预言家 Prophet：基于公信链的预测平台

白皮书

版本：V1.0

范雅芸

目录

第一章：项目概要 4

第二章 项目背景 5

2.1 预测市场的发展历史和现状 5

2.2 预测市场的准确性 6

2.3 预测市场的运行机制 6

2.4 预测市场的关键算法 7

第三部分 传统预测市场痛点 10

3.1 To C 预测市场行业痛点 10

3.2 To B 预测市场的行业痛点 12

第四部分 解决方案和产品 12

4.1 Prophet 预测平台 12

4.2 用区块链解决传统预测市场痛点 15

4.3 Prophet 的技术架构 16

4.4 Prophet 核心架构组成 16

4.5 分布式预言机 Oracle 18

4.6 Prophet 的产品竞争优势 18

第五部分 主要应用场景 20

5.1 政治领域 20

5.2 金融市场 20

5.3 泛娱乐市场 21

5.4 体育预测 21

5.6 数字代币风险对冲 22

5.7 管理决策 22

第六部分 PPS 发行计划 23

6.1 Token 经济 23

6.2 TOKEN 发行方案： 24

第七部分 PROPHET 发展规划 25

第八章. 团队及顾问 26

8.1 核心团队 26

8.2 顾问团队 27

8.3 生态合作伙伴 27

第九章．法律事物和风险声明 28

9.1 PROPHET 平台的法律结构 28

9.2 免责声明 29

9.3 风险声明 30

参考文献 35

第一章：项目概要

预言家 prophet 是一个基于公信链的预测平台。平台充分利用分布式公开账本增加预测市场的透明度。同时平台通过数字代币经济激励开发者在平台发布预测项目，将自己的智慧进行社区共享，为用户提供不同类型的预测事件。预言家致力于“打造世界上最聪明的产品”，汇聚用户群体的智慧从而有效的预测未来。

预测市场是大众汇聚智慧的有效方式，更是未来智慧变现主要的方式之一，是一个万亿级的市场。预测市场作为计算机科学、管理科学和社会科学等交叉领域的新兴产物，依据事件合约的价格波动揭示合约事件的发展趋势，以合约价格的变化情况反映各因素对合约事件的影响程度以及交易群体对合约事件发展的共识。根据美国学者 Hahn（2006）的定义，预测市场是使用特定合约进行交易的市场，其中交易者的收益由未来事件发生结果决定。

这是一个信息爆炸的社会，处处都是利用信息赚取额外收益的机会。而一个人能掌握的信息是有限的，关键在于如何充分利用社会成员所掌握的数据、信息和知识。那么，想要利用社会成员信息的关键又于怎样有效地汇聚这些分散的、隐性的信息。预测市场便是最好的汇聚分散信息的方法。在预测市场的交易有效期内，合约的市场价格呈现一定幅度的波动现象，使得任意时刻的合约价格都能客观地反映当前市场汇聚而来的所有信息，从而为事件预测提供参考。

第二章 项目背景

预测市场以概念或判断等作为交易标的(又被称为概念期货)，从交易中产生的价格代表了市场作为整体对该概念/判断的认识和预测。时至今日，这种市场已经被广泛应用于政治及选举、娱乐、体育、经济及金融等各个领域。预测市场还可以帮助企业等各类 B 端组织进行有效决策、对冲风险和分配资源。

2.1 预测市场的发展历史和现状

2.1.1 预测市场古已有之

预测市场的构想和概念诞生较晚，而实际上预测市场古已有之：自 16 世纪起，人们就已经开始预测教皇的继任者。19 世纪末，美国华尔街开始对总统下注预测。

2.1.2 预测市场的构想诞生

预测市场思想提出的创始者之一 R. Hanso 研究指出，预测市场是一些早期的科学幻想小说的主题，例如 J. Brunner 1975 年的科学幻想小说 The Shockwave Rider 中就有关于预测市场的构想。他在 1990 年的文章中提出了以市场交易为基础来进行预测的构想：因为没有任何人能够掌握所有的信息，而市场可以将很多人的信息综合起来。

2.1.3 预测市场的建立

最早的预测市场是建立于 1988 年的 IEM(Iowa Electronic Markets)，该市场至今仍在运行，成为许多理论研究和后起市场模仿的对象。IEM 缘起于 IOWA 大学商学院希望创建一个方便学生实习的交易市场：参入者可以投入一定数量的金钱，交易标的是未来事件的结果，如谁将当选下一任美国总统等。由于 IEM 建立以来较为准确预测了每次美国总统选举的结果，其预测精确度高于政治评论专家以及民意测验的结果，20 世纪 90 年代中期后该市场引起了世人的广泛关注。

预测市场也逐渐开始应用在了企业应用。如加州理工大学和 HP 实验室合

作建立了 HP 公司内部预测市场，从 1996 年开始，于 2002 年发表研究报告，已经成为预测市场在企业应用的经典案例：HP 市场的参与者来自企业的不同部门，各部门均拥有关于预测事件的不同方面的信息。3 年里 HP 市场共发起 12 个预测，总体预测结果较 HP 官方预测更接近于实际。

2.2 预测市场的准确性

预测市场目前已被广泛应用，利用信息集聚机制，预测市场具有群体智慧的汇聚性和预测结果的高准确性。仅以政治、经济、娱乐三方面的应用为例：

1）政治上，Berg.J.E 等在 2008 年 Prediction Market Accuracy in the Long Run 中将 5 次美国总统选举的预测市场结果与 964 次民意调查结果作了对比，发现预测市场准确率达 74%，更接近选举结果。Rhode.P.W 等统计了 1884 年至 1940 年期间某预测市场对 15 次美国总统选举进行预测的情况，数据表明仅 1916 年大选的预测发生了失误。

2）经济层面，2002 年，Goldman Sachs 和 Deutsche Bank 设立了直接和宏观经济挂钩的预测市场,允许投资者购买多类合同，如非农数据、零售数据、制造业景气指数等。对大约 30 个预测合同分析的结果表明，预测市场的预测要比以调查为基础的预测更为准确。

3）娱乐票房方面，HSX 的电影股票是一种指数合同，该指数合同预测一部电影在首映后的 4 周时间内所获得的票房。A.Elberse 等人考察了 280 部电影的数据，发现在预测市场的预测和实际票房间存在的关联为 0.94，可见该预测市场的预测具有准确性较高。

2.3 预测市场的运行机制

2.3.1 预测市场的市场功能

预测市场的首要目标是揭示价格和促进信息的发现，不同于其他市场的募

集资本、对冲风险、 娱乐等主要功能。预测市场所形成的价格代表市场参与者对在市场中交易的命题所形成的准确、及时、高质量的答案和共识。由于市场机制对参与交易者所具有的激励作用，它会鼓励交易者利用正确的信息去形成判断，参与交易，同时也鼓励交易者去搜索和发现信息。

2.3.2 预测市场的交易标的

预测市场的交易标的是信息，即概念期货，例如“特朗普将取得连任”，“XXX 电影票房将超 20 亿人民币”等等。在这些命题的背后并不存在物质资产。预测市场是对某一个事件，或者某一个结果的出现与否进行交易。

2.3.3 预测市场的交易机制

交易机制中最重要的是合同设计和价格形成方式。在预测市场中交易者的输赢和未来事件的结果有关。这种关联以交易合同的方式固定下来。如何设计事件和输赢的关系反映的是市场的不同预期，可以将市场视为一个整体，代表一个有着确定的预期的个人。

通常有 3 种交易合同的类型，Prophet 平台也将采用这些类型：

1）赢家通吃（Winner Takes All）型合同：例如，定义事件 Y：特朗普将连任，描述为“合同价值为 P，若事件发生，则支付 1 元”，市场预期为“事件发生的概率 P(Y)”。

2）指数(Index)型合同：例如，为特朗普所赢得的每一个百分点的选票，合同支付 1 元市场预期为“结果 Y 的平均值 E(Y)”。

3）分布(Spread)型合同：例如，如果特朗普赢得超过 Y* %的选票比例，对所有合同支付相同 的数额，描述为“合同成本为 1 元， 如果 Y ＞ Y* ，支 付 2 元，否则支付 0 元”，市场预期为“Y 的中间值”。

2.4 预测市场的关键算法

预测市场的合约购买算法，主要用于购买事件合约，根据交易系统中已有的合约数和当前交易价格进行自动判断和计算，以确定购买所需的本金和暂时冻结

的保证金。其中保证金是按照最差的结算情况计算的结果，即如果事件最终走向与用户购买期望相反，则扣除保证金；否则，返还保证金。以赢者通吃型合约（0-100 型）为研究对象，即事件的清算价格是 100 或者 0，分别代表合约描述的命题成立或不成立。

令集合 FurEvent={f1，f2,f3,…,fn}为预测市场系统发布的 n 个事件合约。用户购买的 k 个事件合约描述为集合 UserEvent＝｛ue1, ue2, ue3, …,uek｝是 FurEvent 的一个子集。那么合约购买模型定义如下：

2.4.1 合约购买模型

用户购买事件合约定义为：

$$Pn（f, R, \delta）\rightarrow P$$

模型 Pn 表明在信息真实性 R 和事件合约走势 δ 的影响下，用户对未来事件合约 f 做出的理性的判断和评估过程，以价格 P 形式展示事件合约的发展趋势。在合约购买过程中，信息真实性和事件合约走势只起到了参考作用。根据概率和期望这两种市场预期将合约价格类型分为百分比型％和点数型＄。当合约交易类型为百分比型时，价格取值区间为(0,100)；而当合约交易类型为点数型时，价格取值区间为（0,∞）。从合约购买习惯和用户消费心理角度，购买事件合约必须满足如下条件：

1) 当真实信息的奖励 R 减少时，用户的合约交易积极性下降，市场价格更新缓慢，反之则上升。例如，设置用户预测准确率排名并按照名次提供奖品或奖金，可以显著提升交易活跃度和市场流动性。

2）当事件合约走势 δ 减少时，市场活跃度降低，合约价格波动幅度较低，反之则上升。例如，预测某次总统选举，候选人突然被爆出政治丑闻的影响系数较大，可能会引起合约走势 δ 迅速变化，使得合约的市场价格出现较大的波动情况。

2.4.2 购买方式设计

在购买方式设计方面，给出了两种特殊形式：

1) 看好方式购买(Upward Tendency Purchase, UTP)：参与者购买一定数量的事件

合约后自己持有全部数量，将合约价格描述为P↓。

2）不看好方式购买(Bearish Purchase, BP)：参与者购买一定数量的事件合约后马上将其全部发布到市场上期待与别人达成合约交易，将合约价格描述为P↑。

每个合约都设置价格波动区间。在合约购买时，校验出价是否超出限定范围以避免造成价格数值上的大幅度波动，成为干扰市场正常运作的噪音价格。

2.4.3 合约购买算法

输入：合约 f, 购买方式 w, 价格 p 以及数量 m

输出：提示用户交易是否成功

```
BEGIN
  If f∈UserEvent then
    If w is UTP way then
        Security Check whether p∈P price interval;
        Compute the cash t by the UTP way lok←pw(f,p,m);
        Hold the Amount to S model;
    Else if w is BP way then
        Check whether p∈P price interval;
        Compute the cash t by the BP way lok←sw(f,p,m);
        Put the Amount to sale market;
    EndIf
    If user account acc>=lok then
        Deduct t from account that acc←acc−lok;
    Else
        Output false as error purchase since lack of money;
    EndIf
    Add the User's Credits c←c+c';
  Update price P↓ or P↑ of UserEvent f;
    Output true as successful purchase;
  EndIf
END
```

算法输入参数包括期待购买的合约 f、购买方式 w、价格 p 以及数量 m；算法输出返回用户交易是否成功的提示。首先，根据用户选择的购买方式 w 确定 p 的取值区间，并分别调用函数 pw(f,p,m)和 sw(f,p,m)以确定购买资金。需要考虑本金和冻结资金，令购买价格为 p，购买数量为 m。

当以看好方式交易合约时，函数 pw(f,p,m)计算过程如下：本金需要扣除 p*m，

保证金需要冻结 p*m。当以不看好方式交易合约时，函数 sw(f,p,m)计算过程如下：本金需要扣除 p*m，保证金需要冻结(100-p)*m。

其次，算法判断用户总资金是否大于冻结资金，如果满足则扣除用户账户相应的冻结资金 acc←acc－lok；否则，返回失败提示信息表明合约购买不成功。最后，当冻结资金在用户总资金中扣除操作成功后，需更新个人积分数以及合约 f 的市场价格，同时返回成功提示信息。在算法执行过程中，需要查找事件合约 f 的信息，包括价格和数量。因此，对于预测市场上存在 n 个事件合约而言，该算法复杂度为 O(n)。

第三部分 传统预测市场痛点

3.1 To C 预测市场行业痛点

1）国界和货币通用性使得有效性和规模受限

参与人数越多、越大程度地汇集信息，则预测事件越有效；但是传统预测市场经常受国界和货币不通用的限制，无法解决参与国界以及国际结算问题，使得规模发展和预测有效性受限。如下图，SSD 值（Sum of Squared Deviations）在 0.1 以下有参考价值，而以下这些所谓的预测市场的 SSD 值普遍高于 0.9，有效性非常有限。

	Prediction Source	Prediction Quality	
		MAE	SSD
1.	SRG Prediction Market (Prediki)	0,97	1,39
2.	SRG „Wahlbarometer" gfs.bern (Survey)	1,10	3,24
3.	Sonntagsblick Prediction Market	1,19	3,64
4.	Isopublic Politbarometer (Survey)	1,53	6,57
5.	Demoscope (Survey)	1,53	5,39
6.	NZZ Prediction Market	1,57	11,85
7.	CBC Bern (Survey)	1,87	7,87

例如，同样是预测 07 年瑞士选举，很多预测市场因为参与人数不够，所以

准确率很低，无法超越传统的民意调查。

2）黑箱操作，操控空间大

传统的预测市场存在黑箱操作的问题，也因此催生了部分平台操控比赛的问题。黑箱操作的手段主要为操控获胜倍数，继而通过各类操控手段提前把控预测结果，庄家从资金池获得超额收益。黑箱操作的案例不胜枚举，例如 2013 年 2 月欧洲刑警组织公布数据指出，2008 年至 2011 年间，赌球集团操控了 300 多场顶级职业足球比赛，共有 425 名球员、裁判和足球官员牵涉操纵比赛的活动。而这些数据只是冰山一角，只包括欧洲冠军联赛、欧洲顶级联赛、世界杯以及世界杯预选赛。

而如果平台均采取市场化定价和确定获胜倍数，则操纵比赛将失去意义，因为不管比赛结果如何，预测各方的收益或损失情况实质上为零和游戏，平台收到的是固定手续费。

3）中心化决策和运营

目前的事件预测的选择一般由中心化平台自行决定，用户对于预测事件选择的个性化需求无法得到满足。例如，如果有用户想在一个做世界杯预测的平台发起电影票房的预测，目前的平台则无法支持。国际上较为知名的预测市场平台，如 Lumenogic、TradeSports 等都是只能对于平台自身发起的项目进行预测，无视用户兴趣和个性化需求。

4) 资产安全性低，维护成本高

传统的预测市场平台不会投入大量研发和维护成本来保障资产的安全，用户资金可能随时被盗。在有密码学和区块链技术等保障的情形下，用户资金的安全性将大幅提升，同时有效降低维护成本。

5）运作团队的专业度要求高

从事件的选择和设计到答案的校准再到社区建设，从运作机制到市场监督，全流程对专业度和管理精细度有很高的要求，一个成功的预测市场平台需要一个

专业度高的成熟团队来实际运作，很多团队都曾浅尝辄止。

3.2 To B 预测市场的行业痛点

1）公司重大决策权仅由管理层掌握，可能产生主观偏差

公司重大决策和事件一般由管理层决策，而个人或少数人的决策有时难免会有主观偏差。而广大员工在某种程度上具有一定的局内人的先瞻性，如果能使员工广泛参与，则可在一定程度上纠偏，对管理层的判断起到辅助作用。

2）内部调查的效果有限

内部调查的设计普遍较为固化和死板，如选项四选一或 Yes/No，只能做到最基本的意思表达呈现。而引入市场预测和投票机制，投入代币数量的多寡则能做到多维度的深层意思表达。

3）激励机制不足导致参与意愿不强烈

员工对于内部调查等的态度有时难免敷衍，且一般是匿名进行，和自身利益没有直接关联，缺乏激励机制，导致员工贡献的积极性不高，结果有效性受限。

4）保密性和信息安全

公司的市场预测结果属于敏感信息，事关公司重大决策和公司机密；而传统的互联网投票或调查存在网络安全问题，若数据造成泄露，则影响重大。

第四部分 解决方案和产品

4.1 Prophet 预测平台

预言家 Prophet 是一个基于公信链的预测平台。Prophet 产品分为 To B 和 To C 两个方向。To C，预言家致力于打造移动社交类预测平台； To B，预言家致力于打造企业内部决策支持预测系统。预言家的愿景是“成为世界上最聪明的产品”，

汇聚用户群体的智慧从而有效的预测未来。

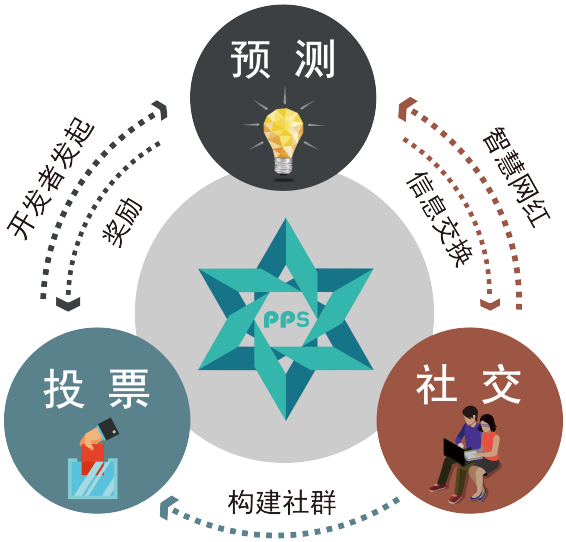
4.1.1 区块链移动社交类预测平台(Prophet Set)

Prophet 的移动端 Prophet Set 基于公信宝布洛克城开发，未来一年共享布洛克城的千万用户。Prophet Set 从布洛克城公民最感兴趣的数字代币话题切入，快速获得用户，通过多元社交增加用户粘性。Prophet Set 主张社区自治，鼓励开发者通过社区投票的途径自主发起项目，和投票用户一起分享手续费分成。Prophet Set 搭建的是一个自治、强社交的预测合约交易平台。

a) **预测：** 预言家基于市场买卖原则来收集整合交易各方对同一事件的信心和判断，从而产生对事件未来结果的预测。用户可以根据自己掌握的信息买入未来事件的结果，一旦买入的结果与未来事件结果一致，便可获得相应回报。

b) **投票：**通过投票，将对于事件的最终选择权交给社区用户。用户可以通过投票去表达自己对开发者和智慧网红的支持，参与到新的预测事件上线过程中去。参与投票的用户可以按照投票占比得到该预测事件的数字代币激励。

c) **社交：**Prophet 平台通过预测事件归类聚集共同事件爱好用户，相互交流，提升预测准确度。开发者可以通过在 Prophet 平台发起预测事件去表达意见，并通过不可篡改的下注表明对事件结果预测的信心。通过汇集用户的预测事件，从而实现全球新鲜资讯的汇聚，一键共享智慧。



4.1.2 区块链企业内部决策支持预测系统 (B-Prophet)

近年来国外许多企业纷纷开始构建内部预测市场平台，并且引起了学术界的广泛关注，但是国内还 没有学者对企业内部预测市场进行深入研究。预言家Prophet 会为每个企业搭建自己的内部预测市场，通过 token 的激励，让企业各个部门员工贡献出自己所掌握的信息。通过预测市场对信息进行汇总，从而得有效的预测结果去辅佐企业决策。

在面相企业的内部决策支持预测系统(B-Prophet)中，有五大主要部件：1.交易者 (Trader) ; 2. 事件合约 (Event); 3. 交易机制 (Trading Mechanism) ; 4合同定价 (Pricing) ;5激励机制(Incentive Mechanism)。

1) 交易者(Trader)：不同Prophet Set, B-Prophet中的交易者是被选择的，企业内部运行的预测市场中的交易者是挑选出来的一小部分人，这部分人通常都拥有关于未来事件的各方面信息。这些分散的信息正是预测市场所需要集聚和整合的信息，因而被选择作为交易者参与市场交易。

2) 事件合约(Event)：一是“是非型事件合约”，如果交易合同的标的是对某一未来事件是否会发生进行预测，则该合约为是非型事件合约。例如：6月，政府部门是否会出台相关政策，影响本企业的销售收入。二是”落点型事件合约，如果交易合同的标的是对某一未来事件发生时， 相关属性(如销量、销售额等)的实际值进行预测, 那么此类合约为落点型事件合约。例如：2018年7月，本公司手提电脑销量是否会超过100,000台？”。

3) 交易机制 (Trading Mechanism)：以PPS Token作为唯一的结算代币，产生双向拍卖合约市场。在每日规定开始交易前的一小段时间内为集合竞价阶段，对这段时间内所接受的买卖申报一次性集中撮合的竞价方式，最终产生开盘价; 紧接着进入连续竞价阶段。预测事件结束后，对于落点型事件合约和是非型事件合约，B-Prophet对于结算价格都将采用金融期货中阿罗一德布鲁证券市场的价格形成方式

4) 定价策略 (Pricing Mechanism): 在B-Prophet，合约的价格与事件发生的概率相关联，将概率作为合约价格的方法，即交易者订单中所填写的价格应该为用户自己估测某合约发生的概率数值。

5) 激励机制(Incentive Mechanism): B-Prophet从Token，荣誉，兴趣三个方面去刺激企业内部员工参与到预测事件中去。从而去鼓励交易者将自己所掌握的隐藏信息转换为买卖行为。

4. 2 用区块链解决传统预测市场痛点

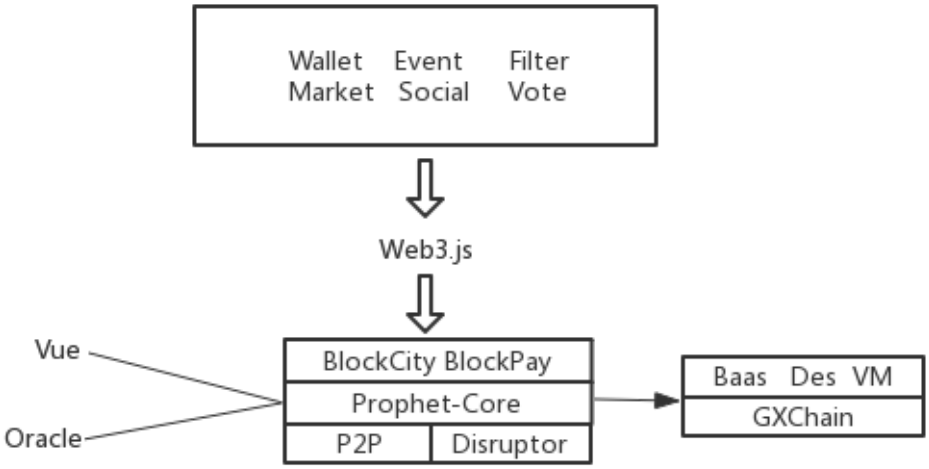
传统的预测市场有上述所陈列的非常多的痛点，而区块链技术正好能很好的解决这些痛点，预测市场是区块链天然的应用。

To C 预测市场痛点	区块链解决方案
国界和货币通用性限制	Token 可以解决国际结算问题，token 的无国界支付让世界各地的社区用户都可以参与到一个预测市场中去
黑箱操作	区块链的交易不可篡改和公开透明很好的解决了传统预测市场的黑箱操作问题，所有交易和结算都公开透明
中心化决策和运营	区块链可以实现去中心化的社区自治，平台用户可以自主地创建感兴趣的话题，通过社区投票的方式决定上线社区感兴趣的预测事件。
维护成本高	基于智能合约的参与方式，机器判断替代人工判断，让预测平台维护成本大大降低
资产安全性低	区块链数字资产的安全性是由密码学保证的，只要用户保管好自己的私钥，钱包里的数字资产就有绝对的安全。
运作团队的专业度要求高	区块链可以实现去中心化的社区自治
To B 预测市场痛点	**区块链解决方案**
管理层主观偏差	通过匿名的预测市场去汇集公司内部的声音，让员工敢于发声，汇聚员工声音，为管理层的判断

	起到辅助作用
内部调查的效果有限	引入市场预测和投票机制，投入 Token 数量的多寡则能做到多维度的深层意思表达。
激励机制不足	Token 激励机制，鼓励员工贡献自己掌握的信息
保密性和信息安全	基于区块链技术将信息和预测结果加密，通过密码学保障信息安全

4.3 Prophet 的技术架构

Prophet 是一个基于公信链的社交性的、分布式、社区自治全开源的全新预测世界。在这个预测世界中将现实世界的信息进行汇总，实现价格发现和信息揭示。



4.4 Prophet 核心架构组成

公信链 GX chain: GXChain（公信链）是国际领先的数据交换公有链，不仅支撑着高频的数据交易交换，还支持开发者开发应用。在公信链上开发应用，不仅可以利用区块链的技术特性实现去中心化运行，还可以获得多维度数据的支持，做

出非常落地于民生的有价值应用。公信宝 Baas 能支持大量数据存储和验证，为 Prophet 发起海量的预测市场项目提供了基础设施。公信链的 TPS 吞吐量非常高，可支持每秒十万笔交易，远超以太坊的性能。Prophet 的智能合约将运行在公信链的虚拟机上，并且公信链的智能合约还可支持跨链通信，为预言家的应用运行在其他公链上打下了坚实的基础。

智能合约： Prophet 的 token 是基于公信链的智能合约发行的。其次，Prophet 还将通过公信链上的智能合约实现 Event 的创建，分布式 Oracle 预言机，市场定价，合约交易，合约清算等等。

数据上链：Prophet 将实现全数据的上链，Prophet 将合约交易数据存在公信链的侧链，将事件结果，也就是分布式 oracle 预言机判定的结果存储在主链。这样不仅能完成全数据的上链，还不会导致主链堵塞。

BlockPay： 基于布洛克城的全币种支付服务，为布洛克城内流通的 Token 提供更高效的结算方式，方便第三方应用的接入。

DES (Data Exchange Service)：数据交换服务，是基于公信链上三方记账合约、以及自主搭建的高可用 IPFS 服务开发的点对点数据交换协议，提供可信、安全、高效的数据交换服务，并自动完成数据交换的记账过程，提供永久存证和数据版权登记

BaaS (Blockchain as a Service)： 区块链即服务，对单链或多链底层 api 进行高可用服务化封装，对外提供简单易用的服务

公信链 BaaS 存储服务： 基于公信链上三方记账合约、以及自主搭建的高可用 IPFS 服务开发的数据存储和存证服务，完美结合了 IPFS 的高效存取能力和公信链的高效记账能力，任何一次数据存储都能链上记账永久溯源，并能在 IPFS 上找到对应的数据。适用于版权登记、电子存证等应用场景。

GID(General Identity)：GID 是布洛克城生态的通用数字身份，GID 授权服务是一种在服务提供方为用户和应用方提供可信和高效授权的机制，这种机制允许用户授权第三方网站或应用访问他们存储在服务提供者方的信息，而不需要分享他们的访问许可或他们数据的所有内容。布洛克城的数据授权场景在 OAuth2.0 的基础上，对数据授权进行了分类和不同权限的划分，涉及个人隐私的数据，需要通过用户在本地用 DataKey 解密并授权，授权的数据通过第三方的 DataKey 公钥加密，整个过程安全、透明，保证传输过程不会造成数据泄露。

4.5 分布式预言机 Oracle

Prophet 中的预测事件（Event）在现实世界中的真实发生结果是通过 Oracle 进行信息发布的。Prophet 中预测事件的结果是由分布式预言机以投票的形式去决定的。分布式的 Oracle 通过 API 调用现实事件的结果数据，从而形成对于预测事件的判定。判定结果的投票决定了预测市场的结果并基于此完成事件相关清结算。

前期 Prophet 将采取中心化的 Oracle 来判定结果，以此来提升前期的运营效率。并且，前期 Prophet 发布的预测事件大多数只需要单点数据即可验证结果，所以中心化 Oracle 即可满足需求。当有争议时，可以通过仲裁委员会进行解决。后期 Prophet 会推出更多复杂与专业化的事件，与此同时，Prophet 便会推出分布式的预言机，去实现更有公信力和更准确的判断。

4.6 Prophet 的产品竞争优势

4.6.1 海量用户

预言家 Prophet 借助公信宝公链生态中的布洛克城，在项目初期即获得了海量用户。在用户数上远远领先了行业内竞争对手。随着布洛克城用户数的不断增长（预计 2018 年底到达 1000 万用户），预言家 Prophet 的用户数也会随之攀升。另一方面，预言家 Prophet 团队拥有卓越的海外推广能力，海外社区已在组件当

中。预言家的团队拥有丰富的海外工作经验和渠道资源，奠定了全球化布局的扎实基础。

4.6.2 用户标签，精准推送

通过公信宝（GXS）的 GID 授权，预言家 Prophet 可以获取用户的身份标签，标签覆盖用户消费能力，信用情况，理财能力，学历水平等等。预言家 Prophet 能根据这些数据标签向用户精准推送符合用户喜好的预测话题

4.6.3 移动社交

预言家 Prophet 从公信宝 Dapp 移动端切入，天生移动，内测期即支持了 IOS 和 Android 移动应用。同时 Prophet 在产品设计上掺入了丰富的社交元素，鼓励用户与共同兴趣社群进行互动与分享，由此增加用户的粘性和使用频率。未来，预言家 Prophet 还会基于好友体系推出匿名社交，即时通信、 OTC 场外交易以及移动支付功能。

4.6.4 关键词过滤器

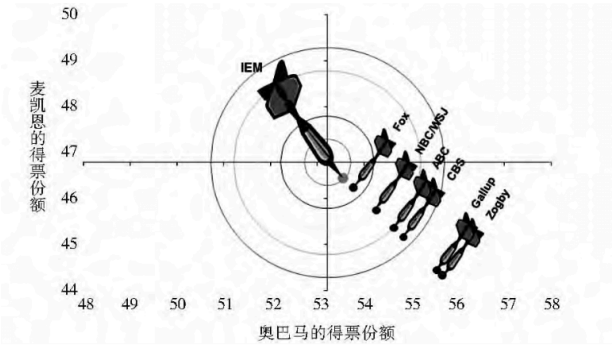
用户在创建完预测事件后需要首先通过“关键词过滤器“(WordFilter)的过滤，包含道德、政治和法律敏感词的预测事件将不会通过“关键词过滤器”。Prophet 将会根据各国的法律和道德氛围，创建不同的“关键词过滤器”，对不道德、不合法、侵犯政治权威的敏感事件进行过滤。

第五部分　主要应用场景

5.1 政治领域

在政治领域，预测市场有着非常广阔且成熟的应用。预测市场被应用于政治选举，公共政策制定以及政治决策。比如，许多国家都有选举的预测市场，比如美国、澳洲、奥地利、加拿大、德国以及荷兰等等。预测市场在政治领域有着非常精准的预测表现。图 1 是 IEM（美国知名的政治预测平台）份额预测市场和各种民意测验的准确度对比。图中显示，IEM 预测市场的预测最接近奥巴马的实际得票份额，比民意调查准确得多。

图 1. IEM 份额预测市场和各种民意测验的准确度对比



5.2 金融市场

预测市场在金融领域有着非常广阔的应用场景，比如股指预测、板块走势预测、个股走势预测，这不仅可以对这些标的实现价格发现和信息揭示，还可以实现风险对冲。预测市场能比现有的金融衍生品提供更大范围、更细化的价格发现和风险对冲功能。首先，目前金融衍生品只被应用于非常有限的金融品种当中，因为金融衍生品对于基础标的资产有着严格的筛选。而预测市场的基础标的资产可以有无限制的覆盖，用户可以根据自己的兴趣和利益相关点去选择预测话题的金融领域。比如，在中国的 A 股市场，金融衍生品只有针对非常小部分的股票品种，但是预测市场却可以覆盖所有的股票品种。其次，目前的金融衍生品主要覆盖为资产的经济价值表达。而预测市场可以给出更为细化和详尽的表达。比如，

预测事件可以表达为：任一使用欧元的国家在 2018 年 12 月 31 日前是否会宣布停止使用欧元。相比于传统衍生品市场中只能单纯围绕欧元价格做信息揭示，预测市场能有更细化的表达，在这里就是欧元的使用范围。

5.3 泛娱乐市场

文化产业的重要性已上升到国家战略层面，即将成为一个万亿级的市场。《十三五规划建议》指出，到 2020 年要让“文化产业成为国民经济支柱性产业”。报告显示，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。文化娱乐产业将在“十三五”期间迎来新的发展机遇。预测市场在泛娱乐领域有很多的应用场景，比如电影票房预测，电视剧收视率预测，综艺结果预测（如最强大脑的胜者），排行榜以及颁奖典礼获奖预测。 预测市场在娱乐方面有着惊人的准确性。对于预测奥斯卡奖的得主，D. M. Pennock 等比较了 Hollywood Stock Exchange (HSX) 的预测和 5 个电影专栏作家的专家预测。在专家开始预测的当天，有一位专家的预测好于预测市场的预测，而从此以后，预测市场战胜了所有的专家以及专家的平均估计。

5.4 体育预测

人们对于体育的预测有着几千年的热爱，预测市场在体育领域有着巨大的潜在市场，但是传统的预测市场却在体育领域发展缓慢。这主要是由于传统的预测市场由中心化操控，话题有限且有黑箱操作存在无法达到公平公正。而基于区块链的预测市场则能很好的解决这两大痛点，为预测市场在体育领域的快速发展扫清障碍。对体育活动作出正确预测是一项挑战，人们从参入这类活动中得到乐趣，一旦获得正确的结果不仅能有高额经济回报还能体会到成就感。 体育预测对于体育迷、运动队管理者、媒体和在联机平台上投注者都是非常重要的。体育博彩中的固定的赔率反 映的是庄家的预测，而预测市场反应的是所有市场参与者的预测。 M. Spann 和 B. Skiera 比较了不同的预测方法即预测市场、专家预测、赌注的预测准确 性。 通过分析德国足球联赛 3 个赛季、678 场比赛的数据，得

出的结论是预测市场和赌注的表现同样好，两者均超过专家预测。S. Schreiber 等比较了 NewsFutures 和 TradeSports 两个预测市场的预测和 1947 位个人预测者的预测 准确性。当赛季结束时，两个预测市场的预测结果超过了 99.74%的个人预测。

5.6 数字代币风险对冲

数字代币近两年在国际范围内发展迅猛，其波幅之大、收益之大都吸引着越来越多的投资者。但是在数字代币领域却没有有效的风险对冲工具。仅有的一些风险对冲工具都只能覆盖很小一部分的币种，比如 OKEX 推出的合约交易仅仅支持 8 种数字货币（2018 年 5 月 24 日数据）。预测市场却能覆盖所有的数字代币领域，为数字代币的投资者提供很好的风险对冲工具。例如，如果一个投资者在交易所买入了 1 个 BTC，他可以在预测市场中买入“BTC 会在未来一周内下挫”的合约去对冲其购买的 1 个 BTC 的市场风险。基于区块链的预测市场因为其社区自治，可以自由发起预测话题，市场流动性充足等特点可以很好的为数字代币投资者提供更大范围，期限灵活的风险对冲工具。

5.7 管理决策

预测市场在各类公司管理决策中运用的实例较多，也是目前预测市场应用探讨最多的领域。由于预测在企业管理中占据着极为重要的地位，所以预测市场在企业经营管理涉及的诸多方面都有应用，包括: 战略规划、项目管理、运营管理、产品开发、质量管理、知识管理、风险管理等。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。

对于企业(部门) 内部设立的预测市场，这种市场的交易参与者来自企业的不同部门。这些人拥有关于目标事件的各方面的信息。这些分散的信息需要以市场价格来进行整合和汇集。预测市场能够汇集企业内部所有相关利益方的信息、知识、智慧和经验，来提升企业管理决策的效率和效益。同时，也能让员工都参与到企业的决策相关过程中去，提升员工的参与度以及企业认同感。

在此以 IT 项目管理为例。有研究者设计和运行了关于 IT 项目管理的预测市场，结果显示: 市场的参与度很高(87%) ，在市场开放的 6 周中，每个交易者平均交易 23 次。在 26 个重要的指标中，预测市场正确地预测了 24 个(92%)，预测市场的引进使得在项目启动之前可以修订和澄清重要指标。预测运行结束后的调查表明预测市场可以促进组织内部的交流。

其实，在国外，很多大型企业都已经在企业内部部署了预测市场。比如惠普、雷诺、高通、通用电气、google、IBM 等等。

第六部分 PPS 发行计划

6.1 Token 经济

PPS 是预言家基金会发行在公信链上的 Token，是预言家 Prophet 生态内必备 Token，也是预言家经济体的载体。用户可以通过空投、活跃奖励等方式获得，同时它将在数字货币交易所交易流通，具有流通价值。它的应用价值主要表现在以下几个方面：

a) **开发**：在预言家 Prophet 上发起预测项目，开发者需要支付或燃烧一定 PPS；
b) **投票**：在预测项目上线投票时作为唯一选票使用；
c) **买入合约**：在预测项目中可用于购买预测合约；
d) **增值服务**：用户购买平台附加智能服务以及在生态中的其他服务使用费；

预言家会通过多重方式将 PPS 奖励给用户和开发者，从而去激励用户开发者共同做大 PPS 的经济体：

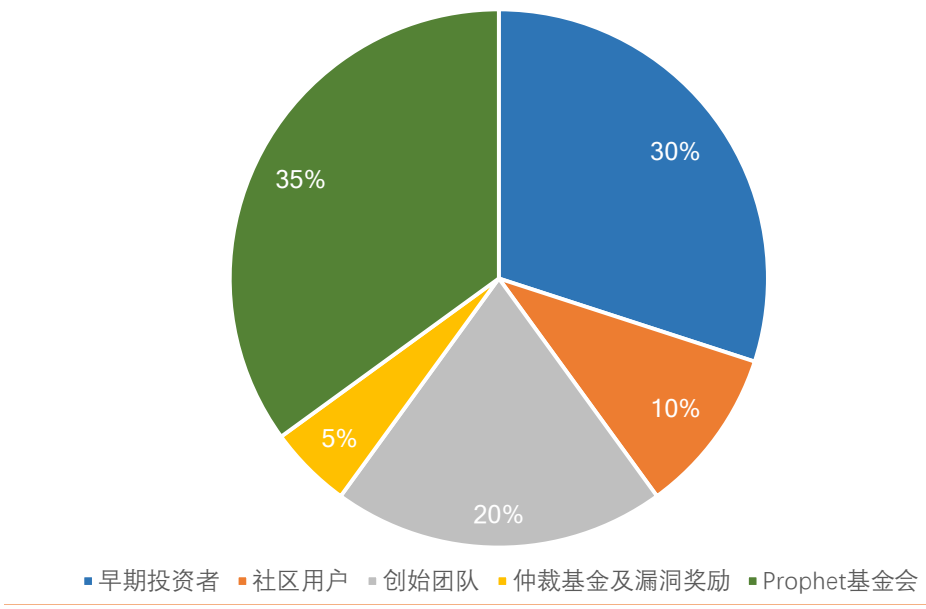
a) **活跃度奖励**：在预言家平台参与预测项目，可以获得活跃度奖励的 PPS，参与金额越高，将获得越多的活跃度奖励
b) **开发者奖励**：在预言家平台内发起预测事件的开发者，将获得部分手续费的奖励，从而激励开发者在平台发起更多样的预测事件

6.2 Token 发行方案：

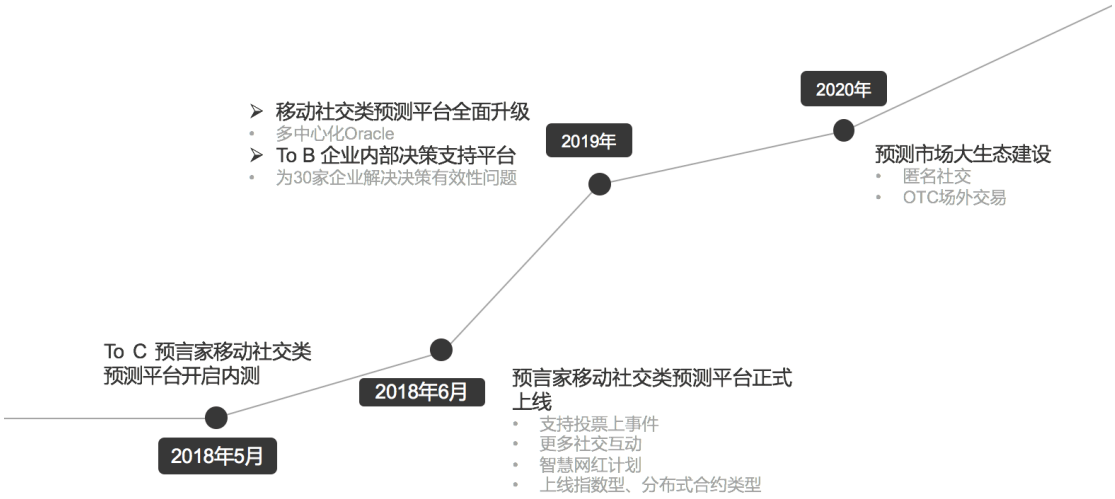
PPS 的总量为 10 亿个，用户可以通过空投、活跃奖励、交易所等方式获得 PPS。预言家基金会将对团队持有的代币实施四年逐步释放计划，以保障团队持久的开发运营以及长期的人员激励。具体分配如下：

- 早期投资者 30%，分发给预言家社区早期建设经费的支持者和投资者；
- 社区用户 10%：用于激励社区用户对于预言家项目的贡献；
- 创始团队 20%： 用于预言家创始团队的研发、运营、物力、资源等投入，PPS 发行后释放 5%，之后每年解锁 5%，三年解锁完毕；
- 仲裁基金及漏洞奖励 5%：用于解决用户发起的需仲裁事件，激励开发者反馈预言家产品内的漏洞奖励；
- 基金会 35%，用于预言家社区生态构建，商务合作，市场推广，海外拓展以及法律合规。

图 2. PPS token 分配比例



第七部分 Prophet 发展规划



2018 年 5 月，Prophet 将开启 to C 移动社交类预测平台的内测。6 月，Prophet 移动社交类预测平台正式上线，支持投票上事件，让开发者共享项目收益。 同时，Prophet 会在应用内加入更多的社交互动，并推出“智慧网红计划”。在产品方面，将推出更多的预测市场合约类型：包括指数型合约以及分布式合约。

2019 年，Prophet 将会把移动社交类预测平台进行全面的升级以及代码开源，推出多中心化 Oracle 预言机。同时，在 2019 年，预言家还会推出 To B 的企业内部决策支持平台，计划为 30 家企业解决决策有效性的问题。

在 2020 年，预言家将会开始构建预测市场的大生态建设，包括匿名社交以及 OTC 场外交易领域。

第八章. 团队及顾问

8.1 核心团队

Jessie Fan, CEO

浙江大学金融学本科，复旦大学金融学硕士，持有 CFA(国际金融分析师), FRM（金融风险管理师）等国际证书。连续创业者，中仓供应链联合创始人，数创科技&中仓物流总经理，公司获得知名 VC 和上市快递公司投资，估值数亿元人民币。曾工作于贝恩咨询，通用电气以及中信建投投行部。参与投资多个区块链项目。在区块链投资和研究，商业运营，供应链管理以及金融领域有丰富的经验。

Isabel Shi, CMO

毕业于浙江大学，拥有风险管理及创新与创业管理双学士学位。毕业后加入法国兴业银行中国总部，在银行多个部门任职。随后加入国内上市公司领益智造股份有限公司(SZ:002600)，主导全资金融类子公司：江粉金服股权投资基金管理有限公司的业务，担任总经理，负责上市公司的投融资、私募基金板块及其他对外业务推广，拥有丰富的金融及市场推广经验。

Erlich Liu，CTO

UIUC 计算机博士，上海交大学士，曾就职于 Google 和 VMware 等公司，负责全球级互联网和企业级分布式系统的设计和维护。博士期间主要研究计算机网络和区块链架构，并发表多篇相关学术论文。曾担任多个区块链项目的首席技术顾问。

Jin Poya, COO

毕业于浙江大学，曾任杭州数创电商副总裁，拥有多年产品以及社群运营经验，负责过 O2O、新零售、B2B、金融等项目。参与多个区块链的项目投资以及社群管理。

8.2 顾问团队

黄敏强，技术顾问

公信宝创始人、CEO，浙江省区块链技术应用协会副会长，前汉鼎宇佑 CTO。在数据交换、互联网金融行业和区块链领域有超过 10 年的从业和研究经验

David Chen，精算顾问

牛津大学工程系，英国精算师协会注册精算师，在年金计划和保险方案的精算测算工作以及模型评估工作有丰富经验。

Darry Gong，数学顾问

英国剑桥大学数字人类学硕士，擅长数学建模，风险控制，合约交易设计等。

8.3 投资机构

GXS　Bit-Z　了得资本 LD Capital

STARWIN CAPITAL 星合资本　GXChain CAPITAL　链电科技

第九章．法律事物和风险声明

9.1 Prophet 平台的法律结构

针对 Prophet 平台，将成立一个位于新加坡的非盈利性的基金会 Prophet Foundation Limited（“Prophet 基金会”）。Prophet 基金会将作为独立的法律主体，全权负责组织团队和培养活跃的开发者社区来开发这个分布式的风险交易市场平台和应用。但 Prophet 本身的运营和使用均完全取决并依赖于社区自治，Prophet 基金会只作为社区内一名普通成员，对 Prophet 的治理提出建议和方案，但不享有超然的或高出其他成员的权力或权威。

Prophet 基金会将会通过定向及公开的方式，出售旨在 Prophet 平台上运行和使用的 PPS，这些 PPS 是用户为了使用 Prophet 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 PPS 承诺回购或赎回。PPS 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。Prophet 基金会不保证 PPS 的内在价值或存在任何回报。PPS 不代表任何现实世界的资产或权利(例如 Prophet 基金会的股份、表决权等)。PPS 的典型受众是对加密货币和区块链系统非常熟悉的专家们。

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

Prophet 基金会在 PPS 销售中所获收入，将由 Prophet 基金会无条件地自由使用，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。Prophet 的预测市场是建立在 GXChain 或其他公链上的完全分布式的平台，全球任何人均能且只能通过消费 PPS 来使用其功能，不受地理位置所限。Prophet 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，Prophet 依然很有可能会在全世界不同国家受到监管机构的质询和监管。为了满足和遵守当地的法律法规，Prophet 平台可能会在有些区域无法提供正常的服务。Prophet 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。

9.2 免责声明

除本白皮书所明确载明的之外，Prophet 基金会不对 Prophet 或 PPS 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 PPS 的公开售卖计划及购买 PPS 的行为均基于其自己本身对 Prophet 和 PPS 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 Prophet 项目启动之后按现状接受 PPS，无论其技术规格、参数、性能或功能等。

Prophet 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 PPS 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 PPS 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 PPS;
3. 由于任何原因 PPS 的公开售卖计划被放弃;
4. Prophet 的开发失败或被放弃，以及因此导致的无法交付 PPS;
5. Prophet 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. Prophet 源代码的错误、瑕疵、缺陷或其他问题;
7. Prophet 平台或区块链的故障、崩溃、瘫痪、回滚或硬分叉;
8. Prophet 或 PPS 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 Prophet 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通证的钱包私钥(尤其是其使用的 PPS 钱包的私钥);
12. Prophet 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 PPS 的交易或投机行为;
15. PPS 在任何交易所的上市或退市;
16. PPS 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。

9.3 风险声明

Prophet 基金会相信，在 Prophet 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 Prophet 基金会的控制。除本白皮书所述的其他内容外，每个 PPS 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 PPS 的购买者应特别注意这一事实:尽管 Prophet 基金会是在新加坡设立的，但 Prophet 和 PPS 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 PPS 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. 不充分的信息披露。截止到本白皮书发布日，Prophet 仍在开发阶段，其设计理念、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 Prophet 最新的关键信息，其并不绝对完整，且仍会被 Prophet 基金会为了特定目的而不时进行调整和更新。Prophet 基金会无能力且无义务随时告知参与者 Prophet 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 Prophet 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情理的。
3. 监管措施。加密代币正在被或可能被各个不同国家的监管机构所监管。Prophet 基金会可能会不时收到来自于一个或多个监管机构的询问、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、Prophet 的开发或 PPS 的交易。Prophet 的开发、营销、宣传或其他方

面以及本次公开售卖计划均因此可能受到严重影响、阻碍或被终止。由于监管政策随时可能变化，任何国家之中现有的对于 Prophet 或本次公开售卖计划的监管许可或容忍均可能只是暂时的。在各个不同国家，PPS 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，PPS 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 Prophet)带来危险。这可能导致任何人持有的 PPS 被盗、失窃、消失、毁灭或贬值。在合理范围内，Prophet 基金会将自我准备采取预防或补救措施，升级 Prophet 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，Prophet 基金会将尽力适应密码学和安全领域的不断变化。
5. 开发失败或放弃。Prophet 仍在开发阶段，而非已准备就绪随时发布的成型产品。由于 Prophet 系统的技术复杂性，Prophet 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，Prophet 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 PPS 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 Prophet 基金会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 Prophet 基金会为 Prophet 开发提供资金的能力。尽管 Prophet 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 Prophet 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 Prophet 的可用性、稳定性和/或安全性，并因此对 PPS 的价值造成负面响。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。Prophet 基金会将与紧密 Prophet 社区紧密合作，今后持续改进、优化和完善 Prophet 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。Prophet 底层的分布式账本是允许存在无准入许可的公有账本，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 Prophet 初始时是由 Prophet 基金会所开发，但它并非由 Prophet 基金会所有拥有、运营或控制。自发形成的 Prophet 社区是完全开放、去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、PPS 持有人和其他参与者组成，这些人大都与 Prophet 基金会无任何关系。就 Prophet 的维护、治理以及甚至是进化而言，该社区将是无中心化且高度自治的。而 Prophet 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 Prophet 的诞生做出过努力和贡献。因此，Prophet 在发布之后，其如何治理乃至进化将并不受到 Prophet 基金会的支配。

9. 源代码升级。Prophet 的源代码是开源的且可能被 Prophet 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的结果，从而对 Prophet 的运行或 PPS 的价值造成重大不利影响。
10. 安全弱点。Prophet 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 Prophet 基金会努力维护 Prophet 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 Prophet 的核心基础设施要素之中，对这些弱点或缺陷 Prophet 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 PPS 或其他数字代币丢失。
11. “分布式拒绝服务”攻击。GXChain 或其他公链设计为公开且无准入许可的账本。因此，GXChain 或其他公链可能会不时遭受“分布式拒绝服务”的网络攻击。这种攻击将使 Prophet 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GXChain或其他公链的区块之中，或甚至暂时无法执行。
12. 区块处理能力不足。Prophet 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区块链网络内届时节点所能提供的负载，则 Prophet 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PPS可能会丢失，Prophet

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 Prophet 的可使用性、稳定性和安全性以及 PPS 的价值。

13. 未经授权认领待售 PPS。任何通过解密或破解 PPS 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 PPS 购买者所购买的待售 PPS。据此，购买者所购买的待售 PPS 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 PPS 的任何人士，而这种发送是不可撤销、不可逆转的。每位 PPS 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. PPS 钱包私钥。获取 PPS 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 PPS 钱包拥有唯一的公钥和私钥才可以操控 PPS。每一购买者应当妥善保管其 PPS 钱包私钥。若 PPS 购买者的该等私钥丢失、遗失、泄露、毁损或被盗，Prophet 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 PPS。
15. 普及度。PPS 的价值很大程度上取决于 Prophet 平台的普及度。Prophet 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，Prophet 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 PPS 需求可能具有投机性质。缺乏用户可能导致 PPS 市场价格波动增大从而影响 Prophet 的长期发展。出现这种价格波动时，Prophet 基金会不会(也没有责任)稳定或影响 PPS 的市场价格。
16. 流动性。PPS 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。PPS 在市场上的流通和交易并不是 Prophet 基金会的职责或追求。PPS 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 PPS 持有者处兑换或购买任何 PPS，也没有任何人士能够在任何程度上保证任何时刻 PPS 的流通性或市场价格。PPS 持有者若要转让 PPS，该 PPS 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 PPS 供公开交易。
17. 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 PPS 交易的二级市场，Prophet 基金会对任何二级市场的 PPS 交易不承担责任。因此，Prophet 基金会没有义务稳定 PPS 的价格波动，且对此也并不关心。PPS 交易价格所涉风险需由 PPS 交易者自行承担。

18. 竞争。Prophet 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 Prophet 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 Prophet 竞争，或甚至赶超或取代 Prophet。Prophet 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 Prophet 产生竞争关系。Prophet 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 Prophet 竞争或取代 Prophet 的竞争性努力。

参考文献

[1] 贺德方, & 潘云涛. (2014). 基于准金融期货交易规则的预测市场机制研究--以基金申请量预测为例. *情报学报*(9), 900-909.

[2] 李国秋, & 吕斌. (2014). 预测市场:理论基础、运行机制及其应用. *图书情报工作, 58*(1), 54-71.

[3] 李国秋, & 吕斌. (2014). 预测市场——一种情报分析研究的新方法. *情报杂志*(1), 11-15.

[4] 李国秋, & 龙怡. (2014). 预测市场应用于技术预见的优势分析——对 13 种常用技术预见方法的 20 个维度的实证研究. *图书馆杂志, 33*(8), 11-28.

[5] 李晶, 孙火军, & 张耀辉. (2012). 预测市场方法以及应用的研究综述——一个基于实验经济学的视角. *产业经济评论(山东大学)*(2).

[6] 李建标, & 赵玉亮. (2012). 预测市场机制的研究进展与展望. *科学学与科学技术管理, 33*(8), 106-111.

[7] 杨晓贤，吕斌（2016），基于群体智慧的预测市场合约交易算法的设计研究，《计算机科学》：235

[8] 张津豪, & 杨颖. (2016). 预测市场在企业群体决策中的应用研究. *情报探索*(12), 126-129.

[9] 张宁, & 李国秋. (2016). 企业内部运行的预测市场研究*--以西门子和惠普内部预测市场为例. *竞争情报, 12*(4), 52-58.

[10] Berg J E，Forsythe R，Rietz T A, The Iowa electronic market, Paxson D, Wood D. Blackwell Encyclopedic Dictionary of Finance, Oxford: Blackwell, 1997.

[11] Chen Kay-Yet，Plott C R. Information aggregation mechanisms: Concept, design and implementation for a sales forecasting problem, Social Science Working Paper, 2002, number 1131

[12] Elberse A，Anand B． The effectiveness of pre-release advertising for motion pictures: An empirical investigation using a simulated market, Information Economics and Policy，2007，19: 3-4．

[13] Giles J． Wanna bet, Nature, 2002, 354-355．

[14] Gurkaynak R，Wolfers J． Macroeconomic derivatives: An initial analysis of market-based macro forecasts，uncertainty，and risk / /Frankel J A，Pissarides

C A. NBER International Seminar on Macroeconomics 2005, Cambridge: MIT Press, 2005: 11-50.

[15] Ho Teck-Hua, Chen Kay-Yut. New product blockbusters: The magic and science of prediction markets, California Management Review, 2007, 50 (1): 144-158.

[16] Hanson R, Market-based foresight: A proposal.

[17] Lightfoot G, Lilley S. The glass beads of global war: Dealing, death and the policy analysis market, Critical Perspectives on International Business, 2007, 3(1) : 83-100.

[18] Pennock D M, Giles C L, Nielsen F A. The real power of artificial markets, Science, 2001, 291: 987-988.

[19] Ray R. Prediction markets and the financial wisdom of crowds, The Journal of Behavioral Finance, 2006, 7(1) : 2-4.

[20] Surowiecki J., The wisdom of crowds: Why the many are smarter than the few and how collective wisdom shapes business, New York Random House, 2004.