SEER

SEER 白皮书

基于区块链的下一代去中心化现实预测市场

SEER

目 录

摘　要

SEER 是基于区块链的下一代去中心现实预测市场平台。SEER 利用市场机制让用户表达对未来事件的判断并集众人的智慧与看法对未来事件进行有效的预测。SEER 通过引入多宿主去中心化预言机（Oracle）功能，为用户提供中立且可信的去中心化现实预测市场服务。同时 SEER 集成理事会以及仲裁机制，使得 SEER 兼具高效，中立，可信，自治等特点。SEER 项目在初期阶段将完成搭建区块链底层以及相关基础现实预测市场的智能合约的编写。SEER 上还会在数据提供方，数据合作方上重点布局，打通区块链与现实世界的入口，拉近产业上游和用户之间的距离。在项目发展的中期阶段以及发展路线图中，SEER 还会专门针对如体育竞猜，金融市场预测，资产价格预测和事件预测等不同行业的需求进行定制开发。

第一章　设计理念

1.1 项目背景

SEER 将在上线初期提供基础现实预测市场功能。现实预测市场将会以小额高频的方式让全球对现实预测有需求的用户参与到预测中来，增强 SEER 代币的流动性，同时对现实预测这个社会学命题提供学术支持。在完成基础区块链的搭建以后，SEER 还会根据其他不同行业的需求，提供不同的操作流程以及界面的应用程序用于构建诸如金融，保险，社会政治，体育竞猜等各行各业的现实预测市场应用。

1.2 发展方向

SEER 上线初期提供现实预测市场等基础应用并且将提供开发接口以及数据集成接口，邀请开发者、数据服务商以及产业上下游的实体，参与开发基于 SEER 的行业应用中去，完善整个 SEER 平台的生态搭建，SEER 将成为连接产业中下游的应用生态平台。

1.3 创新之处

通过基于 Graphene 框架这一强大的区块链平台，在 SEER 中将可提供高速运转的底层区块链系统，可信赖且中立的去中心化预言机框架用于现实预测市场功能。

协议神经中枢(Protocol nerve center)

虽然图灵完备的虚拟机让区块链有了一定的扩展性，但在 The DAO 事件发生之后，以太坊还是需要通过硬分叉来解决 The DAO 事件产生的问题，让以太坊分叉成为 ETH 和 ETC 两条公链。我们认为频繁的硬分叉对于区块链项目本身来说并不理想，为了解决这个问题，SEER 引入了协议神经中枢。

神经中枢是由开发者，理事会，见证人，所有代币持有人和逻辑状态构成去中心化逻辑神经网络。所有的应用逻辑和区块链协议本身都是在协议中枢的控制下运行的。应用和协议的升级都不需要硬分叉，而是由协议神经中枢自适应来完成。

第二章　技术概览

2.1 平台模型

<table>
<tr><td colspan="2">Industry-specific Decentralized Applications And SDKs</td></tr>
<tr><td>Service APIs and Data APIs</td><td>Predictive Markets</td></tr>
<tr><td colspan="2">SEER Core</td></tr>
<tr><td colspan="2">Protocol Nerve Center & Graphene Toolkits</td></tr>
</table>

SEER 主要由 3 个层次组成：

最底层为协议神经中枢和 Graphene 框架用于提供底层区块链服务，协议神经中枢包含区块链完成去中心化的升级，使用 Graphene 框架框架可提供平均 1.5 秒的交易确认速度以及最多每秒 3300 笔交易处理能力，提供高性能并且低延迟的区块链底层平台。

第二层是 SEER Core - 即核心层，在核心层中主要实现与 Graphene 框架的通讯，实现基础的业务逻辑。

第三层为服务层，服务层封装了第三方开发者接口和数据集成接口以及基础预测市场接口。

第四层为行业专属应用以及开发者二次开发套件。根据不同行业的需求，提供不同的操作流程以及界面的应用程序。将会提供基于网页，PC，iOS 和安卓手机的示例去中心化应用程序。同时，第三方开发者可以使用二次开发套件以及示例应用程序，快速开发出自定义界面的环境独立的专属应用程序。

2.2 代币 - SEER Token(SEER)

SEER Token 作为系统的基础代币，主要有以下几个作用：

1. 用于进行交易以及调用智能合约所需要消耗的燃料

2. 用于申请成为预言机的保证金

3. 作为预测市场的流通代币

2.3 现实预测市场功能

现实预测市场的运作机制是集众人的智慧对未来发生的事件进行预测，在准确率方面已经超越了民意调查等常规统计方法。除了通过集群智慧预测出未来事件的发生概率，经济学家也认为边际交易者假说这一市场机制也在预测市场中发生作用 - 即总有人会发现集体可能出现的错误观点，然后买进被低估的资产，卖出被高估的资产，从而使价格回归合理水平，在预测市场中表现为市场将会不断自我修正错误的观点从而不断自我提升准确率。 目前，预测市场已经被应用在多个方面，如选举结果预测，经济指标预测，股票的走势的预测，政策走向预测等。

其中一个著名的例子是自 1988 年就开始运作的 IEM - Iowa Electronic Markets, IEM 是由美国爱荷华大学设立的选举预测市场，主要用于美国总统选举以及美国国会选举预测，该预测市场的最终预测结果与现实结果高度一致，准确率被证明优于民调以及其他取样调查方式。

另外一个例子是台湾的未来事件交易所，未来事件交易所是由台湾国立政治大学创立，曾于 2008 年成功预测了台湾领导人的选举结果而一时声名大噪，目前未来事件交易所提供财经，政治，体育等各种类型的预测市场。

SEER 主将会参考以往的预测市场的成功案例并将完全构建在区块链技术之上，同样的是利用预测市场理论对未来的事件进行预测，得出的结果供社会研究和参考。由于借助区块链技术，系统的运作都将会是去中心化的，是一个自治的现实预测市场。在 SEER 的预测市场应用中，预测正确的一方将可获得全部代币奖励。

例子：如运动员 A 和运动员 B 之间进行比赛，假设有 30 个参与者他们都想对比赛的结果进行预测，其中有一个预测市场设立者在 SEER 的预测市场支付了一定的代币开设了一个预测市场。为了进行预测，参与者需要支付代币参与预测。假设预测的主题设定为：运动员 A 是否能打败运动员 B。其中，有 20 个参与者预测运动员 A 会获胜，而有 10 个参与者预测运动员 B 会获胜。在比赛开始前，预测市场将会被自动锁定并输出一个概率-即预测结果。如上面的例子，现实预测市场给出的结果概率是有 66%的几率运动员 A 是能够打败运动员 B，得出的预测结果可以给予社会大众和统计学家进行统计分析之用。当比赛结束后，预测市场随即关闭，由预言机输入正确的比赛结果数据后，SEER 平台将会自动对奖励进行分配。

2.4 预言机框架（Oracle）

预言机是现实世界与 SEER 区块链平台之间的数据流通桥梁，可靠的预言机机制是确保区块链平台能获得正确的来自现实世界的数据以用来作为判断与执行智能合约的依据。如上面的现实预测市场的例子中，预言机能否提供正确的比赛结果数据对往后的奖励分配会有很大的影响。因此，提供一个可靠，可信赖且中立的预言机是本系统的核心功能之一。

2.4.1 申请成为预言机

成为预言机并为预测市场输入正确的结果可以获得社区奖励，这提供了经济诱因，但为了确保提供的数据真实可靠，若要成为预言机，申请者必须支付一定数量的代币作为注册费以便成为预言机，并且预言机需要在系统中锁定一定数量的代币作为保证金，且锁定的保证金代币价值必须超过特定预测市场场次中参与者支付代币的总和。若预言机多次恶意输入虚假结果，并被理事会裁定为恶意用户，该预言机锁定的定金将会被系统没收，且账号可能被冻结并失去未来的可能的收入，这使得预言机尽可能提供真实可靠的来自现实世界的数据。

2.4.2 去中心化智能预言机

为了进一步确保输入的数据真实可靠，SEER 引入了基于多重宿主（Multiple Hosts）模型的去中心化预言机功能，使用该功能时，预测市场设立者可以指定一个阈值，如该预测市场场次中要有 10 个预言机报名参与输出结果，并要求必须要超过 7 个预言机达成一致才会采纳这个结果。同时，预测市场设立者也可以单独对某个预言机设定权重，比如信誉度较高的预言机的权重可以提高一点。通过多重宿主模型，可以更大程度确保结果可信性并且可以提高整体系统的鲁棒性，避免因系统故障等问题导致的因单点服务不可用时无法提供结果的问题。而对于参与人数不多或者时效性要求更高的预测市场，为求更快得出结果，预测市场设立者也可以采用普通的单宿主模型。

2.4.3 挑战预言机结果的途径

虽然可能性不大，但依然有一种可能就是预言机操控结果，为了避免这种可能，应该允许参与者挑战预言机输出的结果来监督预言机的运行。若参与者有较大把握认为提供结果的一个或多个预言机恶意提供虚假的输出结果时，在特定时限内（7 天），可以向理事会申请挑战预言机的输出结果，参与者在提出申请时应提供/锁定特定预测市场中参与者支付代币的总和的十分之一作为挑战保证金，并提供相应的证据以及证明，当理事会在审查期内（14 天）查阅和验证双方的理由和证据后，在理事会中将会进行投票，若大比数通过认定这些预言机存在恶意提供虚假结果时，如涉事预言机的行为足以影响了该场次的正确的结果时候，那么将会判定该场次的结果无效，并将参与者们支付的代币原路返还，而无论是否影响了结果，被判定提供恶意结果的预言机在该场次锁定的保证金的应该奖励予挑战者。如多次恶意重犯者应冻结账号并没收全部保证金。而若理事会裁定挑战者存在恶意挑战预言机的行为，那么挑战者锁定的保证金将会被没收，挑战者的保证金应给予被挑战的预言机。

2.4.4 预言机声望与信誉系统

预言机的用户资料定义中将会包含信誉值，声望值以及所有历史数据以及违规数据。信誉值是根据理事会的违规处理记录的数量和违规事件的严重程度与预言机参与输出结果的数量计算出来的。声望值是用户根据持币权重对该语言机器投票得出来的，在预测市场设立者一方在设立预测时可以将信誉值或者信用值低于某一个数值的预言机排除在外，不允许其申请成为该场次预测市场的预言机。

2.5 现实预测市场内的锚定代币

我们理解到对于现实预测市场参与者，他们可能需要一种较为稳定的代币参与预测。基于 GRAPHENE 框架上可以轻易实现类似 BITCNY 或者 BITBTC 等系统级锚定货币，但考虑到这种系统级的锚定货币需要足够的需求，流通渠道，流动性以及承兑商（套利者）来维持这种机制，而作为一个单纯的现实预测市场，交易量并无法跟比特股这种去中心化的交易所比较，缺乏交易量，流通渠道，流动性和套利者可能无法实现稳定的系统级锚定，这种情况在同样是基于 GRAPHENE 框架开发的 Steemit 中的 Steem Backed Dollars（SBD）得以验证。虽然 SBD 的目标是利用 Steem 代币的价值为 SBD 提供价值担保，但因上述因素的影响以及发行机制的缺陷使其无法长期锚定预设的目标 - 即 1 SBD 锚定在 1 美元的水平。

为了避免系统级风险以及提供一个相对恒定的锚定代币，SEER 将不会采用系统级锚定代币的方案，而是引入特定预测市场场次范围内的锚定代币可选项给予预测市场的设立者，由预测市场设立者决定是否开启这个选项。做法如下：

1.预测市场设立者启用该选项，并按照见证人和理事会共同制定的强制止损比率，支付锚定保证金

2.预测市场开启时，SEER 通过见证人提供的喂价服务，获取外部的锚定代币价格信息并以此作为基准（基准价）。

3.预测市场关闭时，同样的，SEER 通过见证人提供的喂价服务获取锚定代币的当前价格（当前价）。使用当前价-基准价计算出两者的价差，如当前价少于基准价并且在强制止损比率之内，损失的价差由预测市场设立者承担，而如果基准价高于当前价，那么获得的价差收益则有预测市场设立者获得。通过这套机制，无论目标锚定货币的价格在预测市场进行时是如何变化，只要在止损比率范围之内，预测市场参与者所支付的代币与目标锚定货币之间的汇率就被锚定在开始前的那一刻。

例子：假设预测市场设立者使用 SEER BTC 进行该场场次预测，即产生与锚定比特币的代币进行预测。

假设在预测市场开始时候，SEER BTC 与 SEER 代币的比例是 1：1000.而当预测市场关闭时，比例变成 1：1050.也就是说每个比特币能兑换更多的 SEER 代币，而预测市场结算时依然会按照 1：1000 来结算，多出来的 50 SEER/比特币的收益将会给予预测市场设立者，而相反的，如果产生了亏损，也一样由预测市场设立者来承担。

2.6 学术研究与数据集成接口

为了促进对现实预测市场的学术研究，SEER 除了一般的应用程序开发接口，同时也会提供方便使用的历史数据检索，搜寻以及数据统计接口用于学术研究。全节点调用数据集成接口将会是完全免费的。同时考虑到并不是所有科研人员都希望运行全节点，SEER 将会提供按量计费的远程轻节点数据集成调用接口 - 将数据调用请求打包成交易并由见证人的全节点运行后返回数据，科研人员只需要支付极低的成本即可调用相关的数据接口作科研之用。

2.7 环境隔离的去中心化应用程序

为了满足不同现实预测市场设立者的需求，SEER 将提供一系列的开发套件以及示例去中心化应用程序，设立者可以使用这些工具开发出属于他们自己的去中心化应用程序。在 SEER 链上，设立者可以

对其所建立的现实预测市场设定特定标记，然后在他们开发的去中心应用程序上对在区块链上的现实预测市场进行过滤，如只在程序上只显示由特定设立者建立的现实预测市场。

2.8 加密的私有现实预测市场

我们理解到市场对于私有的现实预测市场有着极大的需求。然而如果采用一般链外实现的方案，现实预测市场的设立者有可能需要与参与者建立直接的链接，这有可能暴露了参与者以及构建者双方的物理位置。而在本系统中我们提出一种构建在区块链上的高效的以及经加密的私有现实预测市场，使预测市场内的所有信息只能被指定的参与者以及设立者获知，也只有指定的参与者能参与其中，区块链上的相关信息也被完全加密。本功能将会联合使用迪菲-赫尔曼密钥交换算法(DIFFIE–HELLMAN KEY EXCHANGE)以及 RIJNDAEL 加密算法进行开发使得本系统不但在拥有高效的处理速度，高等级的安全性，同时拥有一定的"叛徒跟踪"（ TRAITOR TRACING ）能力，具体做法如下：

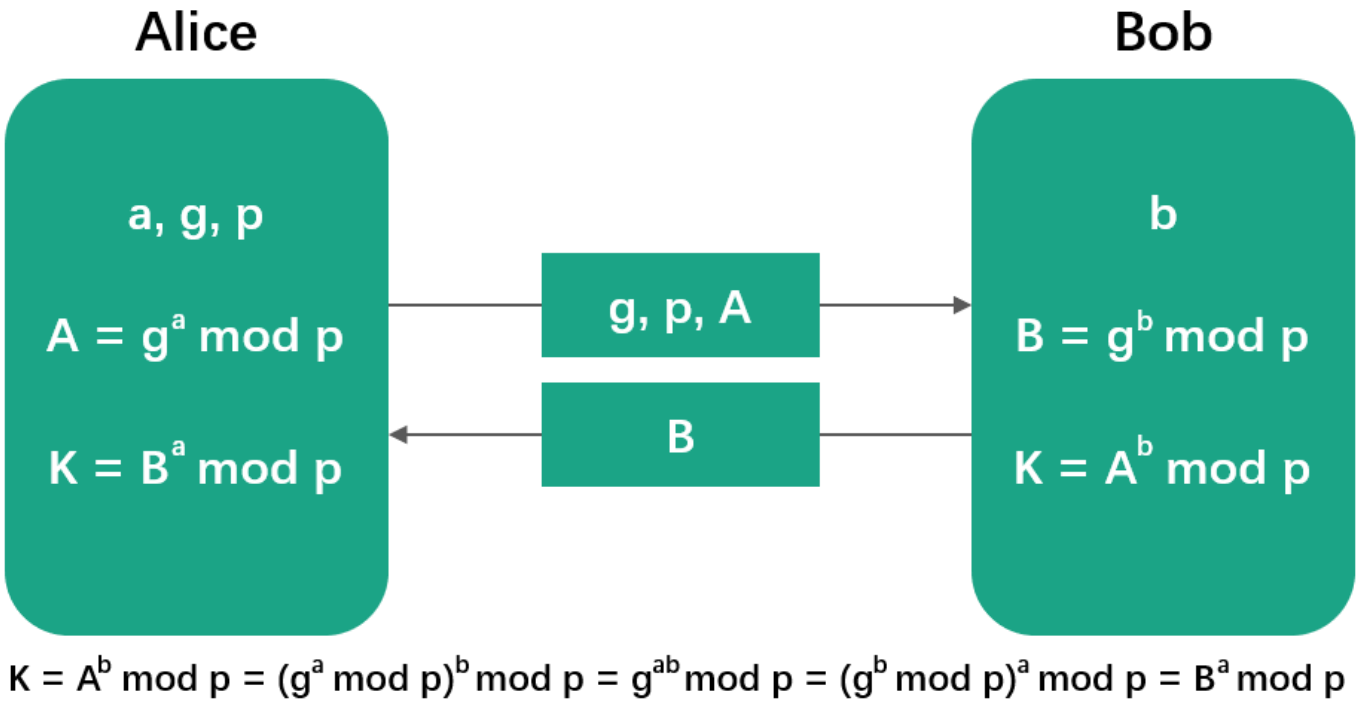
首先在区块链上使用 DIFFIE–HELLMAN 算法通过带有特殊标记的交易，建立初始的安全加密通信信道，让设立者与参与者进行安全的密钥交换操作，该信道直接建立在 SEER 主链上，参与者与设立者各方无法获知对方的物理位置。利用 SEER 的 3300 TPS 的处理速度以及平均 1.5 秒出块时间，我们预计该加密通信信道可在 5-10 秒内完成建立并完成密钥分发。

（ DIFFIE–HELLMAN 算法建立密钥交换的过程 ）

然后利用 RIJNDAEL 对称加密算法对所有传输内容进行一对一加密。现实预测市场设立者利用密钥对该场次现实预测市场的内容进行加密，并通过加密信道将不同的密钥分发给不同的参与者，参与者今后对该已加密的预测市场进行操作的时候便可利用该密钥对区块链上的加密内容进行解密与加密以及进行相关的操作，不必再建立通信信道进行密钥交换操作。由于参与者之间获得的密钥均不相同，

若发现参与者密钥被泄漏，设立者可以根据密钥定位到参与者身份并对子密钥进行撤销处理（“叛徒跟踪”能力），并将其加入到黑名单中。

没有获得密钥的非特定用户，均无法查看区块链上的经过加密的现实预测市场的所有的内容。



第三章　治　理

3.1 理事会

理事会是 SEER 治理架构的核心，理事会的理事由 SEER 的持币用户通投票选出。每位投票者的选票权重通过其持币数量与系统总量的百分比计算得出

在 SEER 中一共有 11 位理事会理事，理事的权限和职责有以下几个方面：

1.调整转账手续费

2.指定区块链的各项参数设定

3.处理预测市场与众筹市场的纠纷

4.处理挑战预言机的请求

5.处理提案，如处理开发人员工资，市场推广项目等提案。

由此可见，理事会将是 SEER 的重要组成部分，除了需要管理区块链的各项参数，还需要处理预测市场以及众筹市场可能出现的问题和纠纷，更为重要的是要为去中心化预言机的结果的正确性做最后的把关者，守门员。

当然由于其特殊的地位，为了保证每个决定都能反映大部分权益相关者的意愿。理事会每做出的每一个决定都需要大部分理事赞成才可以通过，而每一个理事都是由持币用户投票选出，这使得 SEER 的运作能够在运行效率，民主性以及公平性上能够达到一个最优的平衡点。

3.2 见证人

见证人与理事会理事一样需要由的持币用户通过投票选出，投票权重的计算方法与选举理事会理事一致。见证人的产生不受理事会影响。申请成为见证人也需要抵押一定数量的代币。

见证人的主要作用是处理交易，对交易进行签名，然后打包成区块并传送给其他见证人予以确认以及提供喂价(price feed)服务。见证人每月可以获得代币奖励作为处理交易的报酬，而分布在全球各地的见证人正是区块链系统的去中心化特性的关键因素，每一个见证人都需要对投票者负责并正确地处理交易，同样的每个由见证人产出的区块要被大部分见证人确认才可以被全网承认。每个见证人都会有代币奖励用于支付运行服务器费用，维护等用于日常开支以及作为见证人奖励。

3.3 预测市场设立者，预言机以及众筹参与者

SEER 认为预测市场的设立者，预言机以及众筹参与者都是对系统有贡献的个体，预言机提供中立公正的来自现实世界的数据，预测市场设立者和众筹参与者为系统带来更多的人气和更多的赛事。 所以应该与见证人一样能获得来自系统的处理交易的代币奖励。而计算代币奖励的公式应该包含预测市场参与者对特定预测市场的支持度。

3.4 账户恢复

SEER 将会引入密钥恢复功能，通过为账户指定一个密钥恢复伙伴账户，用户可以在密钥恢复伙伴的帮助下使用原密钥来重置账户。

3.5 账户冻结

考虑到预测市场中有可能出现多次恶意提交虚假结果的预言机以及其他可能出现的恶意用户，SEER 将会引入一个完善账户冻结，公告以及上诉机制，经过理事会的审议后并经大多数理事同意可以对恶意用户进行冻结操作。

3.6 微信/微博/支付宝等社交客户端的第三方跨平台用户登录

SEER 将会支持基于 OAuth 网页授权认证协议用于跨平台登陆以及用户绑定功能，目前在开发路线图已经加入微信/微博/支付宝等客户端的跨平台登陆验证功能并有望于在第一个最小可用版本中提供该功能，开发团队已经成功测试 OAuth 协议与 Graphene 框架之间的互通性。

第四章　应用场景

4.1 体育竞猜

体育竞猜是一个庞大的市场，而 SEER 提供一个去中心化并且可信赖的体育竞猜解决方案，除了一般的单宿主预言机功能，用户也可选择使用更为高级的基于多宿主模型设计的去中心化预言机功能，多宿主模型预言机可以避免传统中心化服务可能出现的造假，单点服务故障而无法及时提供结果数据，并且设立了一个理事会为数据正确性做最后的把关者。

4.2 资产价格预测

资产价格如房地产价格，大宗商品价格与人们生活息息相关，通过在 SEER 设立预测市场并让全网参与预测，使得普通用户可以获取对某一类别的资产最直观的价格预期信息，如可以开设一个预测市场预测"2018 年深圳平均房价是多少？"，通过这样的预测市场得出的结果可以让有意购买深圳房产的用户合理安排自己的购房计划。

4.3 金融市场预测

目前，服务于金融市场的预测工具存在着多种不足，如准确率不高，效率低下以及成本高昂。SEER 提供了一个更为简便，可靠，高效的预测市场工具。不需要繁琐的设定，用户可以通过在 SEER 建立相应的现实预测市场，让全网参与预测，如可开设"2018 年美国 GDP 增长率是多高？"等各种类别的预测市场。SEER 可以让基金管理者，专业投资者等人群通过低廉的成本获得人们对未来发生事件的预期，所获得的结果准确率更高。

4.4 事件预测

除了上述类别的预测外，SEER 还可以建立各种不同类别的预测，如政治事件类的预测，如："特朗普在 2020 年美国大选中能否成功连任？"，娱乐产业预测，如："某电影的总票房能否超过 10 亿人民币"，社会话题类预测，如："下一代苹果手机的发行时间会在哪一天？"

第五章　发展路线

5.1 发展路线图

SEER 于 2016 年 10 月启动项目，测试链已经在运行，并且有望于 2018 年年初发布第一个最小可用版本，最小可用版本将包含预测市场等基础功能，第三方开发者接口有望于 2018 年第二季度上线，更多丰富的应用以及面向其他行业的现实预测市场应用接口也随后会陆续上线。

5.2 第三方开发者支持

我们知道 SEER 的不断发展需要不断接入更多应用以及更多的玩法。因此在上线之后，SEER 将会提供一系列的开发接口，示例程序，开发套件以及数据集成接口供第三方的开发者，平台运营商以及数据提供商进行二次开发。SEER 将会预留社区推广基金，社区推广基金将用于推广以及开发者支持，如定期举办开发者会议，活动以及开发竞赛，以便培育更多的开发者为 SEER 编写应用，提供更多玩法，不断完善 SEER 生态圈。