超预测

SuperForecasting

未来工程科技

目录

1 背景

1.1 两则故事

1.1.1 故事一

在上世纪初的南岳衡山，有一位很有名的道士，毛泽东在童年时就知道他。据说这道士能预知未来，当时曾说自己能活 120 岁，但因“泄露天机”，60 岁时双眼就会瞎掉。在道士 40 多岁时曾游方至韶山一带，毛泽东父亲曾请他给十多岁的毛泽东看相。

道士称:“令郎将来贵不可言，只是命途多舛，婚姻多变，会累及家中人丁不旺……”

毛泽东家人曾为此话郁闷多时。

1966 年 7 月中旬，身为中国人民伟大领袖的毛泽东主席在武汉畅游长江后去长沙，在接见湖南各地领导干部时得知这位衡山道士虽然眼瞎多年，且已有 100 多岁，但身体仍很健康，遂决定去衡山看他。

路上，毛泽东兴致勃勃的对随行的华国锋、汪东兴等人讲起这位道士那时曾说过湖南这个地方在一百年内会出现五个帝王级的人物。毛泽东指着自己说：“我应该算一个，刘少奇也应该算一个。还有一个应该是彭德怀，以后还能有谁就不清楚了。”在相关人员指引下，毛泽东一行人在距老道士茅屋百余米的大树下停住。毛泽东让华、汪等随行人员在此等候，自己只身来到茅屋窗前，先吟一句诗：“结庐在仙境”。屋里有人应答：“贵客到柴门”。毛泽东道一声“仙人，打扰了!”随即推门入内。汪东兴安排好周边警戒后，担心主席安危，悄悄靠近茅屋窗前，听到主席在用浓重的湖南乡音和老道士交谈。那道士声音宏亮：“刘这个字，就是这样了。你用好人的法子对付不了他，你是毛他是卯金刀，哪里是对手。可是你有你的办法，乱毛如毡，裹土加沙，水浸油滑，也能挡得住他。可是你要在这上面折阳寿的啊至于那个林，你不必担心。木秀于林，风必摧之。如果他出头，别人会治他，用不着你动手。你是属蛇的，和林没有麻烦。不要被人借刀杀人。可是你这个人，多疑善变，这两件事情恐怕都弄不好，此乃天命，也无法更改。你自己看着办吧。”汪东兴知道毛泽东来看道士的目的了。

听见毛泽东问：“你看我还能活多少年？”道士说：“过来，让我摸摸天门。”汪一阵紧张，怕这时出现万一。道士说：“五十年前，我大概就给你算过。你是长寿人，应当好好做学问的。现在晚了，该干什么就去干吧。”毛泽东问：“要干的事情很多，我还能安排几年？”道士说：“这要看自己

的作为，看心境，看机会。”毛泽东又问：“大体上总得有个数字吧？”道士说：“安排两个五年计划吧。多了就算你赚了。”毛泽东问：“我是个本乡人，又是异乡人。此去经年，你看我还有机会回家吗？”

道士哈哈大笑，随口给毛唱一首诗：“小儿出家娘断肠，返乡原是一黄粱。公说婆说皆真理，自生自灭无汉唐。包公羞居大开封，秦桧喜游小苏杭。南岳不是你宿处，不在沙场在大堂。”毛泽东即兴地说：“我也奉和几句，见笑了。是人岂不恋故乡，红肉辣椒伴谷粱。男儿女儿论孝顺，街前街后说荒唐。人说回首即佳境，我无反顾奔天堂。阴间阳世墙一道，是福是祸随他娘！”道士沉吟半晌，说：“好诗，好诗。谢谢。”毛泽东说：“最后一句不和，请仙人谅解。”道士说：“气势到了那地方，就不能管压不压韵了。这就是你的道。强求不得。我倒是觉得这样的诗好。见了性情。”毛泽东说：“如果仙人不嫌弃，回去后我会将拙诗抄写了寄上。也请您将惠赐的诗寄下。”道士说：“不敢不敢。我差不多知道你是谁了。我不能和你打交道太多。”毛泽东说：“那倒不必顾虑。”出来时，他的手里拿着一张纸，上面写着十六个字：上山走弦，下山走弓；玉全瓦碎，无动于中。“你替我找地方保存起来。将来我要验证的。”毛泽东把字条递给汪东兴，意味深长地说：“哲学上还有很多东西没弄清楚，算命就是一条”。

1.1.2 故事二

2003 年，在美国入侵伊拉克之后，美国情报圈震惊地发现它在萨达姆拥有大规模杀伤性武器问题上的判断大错特错。两年前，它因未能根据种种迹象预见到“9.11”恐怖袭击而受到指责；伊拉克战争后，它又因为胡乱猜测而再次受到指责。2 万名聪明的情报分析师的辛勤工作和数十亿美元付诸东流。

于是，情报圈决定以科学、合理的方式测试如何提高研究水平、判断力和预测事件的能力。它建立了一个新机构，即情报高级研究计划局，该机构于 2011 年委托他人组织了一项预测比赛，任务是每日预测未来 1 个月至 1 年内的事件，在 4 年时间里共计预测了 500 个事件。

共有 5 个团队参加，采用不同的方法，预测结果会得到客观比较。其中，4 个团队由专业人士（例如一流的国防分析师）组成，还有 1 个团队被称为“精准预测项目”，组成人员为数百名普通志愿者，由泰洛克精心组织。它的志愿者来自各行各业，共同特征是都为非专业人士。每个人每天都会收到问题，如石油价格在 6 个月内会不会达到每桶 100 美元，或者约

翰. 马哈马是否会当选下一届加纳总统。他们每天都会提交概率预测，如 65% 的机会或者 20% 的可能性。他们可以按照自己的意愿运用任何研究方法，利用公开的资料，每天自由选择一定的时间来做预测。

泰洛克被邀请加入，是因为过去多年他一直在运作一个研究项目，检验专家的预测准确率比随机预测高出多少。在情报高级研究计划局的比赛中，泰洛克组织的没有专家参加的精准预测项目比各专家团队表现优异。第二年年末，前者的优势非常明显，准确率几乎超出后者 80%，于是情报高级研究计划局终止了与其他团队的合作，只关注精准预测项目的研究成果。

1.2 预测

这两个故事引出了我们现在社会的两大预测体系，第一是传统的周易、紫微斗数、梅花易数、六爻八卦、奇门遁甲、手相面相、生辰八字、风水、占星、神谕、塔罗牌等等；第二是以超预测为代表的工作方法。

我们这里重点来讲述一下泰洛克的《超预测》，预测是一门“科学”或者“艺术”。

我们经常浏览新闻说专家预测怎么样怎么样，但是事后经常被打脸，百年一遇、千年一遇等等发生频率越来越高；当然也有世界杯上的章鱼保罗、乌贼刘这些神奇的存在。

我们也经常“预测”，在考虑换工作、结婚、买房子、投资、推出新产品和退休时，我们的决定是以我们对未来的展望为依据的。这样的展望即是预测。我们自己常常做一些预测。但是，我们都想成为更优秀的预测家，指导自己人生未来的方向，我们可能在心里问自己，面对这现实世界中这么多不确定性，我们可以做到吗？

首先预测简单定义是根据理论假说对事物未来发展趋势和变化的方向等作出判断，它是在理论限定的范围内运用逻辑规则演绎出来的结果。它区别于大数据，大数据是基于历史数据的大量统计分析，在某些领域方面是有优势的 (特别是大量数据可供研究分析)，但是在预测个体事件发生频次都很低的情况下，现实世界的复杂度是它目前所不能解决的。就像蝴蝶效应一样，在世间混沌复杂的背景下，微小的参数扰动就能导致事件走向另一个极端发展方向。

其次泰洛克主持了精准预测项目，研究得出两个关键结论。其一，准确的预测是可以做到的。有些人，绝对具有洞察未来的能力。他们不是能

够看到未来数十年的宗教导师或者祭师，但是他们掌握了一种实实在在的可评估的技能，通过它来判断高风险事件在未来 3 个月、半年、1 年或者 1 年半的发展趋势。其二，这些超级预测家为什么如此出类拔萃？原因绝对和他们的身份无关，而是与他们的方法有关。洞察未来的能力并非天赐的神秘禀赋。它是独特的思维方式、信息搜集方法和不断更新观念的产物。任何脑子不笨、喜欢思考、意志坚定的人都可以学习和培养这样的思维习惯，他甚至完全可以从简单的课程入手。超级预测需要的是最低程度的智力、数学才能和世界知识，任何读过严谨的心理学著作的人都很可能具备以上先决条件。

所以“预测”不是一个与生俱来的技能，它们既可以传授给他人，也可以从他人那里习得，不断的实践、实践、实践。

他在书中提供了预测技巧和若干成为超级预测家的准则，让普通人也可以超越行业专家，成为超级预测家。

对个人来讲，我们可以基于预测来影响自己的就业、投资理财等等；对企业来讲，可以基于预测来制定决策、发展客户、产品定价等等；对于国家，特别是情报部门，通过对地缘政治、经济问题等等的预测来保障国家利益。

虽然已经没有如果，不过我们还是要反问一下：

如果当初预测特朗普会成为美国总统，那其他国家是否会对他的竞选理念做一些准备？

如果乐天预测中国在萨德问题上的反应，乐天还会如此处理吗？

以前的事已经发生，不过我们可以对当下的未来预测一下：

中美贸易战今年年底前会停止吗？

欧美零关税磋商会在年底前达成一致吗？

美国国会会通过《综合关税法》吗？（该法案将降低或取消烤面包机、化学品等约 1660 种进口商品的关税，其中近一半产自中国。）

特朗普和金正恩今年还会会谈吗？

等等，我们都可以去预测这些影响着我们生活的大事件。

当然，还有其它更细一点的：

如果你买了小米的股票，你可能希望预测小米今年的手机销量如何？

如果你是国际贸易者，你可能希望预测国内外的一些货币相关的经济政策，比如是否量化宽松？

如果你是币圈的人士，你可能关注预测美国是否会批准近期的比特币

ETF？

如果你从事金融衍生品行业，你可能关注该金融衍生品的未来期望预测？

如果你喜欢足球竞猜，你可能关注比赛的赛果如何？

包括足球、篮球、地缘政治、经济、科技等等领域，比如原油价格、猪肉价格、房价走势、GDP、经济行情指数、股市指数、电影票房等等，具有极大的商业价值。

这些事件都对我们的日常生活或投资理财都有影响。

讲了这么多，那还等着什么？让我们都成为优秀的超级预测家吧。

2 系统设计

系统分为几大模块:

2.1 精准预测大赛

来源于泰洛克的精准预测项目的预测大赛，通过比赛的形式不仅锻炼大家的预测能力，同时也能筛选出超级预测师。其核心流程如下图：

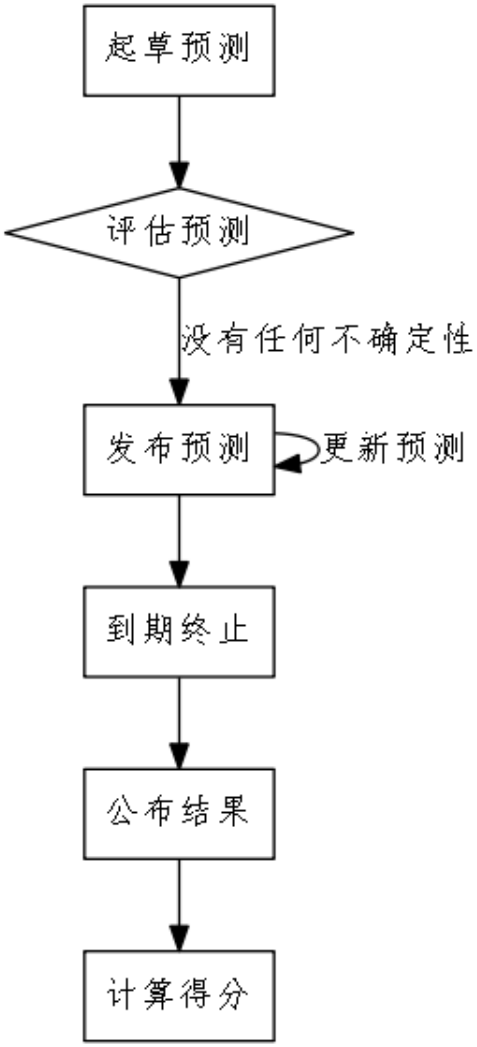

图 1: 精准预测项目比赛流程

规则注意：

- 没有时间表和包含语意含糊措辞的预测是荒唐可笑的。
- 基于布莱尔评分的计分系统。
- 所有预测结果选项的概率和为 1。
- 更新预测时必须附带说明此次更新依据。
- 比赛中发布或更新预测需要一定的时间间隔。
- 每个参赛者更新预测需要一定的时间间隔。

得分规则：

$$BS = \frac{1}{N}\sum_{t=1}^{N}\sum_{i=1}^{R}(f_{ti} - o_{ti})^2$$

其中 f_{ti} 是预测的概率，o_{ti} 表示事件的实际结果（0 如果它没有发生和 1 如果确实发生了），N 是实际预测的数量和 R 是事件可能落入的可能选项的数量。得分越低，说明预测准度越高。

在预测的过程中，我们可以查看某人 (或团体) 的预测结果和预测结果分布。随着时间的推进，我们有大量的实验结果，就会培养或筛选出优秀的预测师，我们可以关注这些预测师的预测，为我们提供参考。

举个例子，我们这一期比赛：北京时间 8 月 6 日足球友谊赛：拜仁 VS 曼联，拜仁相对于曼联的进球数为多少？可能的结果事件集 $(-\infty, -4, -3, -2, -1, 0, +1, +2, +3, +4, +\infty)$，如果比赛最终结果为 2 ：3，则选项为 -1（2 - 3）的选项为最终结果。

例如我首先预测 $(0, 0, 0, 5, 15, 45, 20, 15, 0, 0, 0)$，然后我看到新闻说卢卡库和博格巴回归球队训练基地，我猜测他们很可能会参加此次比赛，我更新我的预测为 $(0, 0, 0, 5, 20, 50, 15, 10, 0, 0, 0)$，并附带上我的更新说明：XX 新闻说博格巴与卢卡库已经回归训练基地，他们可能会上场。后面我又更新了我的预测为 $(0, 0, 0, 0, 20, 60, 20, 0, 0, 0, 0)$，附带我的更新说明：热身赛，分差应该不大。我的预测展示图：

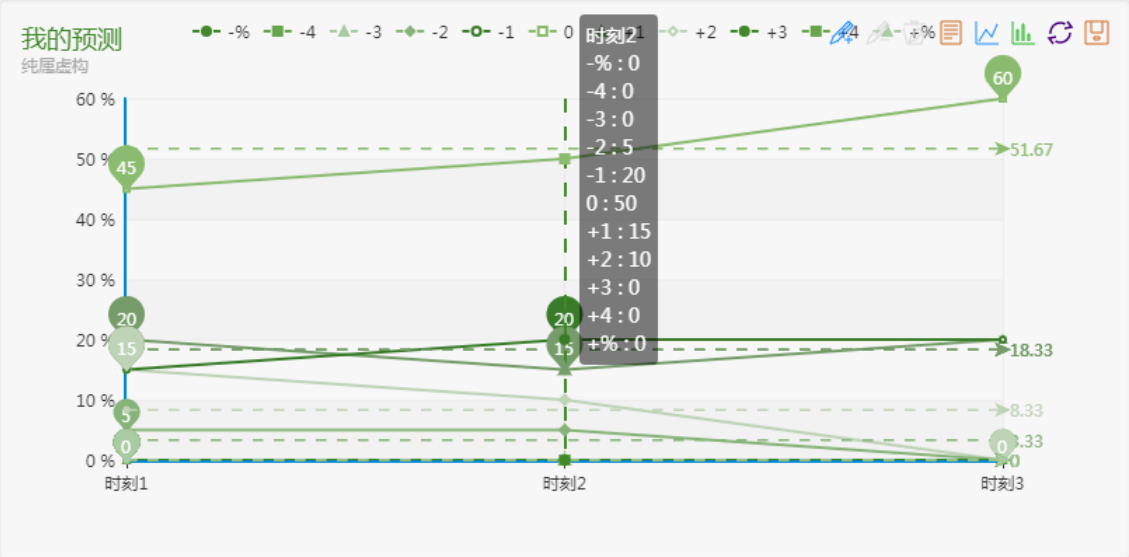

图 2: 我的预测

当然我们不仅可以看到自己的预测图，也可以看到其他人、某些团体、包括所有人的预测，为我们提供参考 (预测权重可以变化)。

如果实际结果为 -1，那我的 BS 得分为 $\frac{0.99+0.925+0.44}{3} = 0.785$，最终成绩进入超级预测战力排行榜。

2.2 传统预测

命运的奇妙离奇, 总是在千百个转折之间, 一步踏出去, 你不知道前面等待你的会是什么样的结果, 唯一能做的, 只是继续走下去。

古代第一女神相许负预言薄姬是天子之母，结果后面薄姬被刘邦纳之，生下刘恒，安然度过诸吕之乱，最终贵为天子之母。她还预测周亚夫“将军三年后定然被封侯，卦侯之后再过八年，定为将相，持国柄，贵重一时，人臣中再无胜过将军者。不过，为相后再过九年而饿死。”，结果“三年后，周亚夫被封为条侯。八年后，于景帝时，他任尉，因平定七王之乱有功，迁为丞相。后因其子私购御用物品，受牵连被下狱，竟绝食而死。”。

汉唐以来，历代都有研究易经的人，尤其在汉宋两代易学宏扬为最，它所包含的思想，接人待物无所不包。易学所言之处，包罗万象而尽精微，为六经之首，一切道理之根源，可应用到任何学术上，如山医卜命相、兵

法、仙学、天文学、伦理哲学……等多方面。易经尊为修身、齐家、治国、平天下的学问，其能流传至今，且有愈盛之势，其中蕴藏着无限的智慧之故。

当今时代，易学预测被较多的人所能接受，也有一部分人认为周易预测是迷信活动的一部分。周易文化经由几千年的发展，周易预测方法从祖先们创立至今已经有着几千年的历史记录，在这么漫长的岁月中，能够走到今天让我们这辈人认识并了解和来运用它、发扬它，说明这套理论系统的存在是有它真实不虚的科学理论观点。

由于学术上缺乏有力的引导，仍表现为与其它迷信术数混杂，许多人仍视易为卜筮之道。周易预测这一整套的科学理论系统，除了需要人们深入了解，还需要社会人士正确弘扬，如何从古老而常新的周易预测中剔除神秘色彩和人身依附关系，提炼、总结出有实质借鉴意义的预测思想成为时代赋予我们的重任。如今，虽然周易预测研究成果层出不穷，但有价值的成果并不多。

中华文化博大精深，就算命术而言，它是古代人民经过多年实践总结而成的智慧结晶，理论系统复杂深奥，一般人穷一生之努力未必能参透十之五六。

因这门学问非现代科学范畴，且比较深奥、神秘，人们对此门学问缺乏正确了解，这便使江湖术士有了宽泛的招摇撞骗空间。再之由于预测术缺乏完善而严谨的科学理论，业界研习者水平参差不齐，半桶水者居多。有需求就有市场，社会上有不少打着“易学预测”的幌子，冠上响亮的名号，名号已不是古时的“半仙”了，而是与时俱进叫做“大师”。这些“大师”当中不乏一些游手好闲的小文化人或粗通一些易理知识的人，号称懂八卦、会看手相面相、能解灾避祸，招摇撞骗，凭三寸不乱之舌忽悠赚钱为生。学问不足但为了谋生惟夸夸其谈、故弄玄虚，搬弄些模棱两可的话语，扯上些迷信的东西，以此自圆其说；还有甚者以帮人化解为由刻意夸大一些因素（比如名字之类）对人命运的影响力，籍此牟利。

由于人们对这门学问缺乏正确的认识，兼且社会上装神弄鬼、故弄玄虚、招摇撞骗的“大师”泛滥，久而久之便使这门学问蒙上了迷信色彩。对这门学问要用科学的视角去看待，盲目迷信或全盘否定都不是科学的态度。

从人民中来，到人民中去。传统预测，比如周易、紫微斗数、梅花易数、六爻八卦、奇门遁甲、手相面相、生辰八字、风水、占星、神谕、塔

罗牌等等，我们不能因为它的“神秘性”而否决它，而是正视它，规范它。命运师需要大量的案例学习，同时也有大量的人需要命运师解惑，借助大家的力量，通过平台的辅助来帮助我们筛选出优秀的命运师。

规则注意：

- 用户分为命运师和一般用户两类，每个用户都有能量值 (power)，如果能量值被消耗，会不停的恢复，最终恢复到固定的能量值 (power)，同时命运师还有命运大师积分（mater），一定程度上代表用户对其预测水平的认可。

- 用户如何发起求测？用户如果想发起一次求测，必须消耗一个命运值 (destiny)。命运值 (destiny) 有何而来？假设系统中有 N 个命运师，每个命运师工作 8 小时，每测一次平均花费 1 小时，则每天可以提供的预测服务为 $8N$ 次，则每天大概的命运值为 $8N$。假设周期为 α，则每周期释放的命运值理论上为 $\frac{8N}{\alpha}$。根据以太坊的某一高度的区块哈希值建立竞猜，用户花费能量值 n_{power} 参与竞猜，根据参与的能量值构成一长度区间 $[0, total_{power}]$，$total_{power}$ 是不小于参与的能量值长度的。当前用户那所属的其实空间为 $[a, b]$，理论上 $(b-a+1) = \beta \cdot n_{power}$，其中 β 是一个不小于 1 的系数，如果用户此次没有预测中，下次参与预测 β 会增大，否则 β=1。用户可以采用系统内置的 Token 购买一定的能量值。

- 用户发起求测之后，需要命运师来解惑。命运师回答的问题可以分为公开和不公开两种情况。不公开情况下，通过迪菲 -赫尔曼密钥交换协议产生安全的“协商密钥”，然后通过该密钥对该消息加密，求测者可以还原“协商密钥”解密消息。公开情况下，可以分为对命运师公开和对所有人公开两类级别，而且这时候还可以设置要求一定的能量值 (power) 才能浏览消息，该能量值与求测者均分。求测者在自己发起的求测帖中可以针对命运师的解惑发起命运师评价，有 5 次机会，每次评价 (不可重复)，该命运师会相应得到一个命运大师积分 (master)，而且该命运大师积分会同时折算成固定的能量值。其它有相应的浏览权限的用户也可以评价，被评价的用户会得到一定的能量值。如果是命运师得到其他命运师的评价，则相应的得到的能量值会有一定的加持，加持比率根据评价的命运师在命运师中的命运大师积分相关。

- 用户参与预测获得或消费的能量值和命运大师积分会影响到激励模型。

2.3 去中心化预测市场

2.3.1 预言机

预言机是一种可信任的实体，它通过引入关于外部世界状态的信息，从而允许确定的智能合约对不确定的外部世界作出反应。在去中心化预测市场中，预测市场需要知道外部世界的事件发生的结果，并做出响应。

基于中心极限定理的集体预言机 设 p 为系统内用户支持某个候选决议的比率。现在“随机”地对 n 个系统内用户进行调查，然后计算这 n 个系统内用户对该候选决议的支持率 M_n,

$$M_n = \frac{X_1 + \cdots + X_n}{n},$$

其中 X_i 是被选择的第 i 个系统内用户的态度，$X_i = 1$ 表示系统内用户支持某候选决议，$X_i = 0$ 表示系统内用户返回某候选决议。假设 p 是这个候选决议在系统内的全用户的支持率，则 X_i 是服从参数为 p 的伯努利随机变量。故 M_n 的均值为 p，方差为 p(1-p)/n, 利用中心极限定理，M_n 近似服从正太分布。

下面计算概率 $P(|M_n - p| \geq \epsilon)$，$\epsilon$ 是估计精度，即计算调查这 n 个人的支持率与全体系统内用户的支持率相差大于 ϵ 的概率。由正态分布的对称性，可得

$$P(|M_n - p| \geq \epsilon) \approx 2P(M_n - p \geq \epsilon).$$

显然 $M_n - p$ 的方差为 p(1-p)/n, 依赖于未知参数 p，所以也是未知的。注意，偏离均值的概率随着方差的增大而增大，所以为了得到概率 $P(|M_n - p| \geq \epsilon)$ 的上界，人们可以假设 $M_n - p$ 有最大的方差，即当 p=1/2 时，方差为 1/(4n)。为此，先计算

$$z = \frac{\epsilon}{\sqrt{1/(4n)}},$$

所以

$$P(|M_n - p| \geq \epsilon) \leq 1 - \Phi(z) = 1 - \Phi(2\epsilon\sqrt{n}).$$

现在考虑一个问题，如果希望估计 M_n 与真值 p 的差距为 0.01 之内的概率至少是 0.95，则样本容量 n 应该多大？现在我们假设最坏的情况发生，此时 M_n 的方差达到最大，这个假设引向条件

$$2 - 2\Phi(2 \cdot 0.01 \cdot \sqrt{n}) \leq 0.05,$$

即

$$\Phi(2 \cdot 0.01 \cdot \sqrt{n}) \geq 0.975.$$

根据正态分布表，可查得 $\Phi(1.96) = 0.975$，所以上式等价于

$$2 \cdot 0.01 \cdot \sqrt{n} \geq 1.96,$$

即

$$n \geq \frac{1.96^2}{4 \cdot (0.01)^2} = 9604.$$

需要 9604 个样本可以保证。所以我们可以基于系统内的足够的用户就可以通过投票对某项决议达成共识。

对于公众可知的事件，我们可以让大家公布自己已知的事件结果，至少需要 9604 个用户参与，那么如果某个事件结果超过 95%(95% 以上的用户是诚实可靠的)，则为事件的最终结果。

我们引入信用和激励制度来奖励诚实可靠的用户。

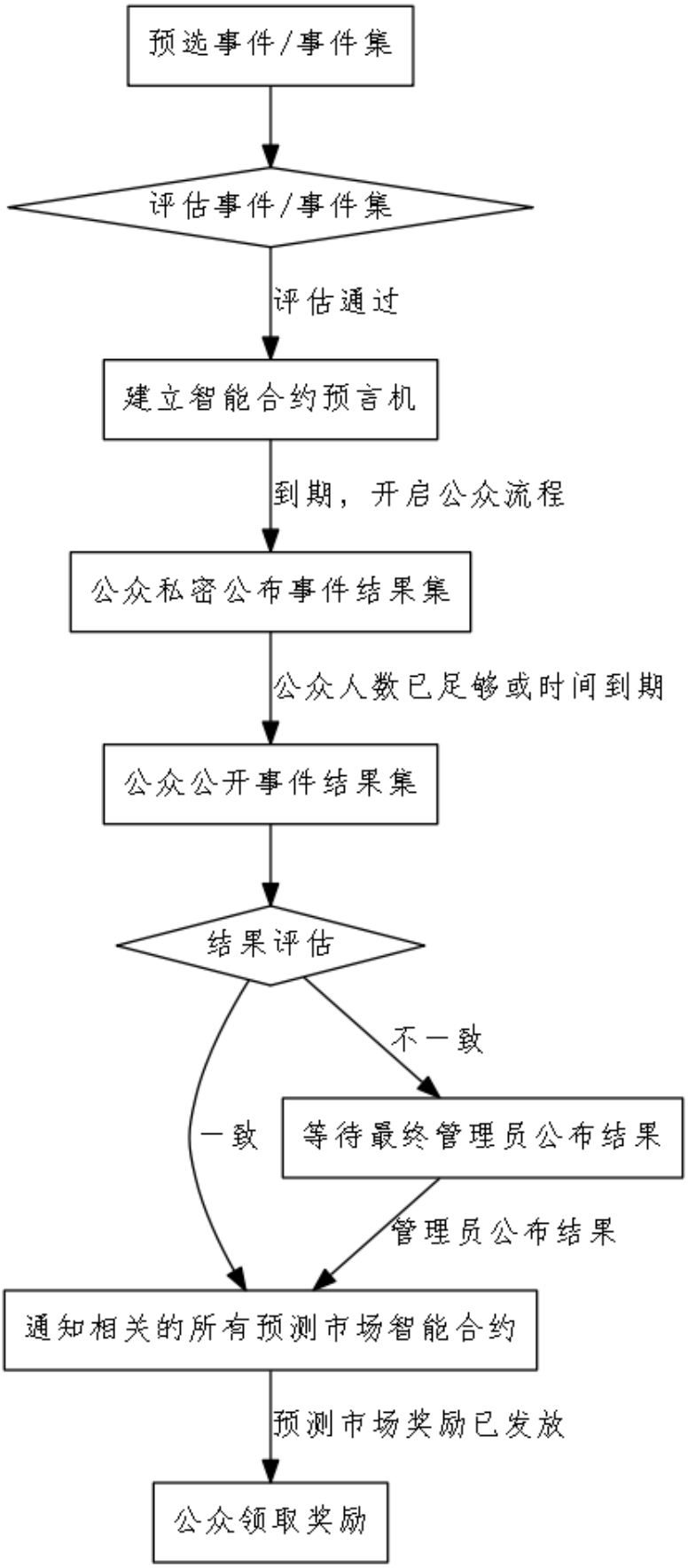

图 3: 基于智能合约的预言机业务流程

2.3.2 预测市场

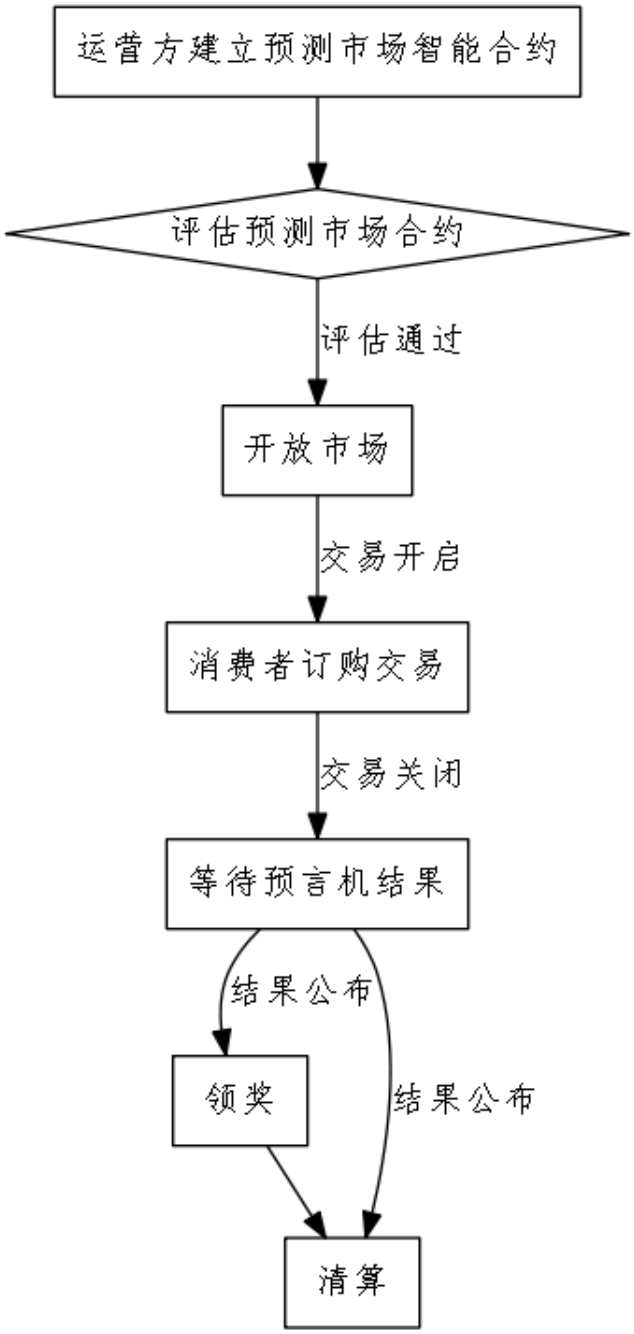

图 4: 预测市场业务流程

预测市场模型

支持 LMSR（Logarithmic Market Scoring Rule-对数市场评价法则）模型 这种机制被很多公司或者项目使用，包括 Microsoft、Augur 以及 Gnosis。

$$C(q_1, q_2, \ldots, q_N) = \ell log(\sum_{j=1}^{N} e^{q_j/\ell})$$

这是成本函数 C，其中 q_j 是结果 j 的股份，N 是所有可能的结果，ℓ 是亏损限制。

当 q_j 都为 0 时，最大的可能亏损为：

$$\sum_{j=1}^{N} e^0 = N \Rightarrow C(0, 0, \ldots, 0) = \ell logN.$$

这部分为 Market Maker 建立预测市场时候的准备金。

用户买 x 份结果 k 的股份，则需要支付：

$$C(q_1, q_2, \ldots, q_k + x, \ldots, q_N) - C(q_1, q_2, \ldots, q_k, \ldots, q_N)$$

当用户卖出结果 k 的 x 份股份，如果结果为负，则盈利:

$$C(q_1, q_2, \ldots, q_k - x, \ldots, q_N) - C(q_1, q_2, \ldots, q_k, \ldots, q_N)$$

当预测事件发生后，结果 i 获胜，则 Maket Maker 的盈利为：

$$C(q_1, q_2, \ldots, q_N) - \ell logN - q_i.$$

支持市面上大部分乐透型和竞猜型 比如强力球、欧洲百万、欧洲大彩、超级百万、La Primitiva、胜负彩、任选九场、大乐透、双色球、3D、排列三、排列五等等。运营商根据游戏规则创建智能合约，其事件结果来源于系统的去中心化预言机。

强力球举例

- 建立强力球智能合约预言机，包含两个事件: 事件 i> 强力球 2018 年 8 月 5 日开奖白球？包括 69 个选项，69 选 5。事件 ii> 强力球 2018 年 8 月 5 日开奖红球是多少？包括 26 个选项，26 选 1。

- 运营商建立强力球预测市场智能合约，其预测事件来源于强力球预言机的预测事件，合约包括奖池、中奖规则、用户领奖、用户购彩、清算等等，审核通过就可以进入预测市场让用户购彩。
- 开奖后，强力球预言机得到结果，强力球预测市场开始领奖并清算。

胜负彩举例

- 13 场比赛可能来源于多个预言机，我们可以建立多个预言机，比如英超比赛的所有球队的预言机、西甲比赛的所有球对的预言机、意甲比赛的所有球队的预言机。
- 运营商建立胜负彩预测市场智能合约，其比赛来源于上面的多个预言机，合约包括相关的规则，审核通过后就可以进入预测市场用户购彩。
- 比赛结束后，预言机得到结果，胜负彩预测市场开始领奖并清算。

2.4 论坛

需要一些板块方便大家一起交流或者一些文化的传播与传承。比如预测文化板块、庙宇道观板块、预测名人板块、养生板块等等。

2.5 私密通信

整合 Telegram 通信客户端 Telegram 是开源 IM 工具，其使用的 MTProto 通信协议是一个 Telegram 自定义的通讯协议，用于移动端 App 与服务器交互数据使用，具有安全性与私密性。

我们可以定制开发第三方客户端，整合进平台，并增加阅后即焚功能，满足平台通信的安全性与私密性。

端对端加密通讯协议 Signal Signal protocol 可应用在双方通讯，群组通讯中，能保证传输的消息，图片，音频，视频等文件的加密传输。即使某个消息的密钥泄露，黑客也无法解密以前的消息和之后的消息，所以 Signal protocol 能提供前向安全和后向安全。

Signal protocol 采用的是 X3DH 协议创建消息密钥。X3DH 协议基于 DH 协议，但是引入更多的公钥参数以提高安全性。

Signal Protocol 采用棘轮算法来生成消息密钥，使用 1 个棘轮算法，能实现每条消息使用不同的密钥，即使一条消息的密钥被破解了，只能推算后面消息的密钥，而不能向前推算之前消息的密钥，我们称之为前向安全。

如果再加上一个棘轮算法，就可以再前向安全的基础上保障后向安全，即一条消息的密钥被破解，之前和之后的消息密钥都无法推算，这种算法被称为“双棘轮算法”

Signal Protocol 在双方通讯中采用的双棘轮算法是“KDF 链棘轮”+“DH 棘轮”，以保证消息的前向安全和后向安全。

2.6 基于加密货币的快捷支付

链上支付成本太高，基于链上链下结合的方式，可以支持支持小额交易，不仅带来支付成本的降低，而且吞吐量和快捷性得到提升。详细参考另一篇文章：**一种以太坊上的链上链下结合实现快捷支付和去中心化交易所的方案**。

2.7 国际化

社区贡献力量，把内容翻译成各国国家的本地语言。

2.8 大数据分析

虽然前期可以通过发展社区用户来帮助团队改善产品体验，但是还是需要大数据分析系统来分析用户行为，为产品的每一步变化提供理论支撑。

2.9 其他

养生等传统文化推广

电商 包括预测服务与风水物件。

广告市场

活动 线下预测交流活动、一些知名庙宇的头香拍卖活动、进香活动、还愿活动等等。

2.10 经济模型的思考

经济的核心是供需，我们需要提供更好的产品、更好的服务来吸引更多的人进来。

相对于传统企业花大力气招聘优秀员工和推广市场，我们考虑的是通过激励来发展社区，社区的每一个成员都是平台的股东，让社区来推动平台的发展。

计划发行 100 亿 Token，其分配比例如下。

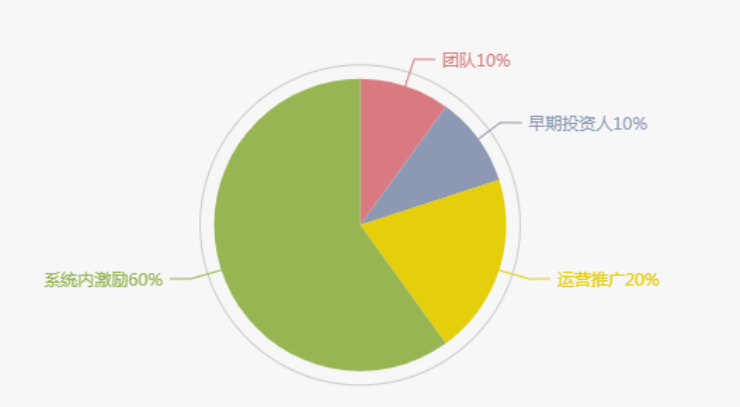

图 5: Token 发行

激励

- 通过空投和社区用户注册推广来吸引对产品或服务感兴趣的用户。
- 系统性激励入驻平台内的用户，培养或吸引更多的未来的超级预测师和超级命运师来。

经济发展周期一般 9 到 10 年左右，我们预计 10 年，每天释放一定额度的代币来激励平台入驻的用户。

释放模型为摆线模型，一共 3650 天，释放总额 60 亿。

$$\begin{cases} x = r(t - \sin(t)) \\ y = r(t - \cos(t)) \qquad (0 \le t \le 2\pi) \end{cases} \tag{1}$$

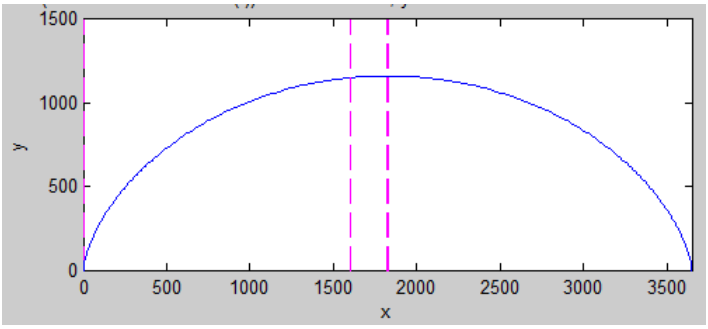

图 6: 系统性激励

天数	激励代币数量
第 1 天 (激励额度最小值)	15566.001225
第 30 天	242434.276443
第 180 天	762378.296154
第 360 天	1147325.994735
第 720 天	1650259.212511
第 1080 天	1957787.848414
第 1440 天	2130890.502326
第 1825 天（激励额度最大值）	2191780.686608
第 3650 天	15566.001225

市场 市场受众庞大，特别是在农村，几千年的传统文化影响，曾国藩通过看相识人用人，李嘉诚也有陈伯这样的风水师顾问。中国有 8 亿农村人口，假设互联网受众在 1/7 左右，那至少也有 1 亿人口，特别在广东、香港、台湾地区可能影响更大。中国内地也将近有 3000 万的公司，摆放风水物件已经习以为常了。

Token 价值

- 平台内置的价值尺度，实现产品与服务资产数字化，用户持有通证可以购买系统内数字化产品或服务。
- 持有 Token 通证可参与平台治理，引导平台走向大家认可度更高的更好的方向。
- Token 的估值

货币属性估值 M=PQ/V，这里的 M 是指货币总量，P 代表商品的平均价格，Q 指商品总量，V 指货币流通速度。如果平台能发展到 1 亿用户，平均每个用户在平台内的购买的产品或服务消费在 500 左右，则每个 Token 的价值应该为：500 亿/(100 亿 * V)，一般货币流通速度小于 10，取中间值为 5，则每个 Token 的货币属性估值为 1。

投资属性估值 如果平台 1 亿用户，每人每年消费 500 左右，平台每年的服务收费率为 5%，加上广告等其它收入，至少不低于 25 亿。这收益一部分返还给 Token 持有者，一部分进入 Token 风险基金，一旦平台发展后期没有市场认可，可以让 Token 投资人能挽回一部分损失。

3 系统技术方案

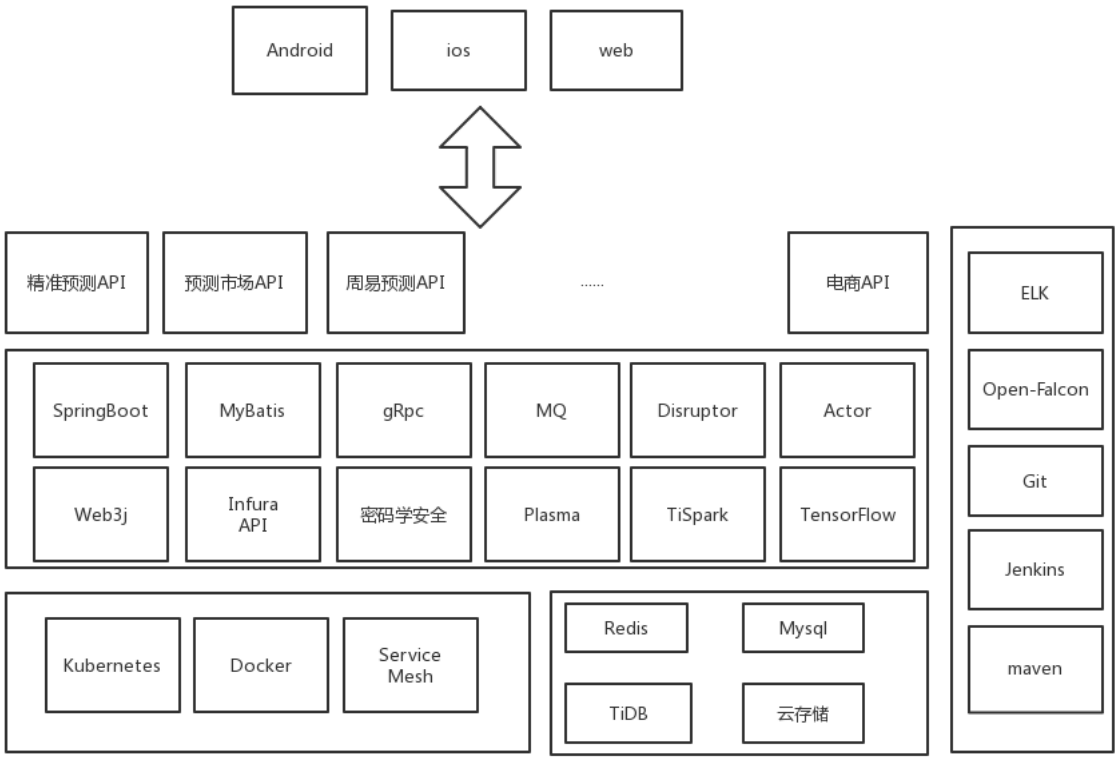

图 7: 系统架构方案

Token 基于以太坊主网发行，Token 快捷支付也是基于以太坊并采用链上链下结合的方案来实现。

参考文献