

竞标技术白皮书

V0.5（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 |  |
|  |  |  |  |  |
|  |  |  |  |  |

# 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

# 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，911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，并有平台提供指导。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合约必定有广泛的应用场景。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。

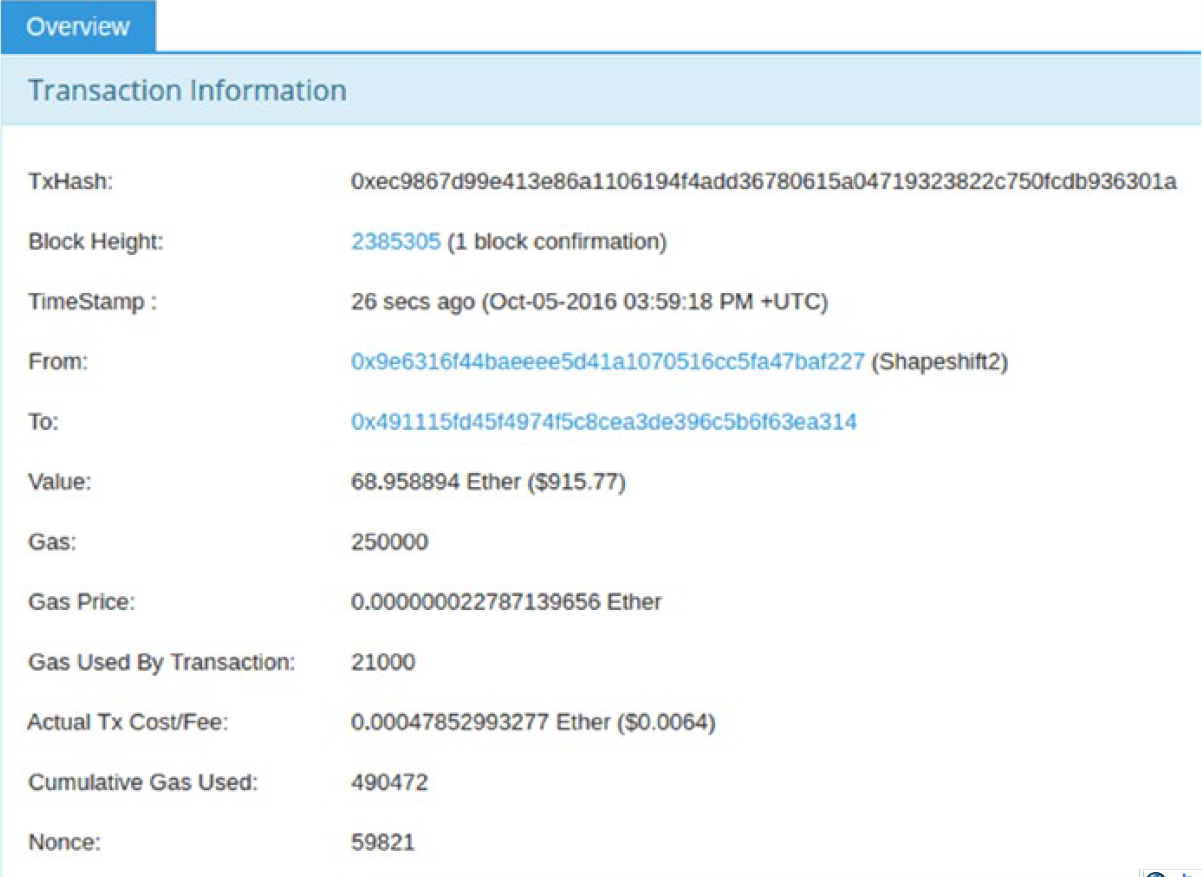
## 随机数生成

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。

## 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，可以通过以下工具查看：

* <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）

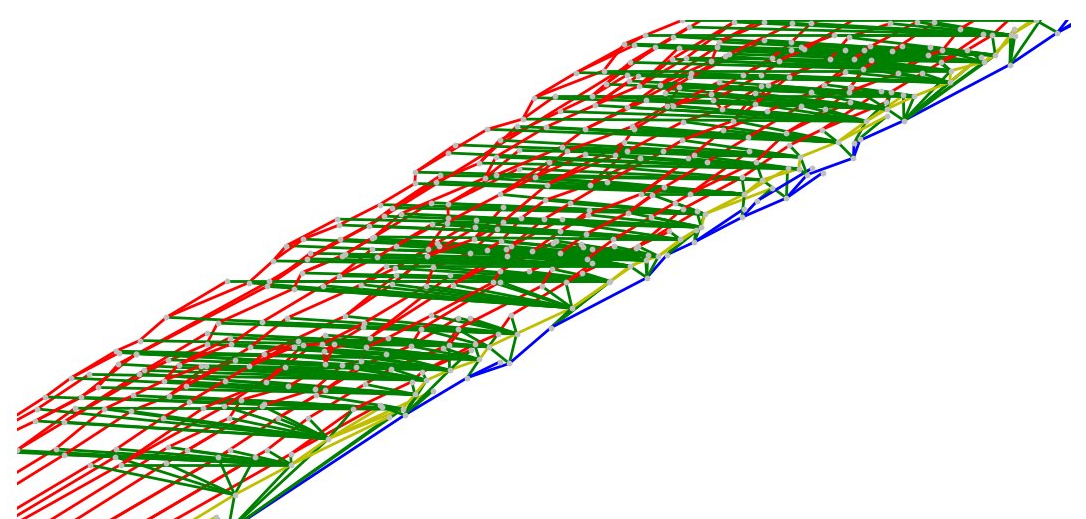
竞标链可以接入第三方信息中介（Oracle），项目的结果由Oracle来决定。这些Oracle提供了一系列的API，竞标链通过调用这些Oracle API来决定项目的中标方。Oracle可以是中心化的，也可以是多中心化的。

### 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。

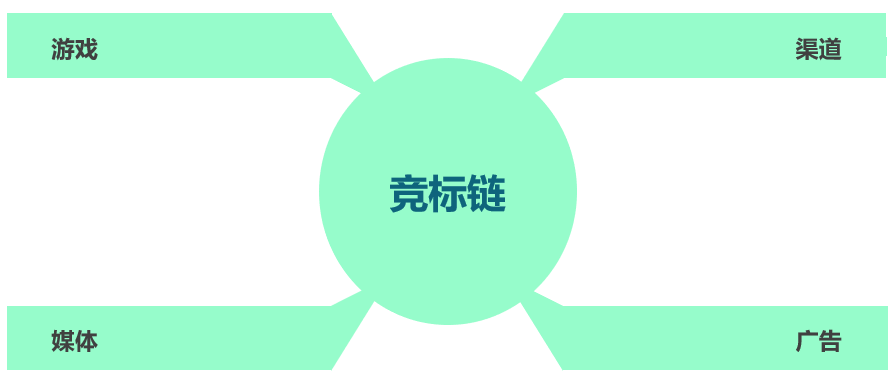
### 以太坊技术的未来可扩展性

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。



### 未来的应用场景

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：



# 通证机制

# 社群组织

# 免责