# 竞猜链

## FAIR GUESSING CHAIN

基于区块链的社交型
泛娱乐化竞猜平台

V2.0

# 目录

# 目录

# 第一章 项目背景

## 1.1 历史背景

“区块链”已成为时下最火的概念。传统互联网解决了信息的传递，但无法低成本解决“信任传递”问题。而通过区块链的应用以及传统行业的区块链化再塑，将形成一个多中心的、去中介的、自组织的、共享数据的可信任网络。区块链技术将驱动世界由信息互联网向价值互联网迁移，通过挖掘实体经济的价值，将资产数字化，打通行业壁垒、释放实体经济的流动性、促进经济的飞速发展。

竞猜是人类日常的一种娱乐消遣活动，起初是为了用于公平抽奖，最后逐步演变成集游戏竞猜、双人博弈、福利彩票、娱乐筹资等于一体的行业。竞猜链是一个服务于竞猜场景公平竞猜服务平台（Fair guessing service platform，FGSP ），以现代社会中涉及到竞猜的场景为切入点，包括体育竞猜、游戏竞猜、彩票等等，利用区块链技术服务于公平竞猜、公开竞猜，旨在解决传统竞猜场景中过程不透明、信息易篡改、中间渠道不可信的争议问题，增加流通效率，降低交易成本，保障客户利益。

## 1.2 产业背景

竞猜行业涉及的领域非常广泛，包括传统彩票、体育竞猜、游戏竞猜，部分国家还包括合法博彩娱乐市场。据统计，全球竞猜行业市场规模达到了5360亿美元（部分国家包含博彩娱乐市场）。东南亚国家作为全球人口规模第三的区域，博彩业的发展一直是这个地区的重要产业。其中菲律宾是东南亚国家博彩业规模最大的地区，2018年菲律宾市场的博彩总收入预计增长9.4%，其中包括在线博彩、网络彩票等新兴互联网博彩细分领域在该国的博彩行业发展中扮演重要角色。博彩将是竞猜链主打是的一个应用场景，竞猜链将与菲律宾、柬埔寨等东南亚国家的博彩娱乐公司构建全方位的深度合作关系，为之提供新型竞猜服务。

## 1.3 区块链背景

区块链本质上是一个去中心化的分布式账本数据库，其价值在于通过构建自组织网络，使用密码学相关联算法产生一串数据块，每一个数据块中包含了多次交易有效确认的信息，且时间有序不可篡改。由此建立分布式共识机制，从而实现去中心化信任体系。比如比特币，其底层

架构技术就是区块链技术，利用去中心化、不可伪造、公开透明、分布式记账、不可篡改、智能合约等特点， 实现不需要中介就能够向世人进行价值传递。

同时，区块链作为一种数据库，具备几大特征。首先，只能在此数据库添加记录，不能移除或更改记录。其二，区块链数据库分布在多个计算机中，这些计算机存有这个数据库部分或完整的副本。例如比特币区块链就储存在数百万台机器上。此外，还有一个重要特征，我们能够将计算机代码部署到区块链中永久性地存储并等待被执行。所以，区块链具备不可变性，再加上其分布在多个计算机上，意味着黑客极难篡改。

## 1.4 代币背景

代币又称数字货币、虚拟货币，是非央行、信用机构、电子货币机构发行的一种加密货币。加密货币首先是一种货币体系，所以它的价值并不体现为制作材料和物理用途上，而是大众对其认可程度上。这种认可无论是主动的广泛使用，还是被强制要求作为法定货币，都是一种规模上的认可，可作为一种基于虚拟或特定环境流通的支付手段。世界最早的数字货币是比特币。如今，比特币是包含一系列概念的生态系统，该系列包括支付系统、加密货币、数字资产和底层区块链技术。除了所有这些概念之外，还是一种信任机制，它能够跨越整个网络的节点建立对等或分布式的信任。

首次代币发行也就是所谓的ICO是一种为项目募集资金的形式，但对于投资人来说是一种权益证明，同时也是平台上购买服务的一种支付手段。发行加密货币，可以让资产在区块链中运行从而具有区块链保护财产安全，降低流通成本等优势，能够让每个人通过保存该数据库实现对自己私有财产的绝对控制权，省去了中介机构从而降低流通成本提高效率。发行代币必须遵循以下的市场经济基本规律：代币的价值应该来源于产品或服务的市场价格，合理定价；加密货币的发行总量应受到严格控制。

# 第二章 竞猜链平台介绍

## 2.1 产品介绍

### 2.1.1竞猜链平台简述

竞猜链利用区块链技术的去中心化、分布式账本、不可篡改的特性，以及一套基于参与式决策（Participatory Decision Making）的随机数生成器，打造了一个公平竞猜服务平台（Fair guessing service platform，FGSP ）。平台集传统彩票、互联网彩票、体育竞猜、个性化竞猜任务发布、线上社交平台于一体，旨在为参与竞猜的客户提供一个安全、规范、公正、极具娱乐多样性的渠道进行娱乐竞猜活动。

竞猜链依托区块链底层技术构建应用生态系统，基于区块链的底层智能合约，利用区块链代码开源、规则透明、去中心化的分权特征，建立了该平台（FGSP）公有链的底层系统和自治社区的治理构架，能够在区块链底层系统上实现智能合约。其定义了一个代币实现的规则，通过双TOKEN经济模型发行FGE、FGC两种TOKEN，前者用于ICO发行作为权益代币，可用来持有竞猜链平台的权益，享有收益分红和事务投票权等；后者与法币锚定保证价格稳定，减少市场波动损失，并作为平台上主要娱乐代币。基于成熟的竞猜链底层协议和基础架构，可以很快实现竞猜产品的发行和清算。用户一方面可以随时随地参与竞猜，另一方面也可以利用 API（应用程序编程结构）&SDK（软件开发工具包）实现各种定制，开设各个垂直领域的竞猜市场。

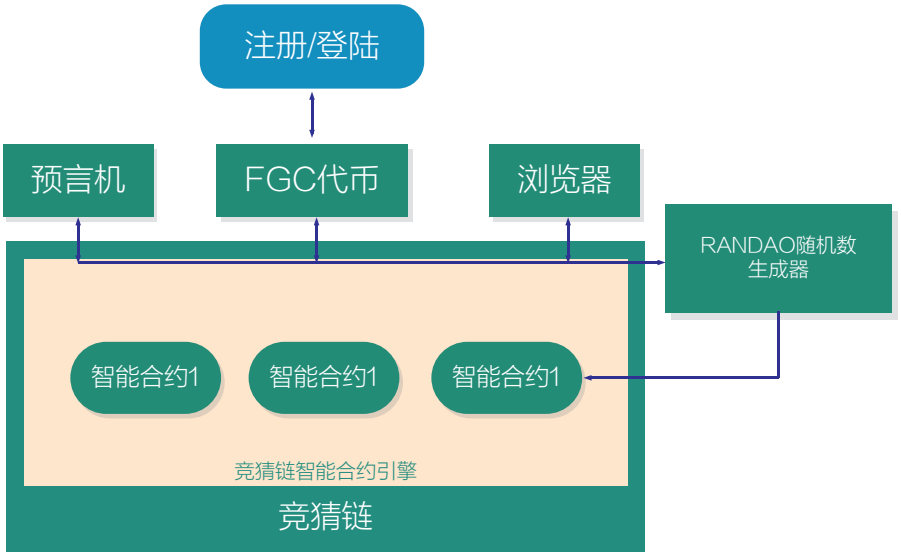



图1 竞猜链—公平竞猜服务平台（FGSP）

### 2.1.2 竞猜链理念

竞猜链旨在打造公平、安全又极具娱乐多样性的竞猜服务平台，一直秉持全流程公开透明（Transparent），操作简洁流畅（Concise），代码开源（Open），社区自治（Community）的TCOC运营理念。

Transparent：关注产品的全流程运营，确保过程公开透明，公平公正无黑箱操作可能，不同于现有的最长链投票机制，竞猜采用的是最先进的基于公开数据产生随机数的参与式决策（Participatory Decision Making）算法，能够确保公开公正公平透明。

Concise：竞猜链整个平台能工具化的模块都工具化，并且集成了很多的开源模块，使所有顾客无论是本身参与竞猜项目，还是自己定制和发布竞猜项目，整个过程简洁流畅，不浪费时间和精力。

Open: 竞猜链平台将上层应用所需要的功能组件进行封装,开发者要实现对应的功能，只需注册成为开发者即可获得接口使用权限（提供RESTFUL，Websocket的RPC访问接口、数据分析、部署智能合约等）。平台提供开发者运维所需要的可视化管理工具。开发者能够通过API&SDK进行个性化竞猜任务定制和发布，开设各个垂直领域的竞猜市场。

Community：竞猜链旨在为喜欢竞猜的客户打造一个公平竞猜服务平台，并能成为区块链技术爱好者、传统彩票、体彩、福彩、博彩等竞猜任务发布公司及爱好者的交流平台。打造有去中心化的IM工具，客户借此建立自己的社区，也可通过社区形成自己的竞猜朋友圈，发布个性化竞猜任务，集竞猜任务发布、竞猜项目参与、线上交流、线上投票于一体的社区平台。

### 2.1.3 竞猜链双链体系

双链体系是很好地一种兼顾区块链去中心化特性和最优效率实现快速交易的方法。竞猜链计划打造双链机制（公有链+专有链），其中公有链作为记账人选举机制的依托，利用公有链的开放特性，让更多的人参与到私有链的登记节点和记账，并给予一定的回报。专有链基于以太坊的开源技术、在对接公有链的基础上也营造相对独立的区块链环境。在此环境中客户可以自行部署专有智能合约，打造专属自治社区。相对独立的环境可以帮助客户进行业务上相对封闭的竞猜任务发布，同时也可以申请公有链的登记节点获得分布式记账权益。双链体系帮助公平竞猜服务平台（FGSP）实现权益、记账和交易的去中心化，同时又支持瞬时、低手续费的链上资产流转，提高交易效率。

竞猜链选择了以太坊（Ethereum）作为公平竞猜服务平台的底层技术。原因如下：

1.以太坊提供了完备编程语言和编程接口；

2.以太坊的ERC20\ ERC721代币。以太坊可以很容易地发行代币，从而很容易地建立基于代币的经济学模型。现在几乎所有的钱包都支持ERC20代币。而以太猫，莱茨狗等的风行，都是使用不可分代币ERC721代币代替所表征的实物。

3.代码开源。所有智能合约代码均位于以太坊的公链上，任何人可以随意查看，理解并验证。

4.以太坊的工具完备。以太坊目前具备了公链圈里最完备的工具集。用户稍加训练，即可掌握。


图2 双链技术构架

## 2.2 竞猜链平台的意义

### 2.2.1 竞猜链的社会意义

多数的竞猜平台对于游戏规则及数据来源都语焉不详。竞猜的中奖算法和竞猜流程不透明既很难获取竞猜的数据也又很难保证获取的数据的真实性，所以很难保证竞猜平台的公平公正。另外，传统的竞猜平台

参与流程需要用户首先充值到渠道中或根据用户的信用开启一定的信用额度，然后渠道在自己账户系统中为用户进行记账。渠道替用户保管资产的能力及是否面临运营监管的风险都决定了用户资产的安全，对用户来说具有一定风险。

竞猜链可以有效保护参与者的竞猜信息，整个竞猜流程公开透明，防篡改防黑幕。竞猜链可以重塑竞猜产业的信托制度，提高参与者的契约精神并提供一个良好的娱乐环境。通过在区块链上部署智能合约可以实现交易的原子性，成交前抵押代币和成交后支付代币均存放在用户本人区块链地址中。整个交易过程用户无需向渠道转账，渠道不托管用户下单资金，资产丢失或者渠道跑路风险为零，哪怕渠道倒闭，也不会对用户产生任何影响 。数字化筹码和其他数据块加密功能，可以有效地保护所有的竞猜娱乐用户的信息安全，尤其是满足高端VIP客户的隐私要求。此外，默认的智能合约还允许长期下注，长期下注一旦触发条件达到，智能合约将直接执行或提供证据。

### 2.2.2 区块链竞猜的经济效益

使用基于区块链的数字货币可以逾越传统彩票等竞猜游戏受地域限制的弊端，可以从任何地方任何地点任何时间完成彩票等竞猜产品的购买和兑付，甚至在没有银行基础设施的地区，只要有网络都能进行。这将极大程度地延伸传统竞猜的覆盖范围，提高竞猜市场的潜在存量。

每一份竞猜都是基于竞猜链平台的一份智能合约，通过基于以太坊的平台，竞猜链技术将使竞猜更为高效、便捷，在根本上完成竞猜行业的更新换代。基于区块链技术的全球竞猜娱乐平台不仅是创新的区块链娱乐平台，还接受数字货币如BTC、ETH等的支付，并将带来超过2000万的全世界的数字货币玩家进入竞猜市场。

### 2.2.3 AI、大数据等新技术的应用

竞猜链将引入大数据技术提高竞猜娱乐产业的服务质量和效率。大数据可以提供全面准确的概率分析。竞猜链的客户可以随时根据竞猜链提供的大数据服务，动态调整赔率和投注金额，并确保自己利益的最大化。另一方面，竞猜链还会对接入平台用户数据的分析，如基于用户、习惯和偏好，个性化的推荐产品等等，可以帮助优化用户服务策略；在此基础上，竞猜链可以提供小额贷款，信用卡，保险等其他数字金融服务，从而更好地为用户提供服务。

竞猜链还将利用人工智能技术改善竞猜娱乐的服务质量水平，结合大数据和机器学习的平台，提高竞猜娱乐的效率与高质量发展。人工智能应用在客户服务中可以深入分析用户的习惯和揣摩用户的意图来进行更个性化的客户服务，节省平台的人力成本。

# 第三章 功能模块介绍

## 3.1 竞猜链基础技术框架

竞猜链基于区块链底层智能合约机制建立基础技术框架，总共包含四层：公有链底层TOKEN、大数据及AI层、Smart Contract层和服务扩展层。第一层是公有链底层TOKEN，其用来发行通兑的加密货币FGE，作为权益证明和平台认可的交易方式；第二层是大数据及AI层，大数据底层为上层的娱乐竞猜活动的应用提供各种数据支撑，其中AI层的人工智能技术还能提供一系列的辅助功能，包括智能投注，智能识别等。第三层是智能合约层（Smart Contract），其基于竞猜公有链的智能合约层，可以定制多种娱乐竞猜场景的智能合约模板，此外还提供封装智能合约的API，将其作为工具包提供给客户，方便自定义开发竞猜项目，开设各垂直领域竞猜市场；第四层是服务拓展层，竞猜链平台（FGSP）会协助客户嫁接自己的分布式应用，客户可在公有链基础上自行搭设专属私有链，打造封闭的及特定规模的专属娱乐竞猜社群，利用平台提供的去中心化IM工具集竞猜娱乐、私密社交于一体。竞猜链平台会提供基于多语言的一系列底层数据访问和交互接口，提供包括登记存证、交易记录、所有权存证、数据查询引擎等一系列服务。

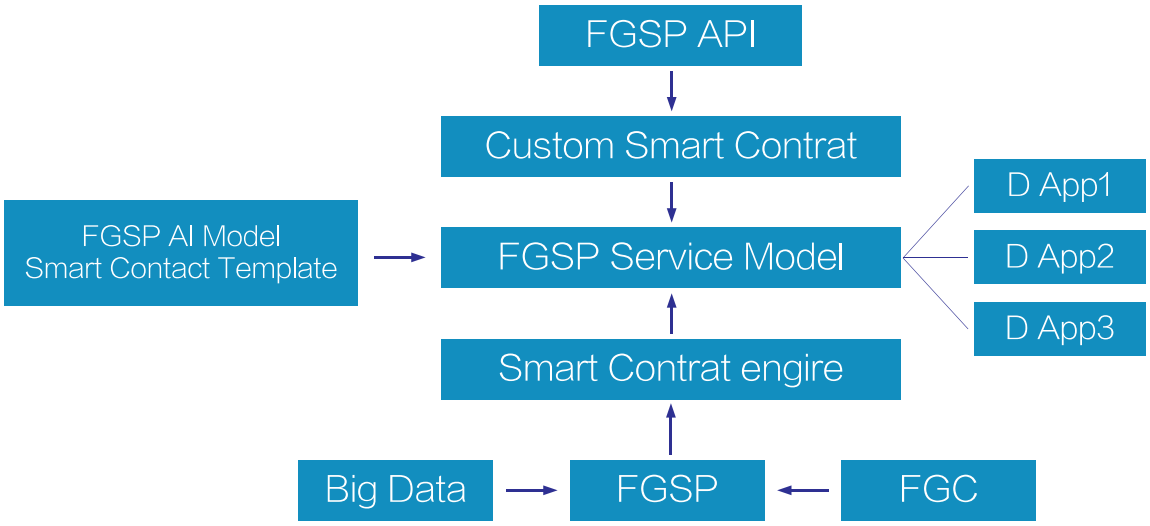



图3 竞猜链基础技术框架

## 3.2 竞猜链关键技术简述

竞猜链允许开发者创建任何可扩展的、标准化的、易开发性的协同应用。竞猜链将是一个全球通用的区块链。基于公有链的底端，形成一个新的软件应用的类型，是一个真正的分散投注应用嵌入在程序运行的信任逻辑链。在最底层，竞猜链是一个多层次的、基于开源技术协议的各功能模块完全集成的封装包，作为一个整体，它是用于创建和部署分散的竞猜娱乐应用的综合平台，实现了公有链与P2P网络的对接。同时，竞猜链也有一个完整的智能合约引擎，用户可以通过图形化界面的方式自动生成模板并部署，大大减轻用户的学习曲线和开发智能合约方面的负担，从而大大降低使用竞猜链的使用门槛，并拥有一套完整的工具，可以扩展智能合约的应用场景。

竞猜链拟发行一种基于以太坊智能合约，符合ERC20令牌（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）标准的双token代币FGE，以开发智能合约引擎，属于权益类凭证，将上线大型主流交易所交易流通。此外，还会发行一种基于以太坊智能合约的、符合ERC20标准的代币FGC（Fair Guessing Coin）。FGC是竞猜链在正式上线运行时由智能合约生成的。竞猜链用户对发布在竞猜链上任何一个项目作出预测时，只能而且必须使用FGC去操作：发起项目，竞猜项目以及验证项目。

竞猜链的随机数生成算法是基于RANDAO思想的以参与者为随机源的参与式决策算法。这种方式基于区块链网络的强鲁棒性和去中心化，根据参与者提供的随机数为随机源进行透明RANDAO算法计算，从而得到基于参与者随机源的绝对随机数，安全可靠。并以此向各种竞猜游戏提供绝对的随机因子，通过随机因子而得到各种玩法需要的透明随机数，保证开奖的绝对公平性和透明性。

竞猜链的去中心化IM工具可以帮助客户点对点地沟通交流，具有即时、高效、隐秘的特点。客户可借此工具打造自己的专属社交圈，作为邀请朋友参与竞猜任务、发布线下聚会信息等私密社交的工具。专有链的搭设机构也可通过该IM工具维护自己的社区网络。

除了对区块链的底层技术的支持，竞猜链还会引进新的高科技技术，包括大数据和AI。竞猜链将基于区块链与大数据，结合人工智能AI开发深度应用，包括但不限于ORACLE预言机、智能客服、智能助手、竞猜娱乐产品的个性化推荐等等，使竞猜链更智能、更安全、更有效的服务博彩娱乐市场和全球用户。

## 3.3 平台参与方

竞猜链公共竞猜服务平台（FGSP）的参与者按照智能合约流程中的功能分类，可以分为三种：项目发起方，项目竞猜方和项目验证方。

项目以智能合约的形式存在。合约的生命周期如下：当一个竞猜方发布一个智能合约后，其中智能合约规定竞猜的形式、开奖方式等等，在全链平台中接受投注；也可以选择在私有链平台中发布，当满足预设开奖条件后进行开奖并自动实现价值转移，若未中奖则流标。

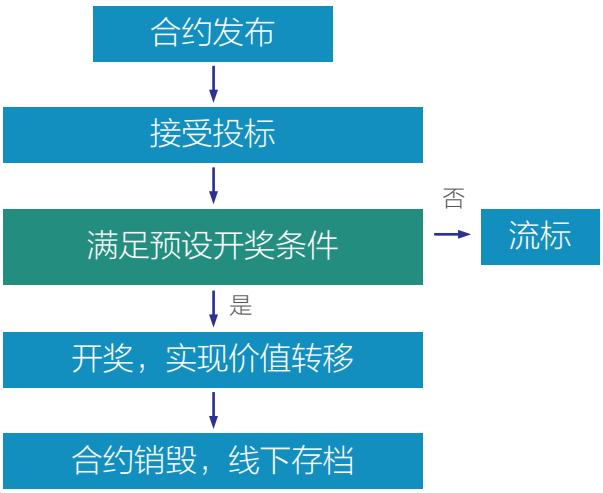



图4 竞猜项目开奖流程图

### 3.3.1 项目发起方

项目发起方可以为竞猜链公有链用户、也可以是利用竞猜链提供的服务接口搭建私有链平台的机构和公司。项目发起方在竞猜链平台上进入发布页面后，填写项目详情，金额以及开奖条件。竞猜链平台会在网络平台中提供常见的固定玩法的合约模板，用户可选择使用该智能合约模板，也可以利用API等软件开发工具开发新的竞猜项目。智能合约模板待完成验证无误后，系统会自动生成智能合约代码，并部署到竞猜链上，如下图:


图5 竞猜项目发布流程图

系统会预置一些智能合约模板，如果项目发起方找不到合用的模板，平台提供定制模板功能。发布成功的合约，项目发起方会获得合约地址，当然也可以通过系统搜索或者项目列表检查合约的状况。

### 3.3.2 项目竞猜方

项目竞猜方为竞猜链客户,也可以是搭建私有链的机构客户。此外平台提供有去中心化的IM工具，项目发起方在发布一项竞猜任务后，可通过IM工具邀请自己的朋友、同伴参与到竞猜项目中，所以这些人也是项目竞猜方之一。同时平台会在此基础上给予一定代币奖励。项目竞猜方可以通过主链发布的竞猜项目列表或者搜索功能直接搜索项目名称或智能合约地址，选择自己感兴趣的项目来参与。

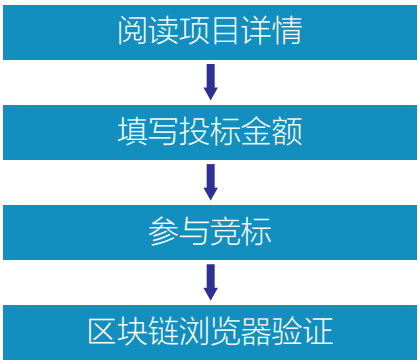



图6 竞猜项目投注流程图

### 3.3.3 项目验证方

基于竞猜链公平，公开，公正、透明的的原则，对竞猜结果有异议的参与方可以通过系统提供的区块链浏览器，凭项目的合约地址查看合约内容，对竞猜结果进行确认，并邀请具有相关资质的权威第三方进行公平公正性的验证。

## 3.4 竞猜链公共服务体系

竞猜链作为一个公平竞猜服务平台，旨在利用区块链技术为项目发起方、项目竞猜方、项目验证方提供安全、可靠、便捷、贴心的全方位服务内容。

### 3.4.1 网络平台服务

竞猜链总部将立足于菲律宾马尼拉，专注于全球线上竞猜市场，并积极拓展其他娱乐竞猜形式，打造开放的、立体的集传统彩票、互联网彩票、体育竞猜、个性竞猜于一体的公平竞猜服务平台。除了构建基于公有链的底层SDK 外，还将提供订制化客户端应用程序，包括但不仅限于PC 端、WAP 站、APP(iOS & Android)、PAD 端、H5 小程序等。

### 3.4.2 第三方访问接入

竞猜链将提供智能化的合约模板和框架，应用程序组件，以及定制的API和SDK给第三方提供娱乐竞猜服务的机构或者个人，降低娱乐竞猜的线上开发门槛，打开专属社区网络接入渠道。

### 3.4.3 竞猜项目综合管理

竞猜链公平竞猜服务平台（FGSP）将提供专为线上竞猜项目设置的综合管理系统，将提供符合各地法律法规的竞猜项目发布、开奖、通兑全流程管理服务，包括用户概览、佣金设置、财务分账等功能。

### 3.4.4 线上线下合作

除了提供在线竞猜娱乐服务以外，同样会对世界其他娱乐公司开放公有链接口，使线下交易方式数字化，逐步打造竞猜客户、竞猜机构等娱乐竞猜项目的爱好者线上服务提供平台。

### 3.4.5 资产兑换

许多用户持有其他主流数字资产（BTC，ETH等）。竞猜链在此基础上打造跨链钱包，可接受主流资产转入和储存，与平台流通的FGE代币自由兑换，甚至以其持有的主流数字资产作为筹码直接参与竞猜。同时竞猜链的双TOKEN机制还发行FGC代币与法定货币锚定，确保筹码的竞猜与持有过程中实现资产保值，避免因币圈波动而造成的价值不稳定。

## 3.5系统模块

本系统的架构基于以太坊技术：EVM机制以及智能合约机制。为了便于EVM调试以及合约的安全性验证，将使用zeppelin库。系统主要由以下部分组成

### 3.5.1 竞猜链账户管理系统

#### 3.5.1.1注册登录模块和可信身份验证

注册登录模块主要的功能是给每个参加竞猜活动的用户分配钱包地址。此功能的目的就是为用户提供傻瓜式服务，获取参与竞猜活动的ID。整个登录过程包括：

给每个注册用户分配一个公钥/私钥对

公钥作为用户身份的唯一ID,用来收发竞猜平台的FGC代币。私钥有两种选择：

（1）私钥存储在服务器端。

这样的好处，是可以在用户忘记私钥的时候，由服务器找回私钥。为此付出的代价就是：服务器是中心化的，信息容易受到攻击，而且容易被故意泄露。

（2）私钥由用户自己保存和管理，服务器不保存副本

好处就是安全性高。潜在的风险就是如果用户管理不善，弄丢了私钥，相应的数字资产也就丢失了，无法找回。

每个用户注册过程中提供助记词。主要是通过助记词来复原用户的私钥

竞猜链用户的身份验证在链上进行，以token的地址作为用户的唯一身份标识和资产标识，并基于人工智能的人脸识别检测技术，确保数字身份同真实个人间的真实性和一致性。实现智能合约控制下的，全流程无中介参与的用户身份验证和资产转移验证，实现整个竞猜生命周期中用户身份的可信验证。

#### 3.5.1.2 去中心化账户管理

账户是用户在互联网世界的通行证，是用户的身份标识。传统的用户身份存储于中心化的网站服务器中，竞猜链的账户管理系统采用去中心化的身份验证体系，用户的身份信息和凭证不属于任何机构所有，真

正完全掌握在用户自己手中；去中心化的账号系统将用户的身份信息和身份验证过程在区块链网络中进行，分散在全球的完全等价的区块链节点，不存在某个权威的节点，保障了系统的安全性。智能合约作为公正的“中心化服务提供者”，代替传统的中心化服务提供者，实现对去中心化组织公开公平的“自治”，规避了中心化账户管理系统，一旦服务器被攻击，或利益驱动、政治等其他人为原因造成的用户信息被泄露、篡改的风险。

### 3.5.2 竞猜数据管理系统


图7 猜链数据管理系统技术模型

在竞猜链搭建的区块链竞猜体系中，用户参与竞猜项目，可以即时在区块链网络上查看到自己的参与项目列表，竞猜记录和过程存储在区块链网络中，无法篡改和否认。竞猜链官方平台提供链上数据查询功能，用户可以通过平台或直接链上交易，确保整个竞猜过程的公正性和安全性。

关于兑奖结算系统，竞猜链将最终竞猜记录联结到其他系统的分布式账本，包含用户身份信息和连接预言机（Oracle）及基于参与式决策（Participatory Decision Making）的随机数生成器，得到竞猜结果后，竞猜链将根据智能合约自动结算奖金代币，不受任何中心化机构或第三方机构的控制，即时将奖金TOKEN分发给区块链网络上用户的身份地址中，保障兑奖过程中绝对的公开、公正和透明。

### 3.5.3 竞猜链智能合约引擎

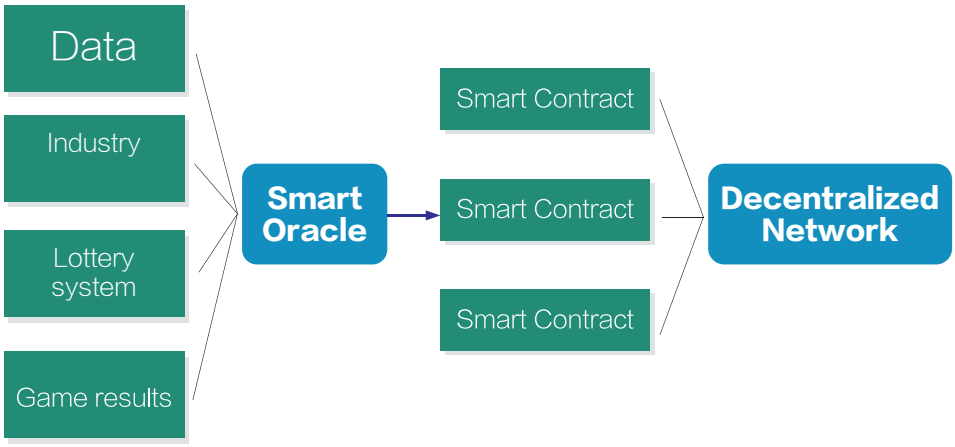



图8 竞猜链智能合约引擎

竞猜链用户的需求是多种多样的，对于中奖者的中奖逻辑，有些用户有非常确定的中奖条件，而有些用户则随机选择。对于中奖条件，有些用户的设定是固定的，比如招人合约对毕业院校的要求，而相对的，有些用户的中奖条件可能是依赖于外部条件的变化而变化的，比如某些岗位的招聘，如果是女的，则40岁以下，如果是男的，则50岁以下。竞猜链平台提供了一些最常用的逻辑的智能合约模板，并融合了智能合约自动化生成引擎技术，用户可以通过图形化界面的方式自动生成模板并部署，大大减轻用户的学习曲线和开发智能合约方面的负担，从而大大降低使用竞猜链的使用门槛。对于没有预置的那些商业逻辑，用户可以选择自己开发，并由平台提供指导。或者可以有平台直接定制开发。

### 3.5.4 竞猜链随机数生成系统

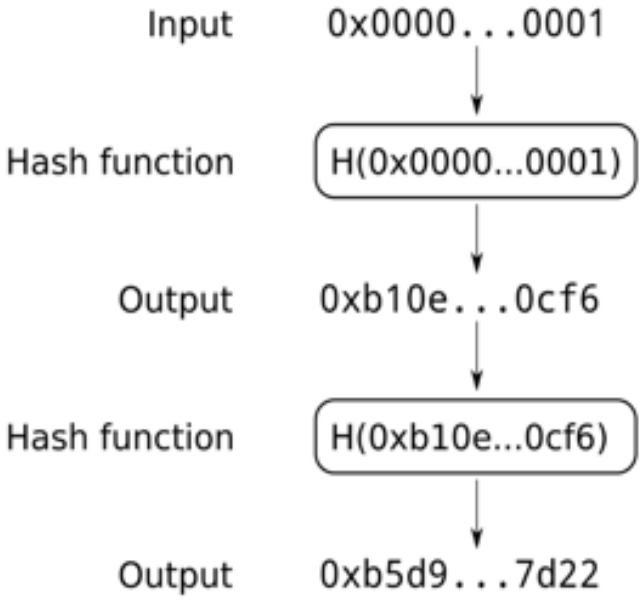
绝对随机数的产生是保证竞猜结果公平、公正重要的技术环节，也可以当作竞猜服务提供商的核心竞争力。业界提供了非常多的伪随机数的方案，而原有的各种方案因为都是基于中心化的方案，理论上都可以通过多种方式进行攻破或修改，尤其各种在线竞猜平台中，随机数生成的安全性和可靠性一直被质疑。

竞猜链设计了一套基于RANDAO思想的以参与者为随机源的随机数生成器，以保证算法的公正性。其中，RANDAO算法被以太坊创始人V神誉为当前最公平最随机的随机数生成算法，竞猜链算法是对RANDAO

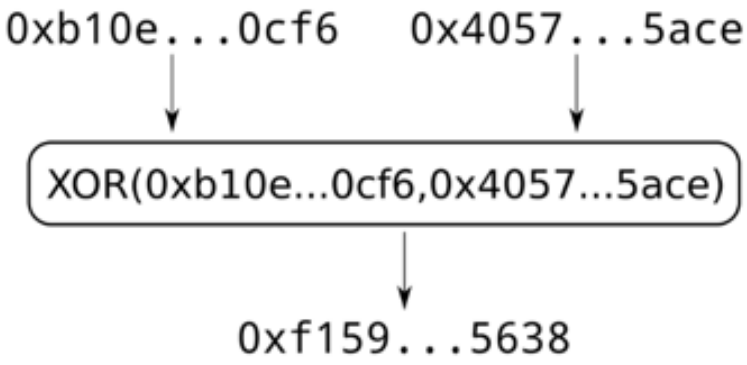
随机数生成算法简化和提升，并进一步避免了最后一人投注相比于其他顺序中奖概率略高的不足。

Randao协议层将一个或多个区块链上智能合约封装成各种随机数以形成算法，对应不同的业务需求。从而能够保证随机数服务的多样性，使得协议可以覆盖更广泛的应用范围中，满足更多的应用需求。随着区块链平台的推进和发展，Randao将结合市场需求封装更多的随机数生成模式，为了把Randao打造成区块链上的标准随机数服务，随机数服务都将经过严格的测试以及安全审计，确保服务上线的质量。

竞猜链的随机数生成算法有2个特点： 重复哈希(Repeat Hashing)和参与者贡献(Participator Contribution)。重复哈希是一个数据源进行多次哈希，上一次哈希的结果输出是下一次哈希运算的输入。下面是示意图：




参与者贡献是指系统可以从多个参与者的贡献中获得一个最终值，参与者贡献不同的值会导致最终值的不同。同时，任何一个参与者在最终值形成的问题上和其余的参与者是处于同一起跑线。参与者贡献的一个很有价值的特性就是，参与者中只要有一个可信，就可以保证最终值是可信的。结果不可信的情况只有一种：所有参与者合谋。



具体随机数生成过程如下：

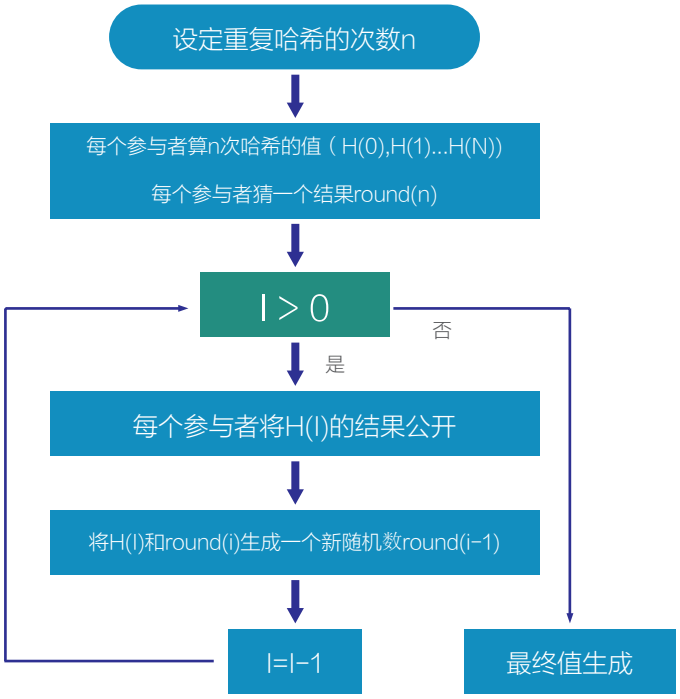



图9 基于Randao 的参与式决策随机数生成模型

### 3.5.5 去中心化信息交流工具

为了扩大竞猜链平台的参与人群，我们在初期设置了基于点对点协议的去中心化信息交流工具，以便竞猜链客户通过该信息交流工具发布项目信息。基于点对点协议的去中心化交流工具能够保证信息安全，防泄漏防检测，并由于其去中心化的储存方式，信息不需要被中心服务器暂存，从而防止被中心化储存机构的数据备份。在交流工具里传输的信息是端到端加密的，使用户不止对于项目的交流交易乃至个人通信更为私密和纯粹。

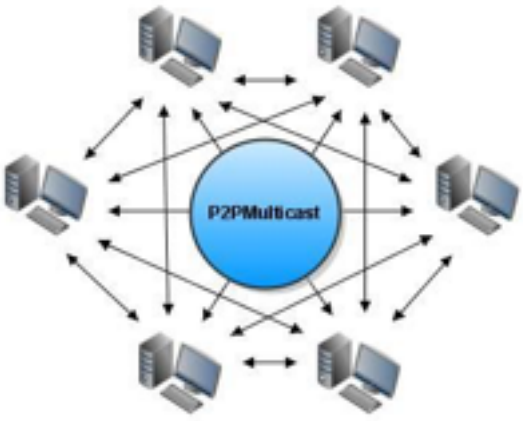



图10 P2P即时通信模型

### 3.5.6 竞猜链其他辅助工具

#### 3.5.6.1 区块链浏览器

竞猜链是基于以太坊技术。对于每一个项目活动，会将包含活动的商业逻辑的代码以智能合约的方式部署在链上。以太坊上所有的智能合约代码都是公开透明的，可以通过区块链浏览器工具查看：

- https://www.etherchain.org/
- https://etherscan.io
- 类似的工具还有很多

竞猜链也提供一个类似以太坊的区块链浏览器，方便用户查询相应的合约代码。

#### 3.5.6.2 合约模板助手

竞猜链预置了一些常用的项目模板，以应付日常高频需求。但是市场总会出现一些独特的需求，而且这些需求是实实在在的。基于市场为王，用户为王的信仰，鉴于目前智能合约的编程的复杂性，竞猜链会推出排名机制，允许平台的注册用户提出编写智能合约的需求，由用户定期投票产生排名。竞猜链平台会为排名靠前的需求开发模板，或者提供指导，并进行安全性检查。经过市场的实际运行检验后，达标的模板会进入预置模板列表，为广大用户服务。

## 第四章 扩展性

### 4.1 预言机（Oracle）

预言机是一种可信任的实体，它通过签名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，如世界杯竞猜，智能合约需要先获得比赛结果才能执行合约内容。预言机具有不可篡改、服务稳定、可审计等特点，通过提供数据上链，保证智能合约的正常运行。但是，单一的预言机存在着来源数据不可信的问题，为了保证结果的正确可靠，我们提出一种多点态势下的去中心化预言机机

制。预言机来源数据将来自于多个可信节点，同时通过代币奖励机制由竞猜链网络上的用户选取志愿者进行参与判定，而当多个可信节点的结果出现不同时，区块链网络上的参与者将进行结果多方验证，通过多点数据+多点验证的方式，保证预言机数据的安全性和可靠性，进而保障整个竞猜体系的公开透明。

此外，竞猜链还可以接入第三方信息中介（Oracle），项目的结果由Oracle来决定。这些Oracle提供了一系列的API，竞猜链通过调用这些Oracle API来决定项目的中奖方。Oracle可以是中心化的，也可以是多中心化的。

以查询小米MIX2价格为例，假设现在有一个第三方系统（预言机）可以提供权威准确、不可篡改、稳定、并可接受审计的价格查询接口，预言机首先从小米官方获取小米mix2的价格，然后向特定区块链上的地址进行转账，并将价格信息写入交易备注，这样智能合约只需要查看特定地址的交易记录，就可以获取小米mix2的价格了。由于区块链会自动同步存储包含交易的区块，所以智能合约几乎只需要访问本地就能得到价格信息。既保证了访问效率，又保证了价格的一致性。总的来说就是由预言机（第三方）将数据推送给区块链，而不需要智能合约主动向第三方拉取数据。

在绝大部分情况下，一台预言机已经足够，但在处理重大资产时，常常一台预言机并不能保证完全可靠，竞猜链建立了多台预言机提供准确数据接口的网络，即多重预言机模型又被称为预言机网络。

## 4.2 以太坊技术的未来可扩展性

以太坊创始人Vitalik公布了其主导的分片（Sharding）技术的最新进展。分片（Sharing）其实是一种传统数据库的技术，它将大型数据库分成更小、更快、更容易管理的部分。在区块链网络中，分片是将网络中的每个区块变为一个子区块链（100个），子区块链中可以容纳交易数据，并最终组成一个在主链上区块。这样，每个区块的交易容量就大概扩大了100倍。新版以太坊推出该项技术已经成为大概率事件。竞猜链基于以太坊技术可以享受到以太坊自身进化带来的好处，大大提升自身交易容量和数据储存效率，进一步优化竞猜链服务平台的用户体验。

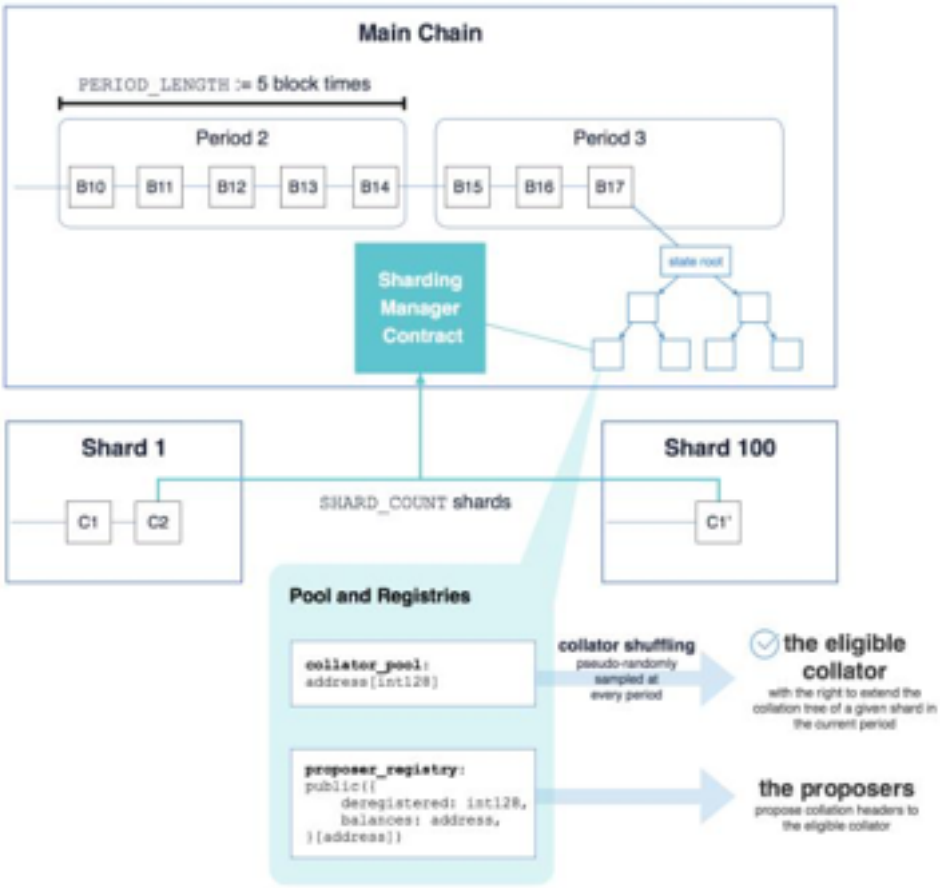



图11 以太坊分片技术模型

## 4.3 应用场景

由于竞猜链提供了公开透明的机制，从而保证了每个项目的竞猜结果的公正性。而项目的定义是非常广泛的：买卖二手家具可以是一个项目，剩女相亲约会也可以是一个项目。因此，竞猜链可以广泛地应用到我们的实际生活中。下面仅仅列出其中一些可能的应用：

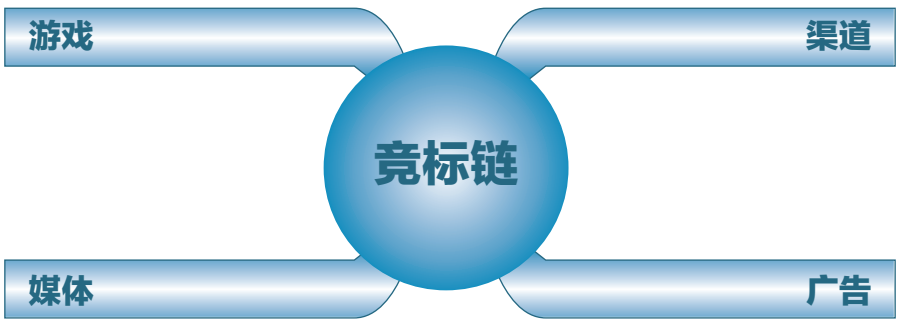



图12 竞猜链的应用场景

以彩票为例，我们坚信区块链彩票是整个彩票行业的未来。竞猜链平台也支持完整的区块链彩票开发者生态。基于竞猜链开发的智能合约区块链彩票系统，以及开发者生态的开发者开发的区块链彩票应用，都支持直接使用FGC购买和交易彩票（在对应合规性的国家）。我们同时将支持以主流数字货币作为筹码和奖金。

再以区块链游戏为例，自2017年11月底以太猫问世以来，一大批区块链游戏开发商竞相模仿，以太猫的成功以及较低的入门门槛在一定程度上导致了区块链游戏初期的同质化。目前的区块链游戏的核心玩法还是比较单一的，主要是抢购、收藏、博彩等类型，无论是宠物、名人，每一个玩家手上的虚拟道具都是独一无二的。从技术层面来看，区块链游戏和炒币是类似的，和传统意义上的游戏——通过操作和剧情来带给玩家游戏体验是不同的，区块链游戏通过获得物品的稀有属性来获取高额收益，实际上就是一个投机的过程。基于竞猜链的平台，区块链游戏将更有趣味性。按照ERC721代币合约，竞猜链的区块链游戏和竞猜同时也是相辅相成的，有着广阔的发展前景。

## 4.4 跨链钱包

我们将允许竞猜方以主流数字货币交易所上线的数字货币作为竞猜保证金，甚至标的物，由此我们将开发一个跨链钱包。通过竞猜链平台的有效运营，跨链钱包将成为一个交易中心以及个人数字资产管理平台。跨链钱包产品将实现多资产支持，包括BTC、ETH、QBT等跨链多币种，并由此延伸到与数字货币相关的社交沟通、币币交易、支付、行情、咨询等功能，并为各种类型博彩平台、游戏厂商提供专属的数字筹码兑换，并对标博彩行业及其配套产业的基础产权发行数字资产。

# 第五章 通证机制及发行方案

## 5.1 竞猜链的双Token经济模型

公有链体系具有极佳的去中心化特性，但是对快速交易（如竞猜博彩）并不友好；联盟链在效率和费率上具有很大的优势，但其达不到完全的数据公开透明监督。

借鉴于此，竞猜链将采取双Token经济模型，一种是FGE(Fair Guessing Equity) Token，属于权益类凭证，将上线大型主流交易所交易流通。一种稳定币FGC(Fair Guessing Coin) Token，属于功能类凭证，用于参与竞猜投注。

## 5.2 FGE Token

FGE Token在交易所交易流通，其主要作用及价值：

金融价值。它的金融价值来源于竞猜链价值的提升。一旦使用竞猜链平台的用户增多，FGE Token的需求增多。随着FGE Token需求上升，FGE的交易价格也随之提高。

使用价值。竞猜链有着真实而明确的场景应用，平台将对每笔成功完成的合约提取一定比例的手续费。FGE Token的持有者每月向平台支付一定数量的FGE可以获得一定比例的手续费减免。

激励价值。为了激励竞猜链使用的深度和广度，未来竞猜链基金会将对在平台上成功完成交易的使用者进行奖励，比如乐透型彩票场景，每达成100元法币的交易，就奖励其1个FGC。这对竞猜链平台成为一个使用者持续导入，不断自我生长的平台具有重要意义。同时，对长期持有FGE和消费FGE的使用者，平台将按一定比例返还手续费。

开发者生态奖励价值。开发者生态是竞猜链系统的重要组成部分，开发者通过基于竞猜链系统的开放API 开发的区块链场景应用，需要向官方递交并冻结一定数量的FGC。这些API不仅使开发者的成果有机会被消费者应用，获得丰厚的开发和发行回报，更能促进FGC Token的流通和规模化应用。

系统回购销毁。竞猜链基金会将每年度收益的一部分进行FGC Token的回购，并进行销毁。

## 5.3 FGC Token

FGC是参与竞猜链场景应用的必要Token。FGC相比FGE的好处是，可以保证FGC 在兑换成法币时保持价格稳定。用户为了参与竞猜和投注项目，需要用到FGC Token。FGC Token可以用FGEToken兑换，也可以通过OTC市场购买。

FGC Token的发布基于专有链网络，可在P2P、匿名、安全、去中心化的环境中自由交易。同时FGC提供有价资产与发行的数字资产的兑付服务，并保证发行的数字货币的价值。

## 5.4 FGE Token的发行方案

FGE Token共发行 10 亿枚，由竞猜链一次性创设出来，其总量上限已设定，不可更改，永不增发。FGE Token按照一定的规则和比例分配给不同的持有人，其中一定比例的FGE Token在合适国家以合规性方式向合适人群进行募资，用于竞猜链项目的执行和运维，包括但不限于本白皮书所涉及的技术研发建设及迭代，以及市场运营等。

## 5.5 FGE Token分配方案

| 数量 | 比例 | 分配方案 | 说明 |
|---|---|---|---|
| 5亿 | 50% | 合规方式向适当人群发售 | 用于竞猜链运营，主要包括开发、市场、运营、第三方机构服务、吸引优秀人才等。 |
| 2.5亿 | 25% | 创始团队<br>开发团队<br>顾问团队 | 用于奖励在竞猜链建设、开发过程中做出努力和贡献的相关团队，感谢他们以人力资源、技术开发、社群建设、咨询顾问等形式对项目的支持。代币将会在　年内被锁定，不可以进行流通，在锁定结束后的两年时间内按月线性释放。 |
| 1亿 | 10% | 市场推广<br>商业分配 | 在寻求资源整合、权益置换、社群支持等过程中的商业分配，以及用于支持项目推广和平台完善所需要的交流，包含“空投”等。 |
| 1亿 | 10% | 用户激励 | 每达成100个FGC的交易，就奖励其1个FGE。这对竞猜链平台成为一个使用者持续导入，不断自我生长的平台具有重要意义。 |
| 0.5亿 | 5% | 基金会运作 | 基金会长期负责平台在开发、建设、发展等方面的管理工作，以及开源社区项目的相关事务。此部分用于基金会长期运作。 |

## 5.6 FGE Token发售方案

FGE　Token的发售将严格按照世界各地的法律法规，以恰当方式面向合适人群进行发售。FGE　Token恒定的发行总量为10亿枚，其中50%即5亿枚用于对外发售。

| | 基石轮 | 私募轮 | 公开阶段 |
|---|---|---|---|
| FGE Token | | | |
| 时间 | | | |
| ETH | | | |

# 第六章 竞猜链核心创始团队和顾问

## 6.1 竞猜链核心创始团队

Leon Liu

大数据技术专家，互联网金融保险产品专家
拥有超过20年的信息产业经验和15年的金融保险业经验
重点工作经历：
——美国三大征信中心之一Equifax资深系统分析员；
——曾任职于加拿大人寿、加拿大皇家银行、财产及意外险应用系统软件公司、惠普旗下保险系统开发子公司、美国友邦保险等金融及保险公司担任技术或管理职位

加拿大约克大学博士；IBM公司资深专家，数据库技术专家
拥有20年的软件产品研发经验
重点工作经历：
自2000年起任职于IBM多伦多实验室，目前担任高级顾问；2004年创办互联网支付网站爱付宝，担任CTO；多次在IBM IOD等大型会议针对数据库相关技术发表演讲；
著书：DB2 UDB V8 and WebSphere V5 Performance Tuning and Operation Guide

Peter Z. He

Sean Tang

毕业于加拿大多伦多大学精算和统计专业
现任职于某全球500强保险公司的量化对冲基金平台
IT+精算跨界专家，拥有10年保险行业工作经验
重点工作经历：
负责保险资金投资的量化对冲，参与平台开发和投资决策；从事或领导团队从事：保险新产品开发定价，保险产品准备金测算，保险产品风险控制，再保险定价，团体保险定价，保险产品核保平台开发，退休金平台开发维护；北美精算师和美国精算协会会员（Actuary and MAAA）

Harry Hsu

剑桥大学科技政策硕士，台湾师范大学图文传播硕士；
重要工作经历：
TutorABC品牌公关总监；DHGate敦煌网高级市场公关经理；
2016年中国创新创业大赛港澳台赛主持人；2018年全球区块链经纪人峰会主持人；2018两岸和平发展论坛主持人；
著有《那一年，我在剑桥揭下伏地魔的面具》、《理查斯特劳斯传》、《尼贝龙指环》等；
台湾天下杂志社、《中国时报》专栏作家。

毕业于加拿大西安大略大学电子与计算机工程专业，硕士学位。
现就职于某再保险公司，负责灾害模型开发
拥有6年项目管理及8年软件开发经验
重要工作经历：
负责灾难模型分析软件开发，灾难模型风险分析，恐怖袭击风险软件开发，再保险条约分析，多个基于GIS的智慧城市项目

Cheryl Ma

## 6.2 顾问

加拿大西安大略大学硕士学位，持有项目管理PMP，风险管控CRISC 等专业证书
前IBM (多伦多) 研发中心Mainframe大型机编译优化开发专员；

Tracy Lee

## 6.3 早期投资人

# 第七章　竞猜链执行路线图

2019年1月 移动端上线；

2019年3月 智能合约引擎上线；

2019年5月 跨链钱包上线

## 2019

2018年2月 完成竞猜链白皮书1.0版，确立技术架构；

2018年3月 启动底层链设计及模块研发；确立与菲律宾、柬埔寨等国家合法博彩娱乐公司合作关系；

2018年5月 完成竞猜链白皮书2.0版本；完成区块链浏览器；第一个DAPP上链内测；

2018年6月 第二、第三、第四个DAPP上链内测；多中心化IM工具开始开发；跨链钱包和ORACLE进入研发阶段；
2018年7月 已上链DAPP公测；基于以太坊一次性创设FGE Token，启动私募；

2018年8月 完成FGE Token 在主流数字货币交易所上线；已上链DAPP上线；区块链竞猜游戏落地海南；

2018年9月 完成多中心化IM工具开发；

2018年10月 预言机（oracle）第一版开发完成；

## 2018

2017年12月 竞猜链核心团队成立，进行市场调研，整合关键资源；

## 2017


THANKS