



匹克链

全球首个颠覆竞技竞猜市场生态的区块链公链

白皮书

WHITE PAPER



- 
- 1 摘要
  - 2 市场与政策
    - 2.1 国际市场
    - 2.2 国内市场
    - 2.3 法律政策利好
    - 2.4 全球资本市场活跃
  - 3 市场痛点
    - 3.1 高抽成
    - 3.2 缺乏流动性
    - 3.3 技术门槛低，缺乏公信力
    - 3.4 竞技作弊，竞猜不透明
    - 3.5 隐私
    - 3.6 支付繁杂、法币结算的法律风险
  - 4 匹克链
    - 4.1 去中心化
    - 4.2 人人都可组局
    - 4.3 防篡改
    - 4.4 基于智能合约的规则透明
    - 4.5 基于下一代的区块链技术
    - 4.6 匹克链平台引擎
    - 4.7 生态系统
      - 业务系统
      - 双币设计
      - 经济模型
  - 5 技术架构
    - 5.1 区块链的六层协议结构
    - 5.2 数据层

---

5.3	网络层
5.4	平台数据上链
5.5	基于 BFT-rDPoS 的共识机制
5.6	激励层
5.7	智能合约层
5.8	保证匹克链公平的真随机数生成机制
5.9	应用层
	<ul style="list-style-type: none"><li>• 符合 BIP-32/BIP-44 标准的平台 HD 钱包</li><li>• 用户账号系统</li><li>• 匹克链引擎</li><li>• 区块链浏览器</li><li>• 跨链交易</li><li>• 安全</li></ul>
6	匹克币 PKC 发行计划
6.1	发行计划
6.2	募集资金用途
6.3	锁定期
7	历程
8	法律法规
	运营主体
9	团队
	团队成员
	<ul style="list-style-type: none"><li>• Viktor Pavletic – 创始人 CEO</li><li>• Adam Seleznev – 首席运营官 COO</li><li>• Eugene Kulbashian – 首席技术官 CTO</li><li>• Duncan- 区块链技术总监</li><li>• Daniel Lemmon - 首席程序员</li></ul>

- 
- Tony Ulyanov - 专业的自由程序员
  - Jamal Seleznev – 前端网页开发者

## 10 合作伙伴

PLAYWORLD PTE. LTD.

- Leo Mu –CEO
- David - COO
- Brain Hu - CTO
- Stephen Chou

## 11 顾问

顾问团队

- Nicko Deng
- Simon Schwerin
- Gi Nam Lee
- Svetlin

## 12 风险与法律免责

风险提示

- 政策性风险
- 市场风险
- 技术风险
- 资金风险

## 13 参考资料

---

## 摘要

2015 年 10 月,《经济学人》发布封面文章:制造信任的机器——比特币背后的技术将如何改变世界。

区块链的优势在于能够用非常低的成本解决网络交易的身份识别和个人征信,以及使用点对点的交易避免了传统集中式的清算结构,从而能够大大提高金融系统甚至整个经济体系的运行效率。

区块链虽然以技术的面目诞生,但是其所带来的,已经远远超越技术范畴本身,正如互联网所给我们带来的一样。区块链不仅仅是一项技术、一个工具,更是一种思想。开放、共享、去中心化,区块链的这些核心精神与互联网不谋而合。而与互联网不同的是,区块链把这样的思想从信息的传递进一步拓展到价值的传输。

目前,区块链主要应用在数字货币市场,而下一个大规模应用场景将会是在竞技竞猜市场,将会颠覆传统竞技竞猜市场生态。

我们旨在通过匹克链为传统的竞技竞猜平台快速切换到区块链,借助于平台引擎,一些传统的地下组局者、私彩投注等都可以在匹克链开展自己的业务;对于普通的用户,也都可以借助平台引擎,像专业人士一样,针对性的发布竞猜项目,成为全球首个颠覆传统竞技竞猜市场生态的区块链公链。

---

# 市场与政策

## 2.1 国际市场

根据英国知名市场研究机构 Juniper Research 发布了一份《Digital Games: eSports 2015 – 2020》所示，到 2019 年，全世界将有 10% 的成年人会在线上或移动端进行竞技竞猜棋牌活动，全球竞技竞猜业收入有望达到 5250 亿美元。

另外，根据 Sensor Tower 发布了 9 月数据报告，报告发布了美国 APPSTORE + GOOGLE PLAY 上的所有 APP 收入排行。报告显示，9 月份最赚钱的 30 个 APP 中，竞技竞猜棋牌类游戏共有 5 款游戏上榜。上榜的棋牌竞技竞猜类游戏分别为：《Slotomania》（排名第 8 位）、《Double Down》（排名第 16 位）、《老虎机》（排名第 18 位）、《House of Fun》（排名第 20 位）、《Big Fish Casino》（排名第 22 位）。

## 2.2 国内市场

智研咨询发布的《2017-2023 年中国游戏市场深度监测及未来前景预测报告》国内游戏市场规模为 1655 亿，手游市场为 819 亿，目前棋牌移动游戏在全部游戏中的占比预计在 5% 左右，那么国内棋牌游戏市场规模为 82 亿，移动棋牌游戏规模为 41 亿。虽然棋牌游戏总体玩法相对传统，但棋牌用户具有明显的特征：

目标用户广泛数量庞大，年轻化是趋势，20-40 岁为主力人群；

用户粘性强，忠诚度高，近六成用户每天棋牌游戏时间超过 1 小时，还有 200 万用户每天超过 8 小时；

游戏生命周期长、开发成本低、盈利稳定。

## 2.3 法律政策利好

目前全球已有超过 100 个国家和地区将竞技竞猜业合法化。近几年来世界

---

各国对在线竞技竞猜合法化的态度均有不同程度的转变，截止 2016 年，共有 85 个国家实施在线竞技竞猜合法化，创造税收约 370 亿美元。

自 2017 年起有诸多国家和地区纷纷加入在线竞技竞猜运营合法化行列，在线竞技竞猜给政府提供高额税收。据不完全统计，今年牙买加、哥伦比亚、瑞士、葡萄牙、波兰、罗马尼亚、美国的马萨诸塞州、密歇根州、宾夕法尼亚州都将实施在线竞技竞猜合法化。

竞技竞猜行业正逐渐获得世界上更多国家的认可，而作为竞技竞猜行业与现代技术结合形成的在线竞技竞猜更是发展迅速。作为未来竞技竞猜业发展方向的在线竞技竞猜市场，发展前景十分广阔，行业蕴含无限的能量。

4 月 11 日，中共中央国务院发布《中共中央国务院关于支持海南全面深化改革开放的指导意见》明确提出“支持在海南建设国家体育训练南方基地和省级体育中心，鼓励发展沙滩运动、水上运动、赛马运动等项目，支持打造国家体育旅游示范区，探索发展竞猜型体育彩票和大型国际赛事等”。

## 2.4 全球资本市场活跃

全球资本市场对于竞技竞猜市场持续活跃。

- ◆ 2016 年 10 月 13 日，巨人网络以 44 亿美元现金收购凯撒娱乐旗下专注休闲社交手机游戏业务的 Playtika 公司。
- ◆ 2017 年 4 月初，IGT 以 8.25 亿美元的价格将社交游戏开发商 Double Down 出售给了韩国公司 DoubleU Games。IGT 于 2012 年斥资 5 亿美元收购 Double Down。
- ◆ 2017 年 12 月初，澳大利亚竞技竞猜机器制造商 Aristocrat 宣布收购美国西雅图的社交竞技竞猜游戏公司 Big Fish Games，收购总额达 9.9 亿美元。

---

# 市场痛点

尽管竞技竞猜市场持续活跃、法律政策不断带来利好，但是市场也存在很多的问题。

## 3.1 高抽成

由于中心化的竞技竞猜平台运营风险极高，平台的运营者需要足够高的收益来保证平台的正常运转。那么就需要有人为此买单。正规的竞技竞猜平台回报率在 7.5%-8%，而那些非法的平台回报率可达到 30%-40%。

## 3.2 缺乏流动性

玩家在竞技竞猜中产生的数字资产，并没有有效的途径流通到市场，玩家在竞技竞猜平台中产出的部分数字资产收益无法有效的转换为实际收益，这本应属于玩家的利益最终还是集中在中心化平台运营者手中。

## 3.3 技术门槛低，缺乏公信力

传统的竞技竞猜平台都是基于中心化的商业模式（由某个公司或个人控制），这意味着参与竞技竞猜的需要将自己的资产交由中心化平台代为托管。然而，事实上由于技术和准入门槛很低，许多中心化竞技竞猜平台的资质和信誉状况令人担忧；这些中心化的竞技竞猜平台普遍存在着技术漏洞、用户敏感数据泄漏等等问题，这给参与了竞技竞猜的用户带来极大的风险和不确定性。

## 3.4 竞技作弊，竞猜不透明

中心化的竞技竞猜平台的运营者可控性非常强，他们拥有随机修改规则甚至推倒重来的权利，过去老玩家都知道棋牌游戏平台或竞技竞猜类的平台的胜负概率都掌握在运营者的后台控制器里，表面上都宣称自己多么诚信，绝无机



---

器人，实际如出一辙。

### 3.5 隐私

由于中心化的支付手段制约，客户支付记录永久存在，客户随时被追踪冻结，客户信息随时都有被泄露或窃取的风险，甚至被中心化平台私自贩卖，个人数据的安全无法得到有力的保障。

### 3.6 支付繁杂、法币结算的法律风险

尽管技术在进步，但是在线竞技竞猜游戏平台的支付仍然存在支付繁杂，而且由于不同国家地区的法律政策限制，使用法币结算存在很高的法律风险。



---

# 匹克链

基于我们在传统竞技竞猜平台的积累，以及对于区块链技术的持续关注和自研开发，我们团队旨在通过基于匹克币 PKC 和 PKDT 双币经济系统设计的解决方案和基于 EOS 优化的匹克链开发，为传统竞技竞猜平台提供基于区块链的全新、健康的平台生态，建立基于匹克链的共识机制，形成建立在匹克链上的利益共同体，解决传统竞技竞猜平台存在的一系列问题，更好的服务这个行业。

## 4.1 去中心化

在匹克链上搭建的区块链竞技竞猜平台，不仅能实现所有传统中心化竞技竞猜平台具备的功能：包括但不限于体育竞猜、棋牌游戏竞技等，它还将能够承载与传统中心化平台一样甚至更大的交易量，同时也解决中心化竞技竞猜平台普遍存在的行业痛点。

基于区块链技术的去中心化特性，这意味着没有任何组织或个体能够控制匹克链，足以彰显其公平、公开、公正、透明等特性。同时我们的所有竞技竞猜业务都是由智能合约来实现的，用户也不再需要为平台信用而担忧。

## 4.2 人人都可组局

在匹克链，不需要技术，也不需要太多的资金，人人都能组局。匹克链内置了许许多多的可配置化平台引擎，用户只需要缴纳少量的保证金，即可成为组局者。

## 4.3 防篡改性

区块链记录的是所有交易的散列值，这些值是由交易的原始数据经过散列运算获得，哪怕原始数据的细微的修改都会有不同的结果，这些区块记录是环环相扣，这些数据都存在各个节点中，想私自篡改数据是不可能的。

---

区块链是基于时间序列的复式记帐本，交易是账本的基本单位，块是交易记录的容器，所有的交易记录通过默克尔树（Merkle tree）记录，每个块通过散列值关联，这些账本记录在网络上的各个节点中，任何人无法篡改，保证用户的资产不会因为某台服务器攻击或部分节点遭受攻击或出现问题而受影响。

## 4.4 基于智能合约的规则透明

区块链的另一项革命性的创新是智能合约，智能合约是一个由代码编写的合约，所有的执行都是预先编写好的，而且智能合约也是记录在区块链上，这些智能合约都可以查到合约代码，规则透明，这样就可以保证竞技竞猜平台的公正性。

区块浏览器是匹克链应用数据展示系统，同时其也为用户提供查阅匹克链上的智能合约的工具，其根据区块链中记录的智能合约、交易数据，显示和查询所有的智能合约代码、交易数据、地址帐户余额、竞猜投注交易以及开奖结果等。所有数据公开透明，并天生具有不可篡改特性。

## 4.5 基于下一代的区块链技术

由于竞技竞猜的特点，会涉及频繁的交易和操作，而区块链 1.0 版的比特币和 2.0 版的以太坊都存在并发低、TPS 处理能力严重不足、网络拥堵严重等问题，而他们高昂的手续费显然不符合竞技竞猜市场的应用。

而下一代区块链 EOS 的出现，很好的解决了目前区块链存在的问题，拥有强大的并发能力、高达上百万的 TPS 以及完全免交易费的基础设计，使之成为构建匹克链的技术基础。

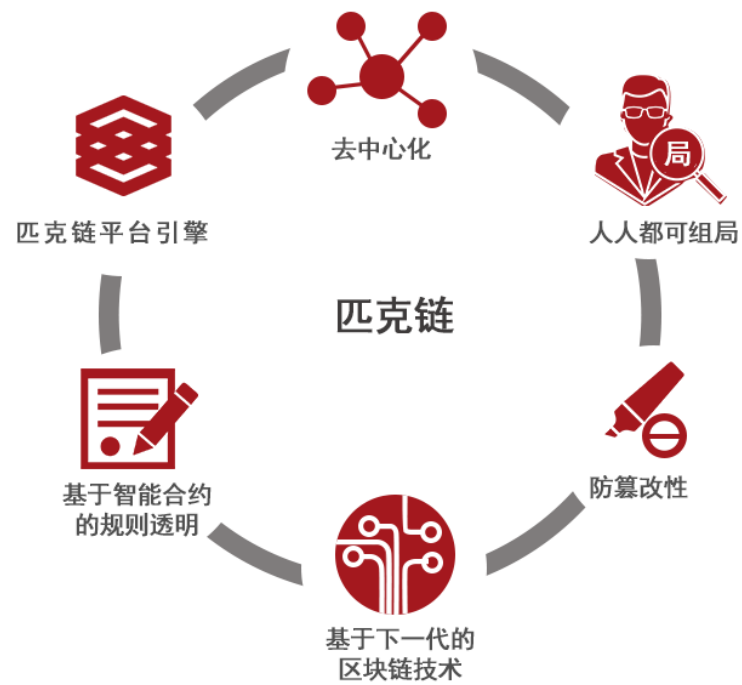
## 4.6 匹克链平台引擎

我们提供匹克链，让已有的竞技游戏平台从业者便捷的将业务迁移到区块链平台上，同时，我们提供一整套的平台引擎，让新进入的从业者也可以利用手中的资源轻易的进入这个行业，降低行业的门槛，让行业进入一个良性竞争

状态。

针对现在很多的线下的彩票站，我们提供平台引擎工具组，让这些线下的彩票站也可以迅速的发行基于区块链的彩票，开启全民参与的状态。

同时，为了方便竞技游戏平台更好的运营自己的业务，我们提供一整套的运营分析平台以及基于 BI 的商业智能分析决策平台。



---

## 4.7 生态系统

### 业务系统

#### 竞技平台

基于我们已有的竞技竞猜平台，通过我们的匹克链平台引擎，我们逐步将现有业务迁移至匹克链上。

提供竞技游戏，引入对战类游戏，例如提供线上桌球比赛等。

通过引入基于匹克链的 PKDT，玩家可以通过基于 H5 的竞技游戏以及端游的大厅，进入到多款竞技游戏，包括德州、百家乐等，通过集成到客户端的钱包，玩家可以便捷的进行法币充值到匹克币 PKC，并且兑换到 PKDT，反之，玩家也可以将游戏赢取的 PKDT，再兑换为 PKC，将 PKC 通过交易所进行变现或者币币交易。

玩家在玩竞技游戏的时候，还为竞技游戏本身提供随机数算力，让竞技游戏更加公平、公正，平台为了鼓励玩家，会提供一定的挖矿奖励，这些挖矿奖励通过智能合约的方式自动发放到玩家的帐户下。

我们也会提供休闲竞技游戏玩法，吸引更多的用户到我们的匹克链上。

我们也会鼓励第三方的竞技游戏服务商接入匹克链，我们会提供一条龙接入服务的支持，包括：

- ◆ 共享匹克链的用户资源
- ◆ 针对要求有 KYC 的地区，提供 KYC 认证服务
- ◆ PKDT 对接服务
- ◆ 竞技竞猜数据的真随机数算法
- ◆ 竞技竞猜数据保存的数据存储服务

不论自营的竞技游戏，还是第三方的竞技游戏服务商的接入，基金会都会抽取游戏不高于 1% 的收益作为匹克链的运营费用，抽取的费用公开、透明，是通过智能合约自动执行，基金会的资金地址会公开，接受所有人的审计。

---

## 竞猜平台

引入匹克链，可以很好的解决竞技竞猜中的公平、公正问题，我们会通过自己提供竞猜平台以及引入第三方竞猜服务商入驻的形式，建立一整套公平、公正的竞猜生态平台。

基于匹克链提供的服务包括但不限于下面的内容

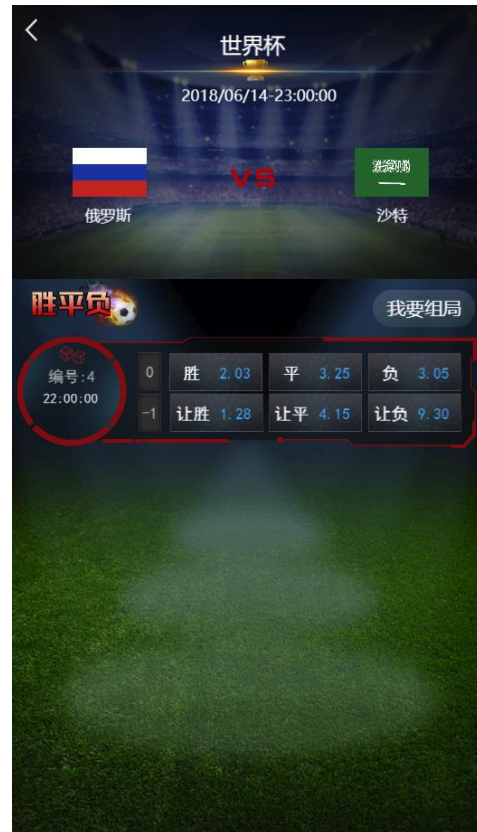
- ◆ 提供赛事竞猜
- ◆ 提供事件竞猜
- ◆ 提供基于链端的竞猜
- ◆ 提供自创事件竞猜
- ◆ 接入权威的彩票平台

竞猜平台，也会提供自营与引入第三方服务商的模式，两者在匹克链上的地位平等，基金会都会抽取收入不高于 1%的收益作为平台的运营费用，抽取的费用公开、透明，是通过智能合约自动执行，基金会的资金地址会公开，接受所有人的审计。

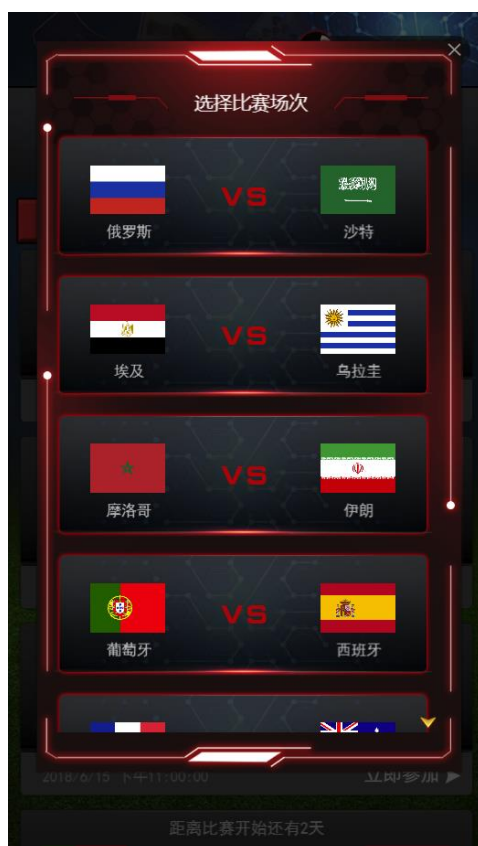
竞技平台	竞猜平台
<ul style="list-style-type: none"><li>• 德州扑克</li><li>• 百家乐</li><li>• 诈金花</li><li>• 斗地主</li><li>• 锄大地</li><li>• 麻将</li><li>• 对战类竞技游戏</li></ul>	<ul style="list-style-type: none"><li>• 体育赛事竞猜</li><li>• 事件竞猜</li><li>• 链端竞猜</li><li>• 用户自创事件竞猜</li><li>• 彩票平台</li></ul>

## 世界杯竞技竞猜

世界杯即将开赛，我们的世界杯竞猜项目已经上线，用户点击我们的竞技竞猜链接就可以参与到活动中：



用户还可以选择我要开房，自己组局竞猜世界杯项目：





## 双币设计

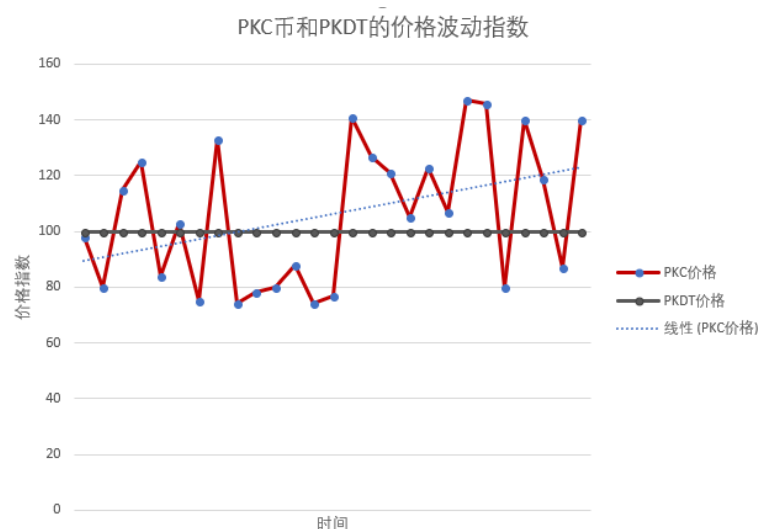
如果直接将在二级市场具有流通、交易性质的匹克币 PKC 作为数字筹码应用到匹克链时会存在很大的问题，包括：

- ◆ 二级市场的匹克币 PKC 货币价格波动，会给客户带来巨大的不确定性，匹克币 PKC 的价格波动，还给投注带来计算上的麻烦，体验大打折扣
- ◆ 作为竞技竞猜服务商需要持有一定数量的匹克币 PKC，来满足客户入场或者出场的需求，而由于二级市场的价格波动，游戏平台上也会承担巨大的不确定性风险

我们会发行基于匹克链的匹克币（PKC），匹克币 PKC 会在二级市场流通，与主流的数字货币 BTC、ETH 等在交易所直接兑换，也可以在线下用户之间进行法币买卖，同时，也会在匹克链上创立 PKDT 作为中间的隔离工具。

PKDT 相当于数字货币市场的硬通货-黄金，价格稳定，PKDT 是由匹克链提供，由基金会进行管理，不在二级市场流通，PKDT 对标 USDT，保持 1: 1 恒定的价格，PKDT 只有通过匹克币 PKC 兑换，而匹克币 PKC 是在二级市场流通的数字货币，价格由市场调节，PKC 兑换 PKDT 的价格是根据当时 PKC 对标 USDT 的价格，用户获取 PKDT 可以直接进行竞技竞猜。

匹克币 PKC 和 PKDT 的价格指数说明

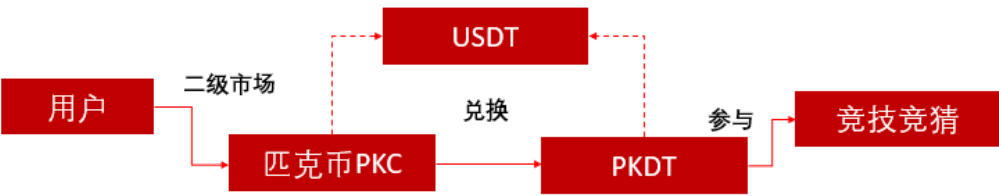


用户游戏完成后，PKDT 通过当时匹克币 PKC 的价格兑换为匹克币 PKC 进



入交易所变现交易。

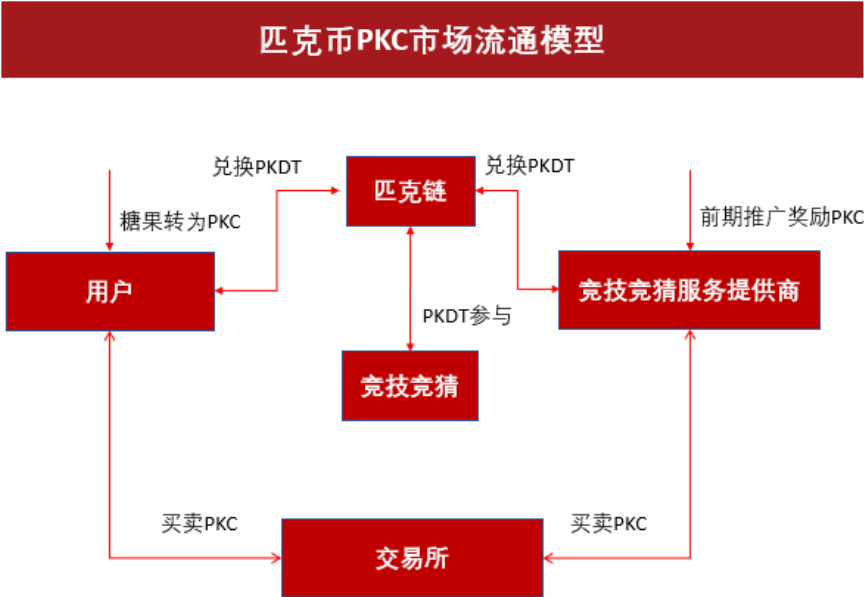
区块链竞技竞猜平台通过双币的设计，避免了 PKDT 受二级市场巨大波动带来的不确定性，玩家用户和游戏平台消除数字货币二级市场价格波动带来的巨大风险的担忧。



匹克币 PKC 和 PKDT 的对比关系

匹克币PKC	PKDT
<ul style="list-style-type: none"><li>• 可以兑换PKDT</li><li>• 在二级市场流通</li><li>• 价格随二级市场波动</li></ul>	<ul style="list-style-type: none"><li>• 可以兑换PKC</li><li>• 不可在二级市场流通</li><li>• 价格恒定,对标USDT</li></ul>

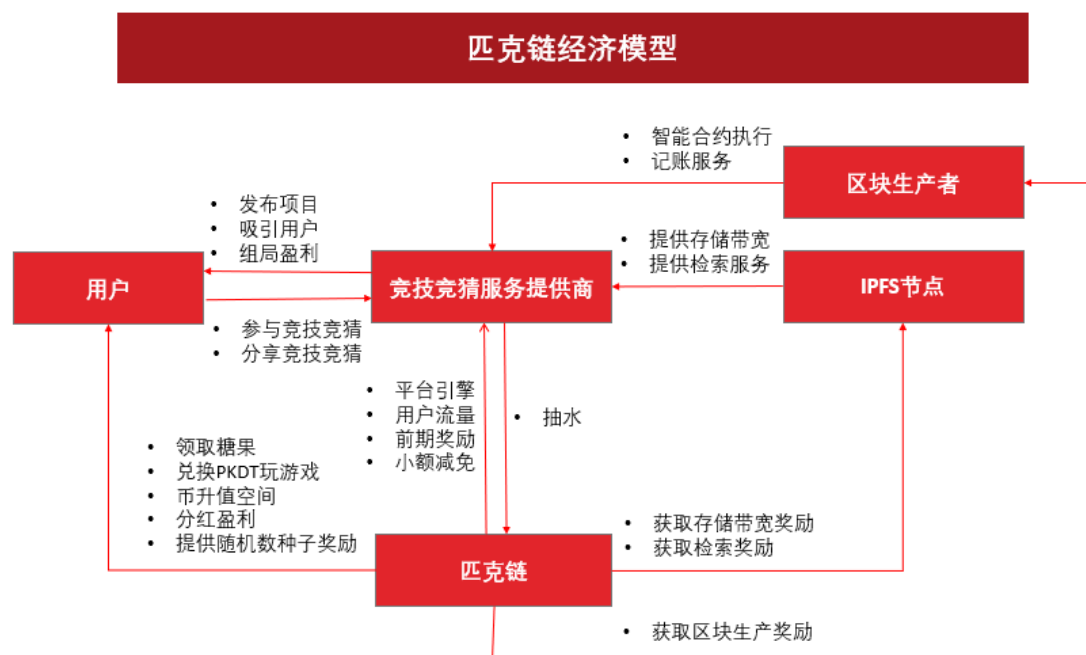
匹克币 PKC 市场流通模型



## 经济模型

匹克链会平衡各方利益，通过基金会来作为匹克链运营的主体，基金会是非赢利的，所有的收益、费用发放都是通过匹克链上的智能合约定义，保证匹克链运营的公平、公正，接受任何人的审计。

相对于传统的中心化的运营的竞技竞猜平台，在匹克链上发布自己的应用，会有很高的回报率，匹克链将竞技竞猜业务自动化，大幅降低竞技竞猜服务提供商运营成本。



竞技竞猜服务提供商在匹克链上，利用平台引擎，快速发布应用，利用匹克链已有的用户流量，也可以自己运营推广吸引用户参与竞技竞猜，组局盈利，同时，会返利给匹克链；用户兑换 PKDT 参与到竞技竞猜，为匹克链提供随机数种子而获得挖矿奖励，持有匹克币 PKC，可以得到平台的分红，预期匹克币 PKC 的升值获利；区块生产者为匹克链提供智能合约的执行和记账服务，IPFS 节点提供竞技竞猜数据的存储、带宽以及检索，匹克链会给予它们相应的奖励。

# 技术架构



我们旨在打造基于 EOS 优化的匹克链，通过引入 IPFS 星际文件系统保存竞技竞猜数据，保证整个平台的公平、公正、不可篡改、可审计。

## 5.1 区块链的六层协议结构



---

## 5.2 数据层

区块链模型的最底层，封装了数据区块的链式结构，以及非对称的公钥私钥加密技术和时间戳技术，保证数据记录公开透明，不可篡改，不可逆。因为区块链是去中心化的体系设计，所有的数据会记录在不同的节点上，没有人可以控制这些数据，也保证了这些数据的冗余备份，避免中心化存储带来的篡改、丢失等问题。

在匹克链设计中，数据节点会分为区块生产者节点和普通节点，其中对区块生产者节点有很高的要求，同时也会给予相应的奖励，保证正常出块和很高的交易并发能力，而普通节点只是参与记账以及传播记账数据，不参与区块生产。

## 5.3 网络层

区块链是采用点对点（P2P）的组网机制，区块生产出来后通过网络广播进行数据传输和数据验证，因为 P2P 的特性，区块链具有自动组网的机制，常常被称作分布式自治系统（DAOs）。

## 5.4 平台数据上链

星际文件系统（the InterPlanetary File System，简称 IPFS）是一个面向全球的、点对点的分布式版本文件系统，试图将所有具有相同文件系统的计算设备连接在一起，IPFS 未来会替代现在广泛应用的 HTTP，可以解决目前 HTTP 低效、过度依赖 Internet 骨干网等一系列的问题，它将文件分片保存在不同的节点存储，避免中心化存储的数据丢失、不可访问等问题。

采用 IPFS 保存平台数据，保证用户随时可以访问这些数据；同时，将平台数据的文件内容散列值上链，与竞技竞猜交易数据关联，这样可以对已完成的所有游戏进行溯源。

休闲类游戏因为游戏本身属性和为了避免浪费星际文件系统的存储和带宽，这类游戏的数据不上链。

---

平台数据保存的 IPFS 节点会由游戏运营商或者第三方提供存储和带宽，这些节点会由基金会从发行预留的 20%和竞技竞猜抽水中提供相应的费用，保证平台的正常运行。

由星际文件系统（IPFS）保存竞技竞猜平台数据，我们也正在研究和开发基于存储和利用带宽的激励机制，会在后期陆续发布一些技术和激励细节。

## 5.5 基于 BFT-rDPoS 的共识机制

优秀的共识机制是保证区块链竞技竞猜平台正常运转的基本条件。

匹克链会采用 EOS 最新版本作为技术的基础，同时它的基础上，进行一系列的优化更新，在 EOS 的 BFT-DPoS（Byzantine Fault Tolerance - Delegated Proof of Stake）的共识基础上提出 BFT-rDPoS（Byzantine Fault Tolerance – randomized Delegated Proof of Stake）的共识机制设计。

EOS 会通过竞选的方式从候选节点中选取 100 个备用节点和 21 个区块生产节点，由 21 个区块生产者生产所有区块，备用节点只有当 21 个节点有问题的时候才会成为区块生产者节点。

我们提出 BFT-rDPoS（Byzantine Fault Tolerance – randomized Delegated Proof of Stake）的共识机制设计，会有 67 个高性能服务器作为区块生产者主节点，每 6 个区块生产周期，会通过一套随机数算法，选出 11 个节点作为这一轮的区块生产和验证，11 个节点轮流作为区块生产；随机数算法不仅可以保证 67 个区块生产主节点都可以参与到区块生产中，还可以保证下一个区块的区块生产者的随机性。

BFT-rDPoS（Byzantine Fault Tolerance – randomized Delegated Proof of Stake）的共识机制设计的优势包括：

- ◆ 通过 BFT 共识算法，随机选出的 11 个节点可以达成共识
- ◆ 通过随机算法（Randomized）在 67 个主节点中选取一轮 11 个生产节点，保证了记账的公平、公正性，虽然 67 个节点没有 EOS 的 100 备用节点多，但是由于这 67 个节点都有机会参与区块的生产和验证，比 EOS 的 21 个节点有更广泛的代表性

- 
- ◆ 所有的主节点都可以参与区块生产，都可以获取奖励，避免了备用节点只有等到区块生产节点“掉线”，才能参与到区块生产的问题，避免了备用节点资源的浪费

匹克链	EOS
<b>架构</b> <ul style="list-style-type: none"><li>• BFT-rDPoS</li><li>• 67个区块生产主节点</li><li>• 每轮随机选择11个节点产生区块</li></ul> <b>特点</b> <ul style="list-style-type: none"><li>• 11个节点，达成共识更快</li><li>• 所有潜在节点都参与，都有奖励</li><li>• 每轮随机选择，不容易被攻击</li><li>• 67个节点，更具公平性</li></ul>	<b>架构</b> <ul style="list-style-type: none"><li>• BFT-DPoS</li><li>• 21个区块生产者以及100个备选节点</li><li>• 21个节点产生区块</li></ul> <b>特点</b> <ul style="list-style-type: none"><li>• 21个节点，达成共识需要更长时间</li><li>• 备选节点需要在线但没有奖励</li><li>• 21个节点固定，更容易受攻击</li><li>• 21个节点，去中心化有限</li></ul>

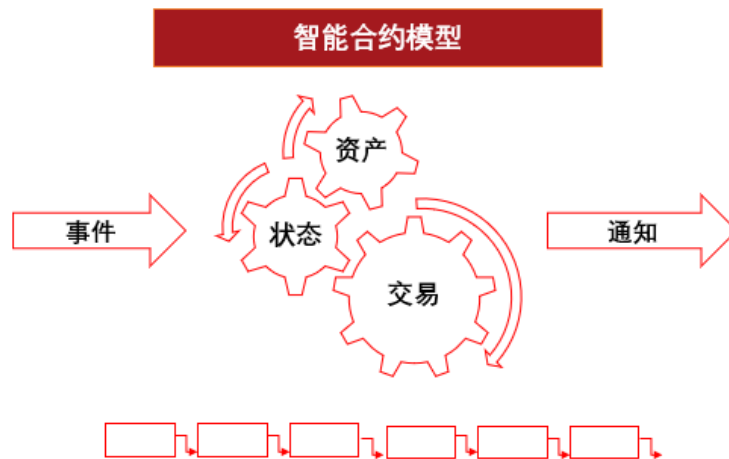
67 个节点和每轮随机选举 11 个节点作为区块生产者的机制，包括这些节点的选取标准、进入退出机制、地域因素等，我们仍旧在讨论和验证中，目的是为了达到去中心化和高效的平衡，以及更加安全的平台。

## 5.6 激励层

在匹克链中，激励层是通过智能合约的形式将各方利益自动发送到各方的帐户中。

## 5.7 智能合约层

区块链每个区块可编程、可嵌入代码的特性，合约层包含了脚本、算法、以及智能合约，可以简单的理解为是一份自定义的电子合同，之所以称为智能合约，是因为这份合约可以在达到约束条件自动触发执行，不需人工干预，也可以在不满足条件时自动解约，理论上可以触发执行事先约定好的一切条款。这也是区块链能够重构信用体系最核心的技术之一。



在匹克链中，智能合约在几个地方扮演重要的角色

- 负责平台运营各个激励机制利益的发放，避免利益发放的暗箱操作
- 为竞技、竞猜以及彩票等提供智能合约模板，用户只需要通过简单的参数设置，就可以进行竞技竞猜活动，而且竞技竞猜活动的奖励分配也是通过智能合约发放，保障了参与者的权益。

## 5.8 保证匹克链公平的真随机数生成机制

传统竞技竞猜平台的随机数生成机制往往是由中心化竞技竞猜平台服务商控制，这样造成生成机制不透明、存在暗箱操作、作弊等嫌疑。

为了保证竞技竞猜的公平公正，随机数生成机制是最重要的保证。

我们提出基于区块链智能合约，由用户参与的随机数生成机制保证游戏的公平、公正，基本流程如下：

- ◆ 准备阶段由用户提交他们自己的随机种子
- ◆ 服务器汇总用户的随机种子、区块链随机数种子，交由智能合约处理，生成竞技竞猜数据
- ◆ 竞技竞猜数据在开始前就会记录到区块链上，保证数据的不可更改，同时用户可以回顾和检查整个流程的透明度





## 5.9 应用层

### 符合 BIP-32/BIP-44 标准的平台 HD 钱包

为了保证匹克链钱包在易用性和安全性的平衡，平台采用符合 BIP-32/BIP-44 标准的平台 HD 钱包，钱包符合 EOS 钱包标准。

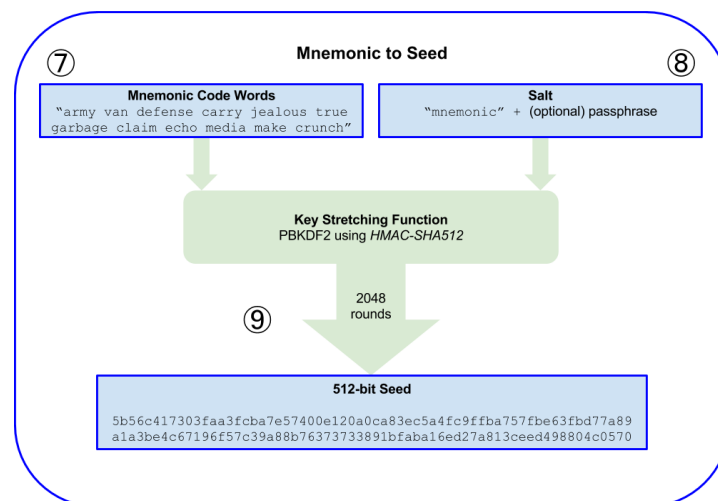
基于 BIP32 标准实现，种子能够推导出主密钥 (master key)，主密钥推导出子密钥 (children keys)，子密钥推导出孙密钥 (grandchildren keys)，以此递推。

通过 BIP39，可以定义了钱包助记词和种子生成规则：

生成助记词的步骤：

1. 生成一个长度为 128~256 位 (bits) 的随机序列(熵)
2. 取熵哈希后的前 n 位作为校验和 (n= 熵长度/32)
3. 随机序列 + 校验和
4. 把步骤三得到的结果每 11 位切割
5. 步骤四得到的每 11 位字节匹配词库的一个词
6. 步骤五得到的结果就是助记词串

通过助记词生成种子



图片来源: <https://blog.lellonek.me/bitcoin-wallet-seed-in-elixir-fabb9753a5ba>

---

## 用户账号系统

匹克链提供统一的账号系统，用户在游戏平台中存在两种角色：用户在竞技竞猜中的角色，这些信息包括游戏用户昵称、电话、头像等；用户在匹克链中的帐目角色信息，这些信息包括匹克链归属账号、账号以及公钥、私钥、授权等。

## 授权注册商

匹克链的用户是由授权注册商才能进行注册，授权注册商由匹克链指定，原则上，在匹克链上竞技竞猜服务商都可以作为授权注册商。

引入授权注册商也可以解决匹克链的安全性，避免僵尸账号和垃圾邮件等困扰业界已久的问题。

## KYC 认证

对于某些竞技竞猜场景下，我们会接入 KYC 认证，KYC 认证数据我们通过加密技术记录在匹克链上，做到数据不可更改。同时，通过智能合约自动签发，可以做到零知识证明，达到既认证了用户信息，又保护了用户隐私。

## 注册

提供注册机制，用户通过手机号码+验证码方式进行注册，注册后，匹克链会自动为用户在匹克链上建立账号，并且生成相应的公钥和私钥

注册时，用户可以设定 PIN 码，以便下次可以登录进入

登录用户通过手机和设定的 PIN 码登录进入系统，如果是绑定到手机等硬件设备，则可以检测用户信息后直接登录进入

---

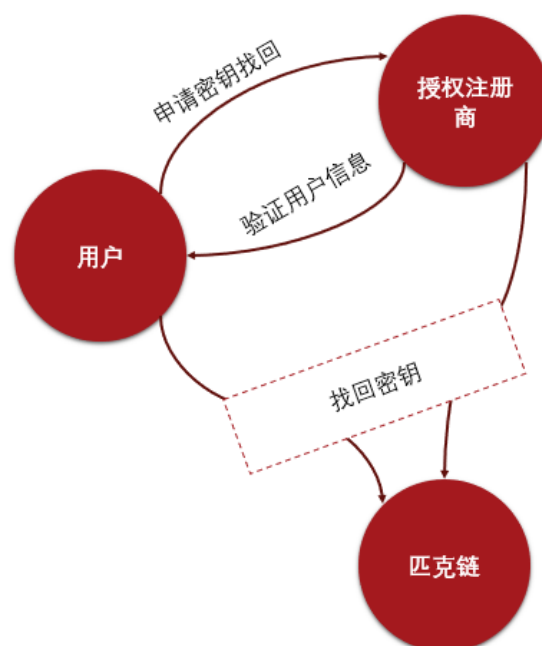
## 被盗密钥找回

在比特币和以太坊上，用户一旦丢失了密钥，那么用户的资金也就无法找回，会给用户造成巨大的损失。

匹克链采用基于 EOS 作为底层技术架构，支持被盗密钥的找回，由于匹克链引入了授权注册商，所以用户的被盗密钥找回也会通过授权注册商来配合完成，具体的处理流程是：

- ◆ 用户向授权注册商提出申请
- ◆ 授权注册商通过用户预留的电话号码、身份信息等信息验证用户信息，
- ◆ 通过授权服务商的验证后，授权注册商作为用户帐户的关联帐户会协助用户找回被盗密钥

被盗密钥找回是通过用户与授权注册商两者的多重签名交易完成的，但是与简单的多重签名有着极大的不同。通过多重签名交易，另一个实体会成为每个执行交易的一方。相比之下，通过恢复过程，恢复合作伙伴仅参与恢复过程，无权参与日常交易。这极大降低了所有参与者的成本和法律责任。



---

## 私钥保存

用户可以选择导出自己用于转账的私钥备份到安全的地方，用户在自己的钱包中管理自己的地址和私钥，平台不会保存用户的私钥，用户通过助记符+密码的方式使用钱包，钱包可以进行转账和收款。

## 帐户安全

匹克链通过具有安全性的 SSL 加密的 HTTP 通道（HTTPS）作为访问后台的唯一通道，提供内容加密、身份认证、数据完整性等建立一个信息安全通道，确认网站的真实性和防止内容被第三方篡改。

平台提供两级的账号验证保证系统平台的安全，用户通过账号、密码登录匹克链、竞技竞猜平台服务器，通过用户的私钥进行匹克链转账交易，登录服务器提供密码策略、登录令牌、失效机制等提供第一层的安全屏障；通过非对称加密的公钥、私钥加密机制保证用户交易的安全性，提供第二层的安全保护机制。



---

## 匹克链引擎

为了保证竞技竞猜平台等规范的接入匹克链，我们定义了一套平台引擎来规范各方的接入

◆ 统一的接入 KYC 标准

匹克链会根据各个地区对于用户参与竞技竞猜业务的要求，对某些用户做 KYC 认证，而各方平台只需要通过接入引擎接口验证用户真实信息，避免开发重复的 KYC 系统。

◆ 统一使用可验证的随机数生成机制

由平台引擎提供的随机数种子的，可以由平台引擎做验证，避免人为操纵游戏。

◆ 统一的数据上链标准

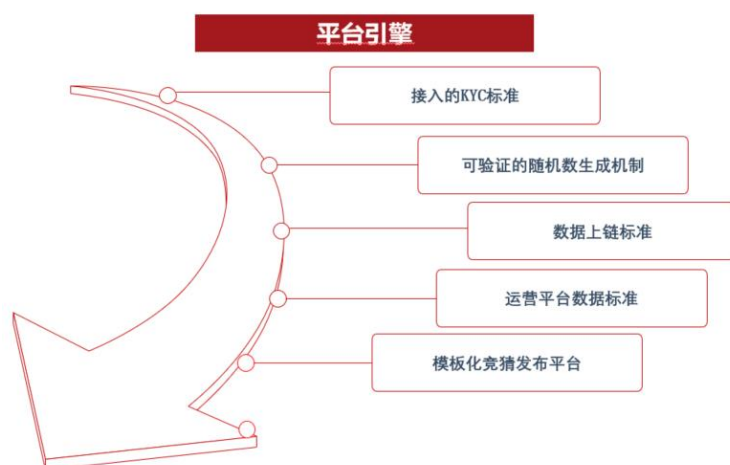
竞技竞猜平台在接入匹克链的时候，使用到链上的记账以及保存竞技竞猜数据的时候，需要提供符合标准的数据。

◆ 统一的运营平台数据标准

提供统一的运营平台，而竞技竞猜平台所要做的就是在通过平台引擎接入的时候使用符合匹克链的数据标准。

◆ 模板化的事件竞猜发布平台

提供后台管理服务，可以根据模板化的事件竞猜模板，按照平台的发布向导，完成事件竞猜项目应用，直接将项目应用分享到各个社交平台。



---

## 区块链浏览器

匹克链是一个开放、公开、去中心化的公链，里面记录的数据是不可更改，人人都可以查阅的账本，对于普通用户如何查阅区块信息，有一定的难度。

每笔交易、竞技竞猜数据都有不可篡改的时间序列，匹克链提供区块链浏览器，用户只需要通过浏览器既可以查询所有的竞技竞猜数据、交易数据，也可以通过匹克链浏览器查询到自己的所有历史记录，让用户一目了然。

## 跨链交易

匹克链提供兼容以太坊标准的 ERC20 跨链交易网关，支持大部分的以太坊以及在以太坊上发行的代币的交易

接入闪电网络，通过可撤销的顺序成熟度合同（RSMC）保障了两个人之间的直接交易可以在链下完成；同时，由哈希的带时钟的合约（HTLC）保障了任意两个人之间的转账都可以通过一条“支付”通道来完成。

通过交易所网关打通匹克币 PKC 公开发行交易的通道，根据不同的交易所的接入接口，做不同的适配；通过打通与交易所的通道，可以有更多的数字货币可以购买匹克币 PKC，参与竞技竞猜，让用户手中的数字货币流通起来。

通过接入支付宝等法币支付通道，让匹克币 PKC 能更加便捷的在二级市场 and 法币进行交易。

在所有的跨链网关交易的业务模型中，智能合约扮演了核心的作用。



---

## 安全

### 节点安全

匹克链的区块生产者选出的 67 个节点，这些节点都是区块生产主节点，每轮随机选出 11 个节点作为区块生产者，这 11 个节点或者 67 个主节点都有可能遭受到恶意攻击者的攻击，这些攻击中，最严重的是 DDoS 攻击，DDoS 的攻击方式有很多种，最基本的 DDoS 攻击就是利用合理的服务请求来占用过多的服务资源，从而使合法用户无法得到服务的响应。

节点生产者节点通过下面的方式避免遭受 DDoS 攻击的影响：

- ◆ 节点生产者服务器采用高防服务器，安装专业抗 DDoS 防火墙
- ◆ 对系统升级最新补丁，并采取有效的合规性配置，降低利用漏洞攻击的风险
- ◆ 节点生产者服务器之间通过数字签名方式相互验证
- ◆ 限制特定的流量，过滤不必要的服务和端口

另外，由于匹克链采用了新的基于 BFT-rDPoS 的共识机制，67 个节点都是区块生产主节点，每轮会随机选择 11 个节点作为区块生产节点，而且算法会暂时剔除工作异常的节点，让攻击者找不到攻击目标，这样大大增加了 DDoS 攻击的难度，即使某几个节点被攻击，还有很多主节点可以继续工作。

# 匹克币 PKC 发行计划

由于现在的匹克链还在开发当中，我们会在以太坊上发行符合以太坊 ERC20 的匹克币 PKC 代币作为前期募资代币，一旦匹克链开发完成，我们将所有在以太坊募集代币映射到匹克链主网。

## 6.1 发行计划

总的发行量：10 亿

团队：15%

私募：35% 接受：ETH，起投量：100ETH 等值

私募：软顶：5000ETH，硬顶：12000ETH

私募：1ETH = 50000~300000PKC

	发行总数	标准定价	私募（第一期）	私募（第二期）	私募（第三期）
	10000000000		3500000000		
1ETH 兑换		20000	50000	40000	30000
募集 ETH 数			7000~12000		
折价			40%	50%	60%

基金会：20%以及从竞技竞猜中的抽水（不高于收益的 1%）来维持匹克链运营的日常开销和匹克币 PKC 持有用户的分红

社区：20%作为社区运营费用 顾问：5% 法律和财税：5%

## 6.2 募集资金用途

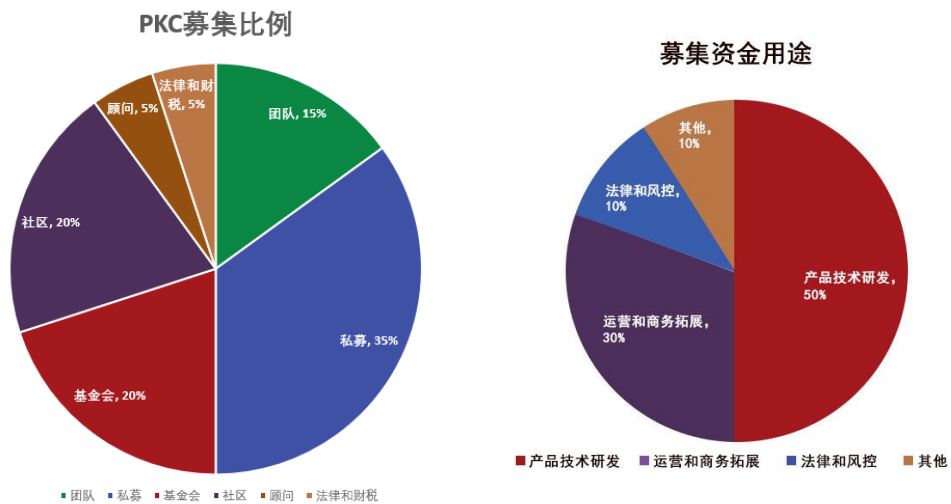
产品技术研发：50%

运营和商务拓展：30%

法律和风控：10%

其他：10%

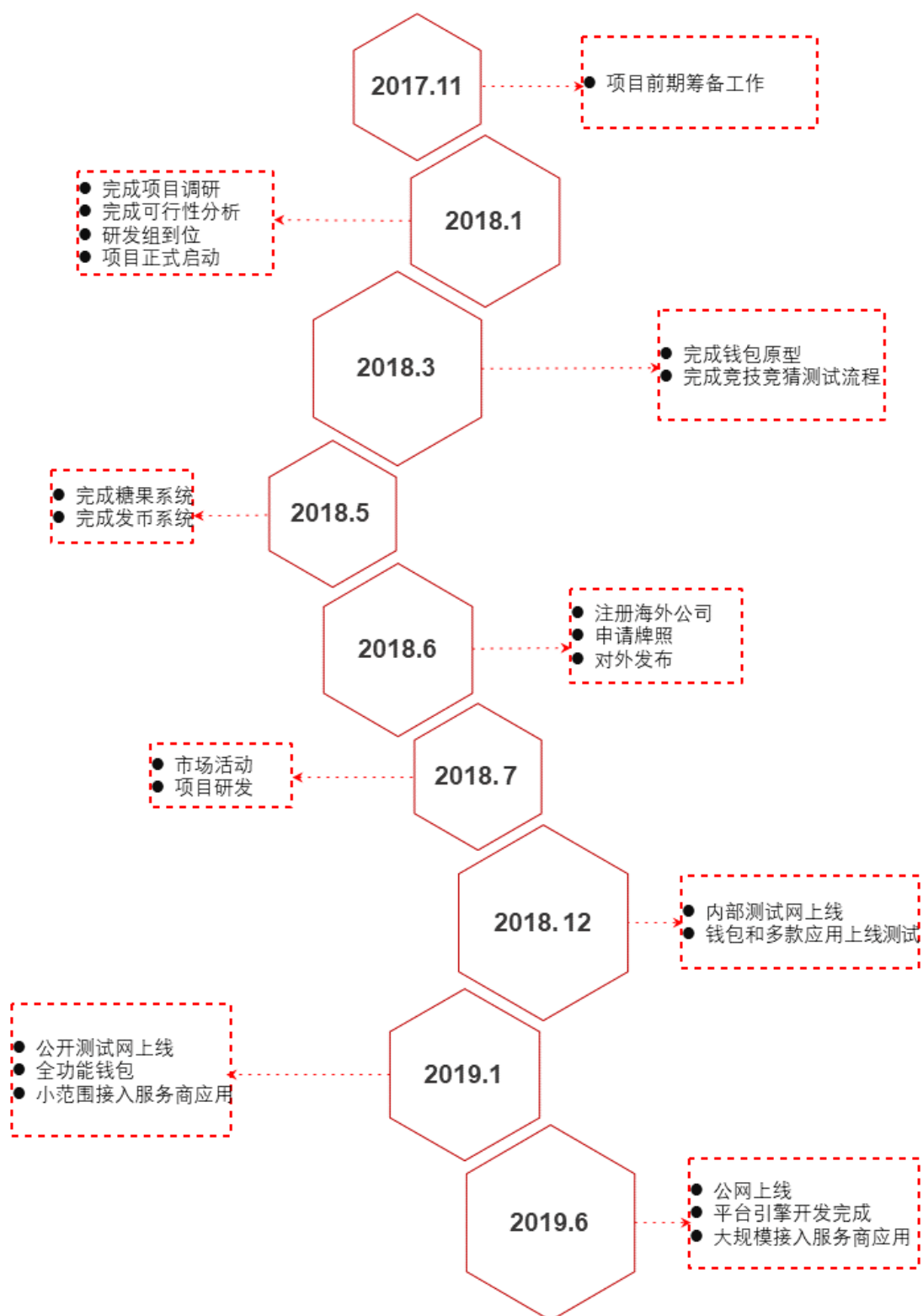




### 6.3 锁定期

成员	锁定期	释放规则
创始团队	24 个月	锁定期后，每月最高释放 20%，20%，20%，20%，20%
顾问、	6 个月	锁定期后，每月最高释放 20%，20%，20%，40%
法律和财务	6 个月	锁定期后，每月最高释放 20%，20%，20%，40%
私募	3 个月	锁定期后，每月最高释放 20%，20%，20%，40%

# 历程



---

# 法律法规

## 运营主体

匹克链作为一个去中心化的平台，各方在此平台上都是自主主权身份，依赖于匹克链建立互相信任的关系，不是一个组织或者个人作为盈利的工具。因此，平台的运营主体会是在新加坡建立的 PlayChain 基金会（PlayChain Foundation LTD.），由新加坡会计与企业管理区（ACRA）批准建立，受新加坡公司法监管。

该基金会主要的任务就是公开、公正且透明不以盈利为目的地运营匹克链，并且为匹克链的开发团队进行资金支持。

匹克链会建立每个国家符合当地法律政策相关内容的审查委员会，以保证在这个国家的内容均符合当地的法律法规和文化。

---

# 团队

团队是由多位长期从事游戏以及区块链行业的专业人士组成，于 2017 年底启动了该项目，在过去的半年时间，项目匹克链的底层技术以及竞技竞猜项目的原型已经开发完成，期间，不同领域的专业人士已经加入了团队，我们的团队包括编程、市场营销、金融和法律等专业人士。

## 团队成员

### Viktor Pavletic – 创始人 CEO

2009 年以来创立多家互联网游戏企业，2011 年后涉足手机游戏行业，自研运营多款口碑良好的手游，2015 年开始关注区块链行业，致力于区块链与游戏行业的结合，2017 年创立 PKC.one，并一直担任 PKC.one 的总经理兼首席执行官。

### Adam Seleznev – 首席运营官 COO

多年以来，一直从事市场营销工作，是市场营销领域专家，主导的手游运营获取行业前列的市场规模和盈利，2016 年开始主要区块链项目的运营策划。

### Eugene Kulbashian – 首席技术官 CTO

主要研究方向是密码学理论和人工智能，信息处理专业硕士，多篇密码学论文的编撰者，在信息安全领域有 10 多年的研究和开发经验。

### Duncan- 区块链技术总监

区块链专家和早期加密技术采用者，参与过许多加密项目，还开发了用于加密货币交易的高频交易算法，CasinoCoin 基金会的创始人，该基金会通过其

---

CasinoCoin (CSC) 品牌开始吸引赌场和在线赌博业。

## **Daniel Lemmon - 首席程序员**

多个 github 社区项目贡献者，精通 C++、ObjC、Ruby 等开发语言，对于 LLVM 编译器架构有深入的研究。

## **Tony Ulyanov - 专业的自由程序员**

社区代码贡献者，github 上多个代码库的开发维护。

## **Jamal Seleznev – 前端网页开发者**

2010 年以来一直从事前端页面的开发，精通 Html5、CSS3、Javascript 等，对于以太坊的 web3 有深入的研究。

---

# 合作伙伴

PLAYWORLD PTE. LTD.

## Leo Mu –CEO

毕业于北方工业大学，工业管理工程专业，15 年游戏开发运营 经验。曾任职卓望数码任产品策略经理，2003 年开始从事手游 开发和运营，曾成功引入和运营俄罗斯方块等知名手游；2004 年联合创立网易达科技，专业从事手机游戏开发，2005 年就组织棋牌游戏的开发和运营，智能手机时代，第一批作为制作人成功制作弹弹岛系列手游、作为创始制作人制作一起来飞车系列，以上产品除部分地区带给英雄互娱、易幻、越南 VNG 等知名发行商外，还自己建立了覆盖全球的发行体系，累计流水超过 10 亿元。

## David - COO

毕业江西师范大学工商企业管理专业，十多年的游戏从业经历，行业精细化服务提出者和建立者。先后就职于各大研发和发行上市公司，负责游戏产品的社区运营，用户运营，达成亿级流水；负责体育棋牌国内外推广，通过线上线下资源整合推广，产品流水过亿。

## Brain Hu - CTO

毕业于西安电子科技大学，曾供职于传媒行业、互联网企业等，近二十年的互联网从业经验，为报纸媒体行业提供数字资产解决方案，报纸媒体客户包括香港苹果日报、经济日报、马来西亚星洲日报等，也为香港周生生、上海迪士尼等提供商业数字资产管理解决方案，近三年主要研究方向为区块链在数字资产以及数字版权行业的应用。

---

## Stephen Chou

十多年游戏研发从业经历，曾多次创业和服务于上市公司，担任 CTO。带领团队独立开发语音社交软件、多套游戏系统框架，实现功能引擎化；做过多款竞技棋牌和预测产品，对竞技竞猜产品有深刻的理解。

---

# 顾问

## 顾问团队

### Nicko Deng

英国诺丁汉大学信息技术与管理学硕士，志成资本创始合伙人、中国新锐投资人。比特币项目早期参与者，以太坊社区忠实粉丝，对区块链技术和应用有深刻的认识和理解。曾参与多个区块链项目并担任顾问。

### Simon Schwerin

曾撰写关于区块链和隐私的硕士论文，特别是关于 GDPR 的论文。毕业后在 XAIN 担任业务发展经理，现为 medixain 公司首席执行官，他致力于在医疗保健和区块链领域构建解决方案。此前，他曾在 BigChainDB 工作，负责商业战略和项目管理。他也曾领导过德国公共区块链（又名联邦区块链）工作组。

### Gi Nam Lee

法律顾问，韩国电竞协会会员，精通各国数字货币相关政策、法律，有丰富的区块链市场法务经验，担任多个区块链项目法律顾问。

### Svetlin

Svetlin 拥有 20 多年的软件工程师，技术培训师和数字企业家的经验，侧重于构建分散式区块链项目的技术挑战。他是几个成功的 ICO 项目的区块链教练，顾问和技术顾问，也是 9 本技术书籍的作者。拥有计算机科学和十项技术奖项的博士学位。他在数字技能大学 SoftUni 中热情地培养了数千名软件工程师。



---

# 风险与法律免责

该文档只用于传达信息之用途，并不构成买卖匹克链项目投资的相关意见。任何类似的提议或征价将在一个可信任的条款下并在可应用的相关法律允许下进行，以上信息或分析不构成投资决策或具体建议。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。

## 风险提示

### 政策性风险

目前国家对于区块链项以及互换方式融资的监管政策尚不明确，存在一定的因政策原因而造成参与者损失的可能性。

包括匹克币 PKC 在内的数字资产交易具有极高的不确定性，由于数字资产交易领域目前尚缺乏强有力的监管，故而代币存在暴涨暴跌，个人参与者入市后若缺乏经验，可以难以抵御市场不稳定所带来的资产冲击与心理压力。如果监管主体对该进行规范理，互换时期所购买的代币可能会受到影响，包括但不限于价格和易售性方面的波动和受限。

### 市场风险

市场风险是指匹克链没有被市场接纳，或者没有足够用户使用，业务发展停滞，没有足够利润支持。

匹克链并不预期在发行后的很短时间内就广受欢迎、盛行或被普遍使用。在最坏的情况下，匹克链可能被长期边缘化，仅吸引少部分使用者。

### 技术风险

匹克链项目仍处于开发阶段，由于产品系统的技术复杂性，会面临底层技

---

术出现重大问题，导致匹克链项目无法实现预期功能，以及关键资料被篡改或丢失的风险。如果确有此类技术瑕疵，将损害匹克链项目的可用性、稳定性或安全性，并因此对匹克链项目的匹克币 PKC 的价值造成负面影响。

## 资金风险

资金风险是指项目资金出现重大损失，例如：资金被盗，资金亏损，储备金大幅贬值等。尽管匹克链项目团队将采取业内最先进的技术方案保证众筹资金的安全，但是某些网络黑客行为仍很难被彻底阻挡。

---

## 参考资料

1. 《区块链：定义未来金融与经济新格局》 - 张健 - 机械工业出版社
2. Merkle tree – Wiki – Source: [https://en.wikipedia.org/wiki/Merkle\\_tree](https://en.wikipedia.org/wiki/Merkle_tree)
3. Bitcoin: A Peer-to-Peer Electronic Cash System – Satoshi Nakamoto – Source: <https://bitcoin.org/bitcoin.pdf>
4. A Next-Generation Smart Contract and Decentralized Application Platform – Vitalik Buterin – Source: <https://github.com/ethereum/wiki/wiki/White-Paper>
5. Bitshares whitepaper – Daniel Larimar – Source: <http://docs.bitshares.org/bitshares/papers/index.html>
6. EOS.IO Technical White Paper v2 – Daniel Larimer – Source: <https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md>
7. IPFS – Content Addressed, Versioned, P2P File System(DRAFT 3) – Source: <https://ipfs.io/ipfs/QmR7GSQM93Cx5eAg6a6yRzNde1FQv7uL6X1o4k7zrJa3LX/ipfs.draft3.pdf>
8. BIP-32 – Source: <https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki>
9. BIP-44 – Source: <https://github.com/bitcoin/bips/blob/master/bip-0044.mediawiki>
10. BIP-39 – Source: <https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki>
11. Lightning Network – Source: <https://github.com/lightningnetwork/lnd>
12. The future of online gambling: Ethereum smart contracts. Source: [http://www.maltatoday.com.mt/sponsored/sponsored/83457/the\\_future\\_of\\_online\\_gambling\\_ethereum\\_smart\\_contracts](http://www.maltatoday.com.mt/sponsored/sponsored/83457/the_future_of_online_gambling_ethereum_smart_contracts)
13. Do casinos cheat? – Richard Glenn – Source: <https://www.quora.com/Do-casinos-cheat>
14. Guide: Proof of Work (PoW) vs Proof of Stake (PoS) vs Delegated Proof of Stake (DPoS) – Source: <https://steemit.com/bitcoin/@mooncrypton/guide-proof-of-work-pow-vs-proof-of-stake-pos-vs-delegated-proof-of-stake-dpos>
15. EOS Official Website – Source: <https://eos.io/>