

竞标链技术白皮书

V0.6（草稿）



2018-5-6

# 版本历史

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **版本** | **时间** | **描述** | **修改人** | **授权人** |
| 0.1 | 2018年2月14号 | 创建说明书草案 | 郑嘉文 |  |
| 0.2 | 2018年2月18号 | 草案定稿 | 郑嘉文 |  |
| **0.3** | 2018年4月15号 | 增加ERC721代币，设计升级 | 郑嘉文 |  |
| **0.4** | 2018年4月27号 | 以太坊私链部署  以太坊区块链浏览器 | 郑嘉文 |  |
| **0.5** | 2018年5月4号 | 竞标技术白皮书草案 | 郑嘉文 |  |
| **0.6** | 2018年5月21号 | 随机数生成，项目背景 | 郑嘉文 |  |
|  |  |  |  |  |

# 参考文档

|  |  |  |
| --- | --- | --- |
| **简介** | **时间** | **文档名** |
| ERC165标准 | 2018-04-25 | [EIPS-165](https://link.juejin.im?target=https%3A%2F%2Fgithub.com%2Fethereum%2FEIPs%2Fblob%2Fmaster%2FEIPS%2Feip-165.md) |
| ERC721标准 | 2018-04-25 | [EIPS-721](https://link.juejin.im?target=https%3A%2F%2Fgithub.com%2Fethereum%2FEIPs%2Fblob%2Fmaster%2FEIPS%2Feip-721.md) |
| RANDO | 2018-04-27 | https://github.com/randao/randao |
| Random org | 2018-04-27 | https://api.random.org/json-rpc/1/ |
| 云购平台 | 2018-04-25 | https://www.yungoucms.cn/ |
|  |  |  |

**目 录**

[版本历史 1](#_Toc514698715)

[参考文档 2](#_Toc514698716)

[第一章 执行概要 5](#_Toc514698717)

[1 技术选型 5](#_Toc514698718)

[2 系统构成 7](#_Toc514698719)

[2.1 概述 7](#_Toc514698720)

[2.2 功能描述 9](#_Toc514698721)

[2.2.1 项目发起方 10](#_Toc514698722)

[2.2.2 项目竞标方 10](#_Toc514698723)

[2.2.3 项目验证方 11](#_Toc514698724)

[2.3 系统模块 11](#_Toc514698725)

[2.3.1 注册登录系统 11](#_Toc514698726)

[2.4 ERC20代币合约 12](#_Toc514698727)

[2.5 智能合引擎 12](#_Toc514698728)

[2.6 ERC721代币合约 12](#_Toc514698729)

[2.7 随机数生成 13](#_Toc514698730)

[2.8 区块链浏览器 15](#_Toc514698731)

[2.9 扩展性 16](#_Toc514698732)

[2.9.1 预言机（Oracle） 16](#_Toc514698733)

[2.9.2 合约模板助手 17](#_Toc514698734)

[2.9.3 跨链钱包 17](#_Toc514698735)

[2.9.4 去中心化的IM工具 17](#_Toc514698736)

[2.9.5 以太坊技术的未来可扩展性 17](#_Toc514698737)

[2.9.6 应用场景 18](#_Toc514698738)

[3 通证机制 19](#_Toc514698739)

[3.1 竞标链的双Token经济模型 19](#_Toc514698740)

[3.2 FBE Token的作用。 19](#_Toc514698741)

[3.3 FBC Token 20](#_Toc514698742)

[4 社群组织 20](#_Toc514698743)

[5 法律事务和风险声明 21](#_Toc514698744)

[**5.1** **竞标链项目的法律结构** 21](#_Toc514698745)

[**5.2** **免责声明** 22](#_Toc514698746)

[**5.3** **风险声明** 23](#_Toc514698747)

# 执行概要

# 项目背景

从技术层面来说，对竞标的最大的质疑是其公平公正性。

* 游戏规则不透明

大多数的竞标平台对于游戏规则都是语焉不详，尤其是对于规则的细节以及数据的来源。

* 存在暗箱操作的可能

竞标的中奖算法，竞标流程不透明，属于集中式管理，而集中则意味着竞标平台对这些数据是可控的。在一个自定游戏规则，且缺乏有效监督的网络平台，很难保证公平公正。

* 不具备事后追踪

由于竞标平台保有所有的数据，对于事后的追查，没有很高的公信力。首先，很难获取竞标的数据。其次，即使获取到了数据，也很难保证数据的真实性。

# 技术选型

方兴未艾的区块链技术很好的解决了上一节里描述的痛点。

* 不可更改的共享账本机制(immutable share ledger)

由于共享账本，所有的信息都是公开透明的。而且信息一旦上链，信息即不可篡改

* 可溯源(Traceability)

所有程序运行的结果都在链上，只要具有一定的IT知识和技巧，都可以到链上查询

* 匿名

链上所有ID的代表就是一个地址，和人的物理信息，社会身份信息没有必然的联系。极好的保护了用户的隐私。

在考察了市场上大多数的链后，以太坊（Ethereum）无疑是最适合用来做竞标技术平台的选择。

* 以太坊提供了完备编程语言和编程接口

以太坊提供了Solidity智能编程语言和定义好的编程接口。在此基础上的平台开发和维护都变得比较简单和轻松。

* 以太坊的ERC20代币

以太坊可以很容易的发行代币，从而很容易的建立基于代币的经济学模型。ERC20代币在ICO风行的时候得到了大规模的验证。现在几乎所有的钱包都支持ERC20代币。

* 以太坊的ERC721代币

以太坊猫，莱茨狗等的风行，使用不可分代币代替所表征的实物

* 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。

* 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。

当然，以太坊也不是十全十美的，从技术上来说，也面临着很多不确定性：

* 网络拥堵

前段时间以太猫流行的时候，造成了以太网络的拥堵。平常发送一个币几分钟就可以到帐，而拥堵的时候有可能几个小时也无法到帐。这个是由于以太坊本身的设计造成的。简言之，就是以太坊的基础设施建设跟不上需求

* 交易费用高昂

随着ETH的日渐坚挺，由于所有基于以太坊的交易都是要付Gas费用，导致交易费用高企。

* 于现实世界的连接性

以太坊并没有接口直接连接到实体世界。比如，天气预报的数据就无法实时接入以太网络

# 系统构成

## 概述

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

* 注册登录

所有想参与竞标的用户，必须在指定的网站上注册，获取相应的以太坊地址。用于购买代币，提币，投资某个特定的项目。

* ERC20代币合约

所有参与竞标项目活动的用户必须通过购买平台的代币实现。当然，相应利益的获取，交换也会以代币的形式获取。

* 智能合约的引擎

每次竞标项目的活动，就是一个智能合约。满足合约预先指定的条件，该合约被触发自动执行。

* ERC721代币合约

每次竞标项目的活动，就是一个智能合约。满足合约预先指定的条件，该合约被触发自动执行。ERC721非同质的特性唯一的标志了每个竞标项目的标的。

* 区块链浏览器



## 功能描述

竞标平台的参与者可以分为3种：项目发起方，项目竞标方和项目验证方。项目以智能合约的形式存在。合约的生命周期如下：



### 项目发起方

项目发起方可以在竞标链平台上进入发布页面，填写项目详细，金额以及开标条件。待验证无误后，系统会自动生成智能合约代码，并部署到竞标链上。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（具体请参考2.9.2节）



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。

### 项目竞标方

项目竞标方可以通过项目列表或者搜索功能，选择自己感兴趣的项目来参与。



### 项目验证方

基于竞标链公平，公开，公正的原则，对投标结果有异议的参与方可以通过系统提供的浏览器，凭项目的合约地址查看合约内容，对竞标结果进行确认，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。

## 系统模块

### 注册登录系统

注册登录模块主要的功能是给每个参加竞标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，获取参与竞标活动的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,用来收发竞标平台的FBC代币。

私钥有两种选择：

* + 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

* + 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

## ERC20代币合约

竞标链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FBC（Fair Bid Coin）。FBC是竞标链在正式上线运行时发行的，由智能合约生成的。竞标链用户对发布在竞标链上任何一个项目作出预测时，只能而且必须使用FBC去操作：发起项目，竞标项目以及验证项目

## 智能合引擎

用户的需求是多种多样的，对于中标者的中标逻辑，有些用户有非常确定的中标条件，而有些用户则随机选择。对于中标条件，有些用户的设定是固定的，比如招人合约，211大学毕业生有可能就是定死的条件，而相对的，有些用户的中标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。竞标链平台提供了一些最常用的逻辑的智能合约模板，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标链的使用门槛。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。

## ERC721代币合约

ERC721同样是一个代币标准，ERC721官方简要解释是Non-Fungible Tokens，简写为NFTs，多翻译为非同质代币。ERC721 是由Dieter Shirley 在2017年9月提出。Dieter Shirley 正是谜恋猫CryptoKitties背后的公司Axiom Zen的技术总监。因此谜恋猫也是第一个实现了ERC721 标准的去中心化应用。ERC721号提议已经被以太坊作为标准接受，但该标准仍处于草稿阶段。

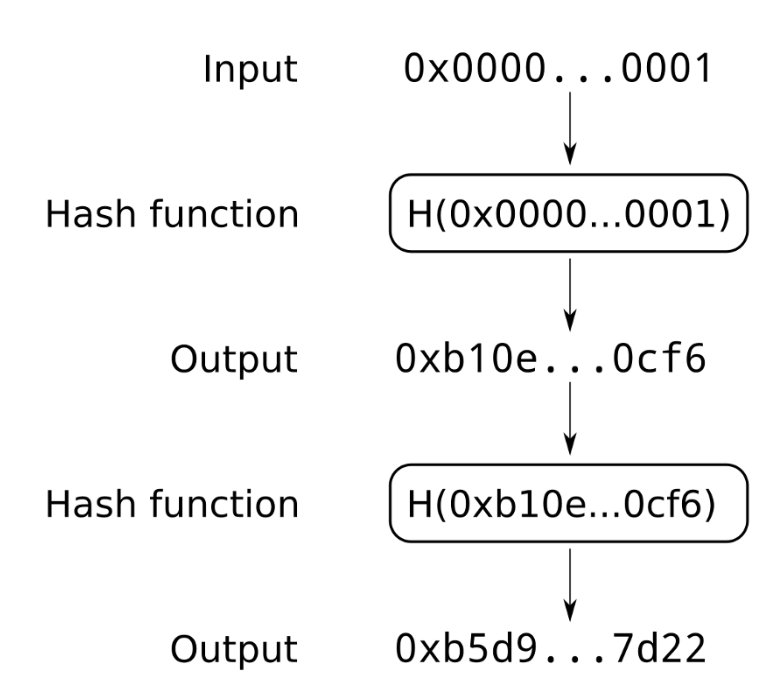
非同质代表独一无二，谜恋猫为例，每只猫都被赋予拥有基因，是独一无二的（一只猫就是一个NFTs），猫之间是不能置换的。这种独特性使得某些稀有猫具有收藏价值，也因此受到追捧。ERC20代币是可置换的，且可细分为N份（1 = 10 \* 0.1）, 而ERC721的Token最小的单位为1，无法再分割。

如果同一个集合的两个物品具有不同的特征，这两个物品是非同质的，而同质是某个部分或数量可以被另一个同等部分或数量所代替。非同质性其实广泛存在于我们的生活中，如图书馆的每一本，宠物商店的每一只宠物，歌手所演唱的歌曲，花店里不同的花等等，因此ERC721合约有着广泛的应用场景。通过这样一个标准，也可建立跨功能的NFTs管理和销售平台（就像有支持ERC20的交易所和钱包一样），使生态更加强大。

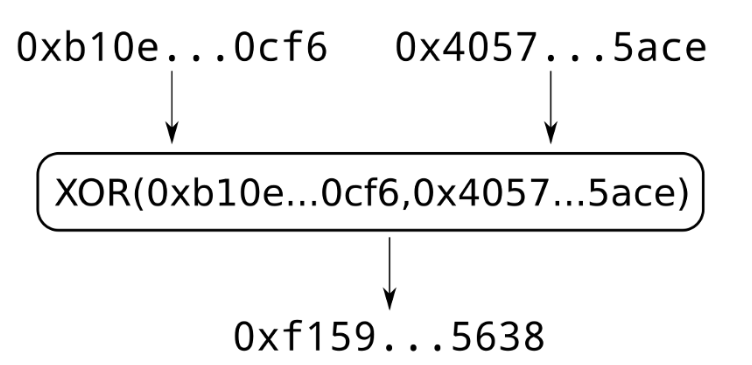
## 随机数生成

在区块链上生成随机数一直以来都是很热门的话题，也是具有高度挑战性工作。有的方案提出了一套独有的基于比特币区块链网络的绝对随机数生成方式，这种方式基于比特币网络的健壮性和去中心化，根据未来一段时间内挖掘的比特币区块的哈希值进行不同的透明算法计算，从而得到基于比特币网络的绝对随机数，从而达到安全可靠随机数，以此向各种彩票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。比较权威而且获得广泛认同的是RANDAO项目。竞标链设计了一套基于RANDAO的随机数生成器，以保证算法的公正性。

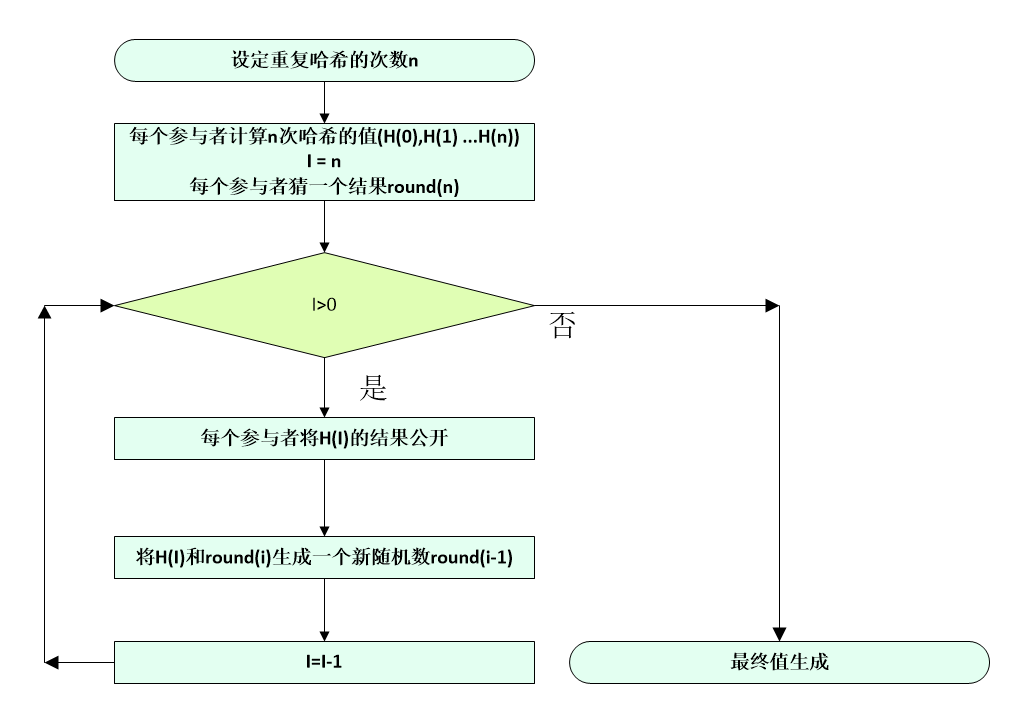
竞标链的随机数生成算法有2个特点： 重复哈希(Repeat Hashing)和参与者贡献(Participator Contribution)。重复哈希是一个数据源进行多次哈希，上一次哈希的结果输出是下一次哈希运算的输入。下面是示意图：



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大致最终值的不同。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。



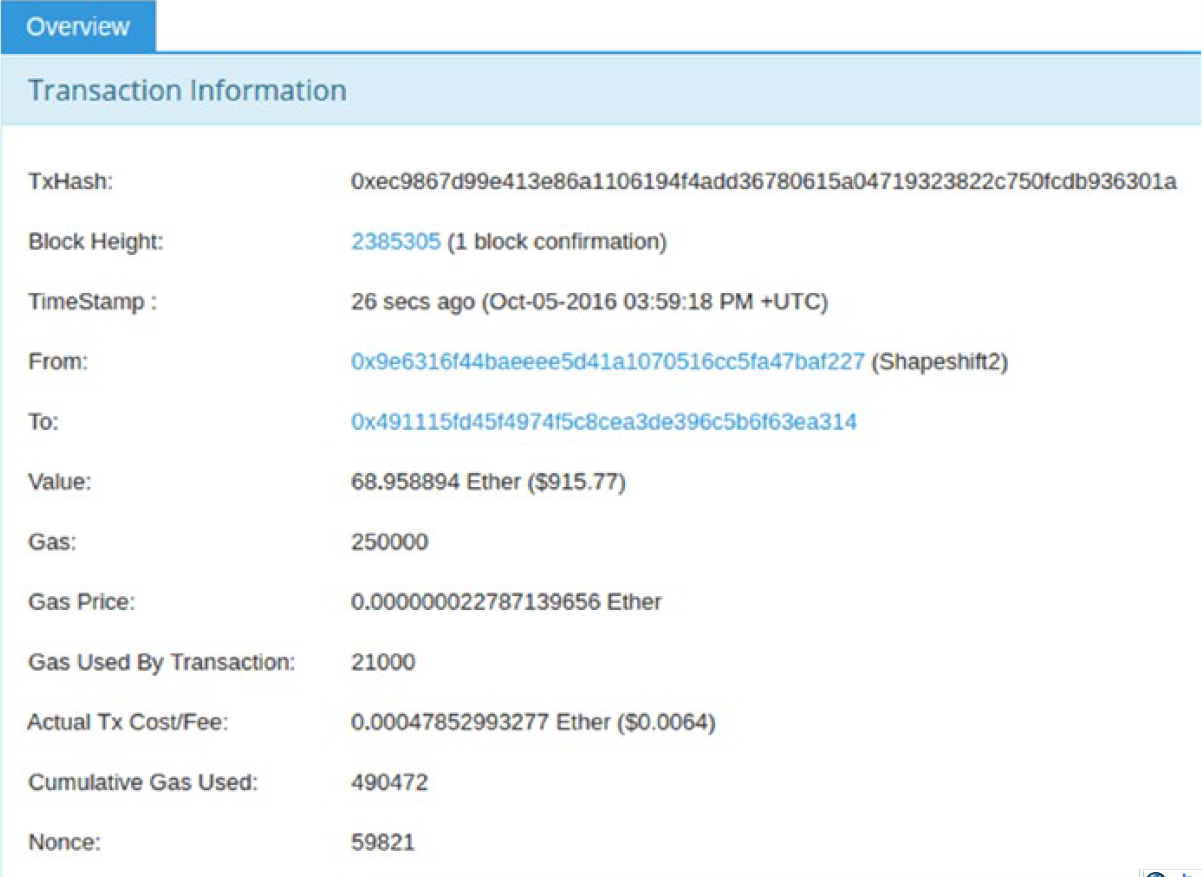
具体随机数生成过程如下：



## 区块链浏览器

竞标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



竞标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。

## 扩展性

### 预言机（Oracle）

竞标链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，竞标链通过调用这些Oracle API来决定项目的中标方。Oracle可以是中心化的，也可以是多中心化的。

### 合约模板助手

竞标链预置了一些常用的项目模板，以应付日常常用的高频需求。但是市场总会出现一些出乎意外的需求，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，竞标链会推出排名机制，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。竞标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。

### 跨链钱包

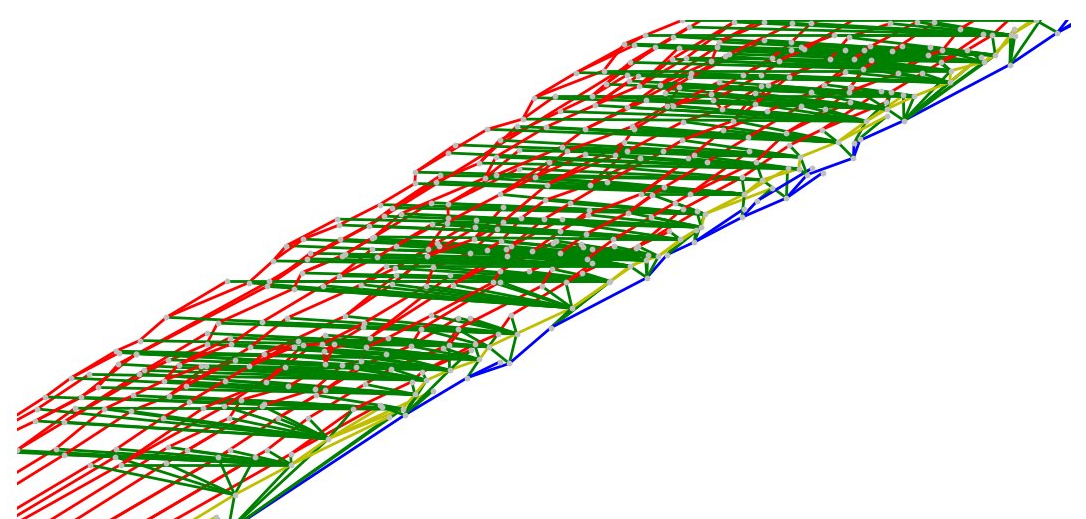
未来我们将允许投标方以各种主流数字货币作为竞标保证金，甚至标的物，由此我们将开发一个跨链钱包。通过竞标链平台的有效运营，跨链钱包将成为一个交易中心以及个人数字资产管理平台。

### 去中心化的IM工具

为了扩大竞标链平台上发起项目的参与人群，我们在初期设置了广播站，以便发布项目信息。未来，我们将设置一个多中心化的IM工具，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。

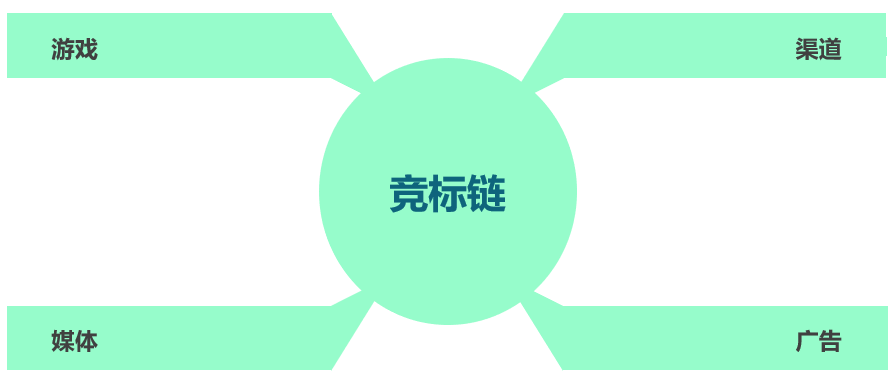
### 以太坊技术的未来可扩展性

Vitalik主导的分片（Sharding）改造最近取得了很大进展。年底新版以太坊的推出已经成为大概率事件。竞标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。



### 应用场景

由于竞标链提供了公开透明的机制，保证了每个项目的竞标结果的公平性。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，竞标链可以广泛的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：



博彩（区块链彩票）

我们坚信区块链彩票是整个彩票行业的未来。竞标链平台也支持完整的区块链彩票开发者生态。基于竞标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FBI 购买和交易彩票（在对应合规性的国家）。

# 通证机制

## 竞标链的双Token经济模型

一种是FBE(Fair Bid Equity) Token，在交易所交易流通。一种稳定币FBC Token，用于参与竞标投注。

## FBE Token的作用。

FBE Token在交易所交易流通，其主要作用及价值：

* 金融价值。它的金融价值根基来源于竞标链价值的提升。一旦使用竞标链平台的用户增多，FBE Token的需求增多。随着FBE Token 需求上升，FBE的交易价格也随之提高。
* 权益价值。竞标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。这些手续费除了用于竞标链的运营和迭代升级，将有一定比例用于FBE Token的分红。
* 使用者激励价值。为了激励竞标链使用的深度和广度，未来竞标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FBC。这对竞标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。
* 开发者生态奖励价值。开发者生态是竞标链系统的重要组成部分，开发者通过基于竞标链系统的开放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FBC。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FBC Token的流通和规模化应用。
* 系统回购销毁。竞标链基金会将每年度收益的一部分进行FBC Token的回购，并进行销毁。

## FBC Token

FBC是参与竞标链场景应用的必要Token。它与法币锚定的好处是，可以保证FBC 在兑换成法币时保持价格恒定。用户为了参与竞标和投注项目，需要用到FBC Token。FBC Token可以用FBC Token兑换，也可以通过OTC市场购买FBC Token。

# 社群组织

# 法律事务和风险声明

## **竞标链项目的法律结构**

针对竞标链的项目，已成立一个位于 的非盈利性的基金会 。基金会将作为独立的法律主体，全权负责组织团队来开发平台和应用。但竞标链本身的运营和使用均完全取决并依赖于社区自治，基金会只作为社区内一名普通成员，对竞标链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。

基金会尽力督促FBC 实现其价值回报。但FBC不代表任何现实世界的资产或权利（例如基金会的股份、表决权等）。FBC 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（中国）公民、永久居民或绿卡持有者将不被允许参加 FBC 的公开出售，

故基金会将不会把 FBC 出售给前述对象。

基金会在 FBC 销售中所获的收入，将由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。

竞标链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 FBI Token 来使用其功能，不受地理位置所限。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，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，平台可能会在有些区域无法提供正常的服务。 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。

## **免责声明**

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

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 FBC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 FBC 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 FBC；

1. 由于任何原因 FBC 的公开售卖计划被放弃；

（4） 竞标链 的开发失败或被放弃，以及因此导致的无法交付 FBC；

（5） 竞标链 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） 竞标链 源代码的错误、瑕疵、缺陷或其他问题；

（7） 竞标链 平台或以太坊区块链的故障、崩溃、瘫痪、回滚或硬分叉；

（8） 竞标链 或 FBC 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 竞标链 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 FBC 钱包的私钥）；

（12） FBC 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；

1. 任何人对 FBC 的交易或投机行为；

（15） FBC 在任何交易所的上市或退市；

（16） FBC 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；

1. 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

## **风险声明**

竞标链 基金会相信，在 竞标链 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 竞标链 基金会的控制。除本白皮书所述的其他内容外，每个 FBC 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 FBC 的购买者应特别注意这一事实：尽管 竞标链 基金会是在 设立的，但 竞标链 和 FBC 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 FBC 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 竞标链 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，竞标链 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 竞标链 最新的关键信息，其并不绝对完整，且仍会被 竞标链 基金会为了特定目的而不时进行调整和更新。竞标链 基金会无能力且无义务随时告知参与者 竞标链 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 竞标链 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。竞标链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、竞标链 开发或 FBC 的行动。竞标链 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 竞标链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，FBC 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，FBC 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 竞标链）带来危险。这可能导致任何人持有的 FBC 被盗、失窃、消失、毁灭或贬值。在合理范围内，竞标链基金会将自我准备采取预防或补救措施，升级 竞标链 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，竞标链 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

竞标链 仍在开发阶段，而非已准备就绪随时发布的成品。由于竞标链 系统的技术复杂性，竞标链 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，竞标链 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 FBC 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 竞标链 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 竞标链 基金会为 竞标链 开发提供资金的能力。尽管 竞标链 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 竞标链 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 竞标链 的可用性、稳定性和/或安全性，并因此对 FBC 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。

竞标链 基金会将与紧密 竞标链 社区紧密合作，今后持续改进、优化和完善 竞标链 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。竞标链 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 竞标链 初始时是由 竞标链 基金会所开发，但它并非由竞标链 基金会所有拥有、运营或控制。自发形成的 竞标链 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、FBC 持有人和其他参与者组成，这些人大都与竞标链 基金会无任何关系。就 竞标链 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 竞标链 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 竞标链 的诞生做出过努力和贡献。因此，竞标链 在发布之后，其如何治理乃至进化将并不受到 竞标链 基金会的支配。

（9） 源代码升级

竞标链 的源代码是开源的且可能被 竞标链 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 竞标链 的运行或 FBC 的价值造成

重大不利影响。

（10） 安全弱点

竞标链 区块链基于开源软件并且是无准入许可的分布式账本。尽管竞标链 基金会努力维护 竞标链 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 竞标链 的核心基础设施要素之中，对这些弱点或缺陷 竞标链 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 FBC 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 竞标链 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

竞标链 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 竞标链 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 FBC 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 竞标链 的可使用性、稳定性和安全性以及 FBC 的价值。

（13） 未经授权认领待售 FBC

任何通过解密或破解 FBC 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 FBC 购买者所购买的待售FBC。据此，购买者所购买的待售 FBC 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 FBC 的任何人士，而这种发送是不可撤销、不可逆转的。每一 FBC 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） FBC 钱包私钥

获取 FBC 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 FBC 钱包拥有唯一的公钥和私钥才可以操控 FBC。每一购买者应当妥善保管其 FBC 钱包私钥。若 FBC 购买者的该等私钥丢失、遗失、泄露、毁损或被盗，竞标链 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 FBC。

（15） 通胀

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

（16） 普及度

FBC 的价值很大程度上取决于 竞标链 平台的普及度。竞标链 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，竞标链 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 FBC 需求可能具有投机性质。缺乏用户可能导

致 FBC 市场价格波动增大从而影响 竞标链 的长期发展。出现这种价格波动时，竞标链 基金会不会（也没有责任）稳定或影响 FBC 的

市场价格。

（17） 流动性

FBC 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。FBC 在市场上的流通和交易并不是 竞标链 基金会的职责或追求。FBC 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 FBC 持有者处兑换或购买任何 FBC，也没有任何人士能够在任何程度上保证

任何时刻 FBC 的流通性或市场价格。FBC 持有者若要转让 FBC，该FBC 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 FBC 供公开交易。

1. 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 FBC 交易的二级市场，竞标链 基金会对任何二级市场的 FBC 交易不承担责任。因此，竞标链 基金会没有义务稳定 FBC 的价格波动，且对此也并不关心。FBC 交易价格所涉风险需由 FBC 交易者自行承担。

（19） 竞争

竞标链 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 竞标链 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 竞标链 竞争，或甚至赶超或取代 竞标链。竞标链 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 竞标链 产生竞争关系。竞标链 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 竞标链 竞争或取代 竞标链 的竞争性努力。