

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一元购技术平台的选择。

* 以太坊自诞生以来，到现在已经是一个成熟的基础设施应用。

已经有很多的Dapps在以太坊上面运行。比如其中最著名的以太猫。这充分证明了以太坊的健壮性和可编程性能。相对于其他的公链，具有无可比拟的优势

* 以太坊已经拥有了一个庞大的P2P节点网络，和矿工人群。

由于以太坊已经建设成功了庞大的社区群，可以很轻松的抵御51%攻击和双花攻击。让一元购平台聚焦在实现商业逻辑，而不用花大力气，大成本在建立公链，和保护公链免受攻击上。

* 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。

* 技术方向

最现实的方向改变就是Vitalik主导的POS改造。如果Vitalik的POS改造确定发生并且被社区接受，对现有以太坊上运行的Dapps会造成什么样的影响，尚不确定。

* 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

低成本，参与自由

# 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

所有想参与一元购的用户，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，投资某个特定的活动（从技术上来说，就是一个智能合约）。

* ERC20代币合约

所有参与一元购活动的用户必须通过购买平台的代币实现。当然，相应利益的获取也会以代币的形式获取。

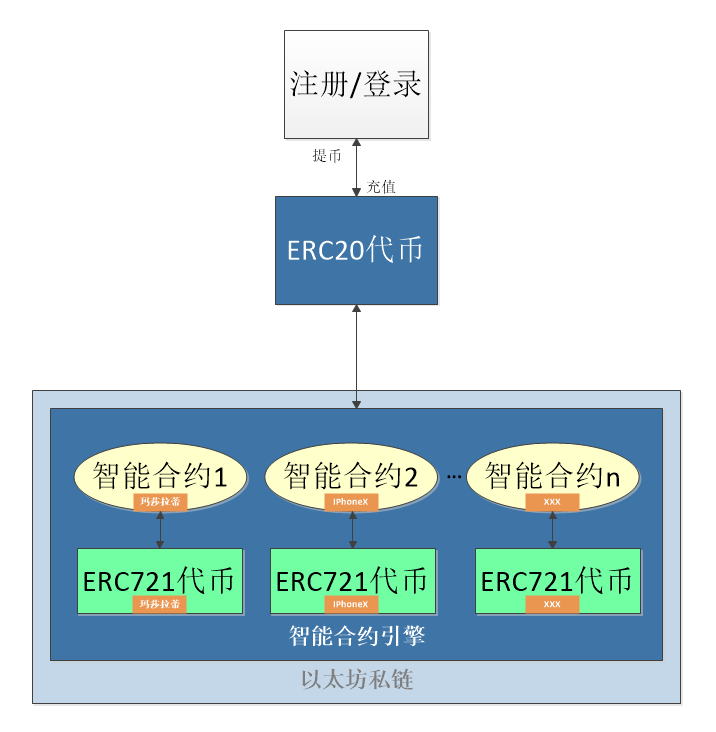
* 智能合约的引擎

每次一元购的活动，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

每次一元购的活动，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。

* 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。

### 项目发起方

### 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

项目验证方可以通过系统提供的浏览器

## 系统模块

### 身份验证系统

注册登录模块主要的功能是给每个参加一元购活动的用户分配以太坊地址。此功能的目的就是为用户提供傻瓜式服务，获取参与一元购活动的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

* 如果用户已经拥有以太坊公钥/私钥对，可以略过这一步

## ERC20代币合约

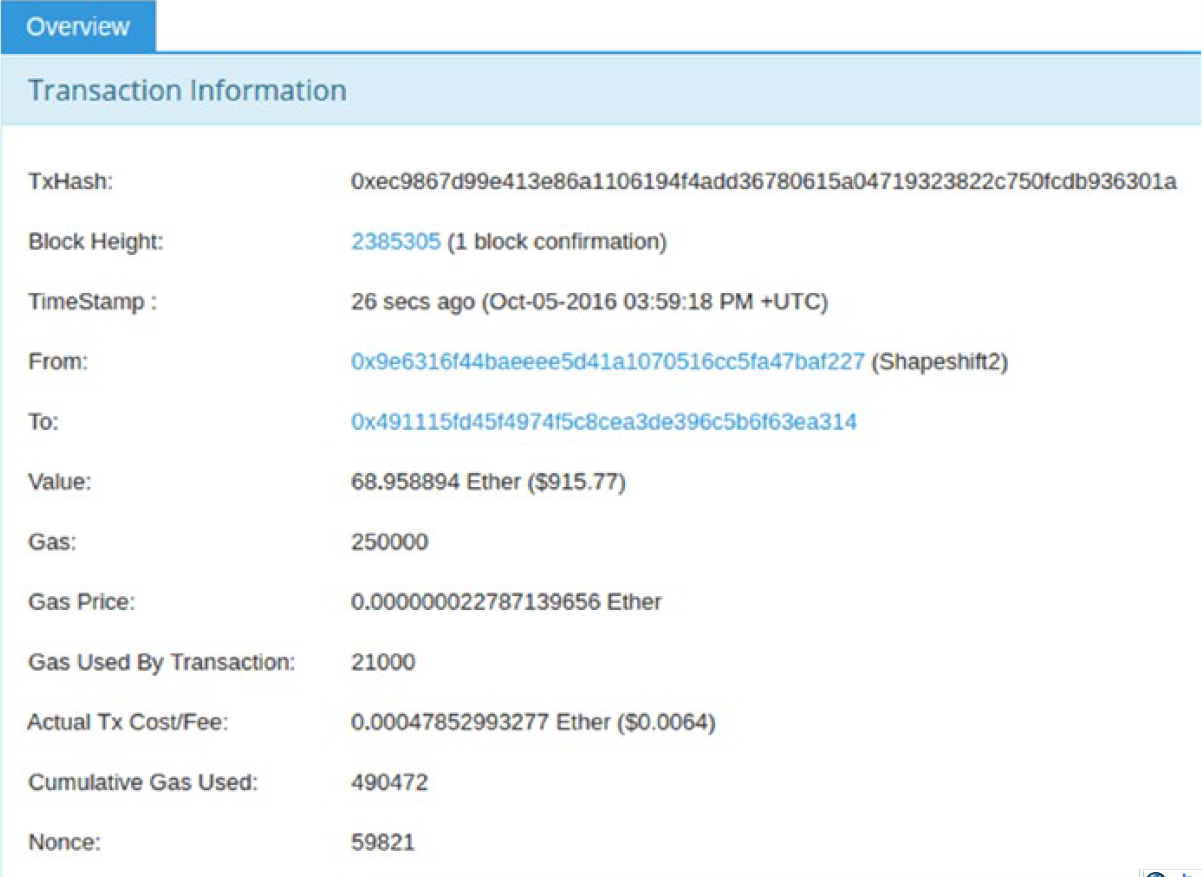
竞标链会发行一种基于以太坊智能合约的、符合ERC20标准（以太坊令牌：允许钱包、交易所和其他智能合约以一种常见的方式对接各种代币）的代币FBC（Fair Bid Coin）。FBC是竞标链在正式上线运行时发行的，由智能合约生成的。竞标链用户对发布在竞标链上任何一个项目作出预测时，只能而且必须使用FBC去操作：发起项目，竞标项目以及验证项目

## 抽奖智能合约

对于每一次一元购活动，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以太坊公链上。所有的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

下面是一个在以太坊公链上查询交易的截图：



鉴于现在交易费用(Gas)高企，而且在EVM里使用持久化存储都需要付Gas，建议使用尽量简单的，尽量随机的算法。

## 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。本文介绍的ERC721标准基于最新(2018/03/23官方提议。

那怎么理解**非同质**代币呢?

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。

### ERC721标准

ERC721最为一个合约标准，提供了在实现ERC721代币时必须要遵守的协议，要求每个ERC721标准合约需要实现ERC721及ERC165接口，

## 随机

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。

## 以太坊区块链浏览器

后补（寻找开源的以太坊区块链浏览器）

## 扩展性

### 预言机（Oracle）

竞标链项目的结果可以由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。

用第三方信息中介（Oracle）自动判断预测结果，以保证决策

过程的效率。与Gnosis的集中式信息中介（Oracle）解决方案不同的是，Bodhi使BOT币持

有者能够接管投票过程，并在发生信息中介（Oracle）故障时做出预测事件的最终决定

### 合约模板助手

### 以太坊技术的未来可扩展性

### 未来的应用场景



# 通证机制

# 社群组织

# 免责