菩提预测市场白皮书

版本号: *0.7*

林吓洪*

**Bodhi Foundation*

摘要

菩提（Bodhi）是一个全新的基于区块链的去中心化预测市场。通过引进信息中介（Oracle）抽象层将第三方Oracle和基于投票的去中心化Oracle统一起来， 整合了现有去中心化预测市场的优点。同时引进首创的可替代Oracle机制使Bodhi预测市场兼具高效和自治的特点。Bodhi平台将首先在量子链上部署。

关键字

菩提，预测市场，智能合约，量子链，以太坊

I. 引言

自古以来人类对未来事件发生与否的预测充满兴趣。明天的天气会如何？今年欧冠哪只球队会夺冠？明年1月1日Apple的股价是否会低于100美元？类似的问题人们每天都在谈论，甚至押注重金在自己看好的结果上。人们对预测的热情催生了像体育竞猜、股市等市值上万亿的传统预测市场。也恰恰因为这种热情，催生了像地下赌场、内幕交易等非法行业，同时也导致了随之而来的严厉监管。监管和法律限制让预测市场无法完全自由发挥其应有的市场效应，大量的资金浪费在监管成本上。与此同时，传统预测市场严重依赖中介从中发挥作用，预测事件的结果和公正性都需要中介从中撮合，这也导致大量的资金

被中介收取。这些高额的成本严重降低了用户的回报率和预测市场应用的大规模普及。

预测市场是指人们对有明确结果的未来事件进行预测的一个平台，人们可以为自己看好的结果进行押注。预测正确的一方将赢得错误一方的赌注。为了尽可能获胜，人们会通过各种方式，如信息收集、数学建模等方法来让预测结果尽可能准确。因此，预测市场的每一个可能结果的价格也一定程度上反应了结果发生的概率。相应的，预测准确率也受到参与人数规模的极大影响。自信息革命开始以来，人类一直致力于将预测市场在线化，以方便所有用户通过互联网快速便捷地参与预测市场。然而中心化的互联网产品无法成为人们信任的基石，同时，过度的监管和法律限制也极大限制了预测市场的发展。

随着区块链技术的发展，公有区块链成为一个公正并且去中心化的信任中介。信息透明、不可篡改等特性让区块链成为预测市场完美的运行平台。区块链天然的公正性让预测市场的运行近乎零成本。智能合约的实现更是让区块链拥有可编程动态决定结果的计算能力。去中心化的预测市场在这样的背景下应运而生。Bodhi [1]的使命就是建立可信、自治、可扩展的预测市场，将预测市场普及全球，提高人们决策的有效性。

II. 相关工作

Augur [2]是第一个基于区块链的去中心化预测市场。使用以太坊 [3]的智能合约，用户可以自由在Augur平台上创建针对特定事件的预测事件。其他用户就可以在预测事件上对自己看好的结果进行押注。最后，在预测事件发生时，Augur的REP持币者将向Augur汇报该预测事件的结果。Augur的事件仲裁机制由REP持币者共同决定，REP持币者是Augur平台的维护者。然而Augur平台的仲裁机制存在规模化问题。当大量的未来事件预测事件在平台上被创建的时候，REP持币者将无法对每个事件都进行投票，同时REP持币者由于各自的领域知识不同，对不同事件的熟悉程度也不同，如何把事件与最了解该事

件的持币者相匹配也是Augur亟需解决的问题。REP持币者的时间成本高，效率低，更导致在预测事件发生后Augur需要较长的时间才能得出最终结果。

Gnosis [4]是另一个基于区块链的去中心化预测市场。同样使用以太坊的智能合约，Gnosis在预测事件的创建和参与上和Augur极为类似。与Augur不同的是，Gnosis采用一个默认情况下中心化的信息中介（Oracle）来判定预测事件结果。这样做的好处是能够将预测事件的判定自动化，极大提高事件的判定效率。然而信息中介（Oracle）也有其不足之处：信息中介（Oracle）由于是中心化服务，极有可能出现服务失败的情况，例如服务器崩溃，外部数据被恶意篡改等。一旦这种情况发生，Gnosis平台的自身信誉将受到重大影响。同时待裁决事件也会因为信息中介（Oracle）失灵致使用户的赌注被智能合约锁定。

III. BODHI预测市场的工作机制

Bodhi是一个全新的基于区块链的去中心化预测市场。结合了Augur和Gnosis各自的优点，致力于创建下一代预测市场的新平台。

Bodhi将首先在量子链 [5]上部署。当前互联网已经是移动互联网时代，未来的用户将优先使用手机来参与预测市场。量子链结合了比特币和以太坊各自的优点，能够在手机移动端提供更加优质的用户体验。与此同时，事件预测是对时间有严格要求的项目，而智能合约目前只能靠区块数来预估时间。以太坊目前仍未实现PoS（Proof of Stake），而当前使用的PoW（Proof of Work）中的难度炸弹（Difficulty Bomb）正在生效，区块数的出块时间将会越来越长（见表 I），这将严重影响预测事件的时间估算。而量子链一开始就会引入PoS，这保证了出块时间的稳定性。基于这些原因，Bodhi将首先在量子链上部署。预测市场是一个全球市场，为了让用户群体最大化，我们未来不排除在其他公有链上

部署Bodhi平台。

表 I
难度炸弹（DIFFICULTY BOMB）生效对出块时间的影响

Block Number	Time	Block Time
3000000	2017-01-16 00:38:33	14.86
3500000	2017-04-11 18:09:34	15.27
4000000	2017-08-15 18:20:24	30.01
4500000	2018-11-03 05:55:48	136.71
5000000	2025-10-02 11:47:30	835.81
5500000	2128-03-20 09:14:16	17183.83
6000000	5189-09-26 20:57:59	520901.19

Bodhi继承了Gnosis的核心理念，预测事件的结果由第三方信息中介（Oracle）来自动判定。这保证了结果判定的效率。与此同时，Bodhi借鉴了Augur的思路，当信息中介（Oracle）失效或错误时，Bodhi代币BOT的持有者可行使投票权，对相关预测事件进行最终裁决。

Bodhi的运行原理详述如算法 1所示。

由于可见，Bodhi的信息中介（Oracle）是可替代的，假如用户对仲裁请求的投票结果仍有异议，用户可以继续支付质押金进行下一轮的仲裁请求。由于每一轮仲裁的质押金越来越多，同时BOT持有者会了维护Bodhi平台的准确性，从而保障自己的代币价值，最终绝大多数的BOT持有者将做出公正裁决。菩提引进了信息中介（Oracle）抽象层，将第三方Oracle和基于投票的去中心化Oracle统一起来。这项技术让菩提同时兼具现有去中心化预测市场的各自优点。

IV. BODHI预测市场的平台费用

Bodhi致力于打造一个自由、低成本的预测市场。信息中介（Oracle）是Bodhi平台事件的裁判，为了激励更多的信息中介（Oracle）为Bodhi提供可信稳定的服务，信息中

Algorithm 1 Bodhi的核心算法

用户在Bodhi平台上创建预测事件
用户针对该预测事件进行押注
当未来指定时间到达时，信息中介(Oracle)将会自动从外部获取事件的结果，并确定该预测事件的结果
$Agreement \leftarrow False$
while $Agreement \neq True$ **do**
    判定结果将在预测市场公示48小时
    if 仲裁结果有效并且无人提出异议 **then**
        $Agreement \leftarrow True$
        预测正确的一方将能够取得自己的本金和回报
    else
        $Agreement \leftarrow False$
        对结果持有异议的用户通过支付质押金的方式提出仲裁请求
    end if
end while

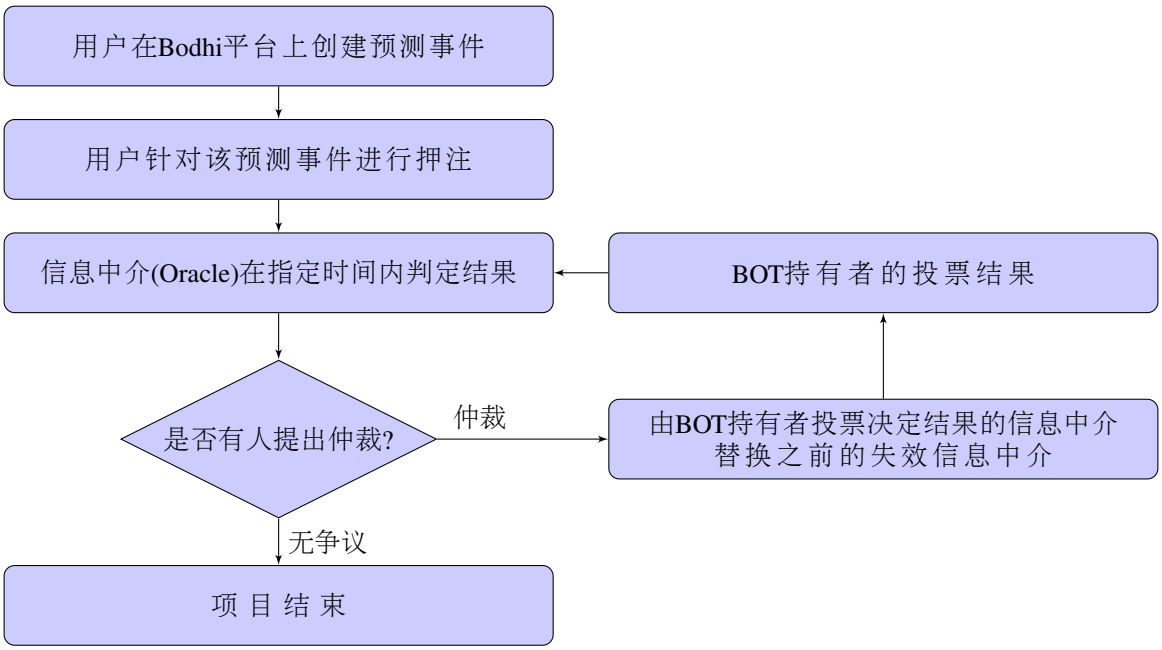

图 1. Bodhi的运行原理

介（Oracle）将获得其所判定的预测事件资金的一小部分作为服务费。与此同时，BOT持币者是Bodhi平台的维护者，为了激励持币者的积极性，平台会从每个预测事件中扣除一笔手续费。这些手续费将作为分红分发给BOT持币者。具体费率，我们将在Bodhi上线时制定一个初始值，假设服务费为F_f（百分比），手续费为F_s（百分比），预测失败一方总

投注为S_{loss}，那么预测正确一方获得的收益S_{win}将是：

$$S_{win} = S_{loss} \times (1 - F_f - F_s) \tag{1}$$

值得一提的是，未来这个费率将是动态的，我们将在Bodhi上创建针对这个费率的预测事件，让所有BOT持有者共同投票决定最佳费率。

V. BODHI代币机制

Bodhi预测市场的代币叫做Bodhi Token，代号BOT。代币将在众筹期间发行，BOT总量为1亿个。

Bodhi不会发行类似Gnosis中的WIZ代币，原因是为了保证平台逻辑的简洁和独立。在Bodhi上线之初，我们将只支持BOT币和QTUM币参与押注，用户可以自行采用对冲的方式来保证押注和法币挂钩。区块链技术正在以飞快的速度向前发展，稳定币和跨链技术正在如雨后春笋般涌现。待技术成熟后，Bodhi将允许使用任意数字货币参与押注。BOT所代表的权益主要有两个：

1) 分红。由于Bodhi预测市场绝大多数预测事件都由信息中介（Oracle）自动判定结果。BOT的持有者将按照持币比例被动获得Bodhi预测市场的手续费收入分红。除此之外，BOT的持有者还能通过抵押BOT的方式对有争议预测事件提起仲裁，如果仲裁成功，将获得败诉方代币的一部分作为回报。BOT的持有者还能通过抵押BOT的方式参与对有争议预测事件的投票，如果投票与最终结果一致，将获得败诉方代币的一部分作为回报。
2) 投票。BOT的持有者在预测事件结果判定出现争议时能够参与投票仲裁。每当预期事件的失败方对结果有异议时，可通过锁定一部分质押金来提出仲裁请求，BOT的持有

者有权参与仲裁，并获得本次仲裁的一部分手续费。BOT的持有者还能行使投票权将非法和恶意的预测事件强行关闭。

VI. BODHI审查机制

Bodhi是一个基于区块链的自由开放预测市场。然而这并不意味着Bodhi是一个完全没有限制的平台。Bodhi平台将提供一个去中心化的审查机制，BOT代币持有者为了保障Bodhi平台不被非法利用并保护自己的BOT代币权益，可以通过投票的形式将某些明显恶意和非法的预测事件强行关闭。

VII. BODHI开发计划

Bodhi的开发时间线如图 2 所示。我们计划在2017年9月底实现菩提预测市场代币ICO，2017年12月实现菩提预测市场测试版上线量子链测试网，2018年6月实现菩提预测市场MVP版上线量子链主网，2018年12月实现菩提预测市场正式版上线量子链主网，2019年6月实现菩提预测市场优化版上线量子链主网。

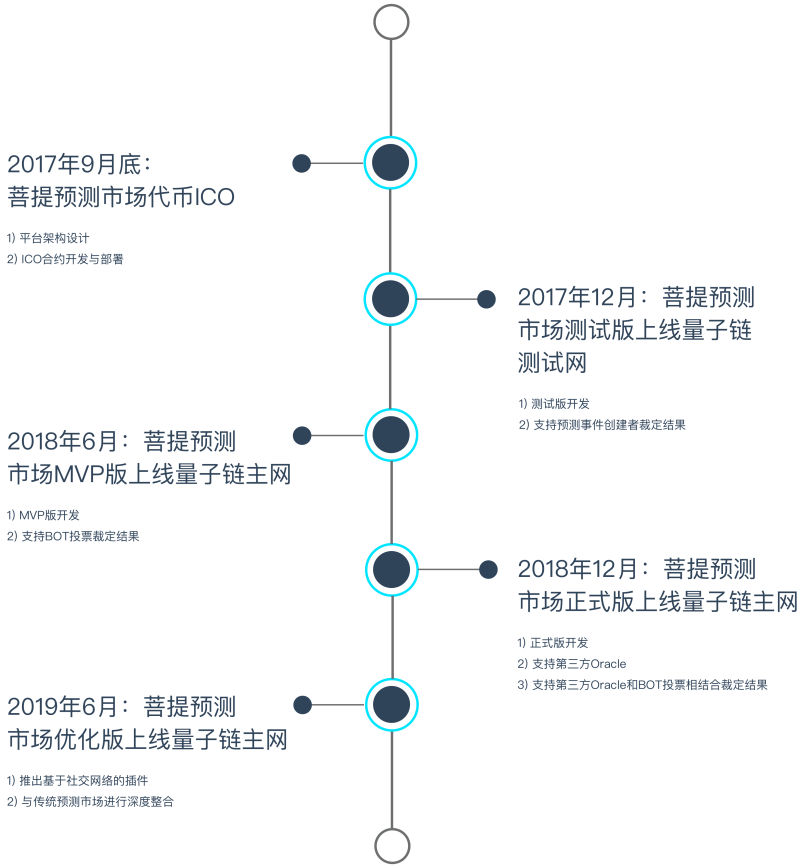

图 2.　Bodhi的开发时间线

VIII. BODHI预测市场的应用场景

A. 场景一：金融工具

目前传统的金融市场预测工具存在许多不足：中介费用高昂，有专业化要求，可拓展性差，表达能力有限，准确率不足，效率低下等。而Bodhi的预测市场有别于这些金融工具的特点是：可以为经济事件带来更加细微和详细的表达方式，从而可以从宏观和微观经济层面更明确地评估价值及风险，并降低中介费用，去除专业化门槛，易于拓展，提高准确率且高效。 例如，创建一个预测事件如“苹果的股票在2018年1月1日的开盘价是多

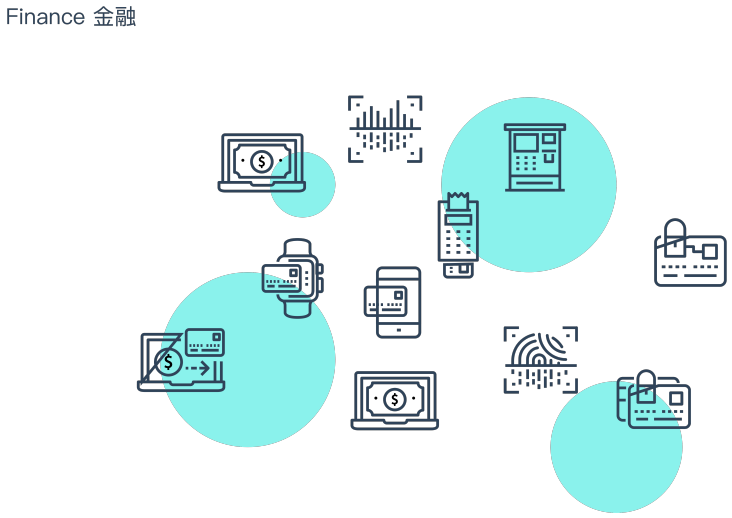

图 3. 场景一：金融工具

少？”，对于这个预测事件，传统的金融市场预测工具需要分析投资环境，了解企业基本状况，核算企业财务，最后计算投资收益，才能粗略的给出预测结果。而同样的预测市场在Bodhi上被提出来，获得的结果是全网的计算结果，不仅成本低廉，而且结果相当于全网模拟股票交易后得出的结果，所以结果更精准，效率更高，而且还能拓展到其他股票，任意时间，收盘价等等。

B. 场景二：信息

信息对于人类社会的发展至关重要，很多决策都要依赖于准确可靠的信息。为了获得精准的信息来提高决策准确度，人们采用多种信息获取方式，如：问卷调查、有偿数据交易等。然而这些信息获取方式不仅成本高昂，而且覆盖面狭窄。预测市场能够激励有消息来源的人通过押注的方式主动提供信息。例如1988年美国爱荷华大学的几位教授建立了一个爱荷华总统选举预测市场，在该市场中，参入者可以投入一定数量的金钱，交易标的是谁将当选下一任美国总统。该市场建立以来，准确地预测了每次美国总统选举的结

图 4.　场景二：信息

果，其准确度要大大高于政治评论专家以及民意测验的结果。Bodhi将让每个人都轻松建立类似的预测市场，区块链的价值传递网络将是预测市场最坚实的信任基础。在Bodhi上发布预测事件，由于Bodhi去中心化的特点，产生的结果更接近大众民意，而且相当于全员匿名参与，这将大大提高预测的准确性。

C. 场景三：保险

保险是一个和大众息息相关的行业。传统保险业由于中心化管理，出现了流程太长，理赔手续繁杂缓慢等令人诟病的问题。同时庞大的保险公司代理体系也使保险的很大一部分收益被用于企业运营。Bodhi的去中心化预测市场能够完美解决这些不足。例如，利用Bodhi平台可以创建一个航空险预测事件。想购买航空险的用户可以在乘坐航班前押注自己所乘航班会延误。大多数情况下，用户的航班都会准时，从而用户押注的代币将锁定在航空险预测事件对应的智能合约里。当某个航班发生延误时，航班信息中介（Oracle）将会把延误航班的航班号写入该航空险的智能合约。Bodhi平台将会自动为购买

图 5.　场景三：保险

了该航班号所对应航空险的客户返还理赔金。整个过程是完全自动化且不需要人工干预的，所有用户的押注代币除了一小部分平台手续费以外都将用于客户理赔。

D. 场景四：体育竞猜

全球在线体育竞猜是一个庞大的市场，受监管市场的金额至少高达数十亿美元。由于不同地区的法规差异，体育竞猜呈现局部化，每个竞猜市场都是单独运营的个体。在孤立数据和碎片化市场中运行的竞猜市场可访问性有限，并且无法及时推出用户感兴趣的新竞猜事件。与此同时，监管是把双刃剑，数据显示未受监管市场的竞猜额是受监管的10倍，这也让欺诈和非法运营成为全球竞猜市场的监管难题。此外，因为中心化的服务，很容易出现用户的资金遭遇黑客盗窃，系统故障和服务商违约倒闭等一系列意外问题。而所有这些问题最终都转化为开设全新竞猜市场的高昂成本和向用户收取的高额税费。这进一步限制了竞猜市场的自由竞争以及用户参与竞猜市场的积极性。竞猜市场的高风险让大众把竞猜和投机划上等号。Bodhi带来的创新旨在解决这些问题。Bodhi是基于区

图 6.　场景四：体育竞猜

块链的开放平台，任何人都可以公开透明地参与进来。基于Bodhi的所有预测事件创建者都是平等的，无需高昂手续费即可创建任意竞猜事件。这种自由开放平台将会大大提高市场流动性，从而转化为客观的赔率。

E. 场景五：传统预测市场

Bodhi预测市场致力于打造下一代去中心化预测市场，我们能预见未来的预测市场将是全球用户参与全球协作的。然而市场的演变不是一朝一夕的事情，传统预测市场在未来的一段时间里依然会扮演其重要角色，在社会决策的方方面面发挥作用。Bodhi同样致力于与传统预测市场发挥协同效应，在未来成为传统预测市场的基础设施。传统预测市场需要花费大量的成本和时间在维护自有的预测市场服务器。Bodhi平台在区块链上提供了预测市场所需的大部分逻辑，并且提供一整套简单可替代的解决方案让传统预测市场使用Bodhi平台作为背后的预测市场引擎。这不仅能大大降低传统预测市场的故障率，更能够大大节省成本，降低市场准入门槛。

Traditional prediction 传统预测行业

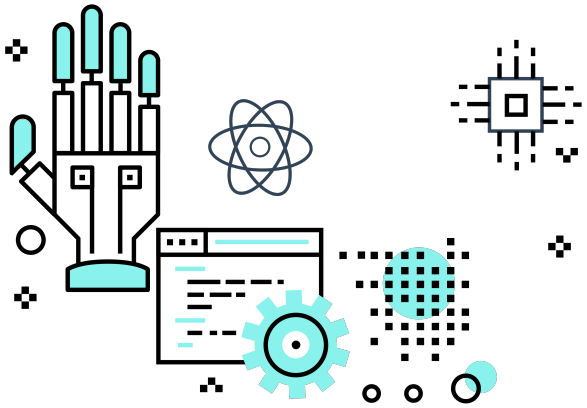

图 7. 场景五：传统预测市场

IX. BODHI代币众筹发行计划

A. *BOT*币分配

BOT总量为1亿个，具体分配比例见表 II。基金会将对团队持有的代币实施四年逐步释放的方案，这是为了保障团队在众筹完成之后能够持续执行开发路线图。

1) 众筹结束后释放20% BOT币
2) 第一年后释放20% BOT币
3) 剩余60% BOT币分三年逐月释放

表 II
BOT币分配表

百分比	用途
60%	众筹阶段分发给众筹参与者
15%	核心开发团队及顾问
10%	长期团队开发激励
10%	基金会锁定，用于早期紧急仲裁
5%	漏洞奖励

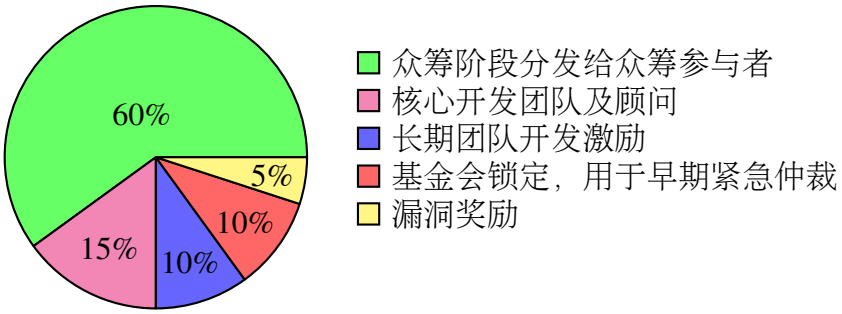

图 8.　BOT币分配饼状图

B. 众筹资金用途分配*:*

众筹资金的具体分途分配比例见表 III。基金会将主要持有众筹所得量子币（QTUM），资金将按五年规划使用。

表 III
众筹资金用途分配表

百分比	用途
65%	开发费用
10%	咨询费用
10%	法律费用
10%	市场营销费用
5%	其他费用

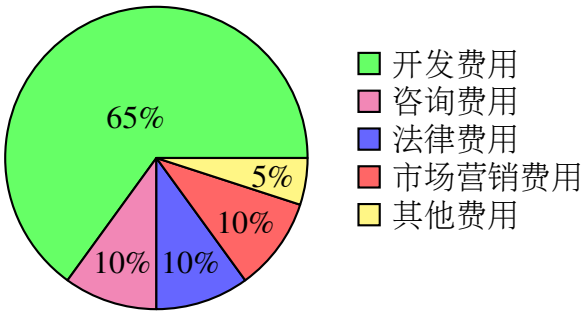

图 9.　众筹资金用途分配饼状图

1) 开发费用：不同于简单的合约开发，预测市场的平台搭建包含了众多模块，平台的开发需要技术研发、招募人才、团队建设，足够的开发费用使得项目得以按计划推进。

2) 咨询费用：预测市场的细分领域繁多，在不同领域的用户习惯将会有很大差异。我们

将用这笔费用来详细咨询相关领域的专业人士和机构，保证充分的市场调研。

3) 法律费用：预测市场是一个法律管控严格的领域，因此大量的法律工作需要资金的支持。同时，针对未来可能出现的某些突发法律事件，我们需要保留一部分应急资金。
4) 市场营销费用：由于预测市场的平台竞争激烈，充分的运营推广及品牌建设是非常重要的。这包括针对传统行业、区块链行业持续不断地推广和普及Bodhi平台；为市场营销提供资金支持；确保Bodhi平台的快速用户增长。
5) 其他费用：除以上之外的各种杂项开支。

X. 总结

Bodhi将打造一个基于量子链的预测市场平台。借助区块链的自由、开放和公正的特性，让全世界的有价值信息自由流通，用群体智慧和激励预测未来。Bodhi的价值中介（Oracle）抽象层将第三方Oracle和基于投票的去中心化Oracle统一起来， 整合了现有去中心化预测市场的优点。同时引进首创的可替代Oracle机制使Bodhi预测市场兼具高效和自治的特点。Bodhi致力于面向世界开拓中国预测市场。

参考文献

[1] “菩提(Bodhi),” https://www.bodhi.network.

[2] “Augur,” https://augur.net.

[3] “以太坊(Ethereum),” https://ethereum.org.

[4] “Gnosis,” https://gnosis.pm.

[5] “量子链(Qtum),” https://qtum.org.