DELPHY

天算

# Delphy 预测市场

# 白皮书

[ v0.6.1 ]

2017 年 6 月 15 日

# 目录

# 第 1 章　执行概要

Delphy 是一个基于以太坊的、分布式的、社交性的、全开源的、预测市场的移动平台。Delphy App 天生就是一个运行在移动终端上的以太坊的轻节点。

Delphy 利用市场的激励机制，帮助市场的参与者透明地、实时地表达自己对未来事件的发生结果的信心和判断，从而实现有效地预测未来。Delphy 内生的分布式的机制保证了预测结果的不可操纵，也为群体智慧所依赖的信息的多元化、决策的独立性和组织的分布式提供了有效的基础设施保障。

Delphy 是一个预测即服务(Prediction as a Service, PaaS) 的移动应用平台和生态链。用户一方面可以随时随地参与预测市场的交易，另一方面也可以利用 Delphy API & SDK 实现各种定制，开设各个垂直领域的预测市场。Delphy 预测市场的应用相当广泛，包括但不限于金融、保险、国防、医疗卫生、公共管理、体育、娱乐，甚至企业内部的预测市场等。

诚如 Delphy 是古希腊神话中的语言与光明之神阿波罗宣布神谕的地方，希望 Delphy 预测市场能利用群体的智慧，从事预见未来的事业，有效地预测、引导甚至创造未来。

# 第 2 章　项目背景

现代的科学预测方法主要有两种，一种是利用统计和数学模型进行预测，另一种是利用机器学习和数据挖掘进行预测。本质上，这两种方法主要利用历史数据和软件系统来产生预测。

近年来，利用“社会化分析（social analysis）”的预测市场作为新的第三种方法呈现异军突起之势。预测市场利用市场的激励机制，使得大众都能贡献出自己的经验和智慧，汇集市场信息帮助人们做决策，让参与者比任何单独的个体、专家更具有智慧。

## 2.1 预测市场：理论和运作方式

信息时代到来以后，科学的预测方法开始被引入。具体而言，预测市场的理论基础是有效资本市场假设（Efficient Capital Markets Hypothesis，ECMH）和海耶克假设（Hayek Hypothesis）。这些假设解释了通过信息的收集整合，市场价格精确地反映未来结果的发生概率。根据 ECMH，资本市场是最能有效地、实时地反映单个股票和整个股票市场信息的机制。海耶克假设认为，市场价格是收集离散信息的有效手段。即使人们对自己的环境和交易对方的知识是有限，市场依然是有效的。

本质上，预测市场是基于市场原则来收集整合交易各方对同一事件的信心和判断，从而产生对事件的未来结果的预测。如果说，股票市场是在为股票未来的预期收益定价一样，预测市场就是在为未来事件的预期结果进行定价。

具体而言，预测市场通常以提问的方式来预测未来某个事件的发生结果，每种结果都有自己发生的概率，所有的结果的概率总和等于 100%。一种结果的概率就代表该结果在市场中的交易价格。交易者可以根据自己对某种结果的信心和判断来购买该结果的股份。比如股份设定为￥1 元人民币的价格，现在发生结果的概率为 60%，它的价格为￥0.6 元人民币。若此结果最终发生，购买该结果的股份的交易者就是赢家，获得的利润每股（1 - 0.6）元的收益，而其他的人不会获得任何收益。

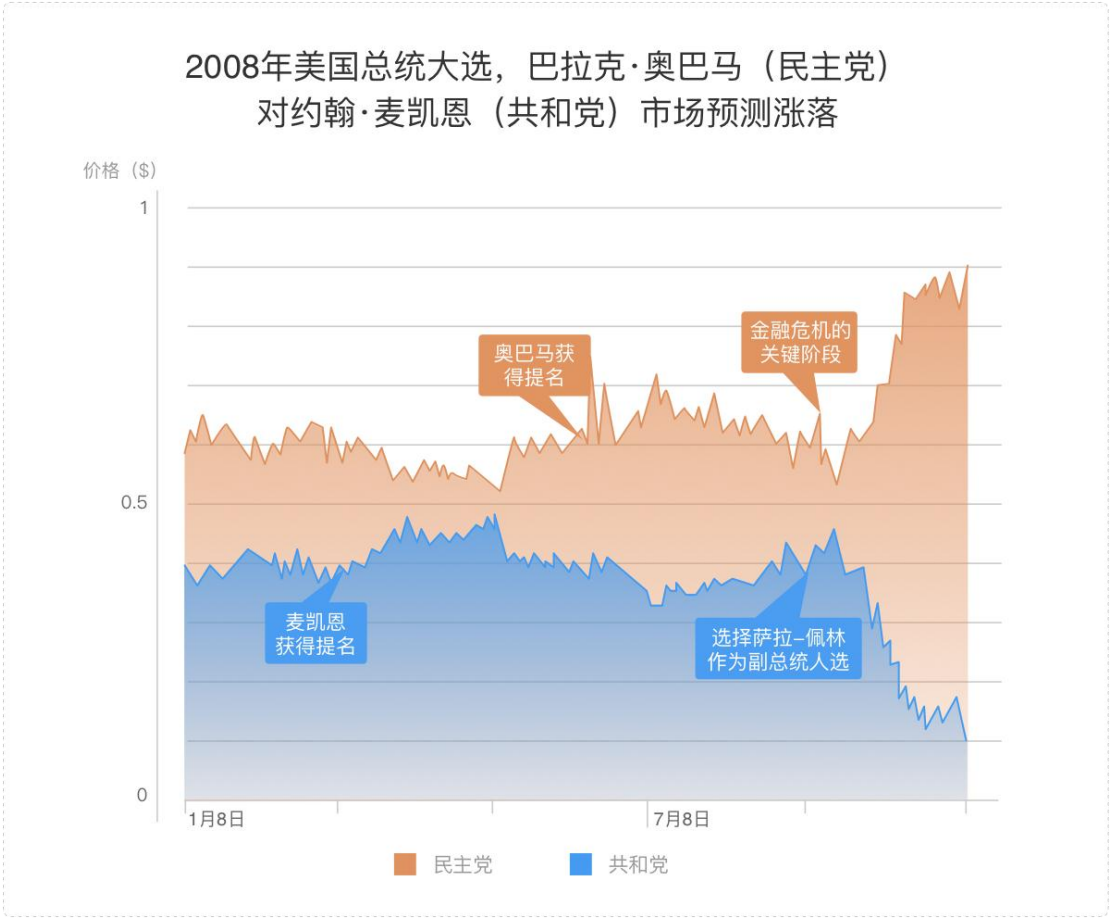
举例：今年的沪深指数是否能够突破 4000 点？

(A) 能够突破 4000 点。(价格为￥0.60) = 60%获胜概率

(B) 不能够突破 4000 点。(价格为￥0.40) = 40%获胜概率

(A) + (B) = ￥1.00 (100%的概率)

在预测市场中，事件结果的概率代表了交易者的判断，而购买的股份数代表了权重和信心，交易者的留言（comments）则代表了交易者的逻辑。




美国著名财经记者詹姆斯·索罗维基曾给出过三种保证预测市场准确的必要条件：信息来源的多元化、独立决策、分布式的组织形式。具体来说，预测市场中的参与者，需要有不同背景，相互之间独立决策，市场的组织形式要是分布式的分布式组织，这样市场最能体现自己的优势。

本质上，预测市场可以帮助把大众的知识（knowledge）和经验（experience），转化为智慧( wisdom)。这是由于预测市场有三大优势：1）它能高效地收集多样而分散的信息；2）它提供了有效的、透明的激励机制以获得真实而相关的信息；3）它提供了近乎实时的信息更新机制从而使操纵结果变得相当困难。

预测市场的应用相当广泛，包括但不限于金融、保险、国防、医疗卫生、公共管理、体育、娱乐，甚至企业内部的预测市场等。举例来说，

1996 年，惠普实验室和加州工学院共同主持了一个为期三年的预测市场的实验。该研究针对惠普实验室的来自不同部门（业务、财务和市场等）的 20 到 30 个员工进行了 12 个不同的预测。实验表明，75%以上的预测比惠普公司的官方预测要准确。

2003 年，美国国防部公布了“政策分析市场”（后来被人戏称为“恐怖主义预测市场”），主要预测中东八个国家的政治和军事的动荡事件及其美国的应对措施，目的是大大提高美国在全球的情报收集能力。后来由于美国参议员的反对，而被迫取消。

2005 年，谷歌宣布在公司内部利用预测市场来预测产品发布日期、新办公室开张和其他有战略意义的事件。

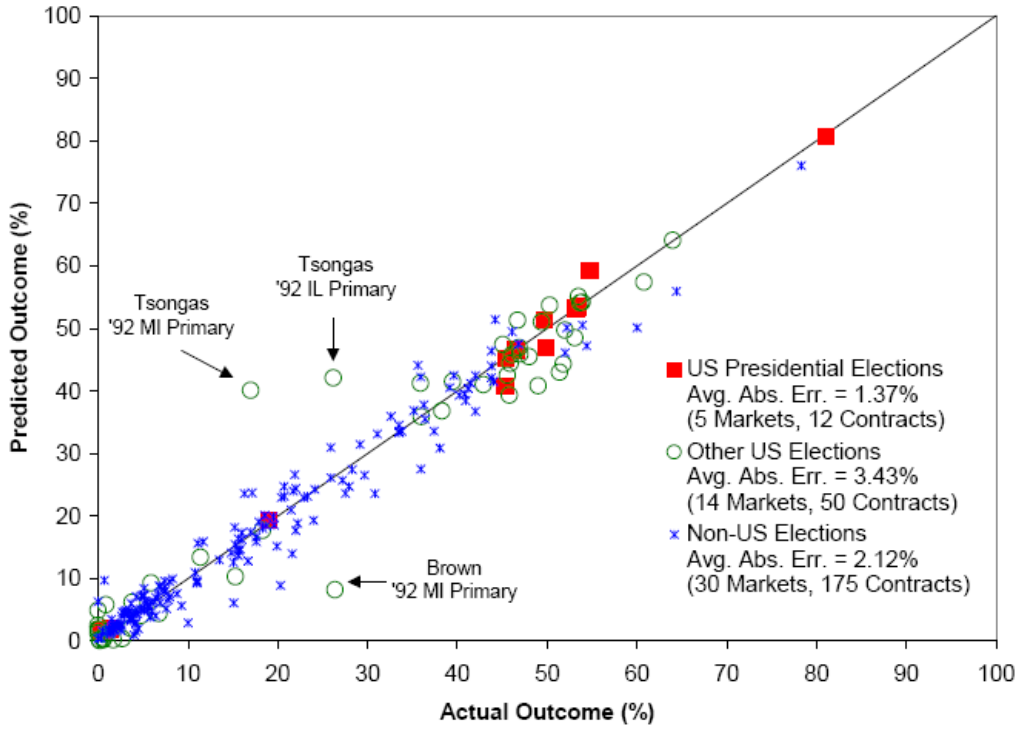
Intrade.com 是著名的政治预测市场。在这里，参与者可以交易各国总统的选举结果，在历年总统大选中，其预测准确度可谓奇高，比如在 2004 年的美国总统选举中，Intrade.com 政治预测市场对布什和克里分别会赢得哪几个州做出的预测，与选举结果惊人的一致。

## 2.2 预测市场的准确性

在预测市场里交易的是未来事件发生的概率，交易合约的价格反映了市场对事件发生概率的动态预期。由于获胜带来的激励，预测市场能够集合所有参与者的共同智慧。实践证明，预测市场的准确度往往比传统预测工具更高，并具备持续实时的信息聚集、积极参与、信息披露、高效率以及可测量性等优势。

由预测市场之父 Robin Hanson 担任首席科学家的网站 Consensus Point 曾

公布，其预测市场的准确度达 92%。在 2008 年，一项调查研究发现，爱荷华大学的 IEM 对 5 次总统选举的预测在 74%的情况下都比普通民调要准确。下图的选举数据很清楚的显示了预测市场的结果的准确性是相当高的。



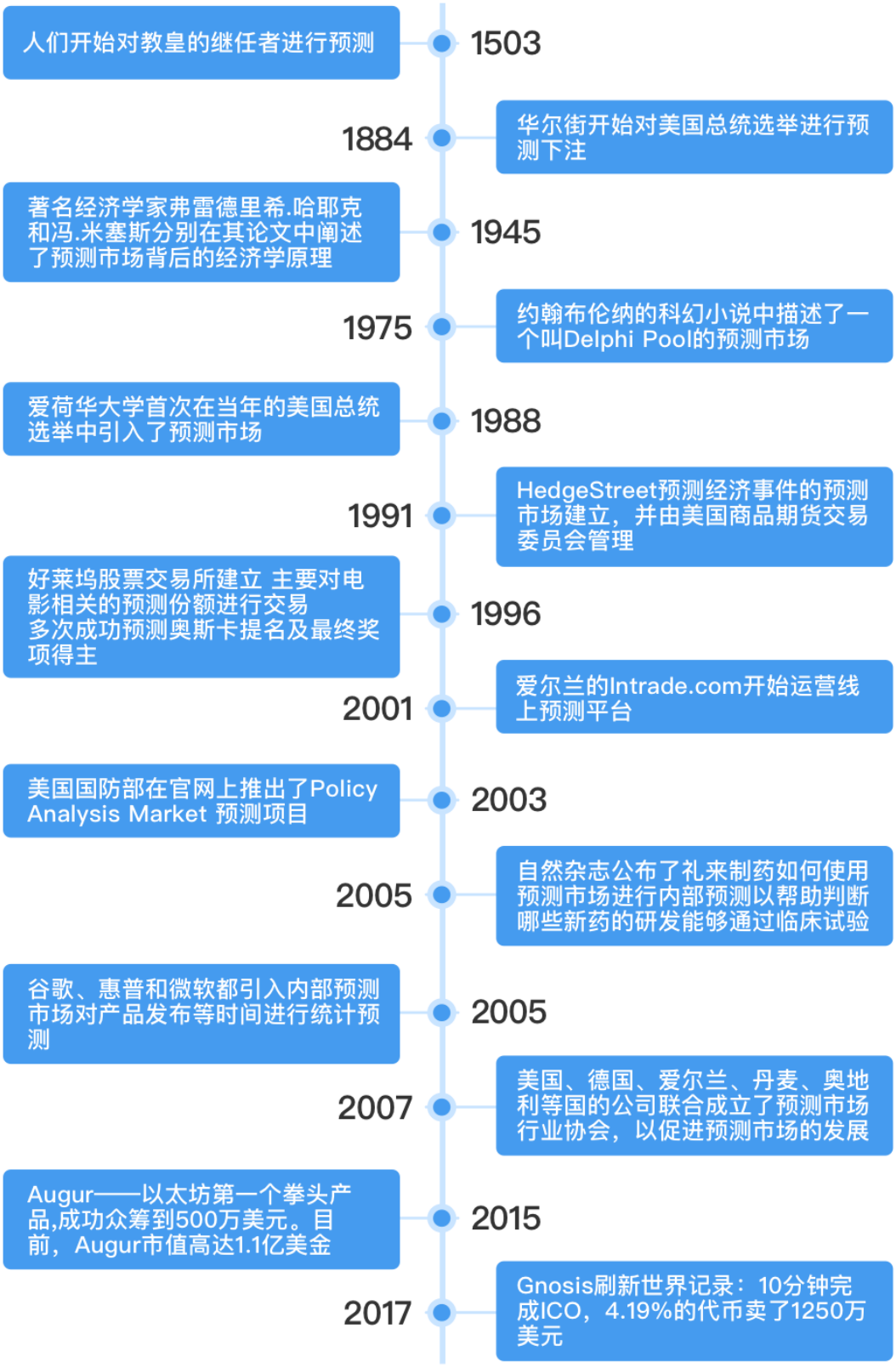

相比个体预测，长期运行的预测市场在准确性上有很大优势，而且参与者越多，预测市场会越准。究其原因，其一是在复杂问题面前，很少会有个体拥有完整的信息，群体知识的多元化往往会胜出；其二是预测市场相当于是为那些掌握市场特别信息的人士提供了一个发表意见的平台，如有不同意见，人们便用买卖预期的方式投票，而不是简单屈服于从众心理或者服从一致的意见；其三是真金白银的交易会使人们采取不同的思维方式，更加谨慎从事。

尽管预测市场相对准确，但也会面临一些挑战，这是由于预测市场是集体民意的体现，而民意会受到很多因素的影响。

细分的预测市场缺乏流动性：人们只关心大事情，或者与自身利益相关的事情，一般的预测容易收集不到足够的样本。如果预测的主题是希拉里还是特朗普当选美国总统就会有很多人参与，但如果是一个第三世界小国的总统选举就不会吸引这么多的注意。

实践中，预测市场就犯下过一些著名的错误，典型案例就是英国脱欧公投。2016 年 6 月 23 日，英国脱欧公投日当天，预测市场认为英国选择留欧的概率为 85%（而现实是英国公众以微弱票差选择脱欧）。

## 2.3 预测市场的前世今生



## 2.4 预测市场与博彩的区别

古往今来，带有博弈性质的金融产品都是在质疑声中改进和发展。在过去，人寿保险被认为是不道德的，股票也被认为是一种博彩手段。然而今天，人们已经完全接受了保险和股票，并将其作为现代金融中不可或缺的部分，保险帮助人们对冲风险，而股票是公司发展重要的融资手段。

预测市场与纯粹的博彩在形式和内涵上都有很大的区别。

首先，与博彩大多没有实际意义不同，预测市场是大众对未来事件看法的汇总，有很强的现实意义。比如美国总统选举的预测市场可以帮助金融市场做风险评估，大众对于房价的期望值可以成为政府宏观调控的参考，天气的预测市场可以帮助农民对冲极端天气带来的风险。

其次，博彩只是个单纯的游戏，有自身的规则，不受外界干扰，相比之下预测市场则受到众多因素的影响，包括经济数据、突发国际事件等人为或自然因素。

再次，与博彩往往涉及到大规模资金不同，参与预测市场的参与资金规模都控制在一定的范围之内，造成的不良社会影响有限。

## 2.5 预测市场 vs 传统预测手段

| | 预测市场 | 民意调查 | 专家意见/座谈 |
|---|---|---|---|
| **参与机制** | 大众主动参与 | 项目随机抽样 | 推荐筛选 |
| **参与人员规模** | 最大 | 次之 | 最小 |
| **意见表达频率** | 连续；直到事件结束 | 一次性 | 一次性；周期性 |
| **意见表达方式** | 互动式 | 独立式 | 独立式；互动式 |
| **意见表达内容** | 预测事件发生的概率 | 表达个人偏好 | 个人偏好+发生概率 |
| **参与者权重** | 按投资比例决定 | 平等 | 不确定 |
| **参与动机** | 等比例的经济回报 | 没有 | 名声；一次性的经济回报 |
| **表达真实观点的动力** | 经济回报激励 | 缺乏奖惩机制 | 民望；缺乏奖惩机制 |
| **意见整理结果** | 以价格变动反映参与者意见的变化；受各个参与者的权重所影响；连续性 | 一次性分析；不具有连续性 | 一次性分析 |
| **预测准确度** | 准确 | 普通 | 略好 |
| **执行方式** | 设立电子交易市场 | 大规模访谈；问卷调查 | 甄选专家 |

## 2.6 区块链重新定义预测市场

预测市场虽好，但传统中心化市场的发展却并不如人意，究其原因，是因为传统的中心化预测市场有其自身的弊端。

其一，中心化的平台无法自证清白，比如很多平台被怀疑操纵市场，让用户受到损失。其二，预测市场自诞生以来就受到严格的金融监管，导致缺乏用户量和交易规模，被冷落在主流市场以外，比如著名的 intrade.com 就是因为不符合美国银行法律而遭到关闭。其三，预测市场与现有的知识界及所有社会舆论渠道都有一定的竞争关系。

今天，随着区块链上点对点技术的发明，将用分布式的思维重新构建预测市场，为预测市场插上飞天的翅膀。其一，区块链上数据全网共识，不可篡改的特点让预测平台能够自证清白。其二，分布式的结构也使得预测市场具有全球流动性，能吸引海量的用户。其三，基于区块链的预测市场由于其代币奖励，能够激励知识界，吸引更多专业人士参与。

## 2.7 Delphy 是一个分布式的预测市场平台

Delphy 是一个基于以太坊的、分布式的、移动社交市场预测平台。它内生的分布式的机制保证了预测结果的不可操纵，也为群体智慧所依赖的信息的多元化、决策的独立性和组织的分布式提供了有效的基础设施保障。

Delphy 是一个预测即服务(Prediction as a Service, PaaS) 的移动应用平台和生态链。用户一方面可以随时随地参与预测市场的交易，另一方面也可以利用 Delphy API & SDK 实现各种定制，开设各个垂直领域的预测市场。

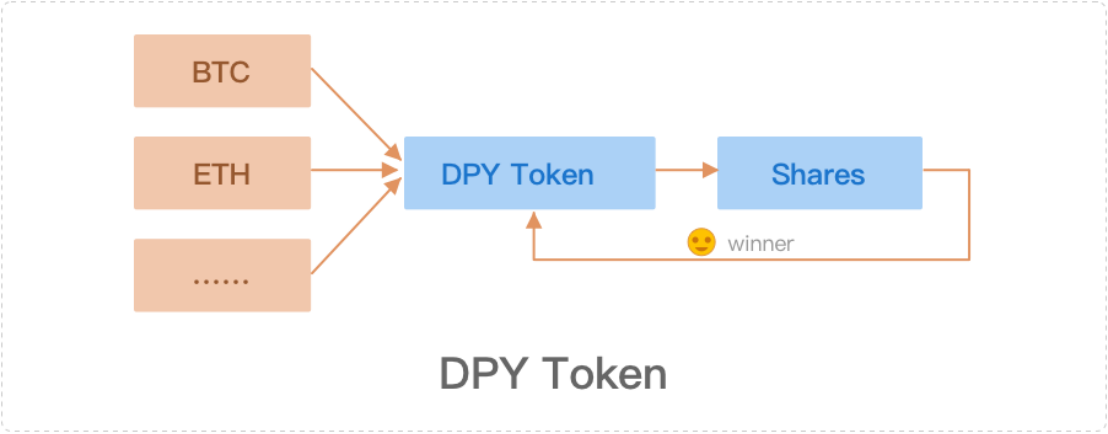
| **Delphy 与现有分布式的预测市场的异同** | | | |
|---|---|---|---|
| **特征** | **Delphy** | **Gnosis** | **Augur** |
| 分布式预言机 Oracle | √ | √ | √ |
| 合约持有的所有资金 | √ | √ | √ |
| 快速清结算 | √ | √ | × |
| 代币持有者承担一定的义务 | × | × | √ |
| 可扩展性 | √ | √ | × |
| 应用生态系统 | √ | √ | × |
| 基于市场的治理协议研究 | × | √ | × |
| 跨平台兼容性标准 | √ | √ | × |
| 手机应用程序就是以太坊节点 | √ | × | × |
| 基于偏好的市场机制 | √ | × | × |
| 事件过滤器 | √ | × | × |
| 社交预测平台 | √ | × | × |

# 第 3 章　Delphy 的机制

## 3.1 机制简介

### 3.1.1 DPY Token

Delphy 会发行一种基于以太坊智能合约的、符合 ERC20 标准（以太坊令牌：允许钱包、交易所和其他智能合约以一种常见的方式对接各种代币）的代币 DPY。DPY 是 Delphy 在 ICO 时发行的，由智能合约生成的，可以用比特币和以太币等数字货币交换而获得。用户对 Delphy 内任何一个目标事件作出预测时，只能而且必须使用 DPY 去购买该次事件预测成功收益的份额（shares）。该事件在 Delphy 内预测市场的资金池都是 DPY 代币，预测成功的赢家收获的也是 DPY。



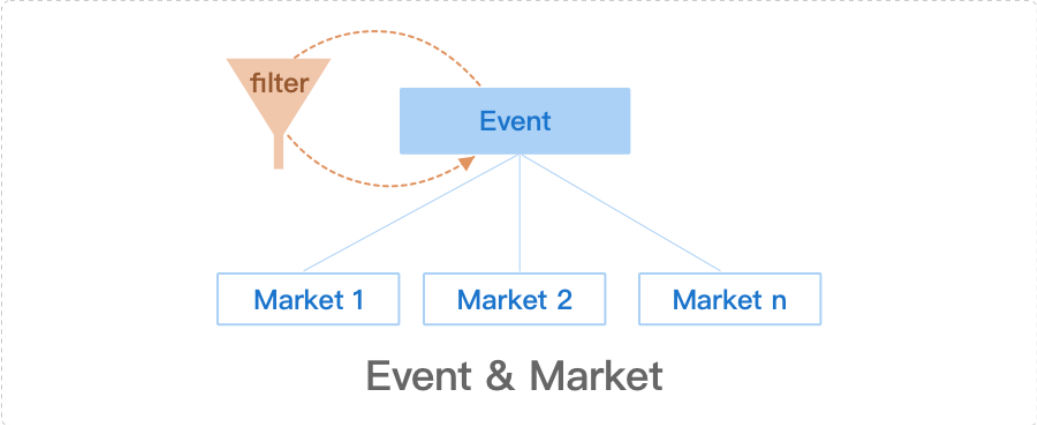

### 3.1.2 创建 Event

Event 在 Delphy 中是指用来预测的未来事件，比如 2018 年足球世界杯德国队能否卫冕。

用户可以利用 Delphy 的 Event Editor 及其 Event Template，根据现实世界中未来的事件来创建 Event。在创建 Event 时，必须给出对 Event 的详细描述、结果的完整性和确定结果的预言机（Oracle）等。

Event 的结果可以为二元类型（binary）、多项选择类型（list）或者范围类型（range）。按照 Event 的开放程度来分类，可以分为开放式的和邀请式的。所有的 Delphy 的用户都可以参与开放式的 Event，而只有被邀请的用户才有资格看到并参与邀请式的 Event。

用户创建好的 Event 会进入一个系统提供的临时的 Event Pool。系统同时会有一个 Event Filter，用来对非法的或者不符合伦理的事件（譬如对某国领导人的暗杀事件或者对某国政府推翻事件的预测）进行过滤。过滤后的事件会进入系统的 Live Event Pool，以供用户自己或其他用户创建 Market。




### 3.1.3 创建 Market

用户创建完预测事件（Event）后，就能开设对应的预测市场（Market），为参与者提供交易平台。

用户可以搜索系统的 Live Event Pool，选择自己感兴趣的 Event 来创建 Market。首先，用户必须确定一个整数型的亏损界，它是庄家有界损失的重要参数。越大表示庄家有可能会亏损越大，但是它越大，表示市场的流动性也越大，参与者购买较多股份时对价格的影响越小。

其次，用户的钱包中必须有足够的准备金。该准备金是由亏损界和事件的结果数量计算出来的，是市场创建者所面临的最大赔金，而且定金的数额大小会跟整个市场的总输赢盘面直接相关的。（详细情况请参与下面的 3.2 定价原理）。系统会在用户的钱包中锁定跟准备金等值的 Tokens，在该 Market 完成交割前，用户将无法使用这些准备金。

同一个 Event 可以被用来创建出具有不同偏好的 Market，每个 Market 的亏损界、准备金、市场流动性、交割日期、预言机 Oracle、和争执仲裁机制可能都不一样。不同偏好的用户可以选择适合自己偏好的 Market 进行交易，真正实现个性化的市场创建和撮合。

### 3.1.4 定价与买卖

Delphy 采用 LMSR（logarithmic Market scoring rule）即对数市场评价法则，来对市场中的每个结果根据市场的交易情况进行瞬时定价。LMSR 为市场提供了几乎无限的市场流动性。这是和传统的非 LMSR 的预测市场和股票市场不一样的地方。（详细情况请参与下面的 3.2 定价原理）。

一般来说，某种结果被购买的数量越多，它的价格就越高；被卖的越多，它的价格就越低。用户可以在 Delphy 中看到每种结果的实时价格及其变化趋势。

Delphy 的用户如果选择并有资格参与某个市场时，可以利用自己的 DPY Token 按照当时的市场价格去购买一定数量的某种结果的股份。同理，用户也可以在市场上出售自己拥有的该市场的股份，获取相应的 DPY Token。

### 3.1.5 交割与闭市

当某个市场到期后，即该市场对应的 Event 在现实世界发生后，Delphy 会根据跟该市场相对应的 Event 的 Oracle 来确定结果的胜负。

拥有预测正确的结果的股份的用户成为该市场的赢家，他们的股份将会自动转换成 DPY Token，在扣除一定的手续费后，剩余的 Token 会被自动按比例转入赢家的钱包。不拥有预测正确结果的股份的用户是输家，将不承担任何其他费用。如果输家们购买的股份的总金额不足以支付赢家的盈利，差额将从市场创建者提供的准备金中支出。这一根据预测正确与否的清算及转账 DPY 的过程称为“交割“。

由于在以太坊上创建 Event、Market 和进行交易，都有相关的交易费（gas）,而且市场的创建者也承担了一定的风险，所以，系统会从赢家的利润

征收一定的手续费。这些手续费主要用于如下几个方面： 1）用于支付跟该 Market 相关的所有的创建和交易费用；2）作为回报分配给市场的创建者；3）作为分红平均分配给 DPY Token 的持有者；4）其他用途。

在市场清结算完成后，该 Event & Market 正式关闭，不允许再进行任何相关的交易。如果该市场所对应的 Oracle 不能决定胜负或者有歧义，或者如果有用户对已经决定胜负的结果提出质疑，Delphy 将会有一系列的解决争执的办法。

### 3.1.6 用户留言与评论

用户在买卖某市场的某个结果的股票时，可以对该事件发表评论并留言。这种基于事件的社交活动提供了在预测价格之外的更多的信号。

## 3.2 定价原理

LMSR（logarithmic Market scoring rule）即对数市场评价法则，由 Hanson 提出。它是一种自动化市场庄家机制，总是保持一致的概率分布来反映市场对每个结果的可能性的估计。LMSR 正成为预测市场（prediction Markets）事实上的标准，它有许多优良的特性，如预测结果对数增长带来的有界损失、无限的流动性和独立关系的模块化等。LMSR 被很多公司或项目使用，如 inkling-Markets.com、Microsoft、yoonew.com、Augur 以及 Gnosis。

在一个预测市场中，庄家（市场创建者）建立一个事件$\Phi$，$\Phi$的结果可以有如下类型：

布尔类型，如“德国队在 2018 年的世界杯能夺冠吗？”，结果只有 yes 或 no；

列表类型，如“2018 年世界杯哪个队能夺冠？”，结果是一个 32 维列表；

范围类型，如“2018 年 1 月 1 日苹果的股价是多少美元？”，结果将是一个较大的范围。

在某个时刻，参与者如何下注、如何确定购买或卖出某结果股份的价格和市场对获胜概率的评估都由 LMSR 完成。

**定义**

对于有$n$个结果的事件$\Phi$，$q_i$表示第$i$个结果的当前的股份（share）数量。

**亏损界$\ell$** 由庄家自行确定的整数。它是庄家有界损失的重要参数。$\ell$越大表示庄家有可能会亏损越大，但是$\ell$越大，表示市场的流动性也越大，参与者购买较多股份时对价格的影响越小。

**准备金$\mathcal{F}$** 表示庄家有界亏损的上界，即最大可能亏损值，也是庄家建立事件时必须提供的准备金。$\mathcal{F}$由$\ell$和$n$共同决定。

$\mathcal{F} = \ell \cdot \ln(n)$。

**市场状态** 市场状态是指$n$个结果股份向量$(q_1, q_2, \cdots, q_n)$，每一次交易只会改变某个$q_i$，从而改变市场状态。

**成本函数$C$** 市场状态的成本函数定义如下：

$$C(q_1, q_2, \cdots, q_n) = \ell \cdot \ln(e^{\frac{q_1}{\ell}} + e^{\frac{q_2}{\ell}} + \cdots + e^{\frac{q_n}{\ell}}),$$

$\ell$是亏损界，ln是自然对数。成本函数$C$是 LMSR 的核心函数，购买和卖出股份的具体支付金额将由成本函数的状态差给出。

若在市场当前状态购买$i$结果Δ份需支付：

$$C(q_1, q_2, \cdots, q_i + \Delta, \cdots, q_n) - C(q_1, q_2, \cdots, q_i, \cdots, q_n)$$

若在市场当前状态卖出$i$结果Δ份需支付：

$$C(q_1, q_2, \cdots, q_i - \Delta, \cdots, q_n) - C(q_1, q_2, \cdots, q_i, \cdots, q_n)$$

卖出支付价格为负值时，表示从市场获利。

因此买卖股份为原子操作，必须等上一条交易完成，才能进行下一条交易，不能并行完成。

**瞬时价格函数$p(q_i)$** 表示当前购买或卖出微量第$i$个结果股份的价格。它是成本函数的偏导数：

$$p(q_i) = \frac{dC}{dq_i} = \frac{e^{\frac{q_i}{\ell}}}{e^{\frac{q_1}{\ell}} + e^{\frac{q_2}{\ell}} + \cdots + e^{\frac{q_n}{\ell}}}$$

当预测事件发生后，若第$i$个结果获胜则$p(q_i) = 1$，$p(q_{j\neq i}) = 0$。

**概率函数$P(q_i)$** 表示当前市场预测事件第$i$个结果获胜的概率。

**庄家盈利额$\mathcal{R}$** 当预测事件发生后，若第$i$个结果获胜，则

$$\mathcal{R} = C(q_1, q_2, \cdots, q_n) - q_i - \mathcal{F}$$

当$\mathcal{R} < 0$时表示庄家亏损。

基于以上 LMSR 的基础定义，有如下命题：

**命题 1** 准备金$\mathcal{F}$等于市场初始状态的成本函数。

这是因为市场初始状态，没有买卖股份，所以$q_1 = q_2 = \cdots = q_n = 0$，则

$\mathcal{F} = \ell \cdot \ln(n) = C(0,0,\cdots,0)$。

**命题 2** 当前市场状态的成本函数等于当前市场的资本总额。

这里说的市场的资本总额包含准备金和投注的资金，不包括交易税。

**证明**：

我们知道市场状态成本函数的差为购买或卖出需支付的金额，从市场初始$\alpha_0 = (0,0,\cdots,0)$到状态$\alpha_m = (q_1, q_2, \cdots, q_n)$一共完成$m$次交易，每笔交易只允许改变一个结果的股份，$x_j$是指第$m$笔交易对市场注入的资金，则有如下等式：

$$x_1 = C(\alpha_1) - C(\alpha_0),$$

$$x_2 = C(\alpha_2) - C(\alpha_1),$$

$$x_m = C(\alpha_m) - C(\alpha_{m-1}),$$

将$m$个等式相加，可得，$\sum_{j=1}^{m} x_j = C(\alpha_m) - C(\alpha_0) = C(\alpha_m) - \mathcal{F}$，所以有

$$C(\alpha_m) = \mathcal{F} + \sum_{j=1}^{m} x_j$$

**命题得证**

**命题 3** $p(q_i) = P(q_i)$。

这个命题揭示了在 LMSR 中，参与者购买某结果的瞬时价格跟市场预测该结果获胜的概率是相等的。

证明：

市场的标准熵为：

$$S(q_1, q_2, \cdots, q_n) = -\sum_i P(q_i) \cdot \ln(P(q_i)) \tag{1}$$

市场的拉格朗日值为：

$$\Lambda(q_1, q_2, \cdots, q_n) = S - \sum_i q_i P(q_i) - 1$$

最大约束熵是在Λ取导时得到，因此

$$d\Lambda = \sum_i dP(q_i)[\ln P(q_i) + 1 + \alpha + \beta q_i] = 0 \tag{2}$$

(2)式需对所有$i$都成立，则有

$$\ln P(q_i) + 1 + \alpha + \beta q_i = 0 \tag{3}$$

又概率和为 1，

$$\sum_i P(q_i) = 1 \tag{4}$$

联立(3)(4)，消去$\alpha$，可得：

$$P(q_i) = \frac{e^{-\beta q_i}}{e^{-\beta q_1} + e^{-\beta q_2} + \cdots + e^{-\beta q_n}} \tag{5}$$

对 LMSR 市场中，$\beta = -1/\ell$，因此有

$$p(q_i) = P(q_i)$$

**命题得证**

**命题 4** 事件发生后，若庄家盈利额$\mathcal{R} < 0$，即庄家亏损时，则$|\mathcal{R}| \leq \mathcal{F}$。

该命题揭示了庄家的有界亏损，最大亏损为准备金。

**购买和卖出流程**

基于以上定义和命题，下面描述预测市场根据 LMSR 买卖股份的流程。

庄家建立$n$个结果的预测事件，确定亏损界$\ell$，并向市场提供准备金$\mathcal{F} = \ell \cdot \ln(n)$。市场建立初始，没有参与者买卖股份，$q_1 = q_2 = \cdots = q_n = 0$。此时各结果概率均等为$1/n$，每个股份的瞬时价格$p(q_i) = 1/n$。

第一个参与者 Alice 看好结果1获胜，够买$a$份，则$q_1 = a$。则 Alice 支付的金额由成本函数状态差确定，即$C(a, 0, \cdots, 0) - C(0,0, \cdots, 0)$，这里需要说明是在 Alice 购买前，结果 1 的瞬时价格$p(q_1) = 1/n$，而 Alice 够买$a$份所支付的金额并不是$ap(q_1)$。这是因为瞬时价格$p(q_1)$只是当前购买足够小（无穷小）份数的价格，Alice 购买的份数$a$越大，付出的成本也越大。Alice 购买后瞬时价格$p(q_1)$会立刻增加，其它结果$j \neq 1$得瞬时价格会减少。可以通俗理解为对于结果$i$的股份购买越多，价格越高，市场就预测结果$i$获胜概率越高。

对某个时刻，市场成本为$C(q_1, q_2, \cdots, q_i, \cdots, q_n)$，

若 Bob 购买$b$份结果$i$，则需要支付

$$C(q_1, q_2, \cdots, q_i + b, \cdots, q_n\ ) - C(q_1, q_2, \cdots, q_i, \cdots, q_n)。$$

此后，Alice 卖掉结果 1 的$a$份，则需支付

$$C(q_1 - a, q_2, \cdots, q_i + b, \cdots, q_n) - C(q_1, q_2, \cdots, q_i + b, \cdots, q_n)$$

这里需要注意若卖股份的时候，成本状态差为负数，则表示 Alice 盈利，可从市场获得成本状态差的资金，而不是支付给市场。当前瞬时价格高于购买时的价格，Alice 卖出时可以盈利。

当预测结束，事件确定后，如结果$i$获胜，持有结果$i$股份的参与者将以单

价 1 赎回所有股份，而持有其它结果$j \neq i$股份的参与者将全部损失。如果结果$j \neq i$股份的总资金都不足以支付获胜结果$i$的总资金，则不足部分从庄家的准备金$\mathcal{F}$中扣除。这意味着市场预测越准，庄家亏损越严重，市场预测越差，庄家盈利越多。LMSR 良好的模型使得庄家最多损失准备金$\mathcal{F}$。

市场在极端情况下庄家将损失全部准备金$\mathcal{F}$，这种情况发生在结果$i$获胜，且所有参与者都够买了结果$i$的股份，没有人购买结果$j \neq i$的股份。即$q_i$足够大，$q_{j\neq i} = 0$。于是，庄家需支付的赎回资金为$\mathrm{q_i}$，此时的市场纯盈利（所有参与者投入的字节）为

$$\mathrm{T} = \mathrm{C}(0,0,\cdots,\mathrm{q_i},\cdots,0) - \mathcal{F} = \ell \cdot \ln\left(\mathrm{n} - 1 + \mathrm{e}^{\frac{\mathrm{q_i}}{\ell}}\right) - \mathcal{F} \cong \mathrm{q_i} - \mathcal{F}，$$

即$\mathcal{R} = \mathrm{T} - \mathrm{q_i} \cong -\mathcal{F}$，所以庄家的亏损达到上界$\mathcal{F}$。

**实例**

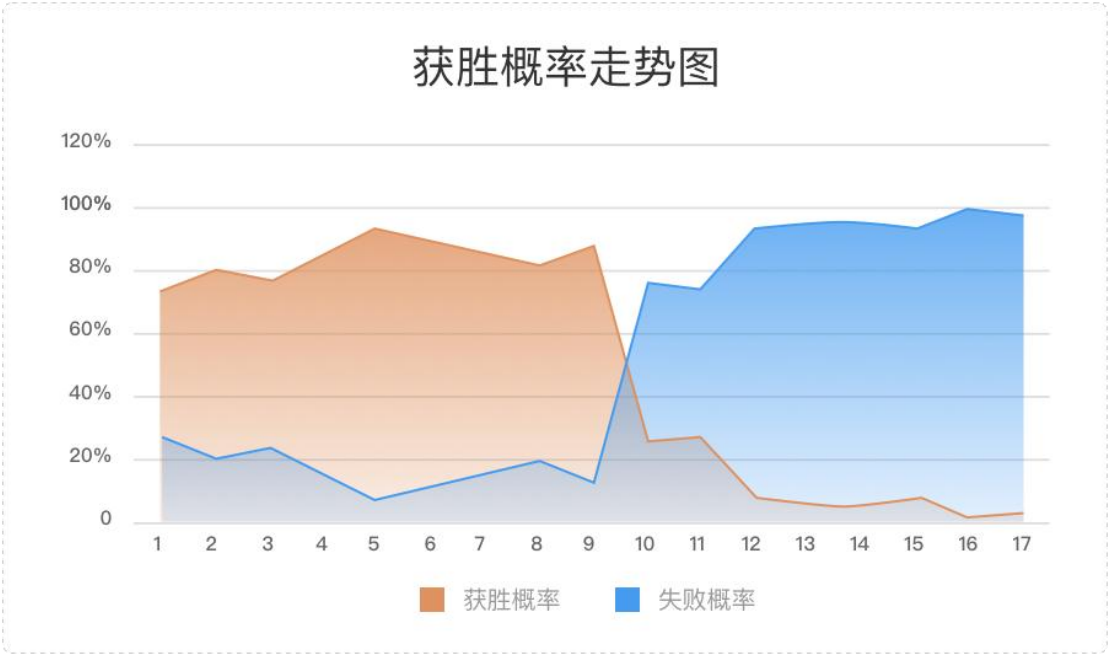
庄家于 2017 年 4 月建立布尔事件“2017 年 5 月 27 日，柯洁对战 alpha-go 无法获胜一局”，它在 2017 年 5 月 27 日之前是一个预测事件，结果只有 yes 或 no。庄家定义$\ell = 100$，则需要支付给市场的准备金$\mathcal{F} = 100\ln 2 = 69.31$。

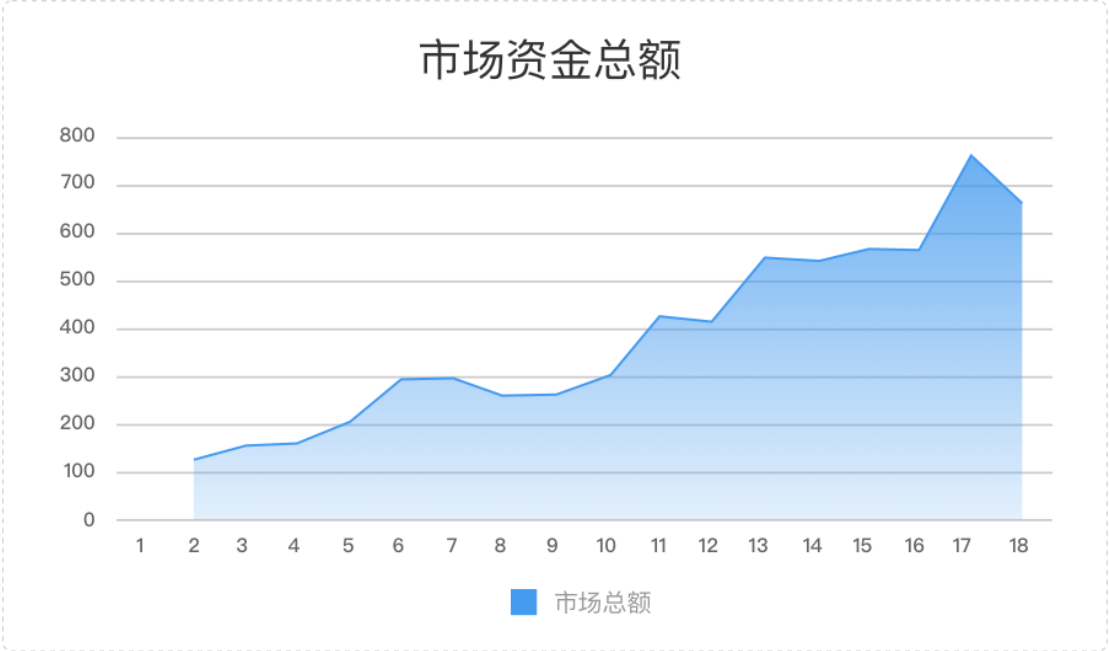
投注前市场总资本为$\mathrm{C}(0,0) = \mathcal{F} = 69.3$。

操作如下（百分比为 yes 的概率）：如第一笔交易，购买 yes100 份，则支出为$\mathrm{C}(100,0) - \mathrm{C}(0,0) = 62.01$，交易后 yes 的概率为$\frac{\mathrm{e}^{\frac{100}{100}}}{\mathrm{e}^{\frac{100}{100}}+1} = 0.731$。以后的交易按上述流程计算。

| 步骤 | 购买（份） | | 支出金额 | 收入金额 | 获胜概率 | | 总量 | | 市场总额 |
|---|---|---|---|---|---|---|---|---|---|
| | yes | no | | | yes | no | yes | no | |
| 0 | | | | | 50.00% | 50.00% | 0 | 0 | 69.315= $\mathcal{F}$ |
| 1 | 100 | | 62.01 | | 73.11% | 26.89% | 100 | 0 | 131.326 |
| 2 | 40 | | 30.72 | | 80.22% | 19.78% | 140 | 0 | 162.042 |
| 3 | | 20 | 4.29 | | 76.85% | 23.15% | 140 | 20 | 166.328 |
| 4 | 50 | | 40.45 | | 84.55% | 15.45% | 190 | 20 | 206.779 |
| 5 | 100 | | 89.73 | | 93.70% | 6.30% | 290 | 20 | 296.504 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 6 | | 50 | 4 | | 90.03% | 9.98% | 290 | 70 | 300.508 |
| 7 | -40 | | | 35.21 | 85.82% | 14.19% | 250 | 70 | 265.298 |
| 8 | | 30 | 4.84 | | 81.76% | 18.24% | 250 | 100 | 270.141 |
| 9 | 40 | | 33.8 | | 86.99% | 13.01% | 290 | 100 | 303.939 |
| 10 | | 300 | 124.79 | | 24.97% | 75.03% | 290 | 400 | 428.734 |
| 11 | | -10 | | 7.41 | 26.89% | 73.11% | 290 | 390 | 421.326 |
| 12 | | 150 | 126.56 | | 7.59% | 92.41% | 290 | 540 | 547.889 |
| 13 | -40 | | | 2.53 | 5.22% | 94.79% | 250 | 540 | 545.356 |
| 14 | | 20 | 19.05 | | 4.31% | 95.69% | 250 | 560 | 564.406 |
| 15 | 40 | | 2.1 | | 6.30% | 93.70% | 290 | 560 | 566.504 |
| 16 | | 200 | 194.4 | | 0.90% | 99.10% | 290 | 760 | 760.905 |
| 17 | | -100 | | 98.46 | 2.41% | 97.59% | 290 | 660 | 662.442 |

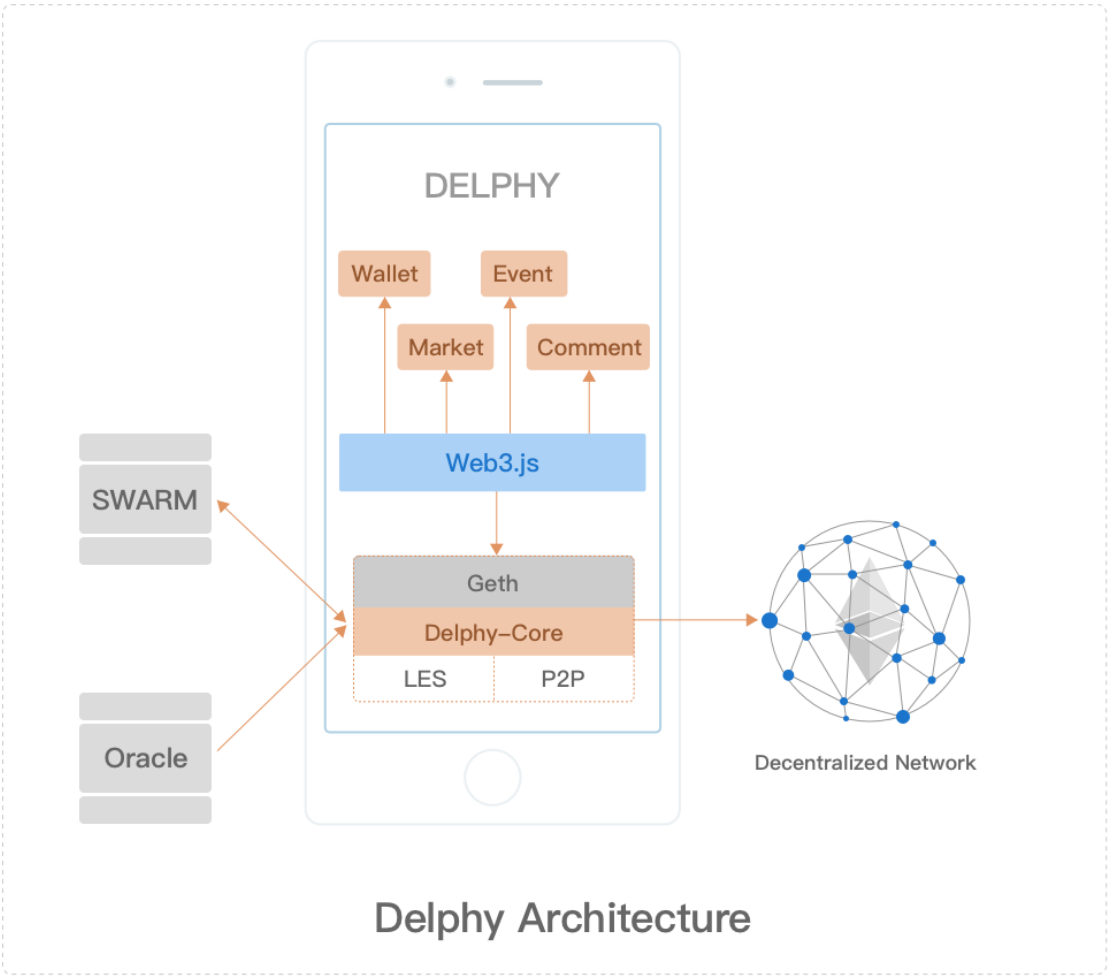





若此时预测结束，从市场预测情况看，no 的概率较高达到 97.6%，表示市场预测柯洁能够至少获胜 1 场。但从比赛结果看，这个预测与真实结果相反，柯洁 0：3 输。所以预测结果很差，则庄家获利。此时 yes 的估计为 1，no 为 0，于是市场需要支付 yes 的 290，市场总金额为$C(290,660) = 662.44$，于是庄家盈利为$662.44 - 290 - 69.31 = 303.13$。

# 第 4 章　Delphy 的技术架构

Delphy 是一个基于以太坊的、分布式的、社交性的、全开源的、预测市场的移动平台。Delphy App 天生就是一个运行在移动终端上的以太坊的轻节点。




Delphy Architecture

## 4.1　Delphy 的核心组件

**以太坊 Ethereum**： 以太坊公链和智能合约及其子协议组成的 web3.0 的主要架构，为 Delphy 提供了分布式的、无需信任和许可的资产发行和交易的基础设施。

与此同时，以太坊本质上讲就是一个社交技术。Delphy 就是一个基于预

测市场的社交网络和手机应用。作为以太坊公链上的一个 Dapp 应用，Delphy 能为以太坊的普及和推广起到强有力的推动意义。

**智能合约**：Delphy 利用以太坊的智能合约发行 DPY Token，创建 Event & Market, Oracle & Event Filter，并且实现定价、交易的买卖、撮合和清结算等等。

**SWARM**：它提供了分布式的文件管理机制，帮助 Delphy 存储跟 Event & Market 相关的静态文件和元数据，为 Delphy 移动应用提供分布式的存储和检索服务。

**LES (Light Ethereum Subprotocol)**： LES 是为轻客户端（如智能手机等）设计的，在区块链同步时只下载块头而不是整个区块的一种机制。它提供完全安全的区块链接入功能，只是不参与挖矿和共识的形成。

## 4.2 Delphy 移动应用

鉴于智能手机的无所不在和微信的伟大成功，Delphy 采用的是“天生移动”的策略，即 Delphy 利用以太坊的 LES 协议首先提供分布式的预测市场的移动应用，是一个独立运行于移动终端的以太坊节点，而非基于浏览器的或者独立的桌面应用。

Delphy 移动应用利用 LES 在智能手机上运行 geth & web3.0 JS 框架，从而提供了非常强大而且安全的功能。用户可以非常方便的创建 Event，根据自己感兴趣的 Event 创建 Market，并设置 Event & Market 的描述和元数据，快速的查询 Event & Market、股价及其走势，针对不同的 Market 去买卖股份、付账和接受赢款等等。

## 4.3 预言机 Oracle

Oracle 是 Delphy 中的 Event 在现实世界中对应的真实事件的发生结果的信息发布机制。Delphy 中一个 Event 的预测结果必须由 Oracle 来决定。这些 Oracle 提供了一系列的 API，Delphy 通过调用这些 Oracle API 来决定预测市场的输赢结果并实现其后的清结算。

Oracle 可以是中心化的（如 RealityKeys），也可以是多中心化的。有些预测应用只需要用单个数据点来验证其结果，所以中心化的 Oracle 就足够了。譬如，NBA 球赛结果的预测，可能 NBA 官网的比赛结果就充分必要了。对于多中心化的 Oracle，我们会设计出一套激励机制，并实现 m out of n 的模式和 Oracle 的争执解决方案。

## 4.4 Delphy 的特色

**Delphy App 就是以太坊的轻节点**

Delphy 就是一个运行着以太坊的轻节点的移动平台。Delphy App 支持以太坊全节点的几乎所有功能，利用 P2P 跟以太坊网络中的其他节点直接通信，极大地提高了效率，使 Delphy App、SDK & API 都具有强大的功能和拓展性。

**天生移动**

智能手机是 Delphy 应用开发的首选。在 Delphy 平台发布的时候，支持 Delphy 的 iOS & Android 移动应用会同步推出，提高用户友好性，最大限度满足用户需求，助推以太坊的普及推广和生态的发展。

**深度定制**

同一个 Event 可以被用来创建出具有不同偏好的 Market，每个 Market 的亏损界、准备金、市场流动性、交割日期、Oralce、和争执仲裁机制可能都不一样。不同偏好的用户可以选择适合自己偏好的 Market 进行交易，真正实现个性化的市场创建和撮合。

**事件过滤器**

用户创建好的 Event 会进入一个系统提供的临时的 Event Pool。系统同时会有一个 Event Filter，用来对 unethical or illegal 的事件（譬如对某国领导人的暗杀事件或者对某国政府推翻事件的预测）进行过滤。Delphy 会提供 API，以供用户创建自己的事件过滤器，满足自己所在的地区国度的法律法规和生态的需求。

**社交预测平台**

Delphy 移动应用是具有社交属性的预测市场。预测是一种社交行为，Delphy 提供的聊天功能（comments）为用户提供了社交活动的平台。Delphy 的扩张功能包括 P2P 支付、P2P 即时聊天、OTC 场外交易等等都具有天生的社交属性。

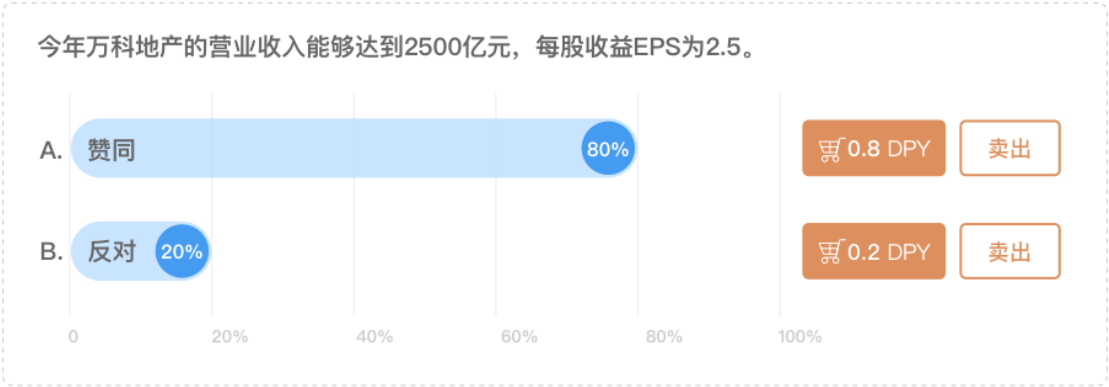
# 第 5 章　Delphy 的主要应用场景

## 5.1　金融市场

预测市场可以实现比现有的衍生品更加细化的金融工具，为资产管理者提供更精准的风险对冲工具。

如果我们将传统金融工具概念化为经济价值的表达，人们可以认为目前金融工具的“表现力”仅限于资产（如货币，股票）的所有权表达，经济实体（如债券）之间的财务关系的表达，以及与工具相关价值（如衍生物）的元表达。预测市场可以为经济事件带来更加细微和详细表达方式，从而在宏观和微观经济层面更明确地代表价值（以及风险）。

对于专业的机构投资者，其管理资金规模都在几十亿甚至上百亿，预测所投资组合的公司业绩表现是重中之重，而预测市场可以给了解相关情况的市场人士一个表达自己观点的机会，也给二级市场股票分析师们提供了更广泛的市场数据。




## 5.2　对冲工具

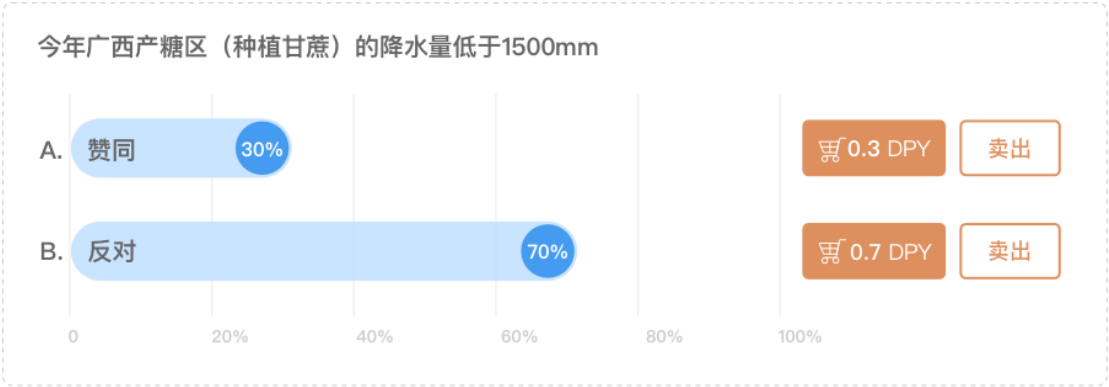
预测市场由于具备高流动性和准确性，可以被用作对冲风险。其本质上是让风险评估众包化，为拥有宝贵私有知识的参与者创造变现机会。这其中的一个典型例子就是农业气象预测。

农业极易受到气象灾害的危害，如暴雨、台风、低温、沙尘暴等都会对农业生产造成很大的损失。据中国气象局的统计，1949至1991我国共经历过14次大的干旱，其中数次造成粮食减产1500万吨以上。

因此，农业生产者有很大的风险对冲需求。根据保监会发布的统计数据，从2007年到2016年的10年间，我国农业保险保费增长了7倍。然而，单纯的农业保险难以个性化地适应每一个地区和作物的对冲需求，而在Delphy预测平台上，农业从业者可以创建符合自身个性化需求的预测主题，得到更细微的风险对冲服务。

比如，东北早稻的播种易受到春季倒春寒的影响，需要对冲低温风险，而作为糖料作物的甘蔗需要的降水量在1500mm-2000m之间，需要对冲降水量过多和过少的风险。

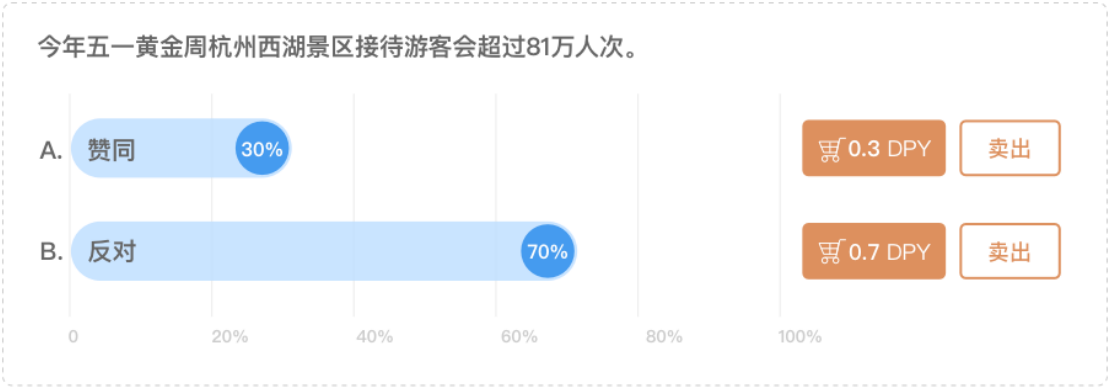
Delphy 预测市场在这个领域颇有用武之地。对于农业从业者而言，参与预测市场可以帮助对冲可能面临的气象灾害风险，减少经济损失，对于气象专家而言，将宝贵的经验贡献出来，可以在帮助农业从业者的同时获得奖励。




## 5.3 景点预测

随着我国人民生活水平的提升，旅游已经成为人们的一个重要的休闲方式。但相应的，由于旅游资源集中且有限，每逢节假日全国人民集中出游时，很多景点不免人山人海，破坏了人们游览的雅兴，而另一些著名景点却因为大家固有的避开热点思维反而不那么火爆，因而提前判断哪个景点游客相对较少

成为大家关注的热点。



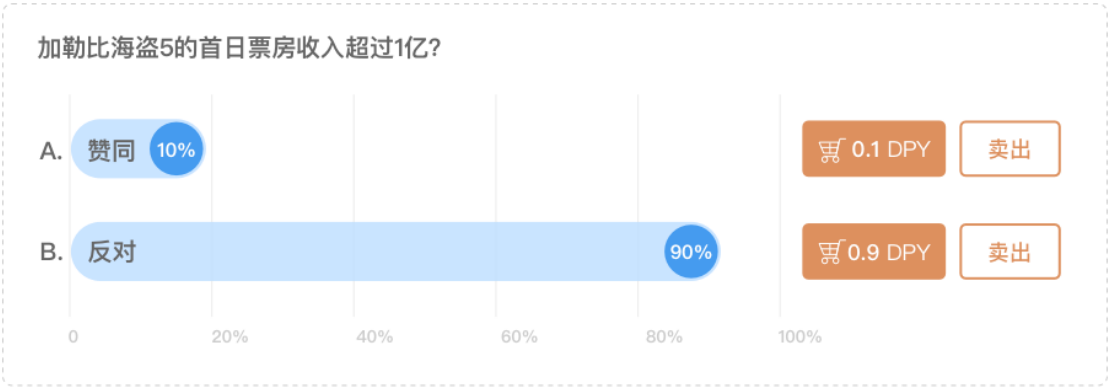

西湖景区是著名的旅游景点，这些年游客接待量屡屡超过国家规定的最大承载量 79.75 万次，因此景区采取了一系列的限流措施。近年来景区还采取了大数据的技术手段来分析游客数据，为管理和游览线路的合理设定以及动态掌握游客信息、制定经营策略提供参考和依据。

## 5.4 娱乐产业预测

娱乐产业是当下最红火的产业之一，据《十三五规划建议》，2015 年文化娱乐产业 2015 年总体规模将达到 4500 亿元，在 2020 年更有望达到一万亿元，其中仅影视产业的市场规模就将达到 5000 亿元。

预测市场在娱乐产业中有广泛的应用，比如各种综艺海选预测(如超级女声)，节目收视率预测，电影票房预测等等。

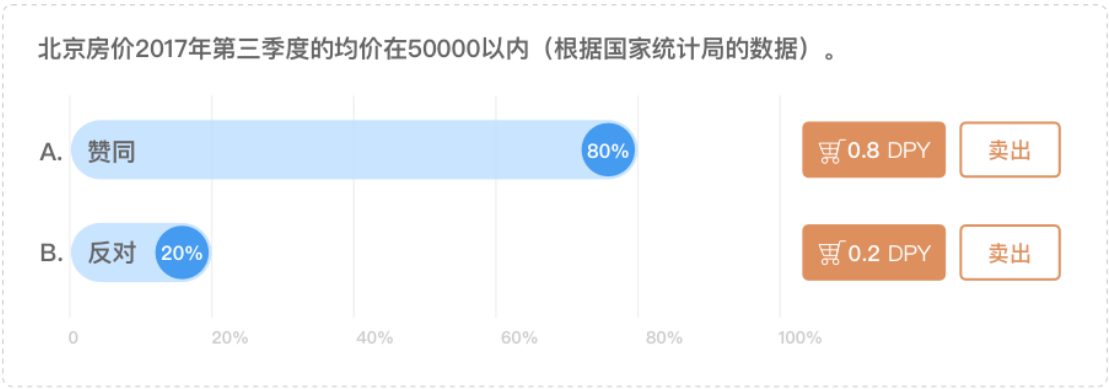
值得一提的是，好莱坞就有基于电影票房的预测市场，其神预测的经典案例是在 2007 年的奥斯卡颁奖典礼上，当年的奥斯卡共有 39 项提名，好莱坞证券交易所通过交易价格排名，成功预测了其中的 32 项提名，并在颁奖典礼之前成功预测出 8 项大奖中的 7 项，准确率之高，令人叹为观止。




## 5.5 房价预测

房子，作为绝大多数中国家庭比例最高的资产，其价格是最为牵动中国老百姓的心弦，然而目前对于房价的预测主要来自于意见领袖，或者根据第三方交易数据来推测。

显然，预测市场作为一个大众参与意见领地，可以直观的了解到目前民众对于房价的期望值，这对于政府的宏观调控，房地产公司的投资计划，买房和卖房的民众都是有重要的参考意义的。




房价的统计口径很多，预测市场将采用国家统计局每季度发布的房价统计数据，确保数据的可靠性。

## 5.6 游戏预测

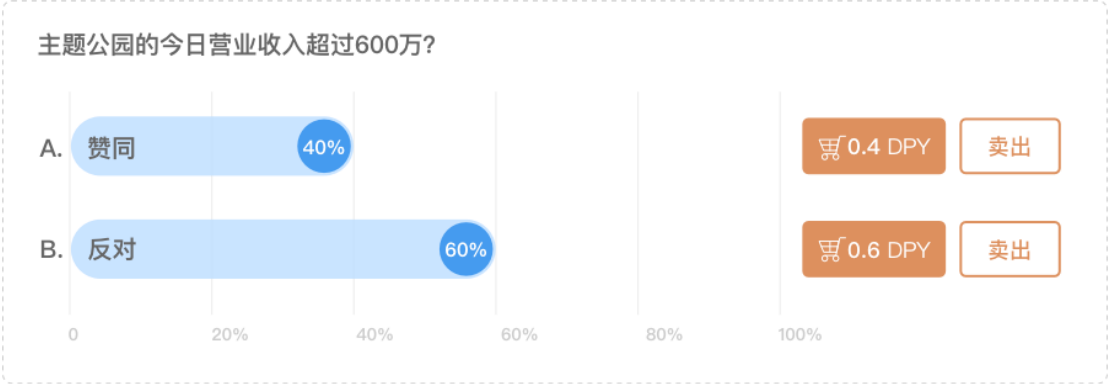
游戏是个巨大的市场，根据“2016 年中国游戏产业报告”，我国的游戏产业规模超过 1600 亿元，还在高速成长当中。

对于预测市场而言，游戏作为一种应用场景，可以在游戏内部通过调用我

们的 API，为游戏玩家提供预测市场的玩法和机制，而不需要游戏厂商自己开发。

比如著名的运营类游戏-主题公园世界，玩家可以建设和经营自己的主题乐园，而且事无巨细，还可以邀请同伴和自己一起。比如，在游戏中玩家需要先购买土地、雇佣员工、按照自己的心意布局园内的游戏设施等。

这其中就有大量的场景可以产生预测市场，比如不同的玩家可以预测主体乐园的营业收入，游客数量，有没有发生事故等等。

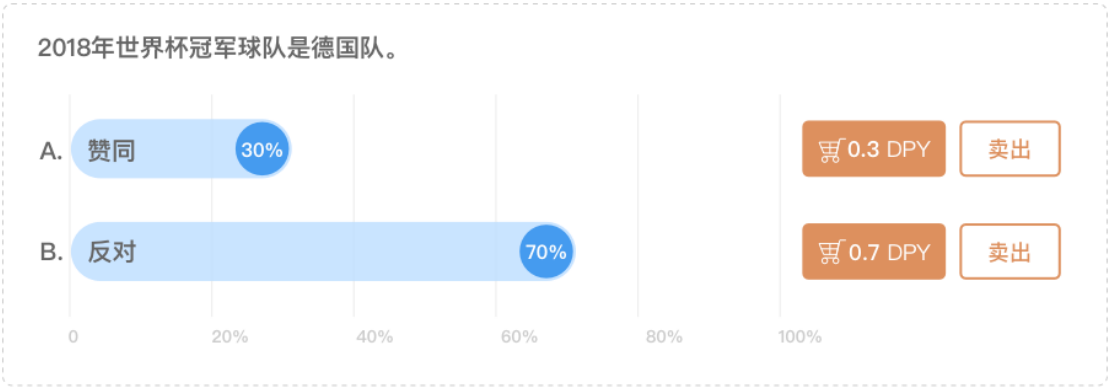



## 5.7 体育预测

体育博彩的历史悠久，我国春秋时期著名的田忌赛马就是中国古代体育博彩早期的有关记载之一。在国外，一百多年前的澳洲就出现了合法的赛马博彩。在英国，体育博彩在 1961 年 5 月 1 日合法化，1998 年，英国的威廉希尔公司开展了网上体育博彩业务，是有记载的最早开展合法互联网体育博彩业务的经营者。

然而，中心化的预测市场应用于体育博彩的速度缓慢。这是由于一方面，设立公司的门槛很高，另一方面平台无法自证清白，难以提供公开、公平、公正的可信市场环境。此外，在中心化平台里，用户还会面临额外的风险，例如盗窃或其他故障，以及付款处理器的意外问题。

相比之下，分布式的体育预测市场拥有降低发起与参与门槛，自证清白，避免单点崩溃的风险等优势。在 Delpy 预测市场中，球迷可以创设自己喜欢的球赛预测，满足个性化需求，增加参与感。




## 5.8 管理决策

每一个组织都想要最大化其人力资源的利用效率，预测市场可以帮助实现这一目标。

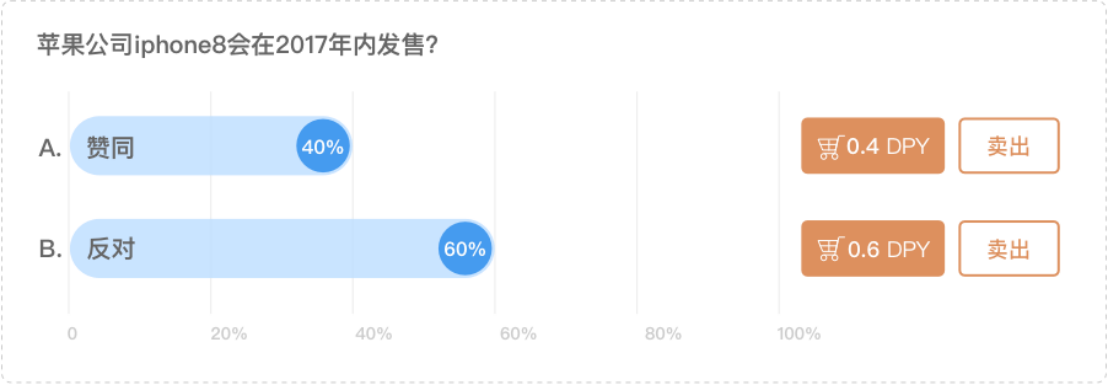
首先，预测市场可以帮助汇集所有相关利益方的知识、智慧、经验，来提升组织的整体竞争力，同时也为所有员工带来一个发声的渠道，为组织的发展做出贡献，更为重要的是，提高员工的参与感，对于千禧一代追求参与感的员工尤为重要。

因此，机构内部的预测市场可以帮助机构的管理者更好地掌握内部的意见，指导组织运作。

比如微软曾使用一个内部的预测市场来预计一种软件是不是能够按时交付。开始交易之后的 3 分钟内，按时交货的合约就下跌了，显示出大多数参与者缺乏对于按时交货的信心。项目经理得知此事后，召开了产品会议探讨并解决了一些可能延迟交付的问题，合约价格随即上涨。最后，由于终端用户对于产品的一些性能不满意，软件还是如合约预计的一样延迟交付了。

这个例子充分说明，在机构内部的管理决策上，汇集各类信息的预测市场，能够起到很大的辅助作用。

微软的例子不是个单独现象，在过去的 10 年间，包括美国的惠普、百思买、通用电气、google、IBM 等世界 500 强都开始在公司内部部署预测市场。




经济学家“David Rothschild”认为，在商业决策中应用预测市场主要有两个目的，一个是让参与者了解未来可能发生什么事件，他们才能够更有效地搜集信息和资源，第二个目的是了解各种因素是如何影响预测结果的。

除此之外，预测市场还可以帮助机构更有效地管理经济和社会风险，比如消费者需求的下降，疫病、环境灾难的爆发。

# 第 6 章　法律事务和风险声明

## 6.1 Delphy 项目的法律结构

针对 Delphy 的项目，会成立一个位于新加坡的非盈利性的基金会。该基金会将作为独立的法律主体，全权负责组织团队来开发、推广和运营这个分布式的预测市场平台和应用，并承担所有相关责任。

Delphy 基金会通过定向及公开出售的方式，出售旨在 Delphy 平台上运行和使用的 DPY Token，这些 DPY 是用户为了使用 Delphy 的服务的付费手段和结算单位，一旦出售后就不会有任何人对 DPY 承诺回购或回赎。DPY 作为一种具有实际用途的虚拟商品，不是证券，也不是投机性的投资工具。Delphy 基金会不保证 DPY 的内在价值或存在任何回报。DPY 不代表任何现实世界的资产或权利（例如 Delphy 基金会的股份、表决权等）。DPY 的典型受众是对加密代币和区块链系统非常熟悉的专家们。

任何美国公民、永久居民或绿卡持有者将不被允许参加 DPY 的公开出售，故 Delphy 基金会将不会把 DPY 出售给前述对象。

Delphy 基金会在 DPY 销售中所获的收入，将由 Delphy 基金会无条件的自由使用，主要将用于技术开发、市场营销、法律合规、财务审计、商务合作等用途。

Delphy 的预测市场是建立在以太坊上的完全分布式的平台，全球任何人均能且只能通过消费 DPY Token 来使用其功能，不受地理位置所限。Delphy 平台不具有物理实体存在，与任何国家或地区的地域和法币均没有任何关系。即使如此，Delphy 依然很有可能会在全世界不同国家受到主管机构的质询和监管。为了满足和遵守当地的法律法规，Delphy 平台可能会在有些区域无法提供正常的服务。Delphy 基金会及其团队会尽力争取“沙箱政策”（sandbox policy）或者安全港待遇，为用户提供尽可能友好的服务。

## 6.2 免责声明

除本白皮书所明确载明的之外，Delphy 基金会不对 Delphy 或 DPY 作任何陈述或保证（尤其是对其适销性和特定功能）。任何人参与 DPY 的公开售卖计划及购买 DPY 的行为均基于其自己本身对 Delphy 和 DPY 的知识和本白皮书的信息。在无损于前述内容的普适性的前提下，所有参与者将在 Delphy 项目启动之后按现状接受 DPY，无论其技术规格、参数、性能或功能等。

Delphy 基金会在此明确不予承认和拒绝承担下述责任：

（1） 任何人在购买 DPY 时违反了任何国家的反洗钱、反恐怖主义融资或其他监管要求；

（2） 任何人在购买 DPY 时违反了本白皮书规定的任何陈述、保证、义务、承诺或其他要求，以及由此导致的无法付款或无法提取 DPY；

（3） 由于任何原因 DPY 的公开售卖计划被放弃；

（4） Delphy 的开发失败或被放弃，以及因此导致的无法交付 DPY；

（5） Delphy 开发的推迟或延期，以及因此导致的无法达成事先披露的日程；

（6） Delphy 源代码的错误、瑕疵、缺陷或其他问题；

（7） Delphy 平台或以太坊区块链的故障、崩溃、瘫痪、回滚或硬分叉；

（8） Delphy 或 DPY 未能实现任何特定功能或不适合任何特定用途；

（9） 对公开售卖所募集的资金的使用；

（10） 未能及时且完整的披露关于 Delphy 开发的信息；

（11） 任何参与者泄露、丢失或损毁了数字加密货币或代币的钱包私钥（尤其是其使用的 DPY 钱包的私钥）；

（12） DPY 的第三方众筹平台的违约、违规、侵权、崩溃、瘫痪、服务终止或暂停、欺诈、误操作、不当行为、失误、疏忽、破产、清算、解散或歇业；

（13）任何人与第三方众筹平台之间的约定内容与本白皮书内容存在差异、冲突或矛盾；

（14）任何人对 DPY 的交易或投机行为；

（15）DPY 在任何交易所的上市或退市；

（16）DPY 被任何政府、准政府机构、主管当局或公共机构归类为或视为是一种货币、证券、商业票据、流通票据、投资品或其他事物，以至于受到禁止、监管或法律限制；

（17）本白皮书披露的任何风险因素，以及与该等风险因素有关、因此导致或伴随发生的损害、损失、索赔、责任、惩罚、成本或其他负面影响。

## 6.3 风险声明

Delphy 基金会相信，在 Delphy 的开发、维护和运营过程中存在着无数风险，这其中很多都超出了 Delphy 基金会的控制。除本白皮书所述的其他内容外，每个 DPY 购买者还均应细读、理解并仔细考虑下述风险，之后才决定是否参与本次公开售卖计划。

每个 DPY 的购买者应特别注意这一事实：尽管 Delphy 基金会是在新加坡共和国设立的，但 Delphy 和 DPY 均只存在于网络虚拟空间内，不具有任何有形存在，因此不属于或涉及任何特定国家。

参加本次公开售卖计划应当是一个深思熟虑后决策的行动，将视为购买者已充分知晓并同意接受了下述风险。

**（1） 公开售卖计划的终止**

本次 DPY 公开售卖计划可能会被提前终止，此时购买者可能由于比特币/以太币的价格波动以及 Delphy 基金会的支出而仅被部分退还其支付的金额。

### （2） 不充分的信息提供

截止到本白皮书发布日，Delphy 仍在开发阶段，其哲学理念、共识机制、算法、代码和其他技术细节和参数可能经常且频繁地更新和变化。尽管本白皮书包含了 Delphy 最新的关键信息，其并不绝对完整，且仍会被 Delphy 基金会为了特定目的而不时进行调整和更新。Delphy 基金会无能力且无义务随时告知参与者 Delphy 开发中的每个细节（包括其进度和预期里程碑，无论是否推迟），因此并不必然会让购买者及时且充分地接触到 Delphy 开发中不时产生的信息。信息披露的不充分是不可避免且合乎清理的。

### （3） 监管措施

加密代币正在被或可能被各个不同国家的主管机关所监管。Delphy 基金会可能会不时收到来自于一个或多个主管机关的询问、通知、警告、命令或裁定，甚至可能被勒令暂停或终止任何关于本次公开售卖计划、Delphy 开发或 DPY 的行动。Delphy 的开发、营销、宣传或其他方面以及本次公开售卖计划军因此可能受到严重影响、阻碍或被终结。由于监管政策随时可能变化，任何国家之中现有的对于 Delphy 或本次公开售卖计划的监管许可或容忍可能只是暂时的。在各个不同国家，DPY 可能随时被定义为虚拟商品、数字资产或甚至是证券或货币，因此在某些国家之中按当地监管要求，DPY 可能被禁止交易或持有。

### （4） 密码学

密码学正在不断演化，其无法保证任何时候绝对的安全性。密码学的进步（例如密码破解）或者技术进步（例如量子计算机的发明）可能给基于密码学的系统（包括 Delphy）带来危险。这可能导致任何人持有的 DPY 被盗、失窃、消失、毁灭或贬值。在合理范围内，Delphy 基金会将自我准备采取预防或补救措施，升级 Delphy 的底层协议以应对密码学的任何进步，以及在适当的情况下纳入新的合理安全措施。

密码学和安全创新的未来是无法预见的，Delphy 基金会将尽力迎合密码学和安全领域的不断变化。

**（5） 开发失败或放弃**

Delphy 仍在开发阶段，而非已准备就绪随时发布的成品。由于 Delphy 系统的技术复杂性 ,Delphy 基金会可能不时会面临无法预测和/或无法克服的困难。因此，Delphy 的开发可能会由于任何原因而在任何时候失败或放弃（例如由于缺乏资金）。开发失败或放弃将导致 DPY 无法交付给本次售卖计划的任何购买者。

**（6） 众筹资金的失窃**

可能会有人企图盗窃 Delphy 基金所收到的公开售卖所获资金（包括已转换成法币的部分）。该等盗窃或盗窃企图可能会影响 Delphy 基金会为 Delphy 开发提供资金的能力。尽管 Delphy 基金会将会采取最尖端的技术方案保护众筹资金的安全，某些网络盗窃仍很难被彻底阻止。

**（7） 源代码瑕疵**

无人能保证 Delphy 的源代码完全无瑕疵。代码可能有某些瑕疵、错误、缺陷和漏洞，这可能使得用户无法使用特定功能，暴露用户的信息或产生其他问题。如果确有此类瑕疵，将损害 Delphy 的可用性、稳定性和/或安全性，并因此对 DPY 的价值造成负面影响。公开的源代码以透明为根本，以促进源自于社区的对代码的鉴定和问题解决。Delphy 基金会将与紧密 Delphy 社区紧密合作，今后持续改进、优化和完善 Delphy 的源代码。

**（8） 无准入许可、分布式且自治性的账本**

在当代区块链项目中，有三种流行的分布式账本种类，即：无准入许可的账本、联盟型账本和私有账本。Delphy 底层的分布式账本是无准入许可的，这意味着它可被所有人自由访问和使用，而不受准入限制。尽管 Delphy 初始时是由 Delphy 基金会所开发，但它并非由 Delphy 基金会所有拥有、运营或控制。自发形成的 Delphy 社区是完全开放、无中心化且无准入门槛即可加入的，其由全球范围内的用户、粉丝、开发者、DPY 持有人和其他参与者组成，这些人大都与 Delphy 基金会无任何关系。就 Delphy 的维护、治理以及甚至是进化而言，该社区将是无中心化且自治的。而 Delphy 基金会仅仅是社区内与其他人地位平等的一个活跃成员而已，并无至高无上或专断性的权力，哪怕它之前曾对 Delphy 的诞生做出过努力和贡献。因此，Delphy 在发布之后，其如何治理乃至进化将并不受到 Delphy 基金会的支配。

**（9） 源代码升级**

Delphy 的源代码是开源的且可能被 Delphy 社区任何成员不时升级、修正、修改或更改。任何人均无法预料或保证某项升级、修正、修改或更改的准确结果。因此，任何升级、修正、修改或更改可能导致无法预料或非预期的结果，从而对 Delphy 的运行或 DPY 的价值造成重大不利影响。

**（10） 安全弱点**

Delphy 区块链基于开源软件并且是无准入许可的分布式账本。尽管 Delphy 基金会努力维护 Delphy 系统安全，任何人均有可能故意或无意地将弱点或缺陷带入 Delphy 的核心基础设施要素之中，对这些弱点或缺陷 Delphy 基金会无法通过其采用的安全措施预防或弥补。这可能最终导致参与者的 DPY 或其他数字代币丢失。

**（11） “分布式拒绝服务”攻击**

以太坊设计为公开且无准入许可的账本。因此，以太坊可能会不时遭受“分布式拒绝服务”的网络攻击。这种攻击将使 Delphy 系统遭受负面影响、停滞或瘫痪，并因此导致在此之上的交易被延迟写入或记入以太坊区块链的区块之中，或甚至暂时无法执行。

**（12） 处理能力不足**

Delphy 的快速发展将伴随着交易量的陡增及对处理能力的需求。若处理能力的需求超过以太坊区块链网络内届时节点所能提供的负载，则 Delphy 网络可能会瘫痪和/或停滞，且可能会产生诸如“双重花费”的欺诈或错误交易。在最坏情况下，任何人持有的 DPY 可能会丢失，以太坊区块链回滚或甚至硬分叉可能会被触发。这些事件的余波将损害 Delphy 的可使用性、稳定性和安全性以及 DPY 的价值。

**（13） 未经授权认领待售 DPY**

任何通过解密或破解 DPY 购买者密码而获得购买者注册邮箱或注册账号访问权限的人士，将能够恶意获取 DPY 购买者所购买的待售 DPY。据此，购买者所购买的待售 DPY 可能会被错误发送至通过购买者注册邮箱或注册账号认领 DPY 的任何人士，而这种发送是不可撤销、不可逆转的。每一 DPY 购买者应当采取诸如以下的措施妥善维护其注册邮箱或注册账号的安全性：(i) 使用高安全性密码；(ii) 不打开或回复任何欺诈邮件；以及 (iii) 严格保密其机密或个人信息。

**（14） DPY 钱包私钥**

获取 DPY 所必需的私钥丢失或毁损是不可逆转的。只有通过本地或在线 DPY 钱包拥有唯一的公钥和私钥才可以操控 DPY。每一购买者应当妥善保管其 DPY 钱包私钥。若 DPY 购买者的该等私钥丢失、遗失、泄露、毁损或被盗，Delphy 基金会或任何其他人士均无法帮助购买者获取或取回相关 DPY。

**（15） 通胀**

取决于 Delphy 平台发布时的具体底层协议，DPY 总量可能随时间略有增加，且可能会由于采纳 Delphy 源代码补丁或升级而进一步增加。由此产生的 DPY 供应量通胀可能导致市场价格下跌，从而 DPY 持有者（包括购买者）可能遭受经济损失。DPY 购买者或持有者并不能被保证会由于 DPY 通胀而获得赔偿或任何形式的补偿。

**（16） 普及度**

DPY 的价值很大程度上取决于 Delphy 平台的普及度。Delphy 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。在最坏情况下，Delphy 甚至可能被长期边缘化，仅吸引很小一批使用者。相比之下，很大一部 DPY 需求可能具有投机性质。缺乏用户可能导致 DPY 市场价格波动增大从而影响 Delphy 的长期发展。出现这种价格波动时，Delphy 基金会不会（也没有责任）稳定或影响 DPY 的市场价格。

**（17） 流动性**

DPY 既不是任何个人、实体、中央银行或国家、超国家或准国家组织发行的货币，也没有任何硬资产或其他信用所支持。DPY 在市场上的流通和交易并不是 Delphy 基金会的职责或追求。DPY 的交易仅基于相关市场参与者对其价值达成的共识。任何人士均无义务从 DPY 持有者处兑换或购买任何 DPY，也没有任何人士能够在任何程度上保证任何时刻 DPY 的流通性或市场价格。DPY 持有者若要转让 DPY，该 DPY 持有者需寻找一名或多名有意按共同约定的价格购买的买家。该过程可能花费甚巨、耗时长并且最终可能并不成功。此外，可能没有加密代币交易所或其他市场上线 DPY 供公开交易。

**（18） 价格波动**

若在公开市场上交易，加密代币通常价格波动剧烈。短期内价格震荡经常发生。该价格可能以比特币、以太币、美元或其他法币计价。这种价格波动可能由于市场力量（包括投机买卖）、监管政策变化、技术革新、交易所的可获得性以及其他客观因素造成，这种波动也反映了供需平衡的变化。无论是否存在 DPY 交易的二级市场，Delphy 基金会对任何二级市场的 DPY 交易不承担责任。因此，Delphy 基金会没有义务稳定 DPY 的价格波动，且对此也并不关心。DPY 交易价格所涉风险需由 DPY 交易者自行承担。

**（19） 竞争**

Delphy 的底层协议是基于开源电脑软件。没有任何人士主张对该源代码的版权或其他知识产权权利。因此，任何人均可合法拷贝、复制、重制、设计、修改、升级、改进、重新编码、重新编程或以其他方式利用 Delphy 的源代码和/或底层协议，以试图开发具有竞争性的协议、软件、系统、虚拟平台或虚拟机从而与 Delphy 竞争，或甚至赶超或取代 Delphy。Delphy 基金会对此无法控制。此外，已经存在并且还将会有许多竞争性的以区块链为基础的平台与 Delphy 产生竞争关系。Delphy 基金会在任何情况下均不可能消除、防止、限制或降低这种旨在与 Delphy 竞争或取代 Delphy 的竞争性努力。

# 第 7 章　开发计划

**2017 Q3**

1）　Delphy-Core 开发

2）　Delphy.go 开发

3）　Centralized Oracle 开发

**2017 Q4**

1）　Event & Market 编辑器开发

2）　SWARM-based Storage 开发

3）　Mobile Wallet 开发

4）　iOS & android App 开发

5）　Delphy-Core、Delphy.go 和 Oracle 持续开发

**2018 Q1**

1）　Alpha 版开发完成

2）　RealityKeys 集成

3）　提供 API & SDK

4）　Security Auditing 安全审计

5）　Delphy 试运行

**2018 Q2**

1）　Hackathon

2）　分布式的存储与索引开发

3）　KYC 开发

4）　Event Filter 开发

5）　Security Auditing

# 第 8 章　团队

## 核心团队

### 汪波 Bo Wang

北京大学信息管理学士，美国密歇根大学信息经济学硕士学位。原 Factom（公证通）联合创始人，工程副总裁，具有 20 多年互联网及软件开发和管理经验。在中国和美国多次成功创业。区块链技术资深专家，2012 年在美国开始接触区块链，是区块链共识算法和 P2P 网络的先行实践者。

### Tllik

北京大学应用数学博士。研究密码学理论和应用方向，主要研究椭圆曲线双线性对以及离散对数等艰深问题，在信息安全领域有 10 余年研究和开发经验。

### Greentree

郑州大学数学系学士，善于算法和性能优化。前西山居游戏引擎人员，远明山水的创始成员，自研 3D 千人同屏网络游戏引擎泰坦，精通虚幻，Unity 游戏引擎。精通 Mac，Linux, Windows, iOS & Android 等多种平台的服务器端&客户端技术，精通 solidity 智能合约编程。

### Jerry

中科院计算机系硕士。原甲骨文 IoT、云计算中国区主要研发人员；JavaCard、N3、JVM & EVM 虚拟机专家；JavaCard、N3 系统加密库国密算法主要实现人；Hyperledge/Fabric & Ethereum 专家。

### Frank

Frank 拥有丰富的项目开发、管理经验。熟悉 Java, Spring Framework, JavaScript, React, AngularJS 等语言及框架，全栈工程师。

## 理事会 & 顾问委员会

**沈波 Bo Shen**：分布式基金创始人

**龚鸣 James Gong**：《铅笔》创始人

**孙铭 Roland Sun**：世泽律师事务所合伙人

**吴钢 Gang Wu:**币信创始人

**参考文献：**


［1］ Ethereum Whitepaper: https://github.com/ethereum/wiki/wiki/White-Paper
［2］ TruthCoin Whitepaper: http://bitcoinhivemind.com/papers/truthcoin-whitepaper.pdf
［3］ Augur Whitepaper: https://bravenewcoin.com/assets/Whitepapers/Augur-A-Decentralized-Open-Source-Platform-for-Prediction-Markets.pdf
［4］ Gnosis Whitepaper: https://gnosis.pm/resources/default/pdf/gnosis_whitepaper.pdf
［5］ Protess, Ben Intrade Bars U.S. Bettors After Regulatory Action
［6］ Mann, Adam The power of prediction Markets Nature Vol 538, Issue 7625
［7］ Kambil, Ajit Predictive Markets: Predicting the rise of prediction Markets Analytics Magazine, March/April 2011
［8］ Rice, Andrew The Fall Of Intrade And The Business Of Betting On Real Life
［9］ Yeh, Puong Fei Using Prediction Markets to Enhance US Intelligence Capabilities
［10］Hanson, Robin. The Policy Analysis Market - A Thwarted Experiment in the Use of Prediction Markets for Public Policy, innovations： Technology, Governance, Globalization : 73—88
［11］Gelman, Andrew Something's Odd About the Political Betting Markets
［12］Simon de la Rouviere Why & How Decentralized Prediction Markets Will Change Just About Everything.
［13］Hanson, R. Combinatorial Information Market Design[J]. Information Systems Frontiers, 2003, 5(1):107-119.
［14］Hanson, R. Logarithmic Market Scoring Rules for Modular Combinatorial Information Aggregation[J]. Journal of Prediction Markets, 2009, 1(1):3-15.
［15］Arrow K J, Forsythe R, Gorham M, et al. The Promise of Prediction Markets[J]. Science, 2008, 320(5878):877-8.
［16］Hanson R, Oprea R. A Manipulator Can Aid Prediction Market Accuracy[J]. Economica, 2009, 76(302):304–314.
［17］Pennock, David Implementing Hanson's Market Maker, http://blog.oddhead.com/2006/10/30/implementing-hansons-Market-maker/, 2006.
［18］Justin Wolfers, Eric Zitzewitz(2006): Interpreting Prediction Market Prices as Probabilities, Social Science Electronic Publishing
［19］Hanson, Robin (2013) Shall We Vote on Values, But Bet on Beliefs?* Journal of Political Philosophy: 151-178
［20］David Porter, Cary Deck( 2013), Prediction Markets in the Laboratory, Journal of Economic Surveys : 589-603
［21］郑伟（2008）， 地震保险:国际经验与中国思路， 保险研究: 9-14
［22］万国华， 李铭（2016）: 我国二元期权交易的法律规制路径研究，《金融监管研究》 ： 34-50

[23] 张宁， 李国秋（2016）：企业内部运行的预测市场研究《竞争情报》:52-58
[24] 童振源、林馨怡（ 2008）：台湾选举市场预测： 预测市场的运用与实证分析，选举研究: 131-166.
[25] http://consensuspoint.com/
[26] https://www.cultivatelabs.com/
[27] https://www.predictit.org/
[28] https://tippie.biz.uiowa.edu/iem/
[29] http://bitcoinhivemind.com/
[30] https://fairlay.com/
[31] https://github.com/psztorc/Truthcoin
[32] https://en.wikipedia.org/wiki/Prediction_market