前言：区块链火了，查文档时发现我2014年博士课程期间关注的区块链相关问题，最后写的网络分布式计算课程的作业。分享给大家。

中国科学院大学 中国科学院计算机网络信息中心 吴双力

摘要： 名字服务在互联网领域是基础服务。名字服务的主要需求有安全性、去中心化和易于记忆。长期以来这三个需求被认为难以同时满足。而域名币（Namecoin）系统被认为同时满足了这三个需求。同时，在它的基础上还不断扩展出其他应用包括物联网设备互联、去中心化认证等。因此，域名币系统综合了名字服务、安全服务、分布式服务的特点，具有很高的参考价值，本文针对该系统进行分析。

关键词：比特币，区块链，域名币，认证，物联网

1.域名币系统简介

域名币是去中心化的开源信息注册与转移系统，域名币以比特币为基础。域名币能安全的记录和转移任意名字（或键值），将名字和其值（数据）关联；域名币本身是一种数字货币，可以用来进行域名币交易。

域名币能够使网络对抗审查、保护网上的言论自由。这主要是因为域名币系统完全是去中心化的，个人访问互联网或者注册域名都不需要与特定的机构联系从而避免被审查。域名币系统可以用来访问.bit域名；存储实体信息例如邮箱、GPG密钥，比特币地址，TLS指纹，比特币信息地址等。域名币系统可以存储人可识读的.onion洋葱域名。比特币域名可以用作为文件签名、选举、股票、信任网络、第三方支付等应用的基础。

域名币系统被认为是破解了Zooko's不可能三角。该三角是安全学者Zooko Wilcox-O'Hearn提出的一个猜想，该猜想指出对于网络协议中的命名系统来说有意义性、去中心性和安全性只能同时满足其中两个，不可能三个都满足。有意义性是指：对命名系统的用户来讲名字有意义并可记忆。例如域名系统。区中心性是指：命名系统不需要一个中心的授权机构定义名字的意义。域名系统就不是去中心的，它只有一个中心授权机构。安全性是指：名字映射到独有的具体实体。例如域名系统是独有的因为只有一个机构可以证明域名的所有者。例如DNSSEC满足了安全性和有意义性，但不满足去中心性。域名币系统同时满足了有意义性——它使用人可记忆字符，去中心性——不需要一个中心授权机构，安全性——可以保证域名映射的独有性。

域名币系统的基本规范沿用了大部分现有域名相关规范。域名币系统中的名字域（域名）以 “d/” 开头，随后是域名，兼容域名币解析的解析器会自动加上顶级域.bit后解析。例如d/example。域名币系统的名字域遵循RFC1035《域名 - 实现和规范》的规定。域名币系统的名字域兼容国际化域名的标准，Unicode编码的名字需要先根据国际化域名标准转换成ASCII码兼容的编码后再进行注册。域名币的值域是UTF-8编码的JSON对象，最大520字节，区分大小写。域名币系统的值域根据现有域名的记录类型定了json的条目。例如"ip"对应域名系统里的A记录，“ipv6”对应域名系统里的AAAA记录等[1]。

2.域名币系统的设计规则

??????????????????????????????????????

- name_new(hash(rand, name), value) 创建新域名
- name_firstupdate(name, rand, value) 域名首次更新
- name_update(name, value) 域名更新

这三种操作和域名币的交易关联在一起。域名首次更新操作需要网络费用。收费后这个以域名币计费的费用被销毁掉。也就是说事实上并没有一个机构收对域名币的域名操作收费。网络费用只是防止域名“淘金热”的一种措施，防止大量无效域名注册、占用掉好的名字资源。

域名操作的具体规则如下：域名首次更新（name_firstupdate）操作会在域名注册(name_new)12个区块时间（约120分钟）之后被接受。如果名字注册发生冲突第一个不可忽略域名注册生效。名字是一个最大长度为255的字节串，值是最大长度为1023的字节串。只有当支付的网络费用不低于当前的系统网络费用时域名交易才会被插入域名链。网络费用以50个域名币每次操作开始，从起始区块开始计算。每个区块的网络费用递减，每8192个区块时间(约两个月)就会减半。如果在36000个区块时间（约200多天）内不更新，域名过期，这个要求类似于域名里的续费操作。在传统域名系统中域名的拥者如果认为域名还应继续生效，就需要续费，在域名币系统里需要进行更新。

域名币中的名字通常解释为以"/"分割的字符串组成的UTF-8字符串。第一个元素是应用标识符。对于域名系统，第一个元素必须是“d”并且仅有两个元素。可以将名字简单的映射到顶级域.bit:d/xyz=>xyz.bit。其对应的值域用区文件(zone file)标准解释。对于个人公开名字，第一个元素必须是“p”并且仅有两个元素。其对

应的值域以json格式的hash值解释，其中的"key"元素包含了PGP编码的秘钥。

3.域名币系统的技术基础

域名币系统以比特币为基础。它使用了同样的工作量证明算法，并且货币总数为2100万个。但是它有自己独立的区块链(blockchain)。它在比特币的基础上实现了额外的远程过程调用(remote procedure call)命令。通过这些命令用户可以记录和交易区块链中的任意名字和相应的数据。因此域名币系统的技术基础是分布式网络基础上的区块链、时间戳、工作量证明等。

3.1 区块链

区块链被认为是比特币系统的最大创新之一。区块链是所有网络参与节点之间共享的交易数据库。每个区块包括前一个区块的哈希。每个区块是不可以通过计算更改的。因为如果它被改变，它之后的每个区块必须随之改变。这些特性使得双花（double-spending）比特币非常困难。通过区块链比特币解决了数字货币的一个关键问题。区块链数据通过洪泛协议广播到每个网络节点。

每个区块包括一些或所有近期交易、前一个区块的引用、以及其他数据。它还包括一个工作量证明的结果，该结果对每个区块是唯一的。 [2]。工作量证明的结果很容易验证，没有通过工作量证明的区块不会被加入区块链。区块头的数据结构如表1。

?1 ???????

???	??	????	?? (Bytes)
??	?????	?????	4
??????	?????256-bit	???????	32
??Merkle??	256-bit hash ba sed on all of t he transactions in the block	?????	32
??	?????????? 197 0-01-01T00:00 U TC	?????	4
????	??????????	?????	4
???	32-bit ?? (???0)	??????	4

??????????2?

?2 ??????

???	??	??
Magic no ???	??0xD9B4BEF9	4 ??
Blocksize ???	??????????	4 ??
Blockheader ??	??6????	80??
Transaction counter ????	??? VI = VarInt	1 – 9??
transactions ??	????(??)	<Transaction counter >-????

随着交易的进行区块不断地产生，大约每10分钟就会产生一个区块。到目前（2015年1月26日21:00）为止比特币的区块数为340544。随着区块数的增长区块链的大小也不断增长。图1[3]给出了比特币两年内区块链大小的曲线。可见区块链大小增长很快，当前大小已经超过20GB。域名币系统也是一样的，这也会造成域名币系统查询客户端的一些问题。由于域名的查询都是查询区块链数据，如果都是本地查询，客户端就要保存大量数据，这对于手机等移动端设备是不适合的。

图1 区块链大小曲线

3.2 时间戳

每一个区块包含一个Unix时间戳，除了作为区块哈希的一个变量外，还使得攻击者修改区块信息更加困难。如果一个时间戳比之前11个区块的时间戳的中值大，并且比网络调整时间小2小时以内就会被认为有效。其中的“网络调整时间”是指与你相连接的所有节点的平均时间。当节点A连接到节点B时，A从B处得到一个UTC标准的时间戳，A先转换成本地UTC标准时间保存起来，网络调整时间等于所有节点的本地UTC时间+所有相连节点的偏移量平均值，该网络时间永远不会调整到超过本地系统时间70分钟以上。

域名币的时间同步，也是其基础技术之一。如3.1节中表1看到的一样，每个区块都包含了时间戳。该时间戳能够证实特定数据必然于某特定时刻是的确存在的，因为只有在该时刻存在了才能获取相应的随机散列值。每个时间戳又将前一个时间戳纳入其随机散列值中，每一个随后的时间戳都对之前的一个时间戳进行增强(reinforcing)，这样就形成了一个链条（Chain）。

3.3工作量证明

由于域名币与比特币系统是完全去中心化的分布式网络，它不以任何参与者的诚实和信用甚至审查为基础，因此会有不少对系统不利的使用者。例如域名币系统中企图大量注册较短域名者；比特币中企图占有更多比特币者。一个最直观的办法是限制每个参与者注册域名的数量，但是参与者本身就是程序，系统无法判断每个参与者运行了多少了程序，这个方法是不实现的。而工作量证明提供了分配参与者获取共同资源当中份额的方法。它是利己而不从属于别人的一群人消除分歧取得共识的手段。

域名币系统的工作量证明机制基于密码学算法。每个数据区块的头部信息中都含有一个随机数（nonce），当计算出来的sha256值不满足要求时，那么这个随机数（nonce）便增加一个单位，直到满足要求为止。现在没有发现预测sha256值的方法，所以需要大量的计算来找到符合要求的头部sha256值。但是一旦找到答案，验证信息的sha256值是非常容易的。因此，数据区块(block)生成的这一过程便成为了网络参与者工作量的证明。随着参与者的增多和整个域名币的工作量证明的难度也会变化。以h表示SHA256函数，I表示区块信息，x表示随机数，N表示难度条件。该问题可以描述为h(I+x)<N。由于哈希运算是单向函数，该问题只能以尝试的方式求解。

```
??l="Hello, world",N=0000ffffffffffffffffffffffffffffffffffffffffffffffffffff,???????????4???0???????x=0?

h("Hello, world!0") = 1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64

h("Hello, world!1") = e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8

...

h("Hello, world!4250")=
```

0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9

?????x=4250????????????x???????x?????????????????????????????

4.域名币系统的应用

域名币系统的设计初衷是一个去中心化、能够免于审查的域名查询系统。希望成为现有域名系统（DNS）的替代方案。然而目前它的应用领域已经远超出域名领域。作为对数字货币系统的一个实用化应用基础，研究者在深入考虑其应用到去中心化认证、物联网等领域。数字货币因为其颠覆性属性，短期内难以看清其前景，学术界也很少公开讨论。但是以域名币为基础的各类应用已经被麻省理工学院、德国慕尼黑工业大学等顶级高校，国际商业机器（IBM）、三星、趋势等全球化公司关注和深入研究。

4.1去中心化认证应用

????????????????????????(CA)???????????????(Web of Trust)???????CA?????????????????????????????CA?????????CA??????? ??????????????? DigiNotar??????????????????TrustWave???

基于以上原因麻省理工学院（MIT)的Conner Fromknecht，Dragos Velicanu，Sophia Yakoubov提出了基于域名币系统的认证体系Certcoin【4】。Certcoin系统以NameCoin为基础将域名币系统的区块链当做一块公共白板，用来永久记录认证信息。Certcoin的每次交易都是收费的，目的是为了激励参与者包含Certcoin的信息。Certcoin是完全分布式的并且只要求用户信任网络中的非恶意节点占大多数即可。Certcoin基于域名币系统完整的设计了注册公钥签名实体、更新实体、查找实体公钥、验证实体的公钥、恢复实体公钥的整个过程。并对验证过程中的效率，查找过程中的存储空间和效率进行了优化。以ID的注册过程为例说明Certcoin以域名币系统为基础的基本思想。详细系统可以参考文献[4]。

???

????????(id; register; online; values = (pkn;)) ?(id; register; online; values = (pkf))????, ??:

id ?????, pkn ????, pkf ?????, ? ???????? = sig(skn; id) , = sig(skf ; id). ?????????????????????skn?????skf???

?????????????????

l ??id???????

l ??

l ??

????????????????????????????????

????????????????????????????

???????????????????????

l ???????????????id????????id

l ??

l ??

???????????????????????

???[4]????????????DHT???????????????

以Alice和Bob进行通信的场景来描述，该系统的过程和其他PKI系统并无不同。Alice 给Bob发送一个形式为(idA,

,w)的消息，其中idA是Alice的身份信息，

是Alice的公钥，w是累加形式的证据。Bob验证

确实是Alice的公钥。Bob接着发送给Alice一个随机挑战信息h,如果Alice可以响应消息

,使得验证结果

,Bob就认为她就是idA的拥有者。这样Alice 就认证成功了。

4.2物联网应用

随着物联网的发展物联网的系统架构也逐渐受到重视，其中的名字系统更是其中的关键。而物联网中的联网实体将以百亿级，并可能达到千亿量级。目前的名字系统主要以域名系统为主，但普遍认为域名系统在物联网中将遇到挑战。因此，以国际商业机器（IBM）为代表的公司提出了“设备的民主化”的愿景[5]，并联合三星等公司开展Adept项目。其主要的思想就是建立一个不以信任为基础的设备自治、对等和无信任互联互通架构，而这正是以域名币及比特币的区块链为基础。其目标基本是通过区块链去解决名字、认证、通信的大部分问题。

由于物联网中联网物体数量巨大，服务期限长，难以建立信任网络，导致目前的互联网架构应用于物联网将面临巨大问题。IBM通过分析认为在物联网时代无论是产品设计、商业模式还是技术基础都要根本改变。图2给出了各个方面的具体要求。其技术层面就要以前面提到的设备自治、对等和无信任互联互通架构为基础。

物联网时代的成功金字塔

??—??

??????IBM?????????????????????????????????,????????????????????????????3???????????

物联网架构演进

??IBM???

??IBM????????
??????????????????

5.总结

本文分析了一个分布式系统——域名币系统。它以分布式系统的网络通讯、远程系统调用、时间协调、安全机制等为基础，加上其特有的工作量证明、区块链等技术，面向名字系统这个网络中的基础问题，创新的提供了一个去中心化、安全、对人有意义的名字系统。该名字系统的初衷是应对网络审查，然而随着研究的深入和扩展，以其为基础的分布式认证系统、物联网基础架构等也成为其应用场景。这些研究和扩展已经得到麻省理工学院、德国慕尼黑工业学院，以及IBM、三星的重视，前景可期。然而由于该系统的一些特点，真正实现应用还有一些距离，是一个值得研究的新兴领域。

?????

[1]https://wiki.namecoin.info/index.php?title=Domain_Name_Specification

[2]http://www.chinabtcc.cn/bl/2014-04-01/2869.html

[3]https://blockchain.info/charts/blocks-size?timespan=2year&showDataPoints=false&daysAverageString=1&show_header=true&scale=1&address=

[4] A Decentralized Public Key Infrastructure with Identity Retention,http://eprint.iacr.org/2014/803.pdf

[5]Device democracy, http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=PM&subtype=XB&htmlfid=GBE03620USEN