链滴

Handshake 入门笔记

作者：88250

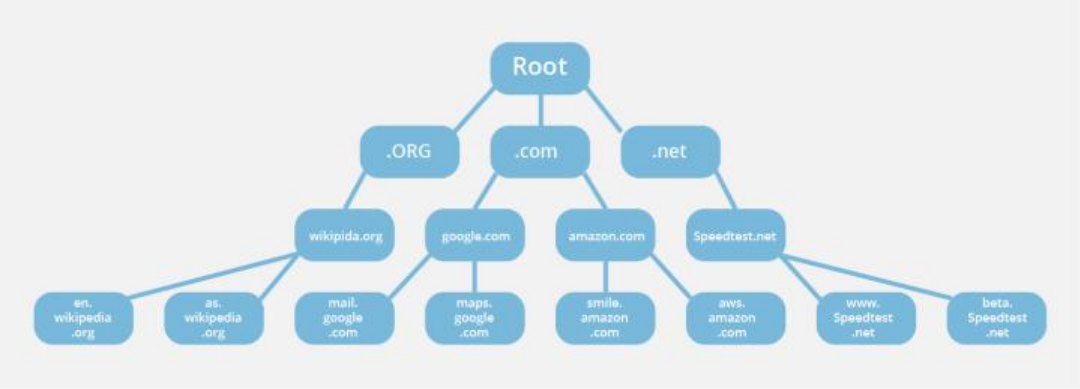
原文链接：https://ld246.com/article/1582353370023

来源网站：链滴

现有 DNS 存在的问题

Handshake 的存在是为了改进现有 DNS 存在的问题：

● **ICANN 作为顶级域名（Top-Level Domain, TLD）管理机构是中心化的。**所谓的 TLD 即我们熟的 org、com、net 等域名后缀部分，现有完整的列表见此。如果需要申请新的顶级域名需要交纳大约 $18.5W，申请不一定能过，这意味着顶级域名是人为控制的稀缺资源



● **容易被审查以及泄露隐私**，即使域名注册商提供了 WHOIS 保护，但实际上注册域名时提供的信息然是可以被审查的。另外，网络服务提供商甚至会通过出售用户个人 Web 浏览历史记录 DNS 解析据来获利

● **证书颁发机构系统存在固有缺陷**，证书颁发机构是中心化的，会因为滥发证书或者被某种力量用于量审查，这破坏了 SSL 本身的安全性，对用户个人造成风险

● **不提供真正的域名所有权**，域名需要续费才能保证所有权，并且费用是域名提供商单方面决定的。其实是域名租赁，没有提供真正的域名所有权给用户

Handshake 是什么

Handshake 是一种基于 UTXO 区块链的域名解析协议，兼容现有的 DNS。它不能完整替代现有 DN，但能通过基于区块链的机制替代根域名服务。官方的全节点代码源自 bcoin（JavaScript 实现的 BT）。

每一个加入到 Handshake 网络中的对等节点负责验证和管理根域，同时也就不需要证书颁发机构了域名将被记录在 Handshake 区块链上，每一个人都有权添加自己的域名。

已有的 TLDs 作为保留域名不允许在 Handshake 上注册，如果用户请求传统域名（比如 namebase.io 时将走现有的 DNS 进行解析；如果用户请求域名（比如 namebase/）将走 Handshake 解析。

综上，Handshake 主要解决了现有 DNS 的这些问题：

● **无限可注册的顶级域名**，任何人都可以注册顶级域名，比如可注册类似传统的 satoshi.nakamoto/ 或者独立的顶级域名 satoshi/

● **更安全和隐秘**，DNS 记录只有所有者能够修改，这保证了域名指向不会被审查或者恶意重定向。册域名时无需提供个人信息，只需提供公钥即可

● **更安全地替代证书颁发机构**，Handshake 移除了原有对 CA 的依赖，因为使用 Handshake 后就再需要通过 CA 证书验证域名所有权了

● **域名所有者的自主权更多**，域名所有者可以用自己拥有的 TLD 干很多事情，除了伺服网站，早期有者甚至可以成为域名提供商来售卖域名，比如将 creator/ 的所有者可以售卖 adam.creator、john.creator 给其他用户

Handshake 代币 HNS

Handshake 代币简称 HNS，用于注册、更新和转移域名。同时也有助于防止对 Handshake 网络发垃圾内容攻击。HNS 的 2/3 已经对免费软件和开源社区贡献者空投。

用户可以在 Namebase 上管理钱包和交易。目前已经支持通过 BTC 买卖 HNS，HNS 持有者可参与拍域名。namebase 在 Handshake 每周会上架一些域名用于竞拍，竞拍域名的产生机制暂不明晰。

如何获得 HNS

如果你在 2020 年 2 月 4 日前，在 GitHub 上超过 15 个粉丝并且绑定了 SSH 公钥和 PGP 的话，就以参与空投来获得 **4,246.994314** 个 HNS。具体操作方式可参考官方的空投项目。我个人的操作方是通过阿里云临时拉起一台海外节点，然后安装 Git、Node 环境来参与，因为国内访问 GitHub 实太慢了，而验证所需的数据都是从 GitHub 上下载的。

如果你不是开源项目贡献者，可以选择在 Namebase 上通过 BTC 购买 HNS。如果你是加密货币爱者，可以试着买卖，普通用户不建议涉足交易。另外，也可以通过挖矿获得，可以参考石榴矿池上的程搭建。我在自己笔记本上挖了大概 2 个小时，收益 0.36 个 HNS：

挖矿账户	Handshake 算力	矿工状态			Handshake 收益			
矿工	当前算力	在线	离线	在线率	总收益	已支付	账户余额	未成熟
shenzhou	0.0H/s	0	1	0.00%	0.3627 HNS	0.0000 HNS	0.0144 HNS	0.3484 HNS

哪些域名可以买到

Handshake 保留了两种域名：

- 现有的 TLDs，比如 org、com 和 net 这类
- Alexa 排名前 10W 的

原文链接：Handshake 入门笔记

主要是为了避免滥用注册同时保护现有知名站点的权益。除此以外的域名都可以购买，可以在 Namebase 上搜索你想要的域名，并关注何时可以开始竞拍。

现阶段如何使用

应用场景的落地对于区块链项目来说是最为关键的。已经有爱好者通过浏览器插件来支持 Handshake 域名解析了。

看了下代码，大致是通过拦截代理请求实现的：

1. 识别请求 URL 是否为 Handshake 域名（用 / 结尾的非现有 TLDs）
2. 通过 https://namebase.now.sh/resolve 接口解析域名为目标 IP
3. 代理请求到目标 IP

now.sh 上的服务比较慢，可以考虑自己搭建服务端。相关项目的依赖关系：

浏览器插件 -> 服务端 -> hdns -> bns，bns 实现了传统 DNS 解析（附带一提，bns 和 marked 的创是同一个人）。hdns 在中间通过设置 Handshake 域名解析服务器来实现代理链上解析：

```
const HANDSHAKE_NS = [
  'aoihqqagbhzz6wxg43itefqvmgda4uwtky362p22kbimcyg5fdp54@172.104.214.189',
  'ajk57wutnhfdzvqwqrgab3wwh4wxoqgnkz4avbln54pgj5jwefcts@172.104.177.177',
  'akimcha5bck7s344dmge6k3agtxd2txi6x4qzg3mo26spvf5bjol2@74.207.247.120'
];
```

客观来说，现阶段该浏览器插件的实现路线可以看作是“换汤不换药”，因为实际上依然走的是传统域名解析，由这几个 IP 代理返回链上结果。不过对于用户来说似乎也只能如此，毕竟不可能每个用都搭建一个全节点。

参考资料

- Handshake
- Namebase