第2卷 第5期 2020年10月
Vol.2 No.5 Oct.2020

ISSN 2096-742X
CN 10-1649/TP

文献DOI：
10.11871/jfdc.issn.2096-742X.2020.05.006

文献PID：
21.86101.2/jfdc.2096-742X.2020.05.006

页码：52-64

开放科学标识码（OSID）

基于区块链的网络空间标识服务

张曼，李洪涛，董科军，延志伟*

中国互联网络信息中心，北京 100190

摘　要：【目的】本文主要根据当前网络发展存在的问题及基于区块链的网络空间标识系统的关键技术等方面展开介绍，为后续相关工作的开展提供参考。【方法】本文梳理了基于区块链的网络空间标识系统的研究现状，介绍了Namecoin、Blockstack、Handshake、Ethereum Name Service等几种系统的设计架构、技术方案，并对不同项目进行了对比分析。【结果】相较于现有DNS系统，基于区块链的网络空间标识实现了安全平等、抗审查的网络基础架构，并且在数字认证、全球统一身份标识等领域积极探索展开合作，得到了一定程度的应用。【结论】基于区块链的网络空间标识服务为未来网络基础资源发展提供了一种新的思路与趋势，同时也面临着如何处理与现有系统的关系及广泛推广等问题。

关键词：网络空间标识；区块链；Namecoin；BNS；Handshake；ENS

Cyberspace Identification Service Based on Blockchain

Zhang Man, Li Hongtao, Dong Kejun, Yan Zhiwei*

China Internet Network Information Center, Beijing 100190, China

Abstract: **[Objective]** This paper mainly introduces problems of current network development and key technologies of the blockchain-based cyberspace identification system. It aims to provide a reference for the subsequent works. **[Methods]** This paper analyzes the current research status of the blockchain-based network identification system, introduces the architecture designs and technical solutions of the systems such as Namecoin, Blockstack, Handshake, Ethereum Name Service, and compares different projects. **[Results]** Compared with the existing DNS systems, the blockchain-based cyberspace identification has realized a secure, distributed, decentralized, and censorship-resistant network infrastructure. It is also used in active exploration and cooperation in the field of digital authentication and global unified identification, and has got a certain degree of application. **[Conclusions]** The blockchain-based network identification service provides a new idea and represents a trend for the development of basic network resources in the future. There are still several problems that need to be solved, such as, how to deal with the relationship with the existing systems and how to extend the application of the system widely.

Keywords: network identification; blockchain; Namecoin; BNS; Handshake; ENS

基金项目：北京市科技新星计划项目（Z191100001119113）
* 通讯作者（E-mail: yanzhiwei@cnnic.cn）

引　言

互联网的发展经历了不同的阶段，最初的 Web 1.0 时期用户只能进行网页浏览，只有少数的技术人员才具备在网络上发布内容的资质；然后到 Web 2.0 阶段网络已能提供丰富的内容管理与交互方式，每个用户都能成为网络内容的发布者，在应用场景上涵盖了社交、购物、点评等各个方面，内容形式也更加多样化，包括文本图像音视频等 [1]。但是发展至今，当前网络依然存在一些问题，比如因安全与隐私漏洞导致的数据泄露丢失、网络审查、非法网站攻击等。Web 3.0 致力于更好的解决这些问题，在去中心化、语义理解、人工智能、多维度空间等方面构建新一代网络 [2]。

网络空间标识是互联网的基础资源架构，关系着互联网的安全稳定和良好可用性。全球范围内构建起的 DNS 系统负责将可读性强的域名地址转化为枯燥难记的 IP 地址，是保障互联网正常访问的基石；另一方面由于 DNS 的特殊地位致使其很容易成为网络攻击的目标，存在着安全隐私隐患。当前的 DNS 层次结构中，顶部是由互联网名称与数字地址分配机构（The Internet Corporation for Assigned Names and Numbers，ICANN）管理的根区域，ICANN 将根域分配给政府、机构和像 Verisign 这样的营利性公司进行管理，如注册 .com 域名需要向 ICANN 和 Verisign 支付一定金额的费用。域名系统的根区文件由互联网数字分配机构（The Internet Assigned Numbers Authority，IANA）管理，更新区文件内容需要向 IANA 提出申请，极端情况其可以直接修改或者删除区文件的内容。

当前数字认证体系建立在受信任的第三方之上，通信时为防止消息被第三方窃取，需要验证对方身份，数字证书由证书颁发机构颁发，根证书由全球权威的几家公司颁发，作为整个架构的信任锚。

网络中不同的网站与应用往往使用各自独立的身份验证体系，从用户自身来说，多个繁琐的账户信息不方便记录和保存，同时存在信息泄露被盗的风险。另一方面，应用的账户管理权限掌握在特定公司手里，其可以随时删除、封锁账户或其发布的内容信息。

因此，当前的互联网在基础架构、认证机制及应用层面仍是一个相对中心化的系统，其建立在对少数权威机构的信任机制之上，容易造成网络攻击和信息泄露，普通用户缺少相应的自主权。

区块链相关技术从最初的数字货币逐渐与其他行业进行融合，在网络基础资源领域也展开了相关的探索与研究，基于区块链的网络空间标识服务最早推出在 2011 年前后，主要利用区块链匿名性，不存在中心节点，网络中各个参与者之间相互制衡来保证安全等技术，致力构建新型网络空间标识方案。

1　研究背景

1.1　DNS

当前 DNS 系统可能存在域名劫持、缓存污染、DDoS 攻击、网络钓鱼等问题 [3]。

域名劫持实现方式分为直接对原始登记信息进行破解修改，以及第三方监听请求，截获响应消息，并将虚假信息回复给请求方，从而使请求映射到恶意 IP 等。

DDoS 通过发送过量的请求完全占据应答方资源（例如包括很多最终验证为无效的分组），或冒充目标方向服务端发送大量请求，进而接收过量的应答导致目标方带宽阻塞。其对应的防治措施包括网络防御带宽扩充、分散业务部署、分组清洗；DNS 响应速率限制技术限制突增请求的响应频率；利用系统监测，日志分析等进行处理等 [4]。

部分 DNS 攻击的实施基础是基于 DNS 未进行响应发送方验证，DNS 安全扩展（Domain Name System Security Extensions，DNSSEC）增加了相应校验，并且检查收到的 DNS 响应信息是否被恶意

修改[5]。DNSSEC 的实现基于非对称加密方法，逐层利用私钥进行签名，并利用 HASH 对比检验消息内容是否经过改动；它以根域名服务器作为信任锚，由上到下逐层构建起信任机制，增加了四类资源记录类型和对应的消息 Header 位来实现上述功能[6]。但是 DNSSEC 并未对 DNS 消息进行加密，同时在广泛部署推广上存在一定的困难。

隐私泄露是 DNS 面临的另一问题，DNS 查询经过各级服务器，基本都是基于 UDP 的明文传输，同时支持抢答，各级服务器和第三方监听者很容易能够获取用户的域名查询行为数据，围绕域名系统的隐私信息挖掘、用户分析等已日益严重。针对以上问题现已提出一系列技术方案（DNSCurve、DNSCrypt、DoT[7]、DoH[8] 等），借助 HTTPS、TLS 等技术对消息进行加密，但部分技术本身或在应用层面仍存在一定的局限性。

1.2 区块链

区块链的关键技术主要包含：共识机制、P2P 网络协议、密码加密签名相关方法、数据结构模型、智能合约，同时其实现包括跨学科设计如经济学原理等。

1.2.1 比特币

比特币各区块间通过哈希指针连接，每一笔交易要指明其来源与输出，并加上发送方的签名[10]。在交易中发送方会说明自己的公钥，网络中的其他节点验证该交易时会拿发送方给出的公钥与当前交易的输入来源对应交易的输出地址进行校验，以确定用户身份合法性。

比特币区块大小限制为 1M，由于交易大小不一，平均每个区块包含大约 2500~3000 个交易[13]。其节点分为全节点和轻节点，全节点保存块头和块体，可以参与挖矿；轻节点只保存块头，负责交易验证。nonce 值是一个 4 字节的随机数值，挖矿过程需要求解符合条件的 nonce 值。

比特币的共识是以最长合法链为准，其他分叉链得不到任何奖励，其引入出块时间不过短，增加区块确认等机制防止非法操作。比特币中分叉包括硬分叉和软分叉，硬分叉会形成分裂；软分叉达到半数以上的更新，正常情况下能够自动进行合并。

比特币随着算力变化不断进行难度调整以维持平均出块时间保持不变（每 2016 个区块调整一次），同时阈值改变限定在上下四倍之内。区块头中 nBits 字段表示 target 的编码版本，验证矿工挖出的区块是否合法时，会检查 nBits 标识的版本编码是否与当前 target 一致。

随着网络整体算力增加，单个个体算力有限很难获得较好的收益，于是出现了矿池机制。矿池管理者收取一定的管理费，挖矿成功后收益在内部成员之间分配，分配规则按照提交给矿主的降低难度后近似有效值的数量。矿池使得算力薄弱的个体矿工能够获得相对稳定的收入，但大型矿池会使得对于区块链的攻击变得更加容易。

1.2.2 以太坊

以太坊出块时间是十几秒，因此会出现较多暂时性分叉，临时分叉过多导致不少矿工投入大量资源却得不到任何奖励，高过时率降低了区块链的安全性，另一方面出现分叉时大型矿池由于资源集中将具有更大的优势（高于其占有的算力比例），因此以太坊引入改进的 GHOST 协议解决上述问题[11]。矿工挖下一个区块时可以把其它分叉上的节点当做 UNCLE 区块加入到自己的区块头中，分叉合并后，挖出 UNCLE 区块的矿工可以获得 7/8 的出块奖励，而主链上的区块因加入 UNCLE 区块可以额外获得 1/32 的出块奖励，每个区块最多可以加入两个 UNCLE 区块。同时七代以内的分叉区块都可以作为 UNCLE 区块获得奖励，每代奖励递减 1/8，而矿工因加入 UNCLE 区块获得的额外奖励不变。这种设计方案可以避免恶意竞争，鼓励出现分叉后尽早合并，同时该奖励只针对于每个分叉上的第一个区块，以

避免分叉攻击等问题 [14]。

以太坊挖矿过程想要限制 ASIC 芯片的使用，在求解算法的设计上突出内存要求，包括一个初始为 16M 的伪随机缓存和 1G 的 DAG 数据集，其大小随时间线性增长，缓存用于轻节点验证，DAG 用于矿工挖矿。缓存数据的生成是基于种子值依次计算哈希得出，DAG 中的每个数据都是某个初始选定的缓存数据经过 256 次迭代处理生成，DAG 数据集生成需要数个小时，每 3 万个区块更新一次。挖矿过程是求解符合难度条件的 nonce 值，获取包含 128 个数的 DAG 数据集随机切片，每次读取的数据位置由上一次位置计算哈希得到，初始数据位置由区块头计算得出；一次读取相邻两个位置的数据，迭代 64 次后将这些数据的哈希值与目标 target 比较，判断是否符合要求。

以太坊 2.0 提出分片、PoS、新虚拟机 eWASM 等技术改进，并将 1.0 到 2.0 的转换划分为 3 个不同的阶段依次进行 [12]：最初阶段将创建一个新的 Beacon 链，此阶段将有两个活动的以太坊链，此时所有交易和智能合约的执行仍是在原始以太坊链（Eth 1.0）上进行；然后阶段 1 将引入分片以增加系统的可扩展性与伸缩性，主链上的状态记录和交易信息将被划分为不同的分片进行单独管理，分片机制的引入需要 DAPP 在设计时有更多的考量以选取合适的分片；阶段 2 是各功能的融合和拓展，同时分片链会更加完善 [9]。

以太坊 2.0 计划采用 Casper FFG 算法 [27]，该算法依据股权大小决定投票权重占比，每 50 个区块为单位设置检查点，并形成检查点树，节点针对两个检查点之间片段进行投票，如投票总数超过总存款的 2/3，则该部分两检查点将分别变为已证明合理（justified）和最终确定（finalized）状态。该算法采用动态验证集，只需拥有足够存款（最低 32ETH）即可申请，并能自主选择加入或离开。验证者参与验证可以获得奖励，但是如果恶意投票会受到处罚。

2　新型网络空间标识服务

2.1　Namecoin

Namecoin 发布于 2011 年，其能够防止网络审查与监管，是可读性强和去中心化的网络空间标识体系。

Namecoin 不支持顶级域申请，目前仅支持 .bit 顶级域下的域名注册，在 Bitcoin 的基础上，Namecoin 增加了 RPC 命令进行交易提交等操作。Namecoin 采用基于工作量证明的共识机制，挖矿过程采用 SHA-256 哈希算法求解 H(block header) <= target 函数中符合要求的 nonce 值，其平均出块时间与挖矿奖励设置都与比特币相同。

2.1.1 注册过程

Namecoin 采用基于键值对的数据存储，其域名管理过程如下 [15]：

（1）NAME_NEW：注册 .bit 名字需要 name_new 和 name_firstupdate RPC 命令，name_new 步骤要拿 0.01NMC 与要申请的域名之间绑定生成一个代币，其代表该名字的所有权，绑定的 NMC 将不能用于正常交易。在 name_new 中会将用户注册的域名与一个随机值一起做哈希进行加盐加密，然后发送带有加密值的交易进行域名预定，域名的加密值写在交易的 scriptPubKey 中。

（2）NAME_FIRSTUPDATE：该操作可以设置名字内容值，例如 IP 地址等，为防止抢注，该命令必须在对应的 name_new 之后等待 12 个区块才能执行，以确保区块链已就当前 new_new 交易达成共识 [16]。name_firstupdate 提交的数据会写到对应交易的 scriptPubKey 里，其输出部分包括申请的 < 域名，值 > 对的信息。交易验证时，会拿 scriptPubKey 里写入的域名和随机值跟 name_new 中的哈希值进行校验。

（3）NAME_UPDATE：注册完成后 name_update 命令用来更新名字对应的数据值，重置有效期或进行交易等。域名的有效期是 36 000 个区块，

大约 250 天，到期之前必须通过 name_update 进行更新操作，否则域名将被释放。

对于每个名称操作，交易发起人需要支付交易费（0.005 NMC），预定域名的 name_new 命令具有 0.01 NMC 的额外固定成本。最初 Namecoin 为防止成立之初域名抢注，在 name_firstupdate 阶段还另外设置网络费，创世块处的网络费为 50 NMC，同时随着时间的推移缓慢降低（每 8 192 个区块减少 2 倍，大约 2 个月），2012 年 12 月后，网络费已被取消。

2.1.2 存在的问题

Namecoin 存在的问题包括：

域名抢注导致个别用户拥有大量注册域名，致使 Namecoin 网络上存在大量的垃圾注册信息，已注册的正常使用中的域名占比很小。

另一方面 Namecoin 开发社区较小，同时合并挖矿也造成一些安全问题，Namecoin 使用合并挖矿原本想要吸引算力提高自身安全性，然而由于其自身算力较小，某些在比特币上构不成威胁的大型矿池加入后曾出现长达几个月时间内算力超过 51% 的情况。

此外 .bit 域的解析往往需要用户额外运行本地软件、进行单独配置或增加浏览器扩展才能实现，使用成本及门槛较高。

2.2 Blockstack 名字系统

2.2.1 整体架构

Blockstack 分为四层使各部分相对独立，其架构如图 1 所示 [17]。

底层区块链层：控制模块将底层逻辑与业务抽离开来，底层区块链负责交易的存储及共识机制的实现，虚拟链层在不改变底层链的情况下增加了一些针对名字系统的操作。<name，value> 对状态的改变首先通过交易发布在底层区块链的新区块中。

虚拟区块链层：虚拟区块链层负责交易处理，处理逻辑对底层区块链不可见，其从底层区块链获取交易内容并根据交易类型和转换状态进行对应操作。虚拟链只进行部分校验信息、全局状态数据的存储，区文件内容的完整性可以通过该层存储的哈希值进行验证。

路由层：路由层负责数据查询，为了使用户能够自由地选择存储服务，Blockstack 对查询与存储操作实施了解耦和。

存储层：Blockstack 架构最上层是存储层，存储的数据包括 name-value 对，并且带有该域名所有者的签名。

2.2.2 Stacks 区块链

Blockstack 底层链采用 Bitcoin，虚拟区块链层是自身设计的 Stacks 链，当前部署的是其 1.0 版本，2020 年 4 月 2.0 公开测试网开启 [20,23]，其设计包括以下几个方面：

共识机制采用燃烧证明（Proof-of-Burn，PoB）与工作量证明（Proof-of-Work，PoW）相结合，并且计划用转移证明（Proof of Transfer，PoX）[21] 代替燃烧证明。

由于新链启动时往往没有足够的算力参与其中，Blockstack 在工作量证明的基础上增加了燃烧证明，利用本身的 PoW 和另一种更加稳定的加密货币的燃烧证明，进而在借用算力的基础上逐渐把更多的权重放在自身机制上面，以此来安全地发展 Stacks 链 [19]。

2020 年 2 月 Blockstack 发布了 2.0 版本的草案，提议用 PoX 代替 PoB，PoX 中矿工将提交的加密货币转移给网络中的其他参与者。这种方案主要考量是使用 PoB 需要燃烧一定的基础货币，新链启动时其安全性和对应的货币价值都难以得到保障，矿工可能没有很强意愿燃烧基础货币（如价值比较高的比特币）来获得新链上的货币奖励。

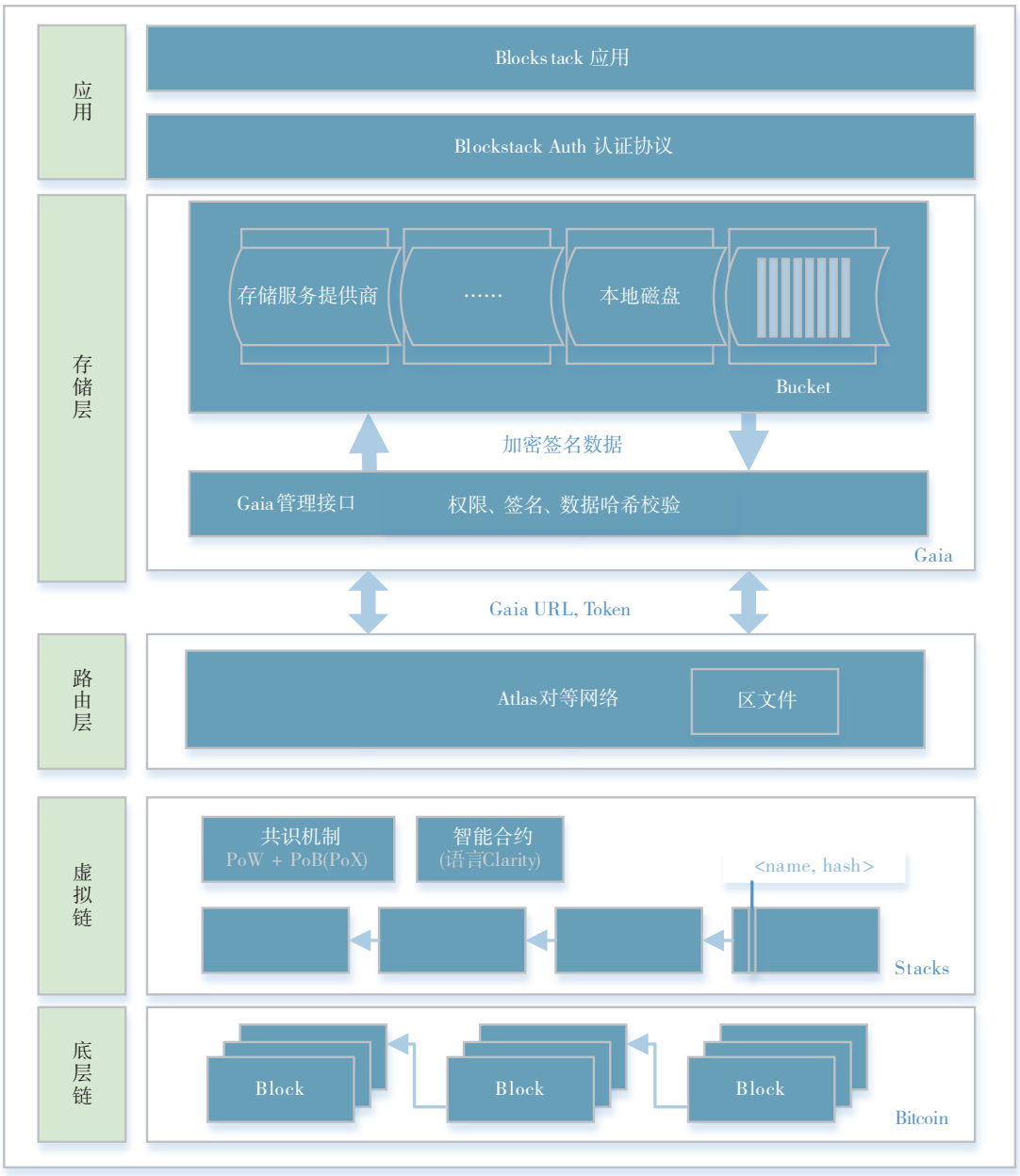

图 1 Blockstack 架构图

Fig. 1 Blockstack architecture

2019 年发布的智能合约语言 Clarity[22] 的设计采用所见即所得的方法，提高了系统安全性。Clarity 是一种可判定语言，具有非图灵完备特性，可以进行静态分析，使得很多复杂性问题可溯源、可预测。同时它是一种解释性语言，能够更加方便地部署 bug 修复方案。

2.2.3 存储系统

Blockstack 中数据主体存储在 Gaia 去中心化存储系统中，只有数据位置的指针及数据内容哈希等被保存到 Satcks 区块链上。Gaia 赋予所有者对其拥有的内容的安全隐私保护，用户数据由密钥加密之后进行保存同时加上自身签名，存储系统本身无法

获取用户数据内容；同时用户可以根据自己需求选择包括各种云存储平台在内的不同存储提供商，通过 Stacks 链上存储的内容哈希值进行校验防止数据被篡改，使得用户与存储平台以去信任的方式建立可信存储机制。

用户向 Gaia 写数据时，写请求需要包含私钥签名的令牌来判断其是否具有写入特定区域的权限，并为同一用户的不同应用设置了单独的私钥，以将不同应用解耦和，其读写步骤如图 2 所示 [18]。

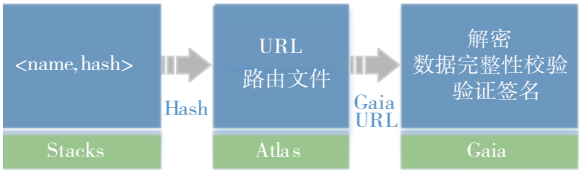

图 2 存储系统读写步骤

Fig. 2 Read and write steps of the storage system

2.2.4 注册流程

Blockstack 名字系统设计全局的名字层次结构，最上层是名字空间，它在功能上类似于 DNS 中的顶级域，其长度为 1-19 位。名称空间实行先到先得的方法并且创建者可以制定相关属性规则，但其不归包括创建者在内的任何用户所有。创建名称空间需要支付一定的费用，长度越短价格越高，创建后永久有效并且存储在区块链上，它可以规定其下的名字规则，例如注册名字的费用，有效期，注册费如何处置等，未来 Blockstack 名字系统将致力于发展类似 DNS 的代理销售商体系。

名称空间的下一级域名（如 test.id）记录存储在区块链上，但其状态通常存储在 Atlas 网络中，所有权和状态通过发送交易控制；持有对应私钥的用户拥有其所有权，名字有效期等由名称空间进行设置。

名字子域（如 sub.test.id）信息不在链上存储，所有权归拥有私钥的用户，但是创建或更新时需要上层名字将其状态广播，同时对应的上级名字到期后其更新会受影响 [30]。

Blockstack 域名管理流程如表 1 所示。

表 1 Blockstack 名字注册管理操作

Table 1 Blockstack name registration management operations

操作	功能
preorder	名字注册
register	最先完成这两个步骤获得所有权
update	名字更新 新值需上传到存储层更新对应名字信息 到期名字需要通过renew续约
transfer	转移域名所有权，仅更改所有权地址
revoke	针对该域名的所有操作不可执行 撤销的名字被锁定一段时间

2.3 Handshake

2.3.1 简介

Handshake 设计理念是兼容同化而不是迁移，它是一种与现有 DNS 向后兼容的名字协议，不会替换 DNS，但其使用基于工作量证明及加密签名产生的区块链系统进行根域管理，同时要求尽量减小对用户的干预，本质是一个分布式去中心化的区文件，任何人都有权在其中添加条目。Handshake 以 UTXO 结构为基础，2020 年 2 月主网发布 [28]。

在 Handshake 中，任何人都可以注册自己的 TLD，其规定当前已存在的顶级域不能申请，并且保留部分公司及组织名对应的顶级域。在货币流转方面，Handshake 将绝大多数（占比 0.7）资产无偿发送给开源代码贡献者，激励研发和软件包维护人员增加其相关集成 [24]。

2.3.2 PoW

Handshake 起初使用具有较强内存限制的图形函数 Cuckoo Cycle[25] 实现工作量证明，后来替换为集成 SHA3 和 blake2b[26] 的方法。鉴于系统发布时整个空间的算力情况未知及使用新的求解函数可能引发的不稳定性，Handshake 设计每个区块进行一次难度 target 调整。具体采用改进的 DigiShield 方法，其在算力动态变化时具有较好的表现。

2.3.3 Urkel 树

Handshake 设计 Urkel 树，又叫做 FFMT（Flat-File Merkle Tree）。FFMT 类似于 Merklix 树，将按位 trie 与默克尔树结合，但是树节点内容存在平面文件（flat files）中。FFMT 是二叉树，包含内部节点和叶子节点两种类别，只需根据指针去对应的文件位置读取内容，即可依次进行节点遍历。内部节点分别包含对应的左右子节点的 hash，内容存储的文件及位置指针等；叶节点包含键值，对应的位置定位信息及空间大小。

叶节点的哈希包含其原始数据内容的哈希，FFMT 基于哈希键值前缀进行构造，在一棵 FFMT 中插入新数据，其会从根节点开始查找，直到新数据所在位置，当插入过程出现键值冲突时，才会新生成冲突路径上的中间节点表示其公共前缀，并根据冲突位数进行分层处理，同时删除操作也需要对应的合并调整。

名字数据每天分四次定期更新插入到树中，并且设定每个区块执行树更新操作的最大次数，保证最坏情况可预测。同时 FFMT 实现了缓存、原子性、崩溃一致性设计，其具有高性能、简单、存储空间小、交易证明所需空间小等优势。

2.3.4 注册流程

Handshake 中域名的注册通过智能合约以拍卖形式完成，流程如下：

BID：拍卖以 BID 类型合约开始，由第一个参与者发起竞标阶段，其他参与者可以自由加入并进行出价。BID 阶段需要输入投标的名字和一个盲值，该盲值是投标金额与一个 256 位的随机值连接组成的摘要，但是可以设置大于等于投标值的锁定值，来混淆其真实投标值。

REVEAL：投标结束进入公示期，公开各参与者投标情况，公示阶段，参与投标的 nonce 值与投标值才会公开。

REGISTER：公示结束最终胜出者进入 REGISTER 合约，支付第二高的出价，剩余的投标值将作为找零返还。

REDEEM：胜出者产生后，投标失败的参与者可以进入 REDEEM 类型合约，将合约中锁定的资金退回。

UPDATE：域名拥有一年有效期，之后需要进行续签，更新合约中所有者地址不允许改变。提交更新时必须提供最近主链上 6 个月以内的区块哈希，以刷新计时器防止用户单次申请过长时间的所有权。

TRANSFER，REVOKE，FINALIZE：TRANSFER 合约改变名字所有权，但为防止名字盗窃等行为，会进行 48 小时延迟锁定，锁定期间名字所有者可以使用 REVOKE 合约撤销转换所有权的操作，撤销后该名字输出不能使用，并且会重新进行投标。撤销操作允许合法所有者在密钥丢失时撤销或质疑名称转让行为。正常转移锁定完成后，执行 FINALIZE 更新地址字段值，完成所有权转移。

Handshake 域名拍卖采用 Vickrey 拍卖，它是一种封闭式投标拍卖，投标者在不知道拍卖中其他人出价情况下提交投标，出价第一的人中标，但只需支付第二名的出价值，Handshake 每周会解锁一组新名字进行竞标。

未被注册并且在推出时间段的名字可以进行拍卖，推出时间的计算方法是对名字进行哈希处理计算 SHA3 值，然后对 52 取模得到特定星期数，保证对于可用名称其推出时间随机均匀分布。

Handshake 设计 SPV 域名解析，其实现了自身的迭代解析器和权威解析器，利用链上的数据进行 DNS 响应，可以无信任地完成解析过程并且具备比较高的速率；此外定义了一个非递归解析器，用于未在 Handshake 中声明的已有顶级域，此时会通过现有 DNS 系统解析该域名。

2.4 Ethereum 名字系统

ENS（Ethereum Name Service）[29] 最早启动于2017 年，由于以太坊中的地址是一串辨识性差的随机字符，ENS 可以用简短的名字将其代替，同时可供以太坊中的 DAPP 接入以提升其操作便捷性。ENS 不支持用户注册顶级域名，主网支持 .eth，可以在去信任机制下安全地购买和管理 .eth 域名。

2.4.1 实现

ENS 的具体实现包括一系列以太坊上运行的智能合约，主要包括注册表、解析器、注册中心等，注册中心是管理顶级域名的智能合约，用户可以按照合约规定注册自己的域名。

域名在智能合约中并不是直接表示，而是用 256 位的加密哈希值标识，ENS 中使用 Namehash 算法为域名生成唯一对应的哈希 [31]。Namehash 过程首先将域名进行标准化，按 '.' 分割成不同的标签，对标签调用 keccak256 得出哈希值，并递归得到完整域名值。最终的输出值称作节点（node），作为 ENS 中该域名的唯一标识。

ENS 中域名的注册权与所有权是分开的。拥有注册权可以改变域名的所有者，所有者可以看做是域名的管理者，真正掌握域名核心权利的是其注册权拥有者。

2.4.2 注册流程

起初域名的注册通过 Vickrey 拍卖的方式，依次进行投标、公示、结标阶段。投标阶段持续 3 天，在此过程中投标金额和投注的域名都不会公布；投标结束后是为期两天的公示阶段，期间未按时公开自己的投标金额将被没收全部投标值，最终未获胜的用户可以取回其投标金额，但是会收取 0.5% 的手续费。中标的用户投标值会被锁定，所有权有效期为一年，期满之后可以退回锁定的金额，最初的投标只对 7 个长度以上的域名开放。2019 年 5 月 ENS 引入永久注册中心已经不需要拍卖的过程，只要进行两个间隔一分钟以上的交易就可以完成域名的注册，并且采用租金的方式，之前注册的域名需要切换到新方式，但免除 2020 年 5 月之前的年费。ENS 注册流程转换成租金方式的原因主要是防范域名抢注，及域名私钥丢失等情况发生时的回收问题。

引入永久注册中心不久 ENS 开放了 3-6 长度短域名注册，短域名注册分为 3 个步骤：预注册，拍卖，最后进行即时注册。拍卖过程采取英式拍卖且最低出价为一年的注册费，拍卖时间的长短由名字长度决定，如表 2 所示。拍卖胜出者获得该域名为期一年的所有权，之后需要付年费进行续约。拍卖结束后所有在预定和拍卖中未被声明的 3-6 字符长度的域名可以按照长域名注册方式进行注册。

表 2 3–6 位长度名字申请设置 [33]

Table 2 Application settings of 3-6 character names

域名长度	拍卖时间（周）	注册费/年（美元）
3字符	6	640
4字符	5	160
5-6字符	4	5

在 ENS 上声明的 DNS 域不需要支付租金，同时 ENS 子域名也不需要租金以减少交易成本，子域注册可以通过合约进行管理，比如控制上级域名所有者无权将子域名收回。ENS 规定并非只有域名所有者才能支付该域名的租金，如果主域名租金未正常支付从而影响到其子域名正常使用，其它用户可以代为支付该主域名租金。

注册域名支付的租金并未被燃烧，而是转入由 ENS 根密钥多重签名持有者控制的以太坊账户中（需要七个签名持有人中的四人签名），作为 ENS 项目生态发展的资金支持及相关项目捐赠。

ENS 正在致力于提供 DNS 顶级域的集成，集成基于 DNSSEC 实现，2018 年 9 月作为尝试 ENS 启动了对 .xyz 顶级域的支持，集成过程完成后可以在 ENS 中声明与 DNS 相同的顶级域下域名（如

ethereum.org）[32]。由于当前 ENS 根由七个根密钥持有者控制，为了方便 DNS 集成广泛部署，ENS 引入一个新合约作为 ENS 根所有者，同时该合约归多重签名持有者管理。任何可以提供有效 DNSSEC 证明的人都可以配置顶级域。

3　对比分析

本节对 Namecoin，Blockstack 名字系统，Handshake，ENS 技术方案进行对比分析讨论，主要包括以下几个方面，如表 3 所示。

表 3　不同系统对比

Table 3 Comparison of different systems

条目	Namecoin	Blockstack	Handshake	ENS
目标	以基于区块链的方案代替DNS	以基于区块链的方案代替DNS	与DNS兼容；仅替代根区管理模块（区文件等）	包括以太坊地址在内的Web3资源解析
区块链	基于Bitcoin代码实现	下层链（Bitcoin） 虚拟链(Stacks)	基于UTXO的区块链	以太坊
结构/算法	SHA-256 Merkle Tree	共识哈希 ECDSA	FFMT SHA3 blake2b	Namehash
共识机制	PoW，同Bitcoin	PoW+PoB 转变为 PoW+PoX （草案阶段）	PoW	PoW 转变为 PoS（Ethereum）
域名注册	只支持.bit顶级域下名字注册，不支持用户申请顶级域	任何人可以创建命名空间，但不归创建者所有；支持名字，子域注册	支持顶级域名和其子域注册	只支持.eth顶级域下名字注册，不支持用户申请顶级域
价格	0.01NMC+ 0.05NMC交易费/交易	指定一系列价格规则；域名的定价规则以名字空间为单位管理； 名字空间也有相应的定价规则	Vickrey拍卖	年度注册费见表2 短域名拍卖费
解析	运行本地DNS解析软件等	Blockstack解析器，已合并到BNS API中	SPV名称解析	自身解析器
智能合约	简单的合约操作	设计一种智能合约语言Clarity	在UTXO基础上增加新的脚本操作码和相关参数来支持智能合约	注册表，解析器，注册中心都是智能合约
身份标识	公共在线身份系统，借助NameID，将Namecoin身份转换为OpenID	Blockstack Auth	申请的域名可以作为用户ID	可以当做身份地址标识
目前应用	使用.bit顶级域访问网站；实现可读性强的Tor .onion域；去中心化TLS（HTTPS）证书验证。	作为基于区块链的名字系统；许多应用程序已在Blockstack上构建。	注册顶级域；作为基于区块链的名字系统；	作为以太坊中转账等操作地址；以太坊DAPP中接入使用；

4 总结

通过对以上基于区块链的网络空间标识系统的分析，不同的项目在域名分配、解析、数字认证、身份标识等方面提出了各自的解决方案，在此基础上部署了一系列应用并取得了一定的成果，但同时也面临一些挑战与问题。

现行 DNS 已有数十亿用户，并且拥有比较高的用户友好性，基于区块链的新型网络空间标识系统需要考虑的问题包括：

（1）域名组织结构：域名以何种方式进行组织及各级域名存储和管理机制等。

（2）域名注册分配机制：包括如何防止名字被少数用户大批量抢注，域名注册方式选择（先到先得，拍卖，押金租金等），如何制定合理的名字定价方案使不同的名字尽量接近其市场价格及子域名注册管理机制等。

（3）名字注销机制：域名所有者对域名的持有权期限，及私钥丢失等情况的处理方案。

（4）解析效率：跟当前 DNS 系统相比解析速率是否足够高效。

（5）易用性：从当前 DNS 系统切换到区块链网络标识系统用户是否需要额外的工作量，能否进行无干预切换。另外从功能角度如何更好地满足用户需求，比如用户想要搜索与给定字符串匹配且低于指定价格的所有可出售的名称。

（6）推广：如何制定更有效的激励措施或通过集成等方式得到更广泛的用户市场。

另一方面，针对利用区块链技术来改进现有的标识服务体系也存在一些争议与讨论，首先网络去中心化是否真正是更好的选择，区块链技术带来一些优势的同时也引发了一些新问题。无监管、抗审查的特性被一些恶意软件所利用来托管命令和操作，使其能够更加隐蔽地实施非法行为，同时发现违法行为后进行阻止的代价也非常大。此外，DNS 系统是相对比较平稳高效的基础设施，当前提出的新型系统一直未得到大规模的应用，一部分原因在于用户没有很强的意愿付出成本进行转换，相比之下现有技术在效率、易用性等方面仍有待提高。此外，对应的硬件支持、性能状况、政策趋势等都是影响其发展的因素。

利益冲突声明

所有作者声明不存在利益冲突关系。

参考文献

[1] UMESHA NAIK, D. SHIVALINGAIAH. Compara-tive Study of Web 1.0, Web 2.0 and Web 3.0[C]. Conference: 6th International CALIBER, 2008.

[2] Lassila O, Hendler J, Embracing “Web 3.0”[J]. IEEE internet computing, 2007, 11(3):p.90-93.

[3] DOI:10.17487/RFC7626, DNS Privacy Considerations [S].

[4] J. Mirkovic, P. Reiher. A taxonomy of DDoS attack and DDoS defense mechanisms[C]. ACM SIGCOMM Computer Communications Review, April 2004.

[5] DOI: 10.17487/RFC4033, DNS Security Introduction and Requirements[S].

[6] DOI: 10.17487/RFC6840, Clarifications and Implementation Notes for DNS Security (DNSSEC) [S].

[7] DOI: 10.17487/ RFC7858, Specification for DNS over Transport Layer Security (TLS) [S].

[8] DOI: 10.17487/RFC8484, DNS Queries over HTTPS (DoH) [S].

[9] Ethereum 2.0 Phases [EB/OL]. 2019, [2020-05-01]. https://docs.ethhub.io/ethereum-roadmap/ethereum-2.0/eth-2.0-phases/.

[10] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System, [EB/OL], [2020-05-01]. https://bitcoin.org/bitcoin.pdf.

[11] Ethereum White Paper [EB/OL]. 2019, [2020-05-01]. https://github.com/ethereum/wiki/wiki/White-Paper.

[12] Ethereum 2.0 specifications [EB/OL]. 2019. [2020-05-01]. https://github.com/ethereum/eth2.0-specs.

[13] Arvind Narayanan, Joseph Bonneau, et al. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction [M]. Princeton University Press, 2016.

[14] GAVIN WOOD. Ethereum: a secure decentralised generalised transaction ledger [EB/OL]. [2020-05-01]. http://paper.gavwood.com/.

[15] Andreas Loibl. Namecoin. Network Architectures and Services[C]. 2014.

[16] Harry Kalodner, Miles Carlsten, Paul Ellenbogen, et al. An empirical study of Namecoin and lessons for decentralized namespace design[C]. WEIS, 2015.

[17] Muneeb Ali, Jude Nelson, Ryan Shea, Michael J. Freedman. Blockstack: A Global Naming and Storage System Secured by Blockchains [C]. Proc. USENIX Annual Technical Conference (ATC '16), June 2016.

[18] Muneeb Ali, Jude Nelson, Aaron Blankstein, et al. The Blockstack Decentralized Computing Network Whitepaper Version 2.0 [EB/OL]. 2019. [2020-05-01]. https://blockstack.org/whitepaper.pdf.

[19] Muneeb Ali. Stacks Token Economics and Incentive Mechanisms Whitepaper v 2.0.7 [EB/OL]. 2019, [2020-05-01]. https://blockstack.org/tokenpaper.pdf.

[20] Diwaker Gupta. Blockstack stacks 2.0 tetsnet [EB/OL]. 2020, [2020-05-01]. https://forum.block-stack.org/t/stacks-2-0-testnet-neon-is-here/10715.

[21] Muneeb Ali, Aaron Blankstein, Michael J. Freedman. PoX: Proof of Transfer Mining with Bitcoin[EB/OL]. 2020, [2020-05-01]. https://blockstack.org/pox.pdf.

[22] Blockstack Clarity: Introduction [EB/OL]. 2020, [2020-05-01]. https://docs.blockstack.org/core/smart /overview.html.

[23] Diwaker Gupta. Stacks 2.0 testnet launch update [EB/OL]. [2020-05-01]. https://forum.blockstack.org /t/stacks-2-0-testnet-launch-update/10683.

[24] Handshake [EB/OL]. 2018. [2020-05-01]. https://handshake.org/files/handshake.txt.

[25] Cuckoo Cycle [EB/OL]. [2020-05-01]. https://github.com/tromp/cuckoo.

[26] DOI: 10.17487/RFC7693, the BLAKE2 Cryptographic Hash and Message Authentication Code (MAC) [S].

[27] Casper the Friendly Finality Gadget [EB/OL]. [2020-05-01]. https://arxiv.org/pdf/1710.09437.

[28] Handshake launch timeline [EB/OL]. 2020. [2020-05-01]. https://www.namebase.io/blog/timeline.

[29] Ethereum Name Service Document [EB/OL]. 2020. [2020-05-01]. https://docs.ens.domains/.

[30] Bloackstack Name Service [EB/OL]. [2020-05-01]. https://docs.blockstack.org/core/naming/introduction.html.

[31] Ethaash [EB/OL]. [2020-05-01]. https://github.com/ethereum/wiki/ wiki/Ethash.

[32] Integration of DNS TLDs in ENS [EB/OL]. 2019. [2020-05-01]. https://medium.com/the-ethereum-name-service/upcoming-changes-to-the-ens-root-a1b78fd52b38.

[33] Ethereum Name Service [EB/OL]. [2020-05-01]. https://docs.ethhub.io/built-on-ethereum/infrastruc-ture / ethereum-name-service/.

收稿日期：2020 年 6 月 29 日

张曼，中国互联网络信息中心，硕士，主要从事互联网基础资源标准研制相关研究。

本文中主要负责论文整体内容的撰写。

Zhang Man, M.A., China Internet Network Information Center. Her research directions are related to Internet basic resources analysis technology and standard development.

In this paper, she is mainly responsible for writing the overall content of the paper.

E-mail: zhangman@cnnic.cn

李洪涛，中国互联网络信息中心总工程师，高级工程师。专业方向为计算机应用技术、下一代互联网架构，当前主要从事互联网基础资源新型解析技术及大数据分析研究。

本文中主要负责新型解析技术研究。

Li Hongtao, senior engineer, is the chief engineer of China Internet Network Information Center. His main research directions include computer application technology, next-generation Internet architecture, and new analytical technology of Internet basic resources and big data.

In this paper, he is mainly responsible for the research of new analytical technology.

E-mail: lihongtao@cnnic.cn

董科军，中国互联网络信息中心，正高级工程师，主要研究方向为互联网基础资源管理、云计算、分布式系统、网络协同技术。

本文中主要负责新型解析技术研究与论文结构设计。

Dong Kejun is the professorate senior engineer at China Internet Network Information Center. His main research directions include Internet basic resource management, cloud computing, distributed systems, and network collaboration technology.

In this paper, he is mainly responsible for the research of new analytical technology and design of the paper structure.

E-mail: dongkejun@cnnic.cn

延志伟，中国互联网络信息中心，博士，研究员，主要研究方向为互联网名址协议及下一代网络架构。

本文中主要负责整体框架设计与指导工作。

Yan Zhiwei, Ph.D., is a researcher of China Internet Network Information Center. His main research directions are Internet naming and addressing protocols, and next generation Internet architecture.

In this paper, he is mainly responsible for the overall framework design and work guidance.

E-mail: yanzhiwei@cnnic.cn

引文格式：张曼, 李洪涛, 董科军, 延志伟. 基于区块链的网络空间标识服务[J].数据与计算发展前沿,2020,2(5): 52-64.DOI:10.11871/jfdc.issn.2096-742X.2020.05.006.PID:21.86101.2/jfdc.2096-742X.2020.05.006.

Zhang Man, Li Hongtao, Dong Kejun, Yan Zhiwei. Cyberspace Identification Service Based on Blockchain [J].Frontiers of Data & Computing, 2020,2(5): 52-64.DOI:10.11871/jfdc.issn.2096-742X.2020.05.006.PID:21.86101.2/jfdc.2096-742X.2020.05.006.