RIF名称服务

规范

版本 1.31-简体中文

索引

序言

万维网的支柱之一是域名系统（DNS）。该系统负责在人类可读名称和数字IP地址之间创建映射。互联网名称与数字地址分配机构（ICANN）是一家公司，负责协调与互联网名称空间和数字空间相关的多个数据库的维护和程序，确保网络运营。ICANN执行DNS根区域注册表的实际技术维护工作。

这些服务是信任和失败的中心点[1][2]；它们可以通过分布式拒绝服务攻击(DDoS)攻击脱机获取，域的映射可以通过强制更改DNS服务器或通过欺骗来自它们的回复进行更改。此外，存在一些安全问题，例如互联网服务提供商(ISP)能够在不容易检测的情况下审查名称。

RIF名称服务(RNS)的目标之一是成为一个分散且安全的类似DNS系统。RNS复制RSK区块链, 从而继承其去中心化性质和安全。

采用加密货币的一个障碍是处理地址的难度。比特币地址有以下几个方面：“06f1b66ffe49df7fce684df16c62f59dc9adbd3f”，当用户试图输入它时，这非常容易出错这么长的字符序列同样难以记住，这样频繁导致采用加密货币不切实际。

总之，RNS是一种区中心化的服务，为用户提供获得人类可读的域或别名，这些域或别名指向不同的资源（例如RSK或Swarm地址）。使用人类可读地址的一个优点是减少了区块链技术的表观复杂性，使最终用户能够更容易使用。

域和子域在公开市场上买卖。首次获得域名的机制通过使用RIF代币的Vickrey盲拍[3]竞标进行。实践表明，人类的心理怪癖，而不仅仅是供需推动拍卖。Vickrey拍卖机制降低了投标人为物品支付过高金额的可能性，并提高了卖家将会取得最高价格的可能性。一旦用户赢得拍卖，域名的所有权将转让给该用户，该用户支付年租金以保留这种所有权。关于如何计算租金的详细信息，请参阅本文件技术部分的“注册商”。

本协议中提供的初始指南可能会有进一步修改，因为未来生态系统讨论和改进这些想法和架构。

RIF生态系统

RIF代币

在RNS代币经济中，RIF代币的主要功能是要防止未使用的域产生的未使用存储，或者防止名称抢占。域所有者应该有罚没任何未使用所有权的奖励。为此目的，域所有者锁定RIF代币，一旦释放了域，这些代币将被退还。此外，任何费用或罚款都必须使用RIF代币执行，这些代币将分配给网络资源池。网络资源工具已存在，以在RIF名称服务采用的早期阶段补贴某些将有必要的网络费用。最终目标是要启用资金的去中心化管理。

RIF开放标准(RIFOS)

RIF实验室实施的RIF Explorer是每个RIF服务的一组抽象层，允许每个RIF服务与特定实施进行分离。特定实施对作为服务提供商的平台是已知的。这种分离能使每个服务随着新技术提升的问世而演化。

为了支持RIF平台的每个服务的不同服务提供商，RNS被用作服务发现机制。这将允许用户和开发人员找出可用的服务提供商以及如何与他们沟通。如需了解关于RIF Explorer的更多信息，请参阅其相应的白皮书[4]。

简介

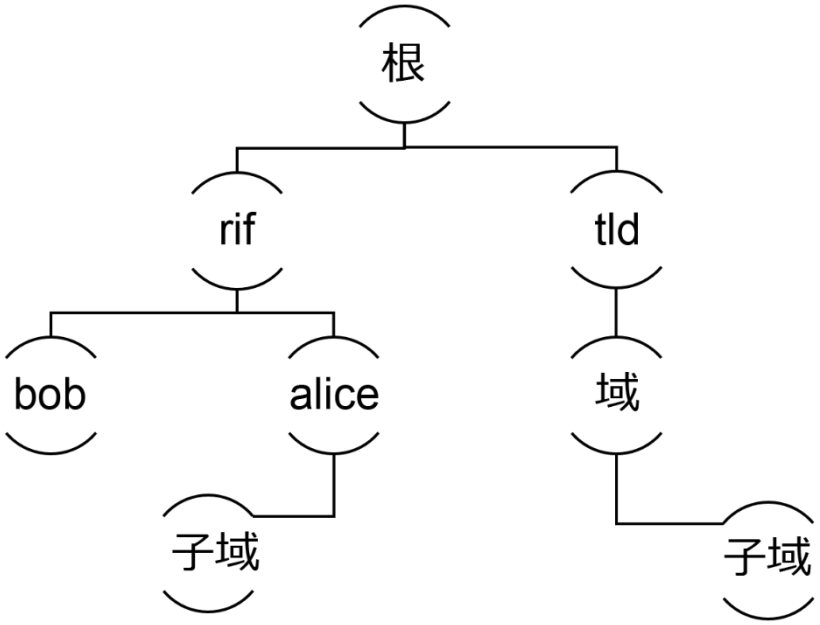
以下部分基本说明了RNS组件。更多详情，请参阅技术部分。

组件概述

RIF名称服务架构基于EIP-137[5]中描述的以太坊名称服务（ENS）。其可划分为三个主要组件：注册表、解析器和注册商。

节点

在RNS上，顶级名称定义为“*.rsk*”。二级名称称为“域”。此外，域可以通过子域指向不同的资源。节点是子域层次结构树的一部分。此树中根的路径是域名。该路径通过点（“.”）分割成各个组件。每个节点存储中间组件名称字符串的散列，由上面解释的这种名称哈希算法计算。



名称格式

RNS名称格式必须符合以下语法：“subdomain.domain.rsk”。简而言之，名称由一系列点分隔标签组成，每个标签都包含一个子域树级别。此外，子域名必须符合名称格式技术部分中说明的规则。

解析器

解析器合约负责解析资源名称。解析器具有许多用户定义的函数，每个函数都允许在同一节点上获取不同的资源类型。

注册表

注册表合约提供域与其解析器之间的简单映射。与域名所有权相关的所有内容均在此合约中进行管理，包括所有权转移和子域创建。

注册商

注册商负责RNS管理。此外，它还负责为用户注册域名，而且是唯一能够更新RNS注册表的实体。如果域被迁移到另一个注册商（迁移流程见下文），它可以将子域的所有权委托给其他注册商。

正如之前所解释的，在RNS初始阶段，将只提供一个顶级域名（TLD）：“.rsk”。通过减少顶级域名的数量，我们可以专注于二级域名的注册，并推迟与标准DNS系统和其他名称服务的顶级重叠讨论。

为了防止域名垃圾邮件或抢注，注册商将管理拍卖过程。由于RNS付款以RIF代币计价，因此注册商与ERC677 RIF代币合约进行交互，以便在账户之间进行支付。最

初它只处理“.rsk”顶级域名和任何字符长度的子域。这将受到RNS根节点的限制，RNS根节点由多签名合约控制。这个多签名合约最初将由RSK Labs在测试阶段进行控制。

契约

为了防止因为未使用的域产生不必要的存储使用，或防止名称抢占，域所有者放弃其域名所有权应取得相应的奖励。为此目的，域所有者锁定代币，一旦释放了域，这些代币将被退还。

主要用例

注册域

用户可以通过两种方式获取域。第一种方式是通过所需域的注册商合约开始拍卖。例如，如果“.rsk”是顶级域名并且用户Alice希望获得域名“alice.rsk”，她可以对此域名进行拍卖，进行出价；如果其是最高出价，她将成为“alice.rsk”域名的新所有者。第二种方式是，如果Bob是“bob.rsk”的所有者并且Alice想要子域“subdomain.bob.rsk”，则Bob可以不通过拍卖将子域所有权转授给Alice。一旦用户获得域，她应在注册表合约上定义解析器，该解析器将进行新域和所需资源之间的解析。如果用户未设置解析器，就是默认已设置。这个默认解析器是新拥有的域的母解析器 。 然后，新域的所有者应使用其新域创建解析器条目。例如，如果Alice未在“subdomain.bob.rsk”注册表条目上设置解析器，则“bob.rsk”解析器被设置。

解析域

Dom域解析式一个流程，验证域是否存在并返回与注册表条目相关的信息。此解决方案可用于钱包、交换或dApp，以处理不了解其各自地址的域。为此，首先，让我们假定域“bob.rsk”已存在。要解析“bob.rsk”域，用户必须使用下面提到的返回节点的名称哈希算法（例如0x231..de3）。之后，考虑到该节点，该用户必须查找与其关联的RNS注册表条目。此条目包含给定节点返回所需资源的解析器。

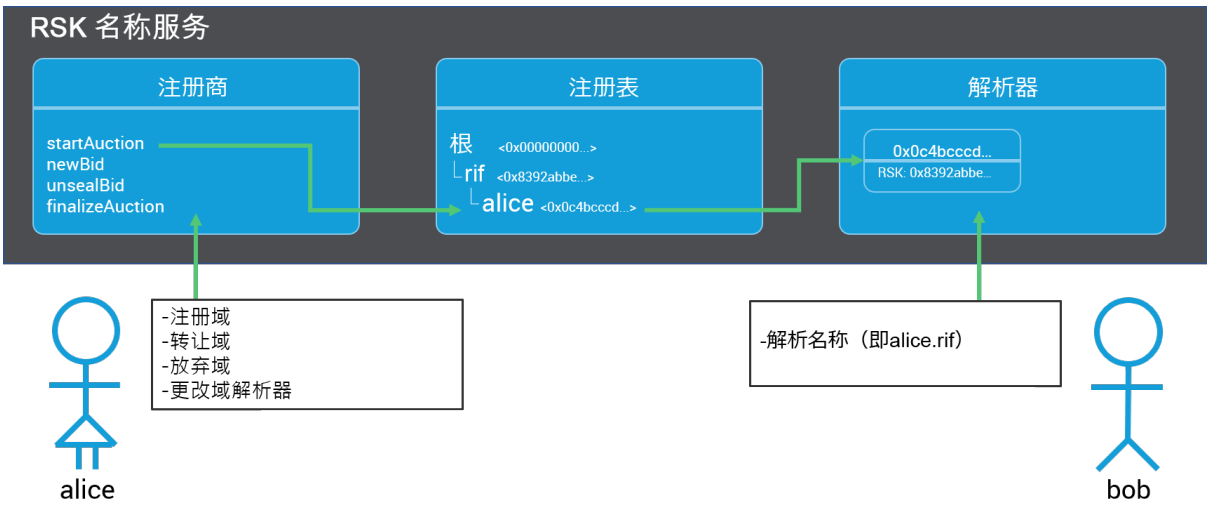
技术概述

RSK Labs部署一个注册表合约，用于处理域名与其所有者之间的映射。每个注册表条目都指向一个解析器，该解析器处理名称域和所需资源之间的解析。

之后，部署管理域名拍卖和供应的注册商合约。对于每个出价，注册商都会创建契约合约，并将用户出价金额转移至该契约。拍卖获胜者必须锁定契约的余额并以该契约换取域名所有权。然后，系统将注册赢家登记在注册表中作为域所有者，她可以设置自己的解析器。

此外，所有者可以使用注册表合约转授子域，无需进行拍卖。

每个名字所有者都有每个名字的契约，并且必须为每个契约支付年租金。收取注册租金的原因是为了防止域名抢注和注册表合约存储中的垃圾域名。如果租金未付，域名所有权将被取消，并且注册商合约中的域名状态将对新的拍卖开放（开放状态）。



组件

注册表

RNSIP01[6]中描述了注册表的指引和界面。

名称格式

RNS名称必须符合以下语法：

```
<domain> ::= <label> | <domain> "." <label>
<label> ::= any valid string label per [7]
```

简而言之，名称由一系列点分隔标签组成。每个标签必须是UTS46[7]中所述有效的标准化标签，使用选项transitional = false并使用STD3AsciiRules = true。对于JavaScript实施，可以使用库[8]规范化和检查名称。

请注意，虽然名称中允许使用大写和小写字母，但UTS46规范化过程会在对它们进行散列之前对标签进行大小写区分，因此具有不同大小写但拼写相同的两个名称将生成相同的名称-哈希。

标签和域可以任意长度，但为了与传统DNS兼容，建议将标签限制为每个不超过64个字符，并将完整的RNS名称设置为不超过255个字符。基于同样的原因，建议标签不要以连字符开头或结尾，也不要以数字开头。

名称哈希算法

RNS使用名称哈希算法。此算法递归散列名称的组件，为任何有效的输入域生成唯一的固定长度字符串

名称哈希的输出称为“节点”。

名称哈希算法的伪代码如下：

```
def namehash(name):
  if name == '':
    return '\0' * 32
  else:
    label, _, remainder = name.partition('.')
    return sha3(namehash(remainder) + sha3(label))
```

解析器

解析器是个界面。用户可以使用RSK提供的公共解析器合约或实施其各自的解析器合约。如果用户不为她的注册表条目设置它自己的解析器，母域名解析器将被使用。 那么该用户应该在母域解析器中注册域名和所需资源之间的解析信息。就像注册表一样，解析器界面和规范在RNSIP01 [6] 中描述。

注册商

注册商界面

constructor(RNS _rns, bytes32 _rootNode, uint _startDate, ERC677 tokcAddr)

- 构造函数接收RNS注册表、注册商所属的根节点以及用于RIF支付的ERC 677代币合约。

startAuction(bytes32 _hash) public

- 将哈希状态从“打开”更改为“拍卖”。

startAuctions(bytes32[] _hashes) public

- 允许任何人开始拍卖多个哈希值。此方法可用于防止攻击者盲目竞价拍卖。在这种情况下，所提交的有些哈希值是虚拟哈希值，而发送者只对一个哈希值出

价感兴趣。这将增加攻击者简单地对所有新拍卖进行盲目出价的成本。开放但未竞标的虚拟拍卖在一周后结束。

newBid(bytes32 sealedBid, uint tokenQuantity) public

- 通过使用sealedBid哈希（使用shaBid函数创建）和许多代币向主合约发送消息创建出价。哈希包含有关出价的信息，包括双向名称哈希、出价值和随机盐。在发布之前，出价与拍卖无关。出价本身的价值可以通过发送超过其实际出价价值进行伪装。一旦拍卖期结束，之后48小时为显示期。 如果在此期限之后发布出价，则可能会使用提供的代币对其进行处罚。由于这是拍卖，预计大多数公共哈希值，例如已知域名和常用字典词，将有多个出价者推高价格。最后，用许多代币和管理这些代币的合约创建契约。

newBidWithToken(bytes32 sealedBid, uint tokenQuantity,) public

- 相当于新出价。它对ERC 677合约的调用很有用。

startAuctionsAndBid(bytes32[] hashes, bytes32 sealedBid, uint tokenQuantity) public payable

- 一个实用程序函数，允许在单个事务中调用startAuctions，然后调用newBid。

unsealBid(bytes32 _hash, uint _value, bytes32 _salt) public

- 竞标期结束后将有显示期，在此期间提交出价所有权的证明。注册商使用shaBid（）函数对这些参数进行哈希处理，以验证其是否与预先存在的保密出价相匹配。如果unsealedBid是新的最佳出价，旧的最佳出价将退还给其出价者。

cancelBid(address bidder, bytes32 seal) public

- 根据以下退款时间表中所述的规则取消未公布的出价。

finalizeAuction(bytes32 _hash) public onlyOwner(_hash)

- 在显示期结束后，必须调用此函数以完成拍卖。拍卖结束后，RNS注册表将以最高出价者作为被拍卖名称的新所有者进行更新。

transfer(bytes32 _hash, address newOwner) public onlyOwner(_hash)

- 更新RNS注册表，将标签哈希的所有权转让给新的所有者。

releaseDeed(bytes32 _hash) public onlyOwner(_hash)

- 契约创建九个月后，名称所有者可以调用此方法放弃名称，并取得其部分契约资金的退款。

eraseNode(bytes32[] labels)

- 允许任何人删除注册商当前不拥有的名称的子域的所有者和解析器记录。例如，要在拥有.rsk的注册商上调零my.example.rsk，传递一个包含[sha3(‘my’), sha3(‘example’)]的数组。

transferRegistrars(bytes32 _hash)

- 如果此注册商不再是RNS中根节点的所有者，此函数则会将契约转让给当前所有者，该所有者应当为新的注册商。如果此注册商仍拥有其根节点，此函数会引发错误。

shaBid(bytes32 hash, address owner, uint value, bytes32 salt) public pure returns (bytes32)

- 哈希秘密出价所需的值。

payRent(bytes32 _hash) public

- 支付域的年租金。

payRentWithTokens(bytes32 _hash) public

- 相当于支付租金。它对ERC 677合约的调用很有用。

acceptedRegistrarTransfer(bytes32 _hash, DeedWithTokens _deed, uint _registrationDate) public pure

- 接受节点转移，并改变其注册商迁移状态。

tokenFallback(address _from, uint _value, bytes _data) public

- 使用ERC 677进行转移所需的函数。

拍卖流程

Vickrey拍卖是个四步流程：

- **打开：**域的默认状态。
- **拍卖：** 拍卖开始。用户可以在72小时内提交保密出价。保密出价可以通过*shaBid（bytes32 hash*、*地址所有者*、*单位值*、*bytes32 标签）*获得。
- **公布：**在拍卖之后，有一个 48 小时的显示期。每个投标者都会显示他/她的出价，注册商会相应地更新拍卖。如果未显示出价，则状态将返回“打开”。
- **已拥有：** 当显示期结束时，拍卖赢家必须提交交易以使用*finalizeAuction*方法最终确定发布时间。这样最终确定拍卖并将拍卖赢家记录为拍卖名称哈希的所有者。

退款和处罚一览表

出价结果	**描述**	**涉及的付款**
用户赢得拍卖	如果用户赢得拍卖，则第二高的出价金额将被锁定	T2：第二最高价 Y：年租金价格

	在其契约（TL）中，其金额与最高出价之间的差额将被退还。当拍卖结束时，此锁定金额减去年租金（Y）的某个百分比金额将作为一项费用（F）支付。	TL：契约中锁定的金额 F：费用 T = (T2 - Y) F= T*0.2 TL = T*0.8
用户输掉拍卖	如果用户因其出价不是最高出价而失去拍卖，则其契约中锁定金额（TL）的百分比将作为一项费用支付（F）	TL：契约中锁定的金额 F：费用 F = 0.05*TL

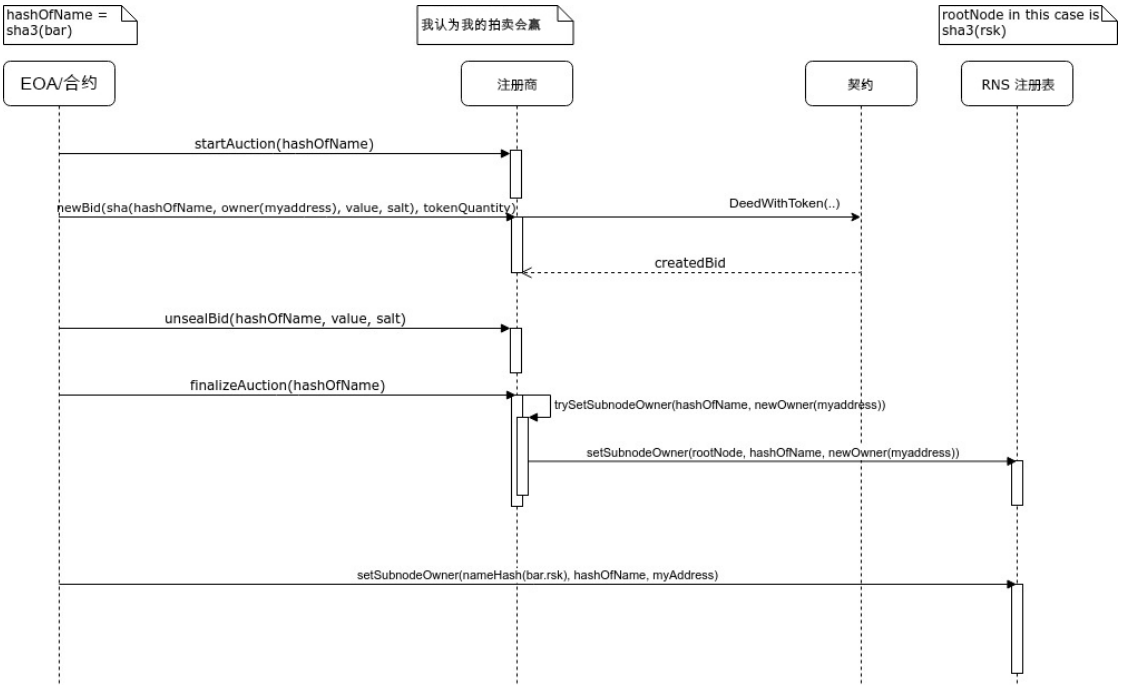
可以显示盲目出价的一段时间（显示期）。 如果投标者在显示期开始之前取消出价，99.5%的出价代币退回。然后，如果出价者在显示期间开始前显示出价，则还原该交易。此期间届满时，每个出价都将结算。假设T是中标金额，T2是第二高的出价金额，而V是在显示期已经结束后公布的出价，付款和退款将按照以下条件进行管理：

条件	**描述**	**涉及的付款**
如果 V > T	如果该出价及时公布，则将获胜	V*0.2将作为一项费用支付，余额则退还
如果 T > V > T2	如果该出价及时公布，它将是第二高价格	V - T2将作为一项费用支付，余额则退还
其他情况	该出价未公布，并且低于第二高价格	V*0.05将作为一项费用支付，余额则退还

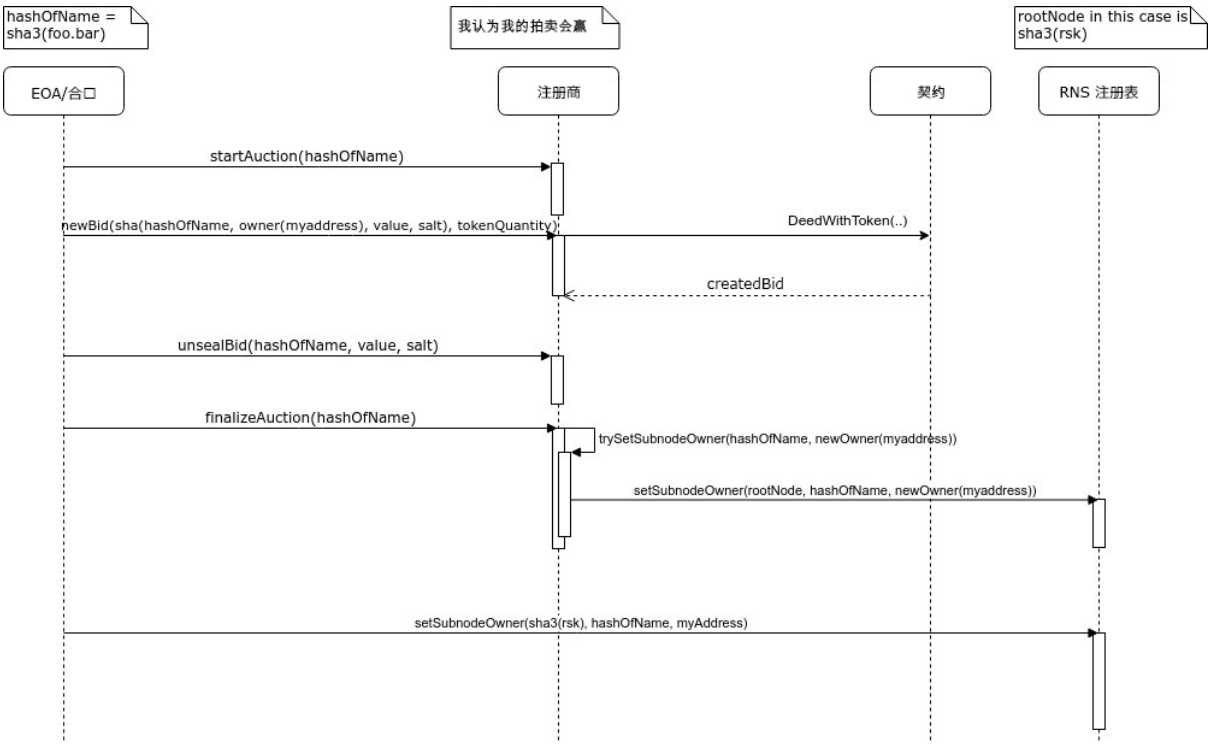
在显示期结束后，用户须在15天内公布出价。如果用户仍未公布，契约上的全部锁定代币则将被发送到RNS网络资源池，其目的是防止RIF代币永远被锁定。

域的唯一性

假设Alice获得域“bob.alice.rsk”的所有权，并将子域“bob.alice.rsk”的所有权转授给另一个用户Bob。获得子域所有权的顺序将如下：



此交互可能表明恶意用户Mallory可以在“.rsk”注册商中开始域名`sha3(“subdomain.bob”)`的拍卖，即使她不是“.bob”的合法所有者。 这是因为拍卖是针对域名的名称哈希而不是名称字符串。假设Mallory想要抢注Bob拥有的“subdomain.bob.rsk”域名。流程如下：



之后，Mallory将会使用他自己的解析器合约在RNS 注册表上为sha3设置条目((sha3(‘rsk’)，sha3(‘subdomain.bob’))， 目的是将“subdomain.bob.rsk”的解析重定向至不同的资源。但是当用户查找域名‘subdomain.bob.rsk’地址时，名称哈希算法（如上所述）将解析sha3(sha3(sha3(‘rsk’),sha3(‘bob’)),sha3(‘subdomain’))而不是sha3(sha3(‘rsk’), sha3(‘subdomain.bob’))。因此，名称哈希算法所解析的域名将会是Bob所定义的那个。

契约

发送给注册商的每个RIF代币都存储在一个名为“Deed（契约）”的单独合约中。每个契约都存储特定名称哈希的代币余额。提交出价时，会创建契约。然后，一旦拍卖完成并注册域名，拍卖赢家的契约和出价将被锁定并交换域名所有权。属于失败出价的契约余额将按要求退还给其合法所有者。与注册商一样，契约合约知道处理代币付款的RIF代币ERC 677合约。

所拥有名称的契约可由其所有者转移到另一账户，从而转移所有权和名称的控制权。该过程通过注册商合约完成。

在拍卖结束九个月后，节点所有者可以选择支付年租金，将域名的所有权更新一年。如果所有者不想再支付年租金，所有者可以选择放弃所有权，并将契约中冻结的资金退还给他/她。

要支付任何域名的租金，用户可以使用注册商的payRent功能。该函数要求支付RIF代币。如果所有者选择放弃所有权，在创建契约九个月后，其可以在三个月期限内调用releaseDeed并将锁定的代币退款。在这三个月期限届满后，该域名的拍卖状态将切换为“开放”，全部契约余额将转移到RNS网络资源池。

未中标出价的契约可以通过各种方式关闭，届时所持有的任何RIF代币将退还给出价者。

ERC 677代币合约

RIF代币使用ERC 677标准进行实施。RNS上年租金或出价的付款使用RIF代币进行。因此，与ERC 677 RIF代币合约交互的过程如下：

- 在具有3个参数的`transferAndCall`函数中，签名必须是：
    - newBid：设置数据参数的签名为0x1413151f，与shaBid函数创建的sealedBid连接。
    - payRent：将数据参数设置为签名0xe1ac9915，与支付租金的标签sha3连接。

改进建议

属于RNS架构的合约可以进行升级，以引入新的改进。这些升级基于社区反馈和RSK实验室提议的方案提供。每个RNS升级都具有向后兼容性，换句话说，域所有权由其所有者保留。

子域管理

用户可以通过两种方式获取指定域的子域。如果域所有者是注册商，用户则可以开始拍卖该域的任何子域。此外，域所有者可以通过使用setSubnodeOwner函数将子域转授给买方，无需经过拍卖流程。最后一个选项不会激励新所有者在不再使用时删除子域的注册表条目，这是因为没有锁定值，因为没有契约合约。我们正在制定更好的转授系统和公平的子域名管理程序。

新注册表结构

对于节点所有权而言，注册表合约是唯一有效的一个。注册表储存所有RNS信息。一旦存储租金已经实施，这就不会再扩大。我们正在研究另一种注册表结构，以使存储租金更加公平。

DNS 域和 Oracles

还可以将常规DNS地址迁移到RNS。DNS地址所有者可以通过使用oracles在RNS中主张一个域，以验证他/她是原始域的合法所有者。如果与ICANN域名发生冲突，将使用仲裁制度解决冲突。该仲裁制度可通过oracles以及其他方法实施。

解析器匿名

用户可能希望隐藏其域映射到的地址。可以使用加密资源完成此操作。所有者可以通过脱链通信渠道根据请求将解密密钥传送给用户。此外，存储的地址可以是隐秘的，因此发件人必须为每个独立付款生成新地址。

创建新的顶级注册商

RSK提供TLD的初始注册商(.rsk)。用户将来可以创建自己的TLD，部署其自己的注册商。用户可以启用拍卖流程（或另一个流程）以使人们获得子域或采用其他手段。

参考文献

[1] M. Ali, R. Shea, J. Nelson, M J. Freedman, "Blockstack: A New Internet for Decentralized Applications" (2017) https://blockstack.org/whitepaper.pdf
[2] "Namecoin FAQS" https://namecoin.org/docs/faq/
[3] "Vickrey Auction" https://en.wikipedia.org/wiki/Vickrey_auction
[4] "RIF Explorer" https://docs.rifos.org/rif-explorer-specification-en.pdf
[5] N. Johnson, "Ethereum Domain Name Service" (2016) https://github.com/ethereum/EIPs/blob/master/EIPS/eip-137.md
[6] J. Len, "Registry and Resolver of RNS" (2018) https://github.com/rnsdomains/RNSIPs/blob/master/IPs/RNSIP01.md
[7] M. Davis, M. Suignard "UTR46" http://unicode.org/reports/tr46/
[8] NPM Library https://www.npmjs.com/package/idna-uts46