**最新以太坊|以太坊命名空间拍卖**

Maurelian 2017.3.13

本文旨在通告以太坊社区并征求反馈意见。我们欢迎所有的问题和意见，并且根据这些问题建议来更新后续的FAQ。本文的第一部分单纯阐述了我们的动机，如果你只是想了解具体的细节，那么可以直接跳到**“名称所有权”**的章节。

**更新：上述FAQ请点击[这里](https://github.com/ethereum/ens/wiki/Frequently-Asked-Questions)**

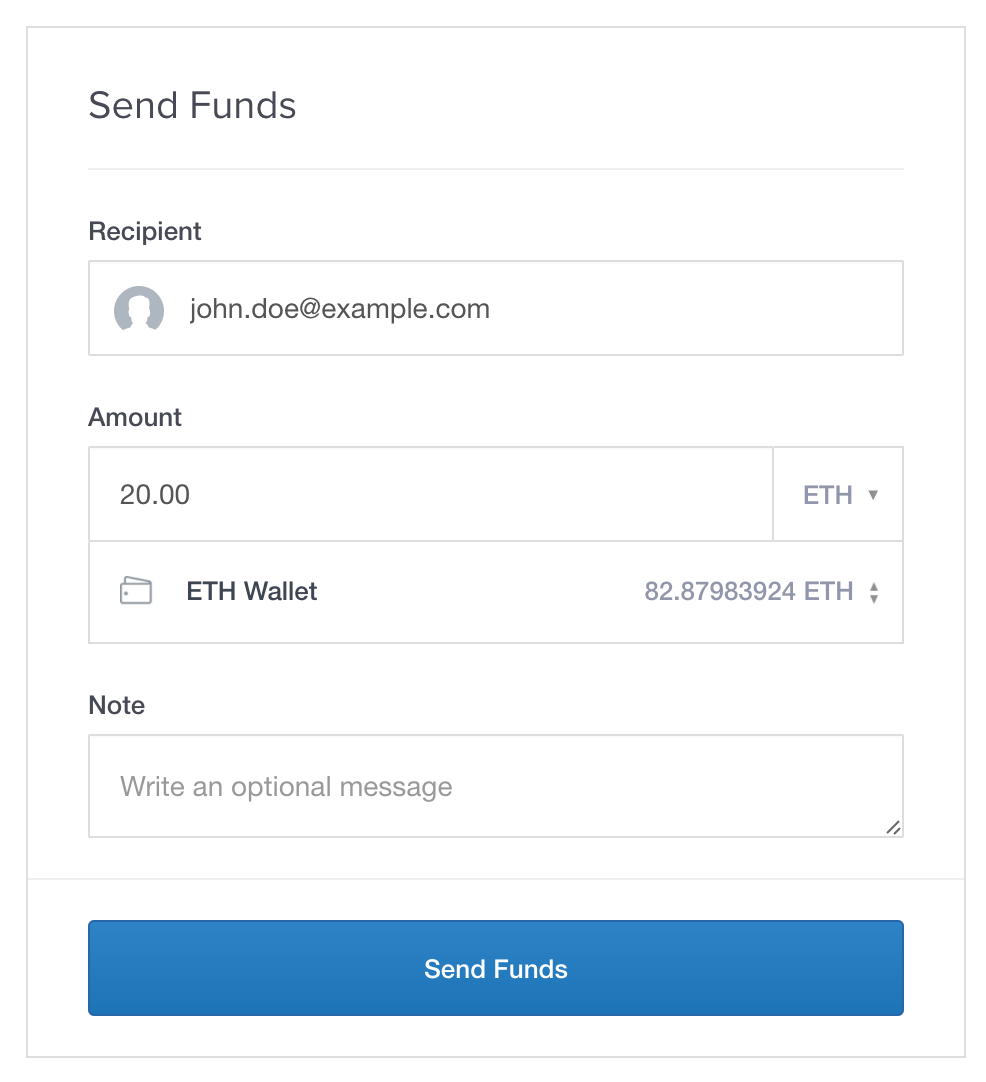
**以太坊的地址是灵活使用的阻碍**



欢迎来到以太坊，这是你的姓名标签

想必阅读本文的每一位读者对经典的加密货币地址都了如指掌，甚至可能把他们视为理所当然。然而，对于一般人而言，通过获取属于自己的160位十六进制哈希编码字符串来登陆并不令人满意。

跟 Coinbase，Circle，Paypal或者Venmo比较一下；你只需要用收款方的邮箱地址或者他们的用户名就能够实现转账。



 Easy（简单）

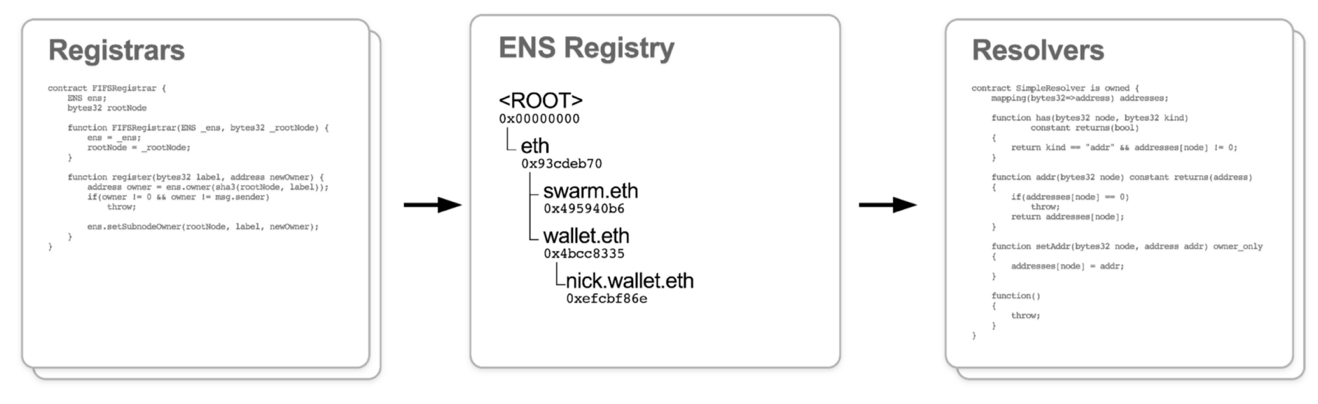
现在我们来想像一下：我们给他人转账或者转交合约就像在Mist或者其它以太坊服务一样简单——我们不需要依靠中心化的服务商来建立名字与地址间的联系。

**以太坊名称服务如何解决地址问题呢？**

以太坊名称服务（在[EIP-137](https://github.com/ethereum/EIPs/issues/137)中有概述）使以太坊得以使用可供人类理解的的名称。它会自动在Mist钱包中进行名称注册。当然，后续我们希望能兼容更多的服务提供商。

以太坊名称服务（ENS）中的名称看起来就跟我们今天广泛使用的DNS地址一样。一开始，它只支持“**.eth**”作为顶级域名（top level domain,TLD）。比方说，你在浏览“www.example.com” 这个网站时，你可以把资金发送到“wallet.example.eth”。

从更高层次来看，ENS包含3种独特类型的合约：



基于Nick Johnson在[Devcon2的演示](https://www.youtube.com/watch?v=pLDDbCZXvTE)

**1. 注册合约**（The Registry contract）是ENS的核心，并且只有一份。它是一个简单的合约，只是单纯地把注册名称映射到名称拥有者的地址，以及解析方合约（见下）的地址。

**2. 解析方合约**（Resolver contracts）将名称映射到一个诸如以太坊地址、Swarm或IPFS哈希值的“资源文件（resource）”。当你说你想要汇款到wallet.example.eth的时候，Mist会从这个合约调用相应的地址。只有名称的拥有者才能更新解析方（resolver）的记录。

**3. 注册方合约**（Registrar contracts）在ENS注册合约（ENS registry）中拥有自己的域名，并且负责在他们所控制的命名空间内分配子域名。第一位ENS注册方将会是ENS中“.eth”顶级域名的所有者。

**设计注册方的挑战**

注册方合约和解析方合约都十分简洁。如果你拥有一个名称，你可以把它们的记录更新为那个名称；否则，它们就忽视你。另一方面，设计一个注册方并不容易，因为它涉及到诸如用户体验、机制设计、公平性以及管理等诸多主观因素。

在命名空间中，每一个名称只能够对应一位拥有者。也就是说，它具有稀有且不可替代的性质。此外，这些名称（通常）用单词构成。这是一个强大的象征：它们可以代表一个品牌，一个动作或者你在多个平台的在线身份。因此，人们自然而然对某些具体名称的拥有权具有权利意识。

与此同时，终端用户在查找一些常用、知名度高的名称时常常会认为这些名称属于他们所能联想到的个体或组织。谁应该控制诸如“**microsoft.eth**”，“**bankofamerica.eth**”或者“**vitalik.eth**”这样的名称？注册方应该如何分配这些名称？这些名称的分配应该完全交由市场驱动还是应该是一个争议解决的过程？

经过大量的讨论，我们选择的名称分配策略是在两者之间折中:

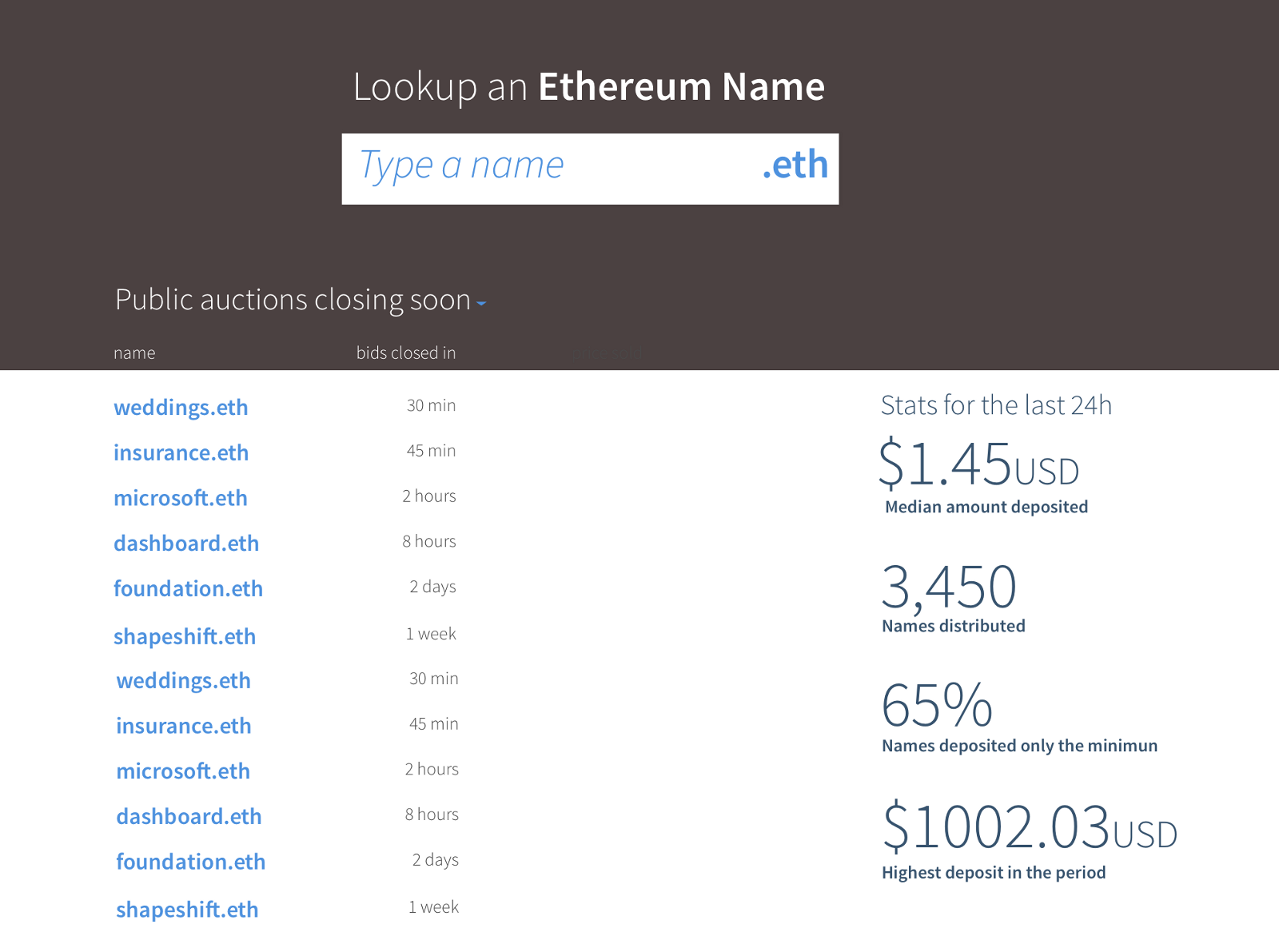
1.一开始，命名空间是有限的，

2.完全市场驱动方式

3.可升级的初始化注册方合约允许在未来引入争议解决过程

本文的剩余部分概述了初始注册方的功能，以及你在注册名称的时候需要了解的事项。我会指出在初始注册方合约接口中的相关函数的名称。如果想要了解所有的接口，请参阅ERC-162以及GitHub储存库的完整代码。

未来还会有一个有助于参与的应用程序。你可以在这里查看该应用程序的设计模型（mockups）。



**名称的拥有权**

名称将会根据下述过程进行拍卖。拍卖胜出方所支付的金额会被锁定在契约中用来交换名称的拥有权。拥有者不需要支付经常性费用或者通过订阅的方式来拥有该名称。在名称注册期满1年后，名称的注册者可以自由选择是否要释放该名称。一旦他们选择了释放，那么契约中锁定的金额将全额返还。

**注册并不保证永久所有权**

初始的注册方并不包括任何争端解决程序。但是，后来继承的永久注册方可能会引入某种形式的争端解决方案。对于如何在未来解决纠纷，我们有很多选择；而新的解决方案肯定会在ENS推出以后提出。

我们来阐述一个可能的方式。比方说，我们可能会要求域名的拥有者周期性地根据所有域名的价值的平均增加金额来调整在契约中锁定的金额。这种方法可能会增加名称被撤回的可能性。一旦这种情况发生，那么该名称拥有者**在契约中锁定的资金将全额返还**。此外，还有可能人们并不认为争议解决是有益的，并且永久注册方引入的变化是极小的——它仅受限于拍卖过程的微小变化。

**名称转让**

名称的拥有者可以随时沿着被锁定在相关契约的资金（以太币）将名称转让给另一账户。这种方式会促使二级市场的行程，并为该名称在拥有者手中达到最大利用率提供了一条理想的途径。

**初始注册方的服务时间表**

我们计划在2017年的第一季度发布以太坊名称服务（包括初始的注册方）。

**升级**

基金会将于应用发布1年后开始接受关于永久注册方的建议。最初的注册方预计将在应用发布后两年内被替换。

在最初的注册方处登记的名称的拥有者将负责把他们的契约转移到永久注册方处。我们目前所考虑到的过渡管理办法包括：

1.要求拥有者在截止日期之前转移他们的所有权以便自身保持所有权以及/或者延续名称解析服务。

2.如果永久注册方遗失了某一条目，它要询问初始的注册方来确认拥有者的身份。

**最后期限**

下列事件以及时间将会硬编码进合约中：

**1. 4年以后，初始的注册方将拒绝登记新的名称。**

**2. 8年以后，由初始注册方保管的资金将不能被拥有者释放，并且该资金不可返还。**

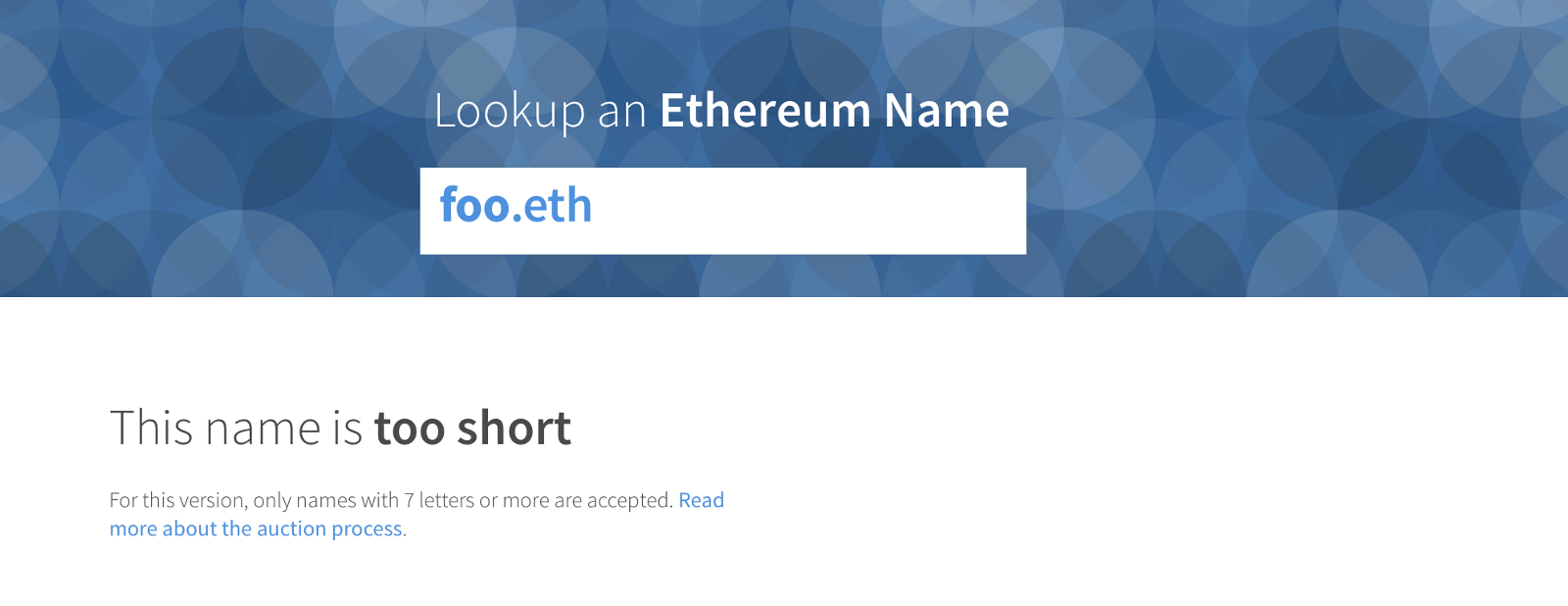
跟以太坊的难度炸弹一样，这些强制性的日期将迫使后续行为以及过程基于永久注册方发生。

**名称限制**

唯一可用的顶级域名就是“**.eth**”。子域名将会被进一步限制在7个或以上的字母。比方说：

1.“**microsoft.eth**”**有效**

2.“**google.eth**”**无效**

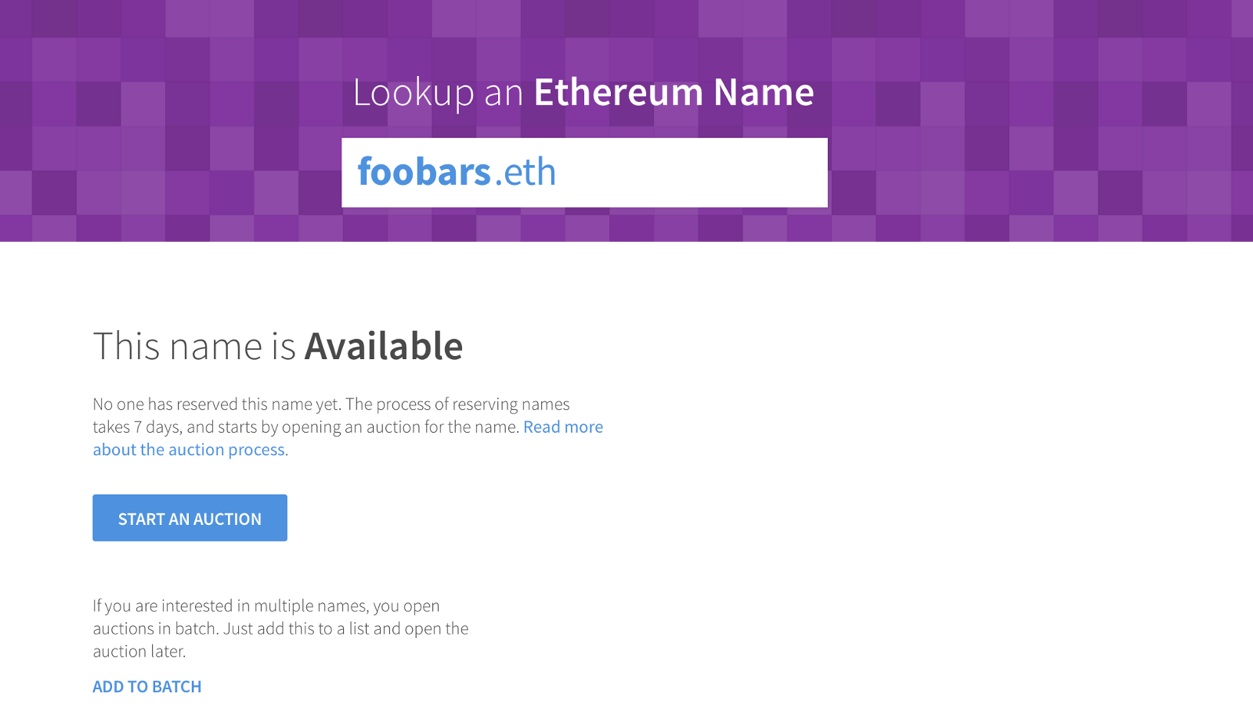


需要注意的是，注册名称的子域名没有任何限制。因此， “**microsoft.eth**”拥有者可以直接注册“**foo.microsoft.eth**”——无论这个名称看起来怎么样。

这些限制规则为拥有更好的名称分配方式的永久注册者保留了最短的名称（这些名称通常很稀有，并且极具价值）。

**初始注册方拍卖过程**

任何人都可以通过调用注册方的**startAuction()**函数来对他们感兴趣的名称进行拍卖。



初始的注册方会以Vickrey拍卖（维克瑞拍卖,也称为第二价格密封拍卖，译者注）的形式来拍卖名称。所有的竞价都会在一个“密封的信封中”提交。竞价最高的胜出方将赢得拍卖并以次高竞价来支付金额。这一形式以经济激励的方式促使竞争者为名称背后的价值而竞价。

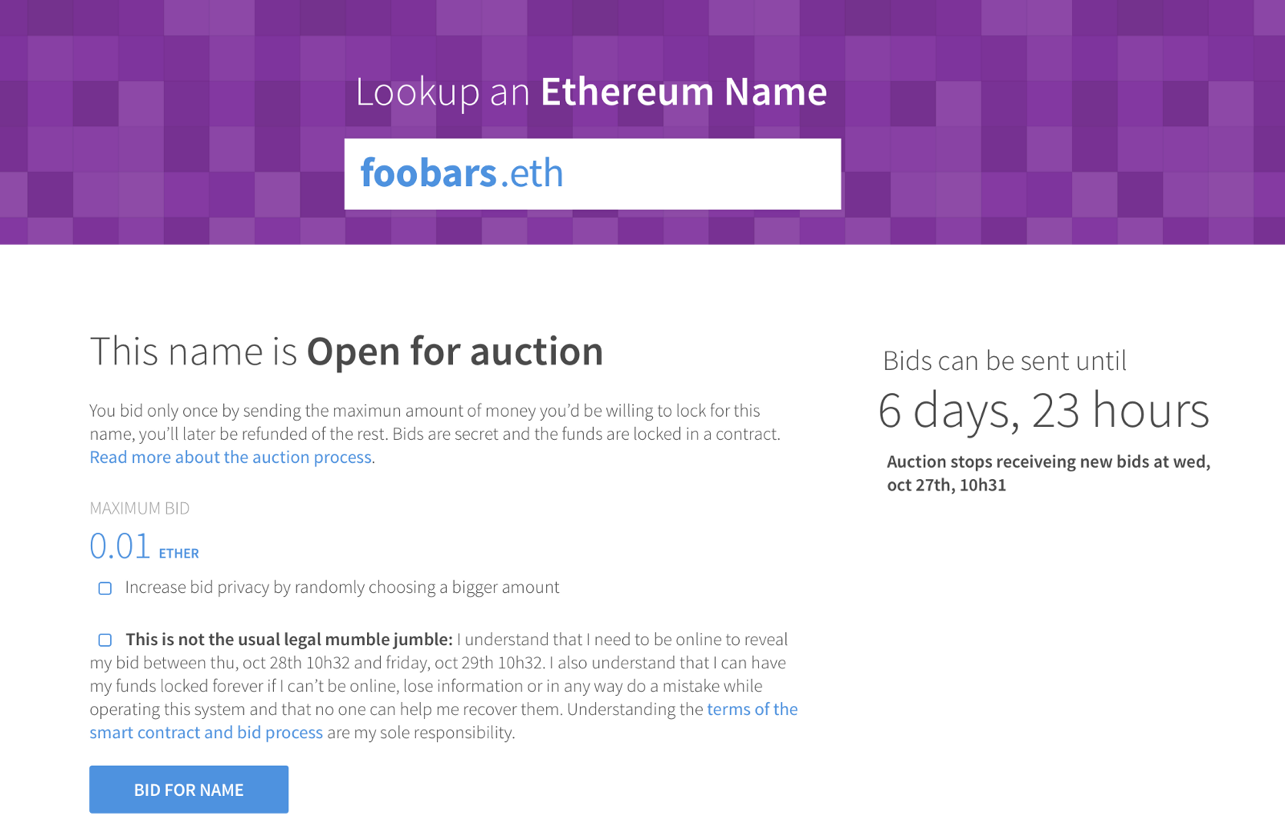
竞价的参数为：

1.一个名称，

2.一个值（用ETH金额表示）。表示你愿意为该名称的拥有权支付的价格。

3.最终拥有该名字的地址。

这些参数将被散布以及哈希编码（通过使用**shaBid()**），并附上ETH的支付金额（通过使用**newBid()**）发送给注册方。对这些参数进行哈希编码处理使得人们不能辨别每笔投标的对象。



**最低价格**

注册某一特定名称的最低价格是**0.01 ETH**。如果没有人跟你竞价，那么这就是你最终支付的金额。

**拍卖持续时间**

在常规的注册操作中，拍卖通常会持续7天。为了让人们有足够的时间来准备竞价，所有在注册方服务时间的前3周开始的拍卖都会延长到第4周的结束。

**揭示期**

拍卖的最后48小时就是揭示期。在这时，投标者必须要提交各自投标的参数（通过使用**unsealBid()**）。新的投标者在揭示期不被接纳。

在揭示期后揭示的竞价将会失效，并且其锁定在契约中的金额将被没收。

在揭示期过后，竞价的胜出者将成为该名称的拥有者（通过使用**finalizeAuction()**）。

如果出现两位投标者竞价数目相等的情况下，最先揭示的那一位胜出。

**招标成本**

没有胜出的投标者将返还99.9%的投标金额。剩下的0.1%将被消耗。这种方法会使对大量名称竞价或者对高价名称竞价的行为产生实际成本。】

**其它资源**

1.Nick Johnson在Devcon2的演讲和幻灯片

2.拍卖应用程序的模型

3.用LLL执行的ENS

4.ERC 137：以太坊名称服务说明书

5.ERC 162:对注册方进行哈希编码的说明书

感谢Nick Johnson,Alex Van de Sande提出建议并编写ENS的合约。同样感谢Nick,Alex,Jorge and Edu在阅读本文以后提出的反馈。