象，呈现出来的形式是一套逻辑完备的可执行的交易指令流程和逻辑控制方案。

1.纪律性

量化交易要求严格按照既定的逻辑进行投资决策，每个操作都是有数据和模型支持的，这样可以克服人工交易带来的情绪波动、主观臆断、恐惧和侥幸心理。比如一个每五分钟执行一次下单逻辑运算的策略，到第五分钟时，不应该出现模棱两可的情况。

2.系统性

在制定量化交易策略的时候，需要从全方位考虑交易品种、交易频率、投资周期、对冲机制、异常处理、资金容量、市场流动性、冲击成本等一系列策略系统元素，另外，需要从海量的历史数据和实时行情中捕捉到统计上大概率盈利的模型，这整个过程，是一个系统性的工程。

3.及时性

正是因为量化交易的系统性，人脑在处理这些系统元素的速度上，是比不上计算机的。信息技术的使用，使得量化策略的执行在速度上是大大优于手动交易的。比如一些微小的套利机会，计算机可以在毫秒之内捕捉到，并执行完套利逻辑，但是手动交易就无法做到这么快速及时了。

随着区块链技术的发展以及人工智能技术的普及，数字资产的交易手法日趋程序化和系统化，越来越多的用户加入到量化交易的队伍中，用更有纪律性、系统性和时效性的方式做出更理性的投资决策。

（五）游戏应用

某市区块链研究院认为，最契合区块链的应用场景是原生数字化领域的，非与现实发生巨大联系的，并且多适用于：交流效率低，信任成本高的领域（产业链条长、环节众多）；对真实性、共识有极大需求的领域（不透明、黑箱）；以及长尾流量、资源分散、参与者之间利益不一致的领域（需要激励）。而电子游戏产业，则很可能是区块链走向大众的一个重要引爆点，其本身原生数字化，并具备了如下优质属性：

全球市场规模超千亿美金，大多数在亚洲，区块链可渗透空间庞大

Pi 游戏生态重构开发者与玩家关系：

（1）游戏上链，透明、公平、可信，同时分叉提供对抗中心化作恶机会

区块链游戏与传统游戏一个很重要的区别在于，区块链游戏的代码及逻辑，是可以被写在智能合约之中，放在区块链上运行的，即上链。游戏上链便意味着透明化，不可篡改，大大改变原先传统游戏规则、数值等不透明，黑箱等一系列问题，让游戏变得公平可信。同时，游戏源代码的透明化，也意味着社区可在游戏开发者作恶的情况下，分叉出新的游戏，或在游戏厂商难以为继的情况下，由社区继续运营。对于开发者与玩家关系来说，是一个从玩家被动接受的不平等地位，到玩家可主动选择，与开发者平等对话的过程。

不过，对于传统的游戏来说，上链所带来的透明化，意味着可为其带来超额利润的优势不再，同时，代码透明化后，一款游戏的可复制性较强，容易被抄袭。因而我们认为，区块链游戏，必将是从没有历史包袱的纯区块链游戏开发者开始的，并逐步迁移、倒逼传统游戏开发者加入区块链化进程。

而传统游戏的区块链化，亦将首先从改良优化的角度出发，逐步深入，且会

经过游戏币上链,到游戏资产上链,再到核心游戏逻辑上链(智能合约运行游戏),最终到游戏整体上链这一缓慢和需要适应的过程。对于面临瓶颈的传统游戏来说,区块链更多是一次跳出原有思维框架、值得尝试的新方向,而非必然。

Token 激励,让游戏社区化,开源,革新不再唯一是开发者的责任

一款优秀的游戏,理应是具备自我繁殖能力的。传统游戏模式下,革新全部依赖于开发者,而持续开发出能让玩家满意的副本、玩法是存在难度的。

区块链、Token 经济激励的存在,由于游戏代码开源,社区可以在 Token 经济激励的前提下,根据自己的需求,利用游戏编辑器创作新玩法或者关卡,进行副本或子世界的拓展,副本或子世界可以有各自的治理方式和游戏规则,所有的副本或子世界与主世界一起,共同构成了一个可无限扩张的交互世界网。而玩家,也会因为场景的持续迭代,而持续保持新鲜感,并继续留在游戏中。总的来说,区块链有望将游戏社区化,有望大幅催生 UGC,并延长部分游戏的生命周期。

基于以太坊开发的 VR 虚拟现实平台,类似《头号玩家》电影中“绿洲”游戏的 Decentraland,就是一个游戏社区化、子世界化和 UGC 化的典型例子,游戏中的土地需要使用原生的通证 MANA 购买,完全由购买人所拥有,并以 Non-Fungible Token 类资产的形式存储在区块链上。用户可以在土地上自行创建和设计 VR 3D 场景,做成能和玩家交互的应用和游戏(Decentraland 世界中第一款游戏将是:《XOM-8: 星际逃生》),未来,用户则能在移动设备、网络浏览器或 VR 头盔中访问土地上的内容。

Pi 游戏生态重构虚拟与现实的关系

传统游戏模式下,虚拟资产所有权不归属用户,且可随意增发,同时,虚拟

资产流通不便，各类场外交易平台，存在一定的信用风险。而区块链游戏，每一个虚拟资产都可以归结为一个独一无二的 Token，称之为 Non-Fungible Token (NFT)，并通过加密方式存储在用户的区块链账户地址之中，安全、可靠，所有权完全归属用户，成为“稀缺性”、“实用性”和“观赏性”结合的收藏品，大大提升了虚拟资产的价值，开辟真正的数字收藏品。而存储在链上的虚拟资产，也可以通过智能合约形式，在去信任的环境下进行无摩擦点对点交易，并可以在区块链上看到所有成交历史，真实可信。

2017 年 6 月 22 日，ERC721 提案最终获得以太坊社区通过，标志着它正式成为以太坊网络的代币标准之一，而对于游戏虚拟资产来说，每一样道具、武器、人物都可以是一个 ERC721 Token，具有唯一性，这就有助于游戏虚拟资产的保值、收藏以及相互之间的点对点交易，能最大化释放和流通游戏的价值，让虚拟资产向现实资产转化。

目前，大部分区块链游戏 Dapp 都搭建在以太坊之上，游戏大多运行在 PC 端的浏览器上，需要载入 MetaMask 等钱包，并支付以太坊 Token，作为智能合约运行的 gas 消耗，门槛较高，限制了一大部分玩家的进入，而即便是采用无 Gas，免费模式的 EOS，实际也是将网络中的带宽、CPU 及 Ram 等资源进行拆分，Ram 需购买并消耗，而对用户来说，支付 EOS 注册账户也存在一定的门槛。

并且，由于非对称加密的特性，用户需自行妥善管理账户私钥，一旦丢失，便无法找回。而随着区块链平台的增多，各区块链账本之间不互通，用户需要管理的账户私钥也越来越多，大大提升了用户参与不同平台 Dapp 的门槛和难度。

我们认为，“区块链+游戏”是分成两类的，一类是传统游戏的区块链化，

将经历游戏币上链, 游戏资产上链, 核心游戏逻辑上链, 到游戏整体上链的过程, 另一类是原生的纯基于区块链开发的区块链游戏。目前来看, 传统游戏区块链化, 仍主要处在游戏币、游戏资产、游戏逻辑上链的初级阶段。大部分的区块链游戏系原生, 玩法还较为原始。

PIGMC 目前一阶段应用 PI 娱乐, 是基于 ERC721 植入算法方式---算力值:

所有玩家娱乐的同时, 类似于 POW 挖矿, 您的在线时间越长, 获得胜率越高, 算力越大, 获得 PIGMC 的 Token 就会越多, 具体算法如下:

算力计算方法, 胜率为 100%, 算力+10 (胜率与算力关系, 95%胜率, 算力+9.5, 83%胜率算力+8.3, 以此类推, 0%胜率, 算力+0, 附加场次, 单日场次低于 100 场, 比如单日为 1 场, 在原有胜率得到的算力值 \times 1%, 场次为 80 场, 在原有胜率的算力值 \times 80%, 等于 100 场次, 则按照实力胜率对应的算力显示, 大于 100 场次, 每增加一个场次对应增加所得的算力值加 1%, 为 101%, 以此类推, 场次越多, 获得增加算力越多)

第三章 技术实现

一、 技术架构

图 3-1 所示为 PiGMC 设计的系统逻辑架构图。

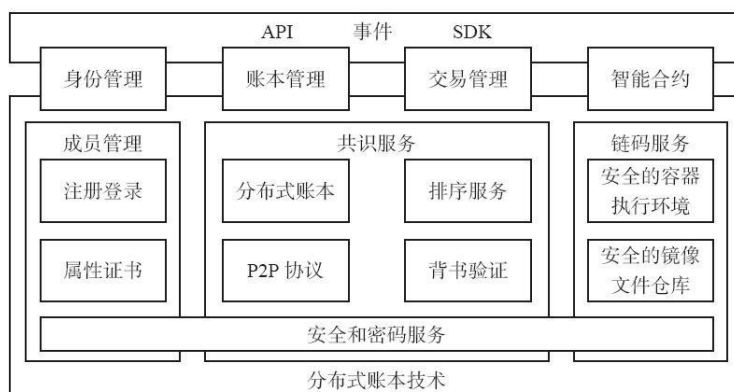


图 3-1：系统逻辑架构图

图 3-1 所示的系统逻辑架构图是从不同角度来划分的,上层从应用程序的角度,提供了标准的 gRPC 接口,在 API 的基础之上封装了不同语言的 SDK,包括 Golang、Node.js、Java、Python 等,开发人员可以利用 SDK 开发基于区块链的应用。区块链强一致性要求,各个节点之间达成共识需要较长的执行时间,也是采用异步通信的模式进行开发的,事件模块可以在触发区块事件或者链码事件的时候执行预先定义的回调函数。下面分别从应用程序和底层的角度分析应该关注的几个要素。

1、应用程序角度

(1) 身份管理

用户注册和登录系统后,获取到用户注册证书 (ECert),其他所有的操作都需要与用户证书关联的私钥进行签名,消息接收方首先会进行签名验证,才进行后续的消息处理。网络节点同样会用到颁发的证书,比如系统启动和网络节点

管理等都会对用户身份进行认证和授权。

(2) 账本管理

授权的用户是可以查询账本数据 (ledger) 的, 这可以通过多种方式查询, 包括根据区块号查询区块、根据区块哈希查询区块、根据交易号查询区块、根据交易号查询交易, 还可以根据通道名称获取查询到的区块链信息。

(3) 交易管理

账本数据只能通过交易执行才能更新, 应用程序通过交易管理提交交易提案 (Proposal) 并获取到交易背书 (Endorsement) 以后, 再给排序服务节点提交交易, 然后打包生成区块。SDK 提供接口, 利用用户证书本地生成交易号, 背书节点和记账节点都会校验是否存在重复交易。

(4) 智能合约

实现“可编程的账本” (Programmable Ledger), 通过链码执行提交的交易, 实现基于区块链的智能合约业务逻辑。只有智能合约才能更新账本数据, 其他模块是不能直接修改状态数据 (World State) 的。

2、底层角度

下面的内容是从 PiGMC 底层的角度来看, 如何实现分布式账本技术, 给应用程序提供区块链服务。

(1) 成员管理

MSP (Membership Service Provider) 对成员管理进行了抽象, 利用 KPI(Public Key Infrastructure) 对成员身份进行认证, 验证成员用户提交请求的签名。结合 Fabric-CA 或者第三方 CA 系统, 提供成员注册功能, 并对成员身份证书进行管理, 例如证书新增和撤销。注册的证书分为注册证书 (ECert)、

交易证书 (TCert) 和 TLS 证书 (TLS Cert) , 它们分别用于用户身份、交易签名和 TLS 传输。

(2) 共识服务

在分布式节点环境下, 要实现同一个链上不同节点区块的一致性, 同时要确保区块里的交易有效和有序。共识机制由 3 个阶段完成: 客户端向背书节点提交提案进行签名背书, 客户端将背书后的交易提交给排序服务节点进行交易排序, 生成区块和排序服务, 之后广播给记账节点验证交易后写入本地账本。网络节点的 P2P 协议采用的是基于 Gossip 的数据分发, 以同一组织为传播范围来同步数据, 提升网络传输的效率。

(3) 链码服务

智能合约的实现依赖于安全的执行环境, 确保安全的执行过程和用户数据的隔离。PiGMC 采用 Docker 管理普通的链码, 提供安全的沙箱环境和镜像文件仓库。其好处是容易支持多种语言的链码, 扩展性很好。Docker 的方案也有自身的问题, 比如对环境要求较高, 占用资源较多, 性能不高等, 实现过程中也存在与 Kubernetes、Rancher 等平台的兼容性问题。

(4) 安全和密码服务

安全问题是企业级区块链关心的问题, 尤其在关注国家安全的项目中。其中底层的密码学支持尤其重要, PiGMC 专门定义了一个 BCCSP (BlockChain Cryptographic Service Provider) , 使其实现密钥生成、哈希运算、签名验签、加密解密等基础功能。BCCSP 是一个抽象的接口, 默认是软实现的国标算法, 目前社区和较多的厂家都在实现国密的算法和 HSM (Hardware Security Module) 。

二、 网络节点架构

节点是区块链的通信主体，是一个逻辑概念。多个不同类型的节点可以运行在同一物理服务器上。有多种类型的节点：客户端、Peer 节点、排序服务节点和 CA 节点。图 3-2 所示为网络节点架构图。

接下来详细地解释图 3-2 所示的不同节点的类型。

1、客户端节点

客户端或者应用程序代表由 终用户操作的实体，它必须连接到某一个 Peer 节点或者排序服务节点上与区块链网络进行通信。客户端向背书节点（Endorser）提交交易提案（Transaction Proposal），当收集到足够背书后，向排序服务广播交易，进行排序，生成区块。

2、Peer 节点

所有的 Peer 节点都是记账节点（Committer），负责验证从排序服务节点区块里的交易，维护状态数据和账本的副本。部分节点会执行交易并对结果进行签名背书，充当背书节点的角色。背书节点是动态的角色，是与具体链码绑定的。每个链码在实例化的时候都会设置背书策略，指定哪些节点对交易背书后才是有效的。也只有在应用程序向它发起交易背书请求的时候才是背书节点，其他时候就是普通的记账节点，只负责验证交易并记账。

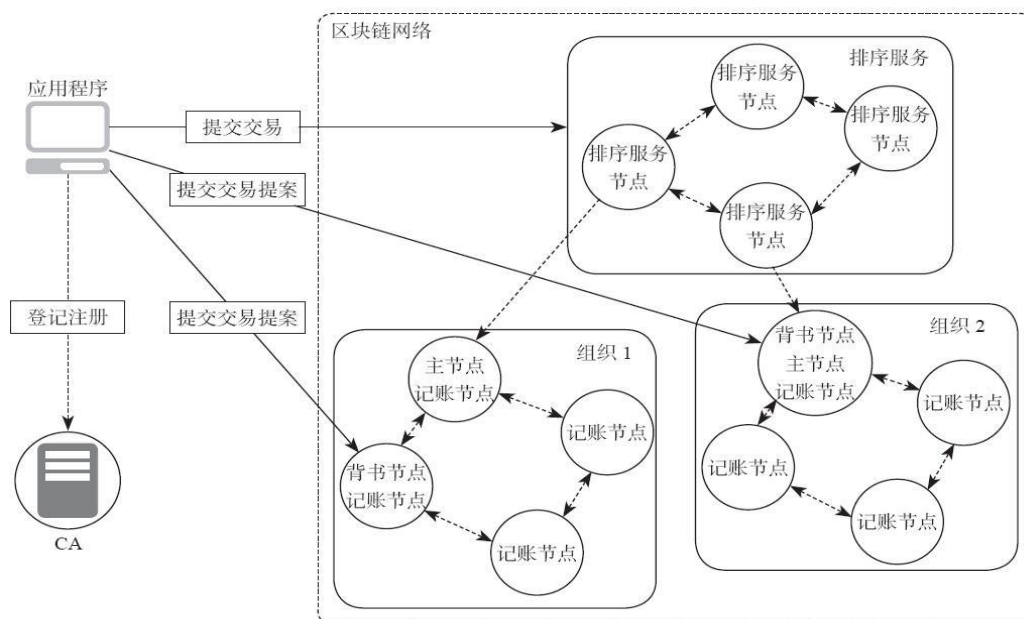


图 3-2: 网络节点架构图

图 3-2 所示的 Peer 节点还有一种角色是主节点（Leader Peer），代表的是和排序服务节点通信的节点，负责从排序服务节点处获取新的区块并在组织内部同步。可以强制设置为主节点，也可以动态选举产生。

在图 3-2 中还可以看到，有的节点同时是背书节点和记账节点，也可以同时是背书节点、主节点和记账节点，也可以只是记账节点。

3、排序服务节点

排序服务节点（Ordering Service Node 或者 Orderer）接收包含背书签名的交易，对未打包的交易进行排序生成区块，广播给 Peer 节点。排序服务提供的是原子广播（Atomic Broadcast），保证同一个链上的节点接收到相同的消息，并且有相同的逻辑顺序。

排序服务的多通道（MultiChannel）实现了多链的数据隔离，保证只有同一个链的 Peer 节点才能访问链上的数据，保护用户数据的隐私。

排序服务可以采用集中式服务，也可以采用分布式协议。可以实现不同级别

的容错处理，目前正式发布的版本只支持 Apache Kafka 集群，提供交易排序的功能，只实现 CFT（Crash Fault Tolerance，崩溃故障容错），不支持 BFT（Byzantine Fault Tolerance，拜占庭容错）。

4、CA 节点

CA 节点是 PiGMC 的证书颁发机构（Certificate Authority），由服务器和客户端组件组成。CA 节点接收客户端的注册申请，返回注册密码用于用户登录，以便获取身份证书。在区块链网络上所有的操作都会验证用户的身份。CA 节点是可选的，可以用其他成熟的第三方 CA 颁发证书。

图 3-3 所示为 PiGMC 典型的交易流程图。

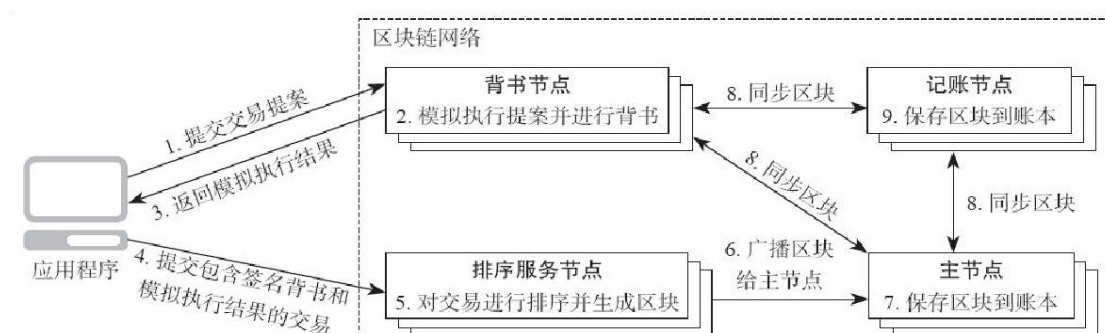


图 3-3：交易流程总图

从上一节的网络节点架构中，我们已经了解到基于 PiGMC 的区块链应用中涉及几个节点角色：应用程序、背书节点、排序服务节点和主节点。在图 3-3 中，假定各节点已经提前颁发好证书，且已正常启动，并加入已经创建好的通道。后面的步骤介绍在已经实例化了的链码通道上从发起一个调用交易到 终记账的全过程。

三、 技术特色与优势

通过大量数据测试分析，PiGMC 交易系统在性能方面可达到：秒级交易验证、海量数据存储，高吞吐量、节点数据快速同步；在扩展性方面可达到：满足

多业务区块结构、权限控制策略；同时，提供安全的私钥存取服务安全的私钥存取服务，以及隐私保护方案。

（一）性能方面

1、快速交易验证

通过对签名算法、账本结构、数据操作、序列化、共识机制、消息扩散等关键环节的优化，PiGMC 交易系统可以实现秒级的快速交易验证。满足绝大部分区块链应用场景的用户体验。

2、海量数据存储

区块链复式记账的模式，在系统长时间运行下，历史数据不断累积；PiGMC 交易系统借鉴传统金融系统中冷热数据分离存储、分表存储的机制，实现海量数据的有效存储。旧的交易数据，非活跃的资产数据等信息可以使用大数据存储平台进行存储（如 Hadoop，满足 PB 级别的数据存储）。

3、高吞吐量

区块链的本质是一种分布式共享记账的技术，其分布式特征主要体现在分布式一致性而非分布式并发处理。为保证数据的一致性，防止拜占庭将军问题，某些特定环节只能串行执行，而无法并行。通过长期的测试与优化实践，DMS 的处理性能已经能满足万级 TPS 的需求。如果再引入 Off-Chain 等机制，还能进一步大幅提高交易吞吐量。

4、节点数据快速同步

PiGMC 交易系统支持镜像(Snapshot)机制，可以定期对本地账本制作镜像，实现便利的回滚机制，在统一共识下，可以指定镜像标签进行回滚；同时，缩短新加节点加入运转的周期，仅需同步最新镜像及少量近期交易集合，即可融入网

络并参与共识验证。

(二) 扩展性方面

1、满足多业务的块链结构

PiGMC 交易系统的块链结构，能够满足不同业务领域的需求，提高系统的可扩展能力和维护效率。即可用于标记资产和资产转移，也可提供不可篡改的多维事件记录，还可以用于溯源以跟踪资产的流通过程。

2、权限控制策略

提供数据信息写入与读取两类权限控制策略。数据信息写入权限，同一账户下设置多个使用用户，并针对不同的操作设置相应的权限，满足多方签名控制的使用场景。数据信息读取权限，用户可以授予和撤回单用户或用户组对数据的操作权限，用户组可以由用户灵活配置。数据包括用户账户信息，交易信息等，粒度可以细化到交易或账户的各属性字段。

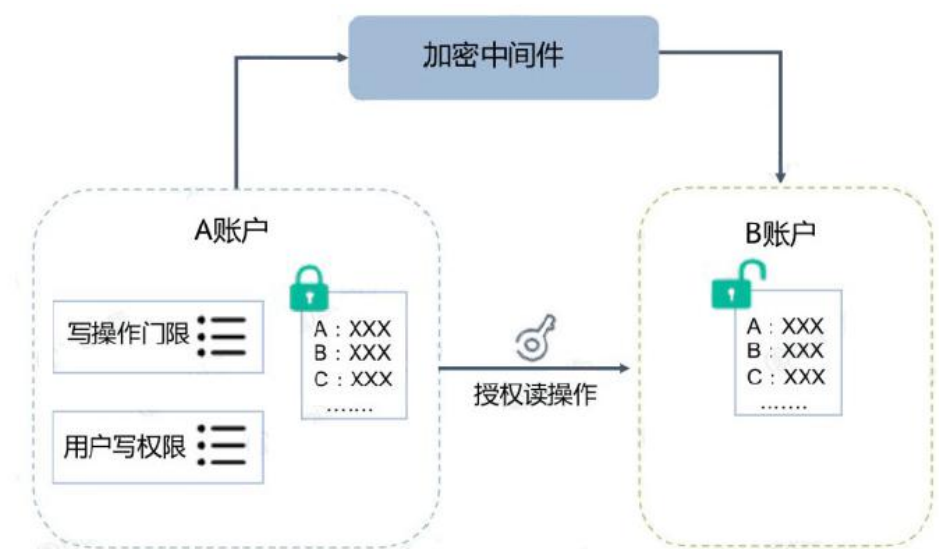


图 3-4：权限控制策略

（三）安全方面

1、安全私钥存取

为了方便用户使用区块链产品服务，除了传统的客户端生成和保存的机制，PiGMC 交易系统还提供网络托管存取和私钥硬件存取（U-key）两种方案。网络托管存取，即把用户名和密码通过特定算法映射成私钥并在服务端进行存储。服务器端存储的私钥均为加密数据，私钥仅能在用户端解密；硬件私钥是为了满足博彩行业的使用需求。

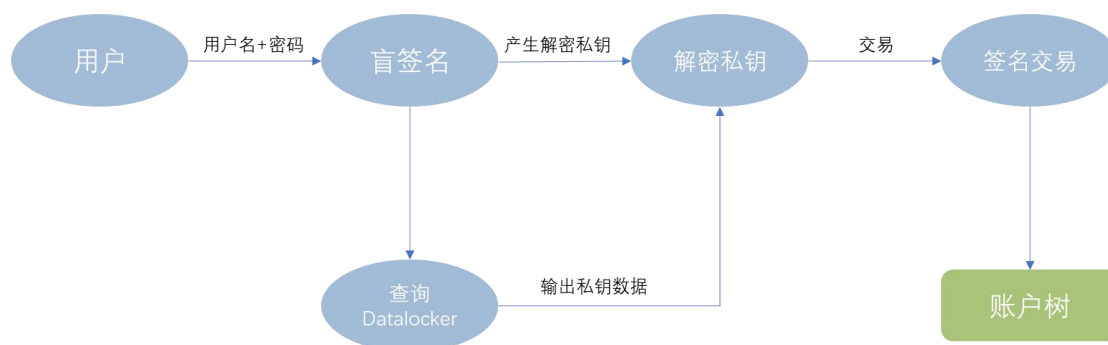


图 3-5：安全私钥存取

2、多重隐私保护

提供多重隐私保护功能。首先，区块链底层提供同态加密方式，用户所有数据均加密存储，仅用户本身可见。其次，PiGMC 交易系统提供加密中间件服务，用户可根据业务需要进行选择。最后，上层应用可以在录入时对数据进行加密处理，PiGMC 交易系统平台负责对用户生成的加密数据进行写入和读取。

第四章 治理结构

PiGMC 项目采用基金会形式进行治理。PiGMC 基金会在新加坡成立，受新加坡法监管。该基金会由具备受托资格人组成的受托董事会或管理委员会独立管理运营并独立于政府之外。新加坡以稳定而健全的法律，金融环境著称。PiGMC 在新加坡成立的非盈利组织，按照新加坡法律，该基金会是为支持或参与公共利益或私人利益的活动，而不具任何商业利益的合法成立的组织。基金会所获的“利润”被称为盈余，将被继续保留作为其他活动的经费，而不在其成员中分配利润。

基金会致力于 PiGMC 的建设与治理工作，主要的目标是保证 PiGMC 项目的可持续发展，以及资金募集安全性和管理有效性。PiGMC 基金会组织架构由决策委员会、基金自治委员会、执行委员会组成，治理架构包含了针对日常工作和特殊情况的操作流程和规则。

为避免社区成员出现方向、决策的不一致甚至因此导致的社区分裂，基金会通过制定良好的治理结构，说明管理社区的一般性事物和特权事项。基金会治理结构的设计目标是保持平台生态的发展可持续性、决策效率性和资金管理合规性。基金会由决策委员会行使日常权力。

决策委员会任期届满后由社区投票选出 5 位决策委员会的核心人员，被选出的核心人员将代表基金会做重要和紧急决策，并需在任职期间接受授信调查。基金会成立初期，为便于专案快速推进运转，首届决策委员会成员将由团队成员及早期投资人代表组成，任期 2 年，期满后由社区投票重新选出。决策委员会由 5 名成员构成，其中团队代表 3 人，早期投资人代表 2 人。所有决策的作出实行 3/5 多重签名制。

第五章 发行说明

【第一阶段】：

发行总量：10 亿

锁仓：8 亿（两年）

流通：2 亿

PiGMC 基于以太坊 ERC20 底层技术开发

Pi-game 社区是伴随 Pi 所诞生的自制组织群体，我们建立以太坊之上打造独特的游戏应用领域，基于以太坊底层开发 GMC 游戏内 TOKEN，利于 Pi 支付打通游戏内外接口，在游戏领域独树一帜，真正打造可信任，去中心，去中介化的游戏平台，将 Pi-game 社区打造成全球最大的游戏社群，最受尊重的区块链社区。

第一阶段 TOKEN 主要流通价值在游戏领域。

GMC 区块链游戏计划：

- 2018 年 5 月发放 TOKEN 到 imtoken 钱包；
- 2018 年 7 月接通 Pi 与 GMC 之间交互。
- 2018 年 8 月扩大对战类游戏开发团队；筹备角色类游戏；
- 2018 年 8 月开始实施社群 DAPP 开发计划。
- 2018 年 8 月开始筹备 Close Token 钱包开发。
- 2018 年 10 月开始筹备基于 ERC20 开发的 PiGMC 映射到基于 EOS 主网中的 GMC 中。
- 2019 年 1 月上线基于 EOS 主网开发 Pi 社群 DAPP 应用 1.0 版本。

【第二阶段】：

基于 EOS 主网上线，我们同步将基于 ERC20 开发代币 PIGMC 映射到基于 EOS 开发的 TOKEN 当中。因为 EOS 机制使用 DPOS 机制，符合我们的 DAPP 应用的承载量。

第六章 团队介绍

本项目团队成员均为行业相关领域资深专家，而且有丰富的资源和经验。而且项目前期已经开展了大量的工作，成绩斐然。具体情况如下：

Gurinder Bhangoo (CEO)



硅谷区著名的区块链技术专家、Peerbuds 区块链首席导师;Chief Blockchain Instructor、世界著名数字加密技术小区 Crypto World 早期成员、最早期区块链智能合约开发者.拥有大量的区块链、分布式账本技术、智能合同和加密交易的开发经验。

Alfredo Aguirre Valdez (CTO)

原特斯拉软件工程师，在不同业务领域的软件开发超过 13 年，从金融到物流以及不同的环境如开源语言如 PHP、Python、等，移动本地开发 iOS 和 Android 以及微软协议栈开发 Web 应用的企业里诺 SOLUCIONES，客户包括美国运通和 BBVA 罗盘。他的个人项目可以在苹果的 App Store 找到多个应用程序，GitHub 的开源库的 4K 以上下载，Facebook APP 与月综合浏览量超过 270 万。





Genevieve Leveille (COO)

爱沙尼亚国家区块链区块链技术顾问、数字货币影响力机构创始人。毕业于美国哥伦比亚大学，具有在信息技术和服务行业工作的经历。有较强的创业精神，擅长现金、市场风险、流动资金管理、金库和业务转型。

Alexander von Preysing (金融顾问)

曾任德意志交易所高级副总裁、发行服务部总裁。2002年加入德意志交易所，先后负责多个部门，精通债券、私募基金、风险管理、IPO 等业务，并作出良好的业绩。



第七章 风险提示及免责声明

- 数字资产投资作为一种新的投资模式，存在各种不同的风险，潜在投资者需谨慎评估投资风险及自身风险的承受能力。
- 本文档用于指导 PiGMC 项目的进展，只用于传达信息之途，并不构成买卖 PiGMC 的相关意见。以上信息或分析不构成投资决策。本文档不构成任何投资建议，投资意向或教唆投资。
- 本文档不组成也不理解为提供任何买卖行为或任何邀请买卖任何形式证券的行为，也不是任何形式上的合约或者承诺。
- 相关意向用户明确了解 PiGMC 项目风险，投资者一旦参与投资即表示了解并接受该项目风险，并愿意个人为此承担一切相应结果或后果。
- 本项目团队不承担任何参与 PiGMC 项目造成的直接或间接的资产损失。
- 项目风险：
 - 政策风险，区块链技术属于早期阶段，各国对于区块链项目的监管政策，会有不明确性，该项目可能会有运营主体和运营管理政府的变化；
 - 波动风险，区块链项目的代币不是法定货币，而是一种区块链项目中的数字资产，且价格上下波动巨大，需要投资者有一定心理承受能力；
 - 技术风险，对于不断发展中的区块链技术，不能保证避免在项目运营中的技术漏洞和黑客攻击；
 - 团队风险，不能保证在 PiGMC 在发展过程中的因压力、身体、个人等

因素造成的核心人员离职，能保证的是团队的更替一定是会让项目更加稳定的发展。