目录

VNS 去中心化 DNS 以及网站系统白皮书

VNS team

一、 现有 DNS 系统

DNS 系统是构成互联网系统的重要基础设施，现有 DNS 系统在长时间的实际运行过程中，暴露出很多的问题。例如，2014 年 1 月 21 日，中国顶级域名根服务器出现故障，中国大部分网站都受到了影响[1]。现有 DNS 系统的问题，主要包括以下几个方面:

1. 安全性和隐私性的问题

由于当前的 DNS 解析请求都需要通过 DNS 服务器进行解析，所以非常容易发生中间人攻击 (man in the middle attact)。用户发送的 DNS 请求可能被攻击者拦截，然后攻击者伪装成 DNS 服务器返回一个虚假的域名信息，在用户 URL 地址不变的情况下，重定向到另外一个虚假的站点。另外，中间人攻击者还可以通过查看未加密的 DNS 请求以及通过分析 DNS 请求的规律，分析和识别用户的行为模式。另外一个常见的风险是 DDOS 攻击，攻击者通过发送大量无效请求，带来大量流量给 DNS 服务器，造成 DNS 服务器无法正常解析域名。除以上提到的中间人攻击和 DDOS 攻击以外，常见的攻击手段还有:域名劫持，缓存投毒等等。这些安全性风险，是现有 DNS 设计架构和协议造成的，在现有的 DNS 架构下，很难从根本上杜绝此类风险。

2. 无法满足去中心化网站域名解析的需要

现有 DNS 服务架构，是一种分层分布式的架构，是一定程度上的中心化结构。去中心化网站系统，从设计上不应该引入一个中心化的域名解析。此外，现有 DNS 系统和去中心化网站系统存在一定程度上的不兼容问题。例如，去中心化网站的站点是以公钥为访问地址，

需要的是公钥和可读字符串之间的映射关系，而现有 DNS 系统一般是将 URL 地址映射成 IP 地址。

3. 体系危险性

由于历史的原因，根域、重要的顶级域和根证书由少数国家政府（主要是美国）掌控，这对各国互联网络的危险性始终存在。解决的思路同样是去中心化 DNS 系统。

二、 现有去中心化 DNS 系统

随着区块链技术的发展，目前已经有一些去中心化 DNS 系统出现，例如 namecoin，eth name service, blockstack dns service. 这些系统由于基础架构的选择不同，也存在着一定的区别

1. Namecoin

Namecoin[2][3]是最早出现的去中心化 DNS 系统。它是一个比特币的分叉，目前使用 auxpow 的机制与比特币联合挖矿。目前 namecoin 最大的安全性风险来自于 51%攻击的风险，历史上 namecoin 曾经多次出现的单个矿池算力超过 51%的情况。Namecoin 的另一个设计上的问题在于数据平面和控制平面的高度耦合。在 Namecoin 中，DNS 条目（entry）的相关映射数据，以 transaction 的形式写入到区块链中。这种形式的数据存储方式，数据的长度受到限制，这也就限制了 namecoin 拓展成为一种通用性的 key-value 存储设施的能力。此外，随着区块数据的不断积累，直接从 namecoin 的全节点区块中查找 DNS 条目(entry)的时间会不断增加。现有的 namecoin 架构并没有经过大数量条件下查询效率的测试。

2. ETH Name Service

ETH Name Service[4]是基于以太坊智能合约提供的域名映射服务。ENS 的各种基础设施和管理方式都是去中心化的，任何人都可以通过拍卖的方式在区块链上注册.eth 域名。由于 ENS 基于以太坊智能合约实现，不可避免的存在以太坊平台的诸多问题。例如，交易量比较大时，以太坊区块的拥堵问题。

3. Blockstack Name Service

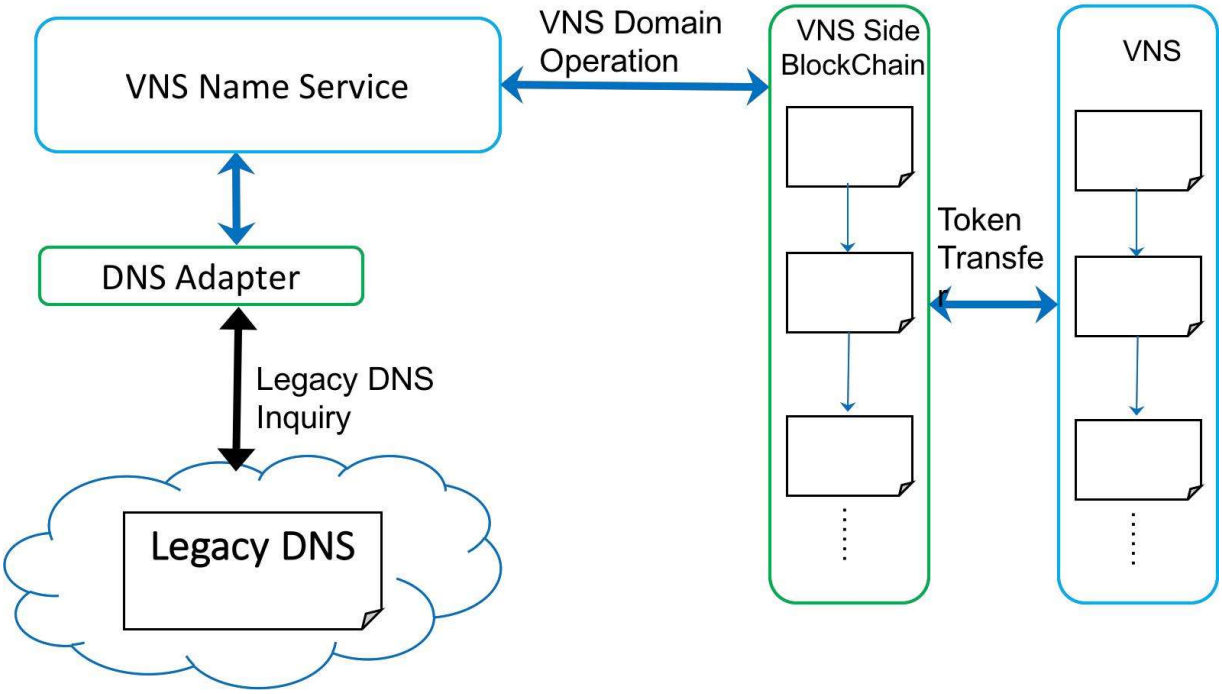
Blockstack Name Service[5]建立在 bitcoin 的基础上，使用比特币 OP_RETURN 这种特殊的操作，记录 meta data。OP_RETURN 这种特殊的操作，并不出现在比特币 UTXO 的条目中，是比特币中一种可删减的数据。由于矿工并不能从 OP_RETURN transaction 中获得收益，OP_RETURN 的 transaction，矿工可以不提供确认，并且 OP_RETURN 的 transaction 的大小也受一定的限制。所以依赖比特币的 OP_RETURN 建立的服务，是存在安全性风险的。比特币未来对 OP_RETURN 存在着不确定性，随着比特币区块数据量的膨胀， OP_RETURN transaction 有非常大的可能会被区块修剪，此外攻击者可以发起大量 OP_RETURN 的 transaction，造成基于 OP_RETURN transaction 的应用瘫痪。s

三、 VNS Name Service

1. VNS Name Service 的架构设计

VNS Name Service 采用主链侧链的设计架构，单独作为 VNSCoin 主链的一条侧链存在。作为一条侧链，VNS Name Service 不产生新的代币，而是与 VNSCoin 主链代币系统实现双向兑换绑定。VNS 主链的代币系统，通过锁定 VNS 代币的方式，在 VNS Name Service 侧链相应的产生对应数量的 VNS 代币，反之通过销毁 VNS Name Service 侧链的 VNS 代币来解锁 VNSCoin 主链锁定的代币。从而实现主链和侧链的双向代币兑换和绑定。

作为一条侧链，VNS Name Service 可以独立的发起 transaction，考虑到发展成为通用 key-value 数据存储的可拓展性， VNS Name Service 可提供两种独立类型的 transaction。第一种 transaction 与 Namecoin 类似，我们可以直接将 value 数据直接写



在 transaction 中。第二种 transaction，只写入 value 数据的 hash value，其内容数据通过 DHT,BitTorrent 或者其他去中心化存储服务作为支持。

为兼容和支持现有互联网体系架构下的各种服务，例如在使用 VNS Name Service 服务的同时，同样可以正常使用现有域名解析服务，访问.com，.cn 等等顶级域名，VNS Name Service 在区块链侧链的基础上，建立一种与现有 DNS 服务兼容的标准化的域名解析服务层。从而避免用户在解析非.vns 域名时，域名解析服务更换的问题。同时此标准服务层会对区块数据进行索引缓存，以提高域名查询速度。对个人用户来说，不需要索引和缓存完整的区块条目。兼容层可以选择性的从区块中查询用户经常访问的地址，将其缓存以提高查询速度。

我们将拥有完整区块数据，并愿意对外提供域名解析服务的节点称为主节点。主节点需要对区块数据做完整的索引。类似于比特币 SPV 机制，其他用户如果不想本地存储区块数据

可以只下载区块的 header，或者直接使用主节点提供的域名解析服务。为了鼓励主节点的建设，使用主节点的服务的用户将向主节点服务支付 VNS 作为费用。为了保证主节点的可信性，主节点需要锁定固定数额的 VNS 作为提供稳定可信服务的抵押。

2. VNS Name Service 安全性分析

VNS Name Service 作为一种去中心化的服务，从根本上杜绝了隐私泄露，内容审查，DDOS 攻击，中间人攻击等等各种风险的可能性。每一个独立运行 VNS Name Service 的用户的节点，都可以从电脑本地查询解析 DNS。本地解析 DNS 请求，同时也节省了网络封包在网络上传输的过程所花费的时间。

与 Namecoin 类似，VNS Name Service 的主要风险来自于 51%攻击。为得到足够算力保证，VNS Name Service 侧链可以与 VNSCoin 联合挖矿。

3. VNS Name Service 拟支持标准

VNS Name Service 支持.vns 为后缀的顶级域名解析服务，支持 new_name(新建域名)，update_value(更新 value 值)和 transfer(域名转让)三种基本操作。兼容层符合现有 DNS 系统查询服务标准。

VNS Name Service 的条目主要包含 Name 字段和 Value 字段。Name 字段拟支持 RFC1035 标准：域名命名要符合 RFC 1035 域名标准:必须以字母开头，以字母或者数字结尾，中间字符可以包括字母，数字和连字符，长度不能超过 63 个字符, ASCII only, 不支持 unicode。校验正则表达式: ^[a-z]([a-z0-9-]{0,62}[a-z0-9])?$

Value 字段以 json 格式字符串形式，支持 namecoin 支持的命名空间[3]，包括:

Namespace

Namespace	Application

d/<domain>	Domain names for .bit TLD
id/<identity>	Public online identity system (e.g. addresses for BTC, NMC, email, ...)
p/<personal>	Personal namespace for PGP, SSL, identities, etc.
m/<message>	Messaging system for Namecoin users
a/<alias>	Alias system to map a name to another address
tor/<domain>	Domain names for .tor TLD for onion websites

四、 去中心化网站系统

基于 VNS 主链和 VNS Name Service，我们提出去中心化互联网的概念。现有互联网架构下的网站系统，最典型的架构是基于公有云服务。基于公有云的服务有着非常明显的缺陷。

公有云服务商并不能提供绝对安全的服务，例如公有云服务数据中心的数据异地备份困难是数据中心常见的问题，中国曾出现某巨头公司因为数据中心网络问题造成上亿中国用户不能正常使用服务的情况。托管在云上意味着敏感的数据和代码也都全部托管给第三方机构，用户必须承担由此带来的安全性风险。除此之外，用户也不得不依赖云服务商提供的防范网络攻击的服务，如防火墙等等。

随着硬件的发展，目前个人 PC 的硬件水平已经完全可以满足建设小型站点的硬件需要。与现有托管在云上的系统相比，去中心化网站系统有如下优点。第一，完全免费，网站全部内容都在用户电脑上，所以免去了支付给云服务商带宽，存储，计算能力 以及其他服务的费用。第二，安全性保障。去中心化网站系统建立在 VNS 主链和 VNS Name Service 的基础上，利用 VNS 主链提供对网站，数据等内容的百分之百的所有权认定和内容掌控，并且可以实现完全匿名化的访问和服务，去中心化的结构保证了网站系统不受单点故障的影响。第三，VNS 代币系统提供的代币可以在去中心化网站上流通。站点访问的 URL 是通过 VNS 主链提供的公钥生成，所以访问者可以方便的将代币发送给网站持有者，以鼓励网站持有者进行内容上的更新和创作。另外配合 VNS Name Service，公钥地址还可以映射成易于记忆的字符串，使 VNS 在去中心化网站系统中更易于流通。第四，更快速的域名解析服务和更快速的访问速度。DNS 解析服务使用 VNS Name Service，可以在本地完成域名解析，免去了 DNS 请求封包在网络上传输的时间。网站的所有内容都要先下载到本地浏览

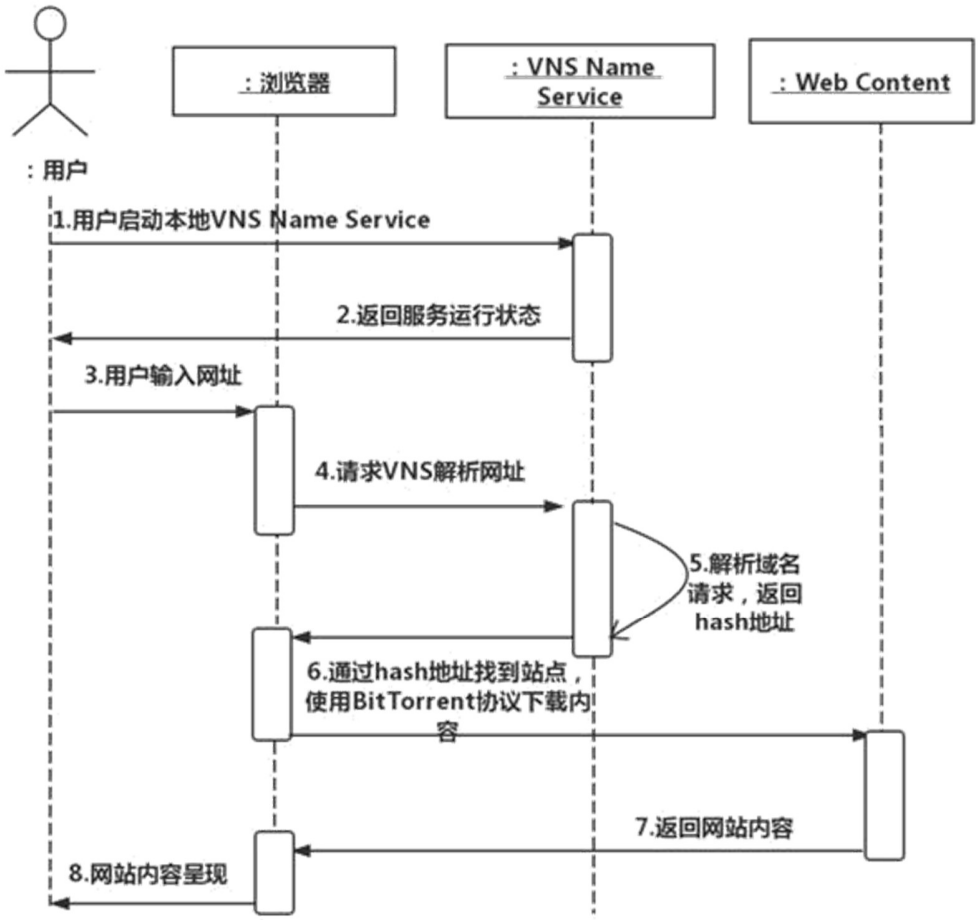
器解析，在此我们将使用 BitTorrent 协议，以提高网站内容下载速度。第五，去中心化站点系统将全面兼容现有互联网服务，用户可以正常连接到现有所有网站系统。

五、 去中心化网站系统的技术路径

1. 本地站点托管

将站点托管在本地个人 PC 上并不是新概念，在现有体系下使用，托管在云端的服务完全可以架设在本地电脑上。然而一个现实的问题是，普通用户很少拥有公网 ip 地址，也就无法正常的通过 DNS 解析等等。虽然在现有体系下，在本地架设站点十分容易，但是想要对外正常提供服务，对普通用户来讲过程十分复杂，并不具有可操作性。

VNS 去中心化网站系统，将使用 VNS 地址作为网站索引寻址的地址而不是 IP 地址，例如使用分布式哈希表（DHT）来建立网站地址索引，这就解决了普通用户缺少 IP 地址的问题。由于要实现基于 hash 的网站地址索引，现有的 web 服务器，如 apache, nginx 等会存在兼容性的问题，所以 VNS 去中心化网站系统，将提供一套完整的 web 服务器功能，提供一个嵌入式的小型数据库以便于使用者进行站点开发。网站访问方面，用户可以通过使用现有主流浏览器访问网站内容。简要工作流如下图:



2. 安全性及隐私

VNS 主链使用了非对称加密的私钥公钥体系。基于 VNS 主链的去中心化网站系统也基于同样的加密体系。对于网站建设者来说，私钥唯一保存在建设者手里，网站建设者可以对拥有的网站的内容签名，以确定其所有权。VNS 主链，可以保证网站建设者通过建设站点得到的 VNS 代币的安全性。对于网站访问者，VNS 去中心化网站系统将运行在独立沙盒（sandbox）中，访问者如果遇到病毒站点等等，将其内容从本地删除即可。同时，对于访问者来说，由于身份暴露在整个系统中的是自己的 VNS 地址，他人无法追踪追踪 VNS 地

址持有者的真实身份，所以整个访问过程是匿名的。我们也会考虑提供对 TOR 的支持，以提高匿名和保护隐私的需求。

另外请重点注意，为符合中国法律法规，对中国用户，我们将嵌入必要的内容校验机制，过滤掉不合法内容。

六、 参考文献

[1] 2014 年 1 月 21 日全国 DNS 污染始末以及分析

[2] Kalodner, Harry A., et al. "An Empirical Study of Namecoin and Lessons for Decentralized Namespace Design." WEIS. 2015.

[3] Namecoin https://namecoin.org/

[4] ETH Name Service https://ens.domains/

[5] Ali, Muneeb, et al. "Blockstack: A Global Naming and Storage System Secured by Blockchains." USENIX Annual Technical Conference. 2016.

[6] Atkins, Derek, and Rob Austein. "Threat analysis of the domain name system (DNS)." (2004).