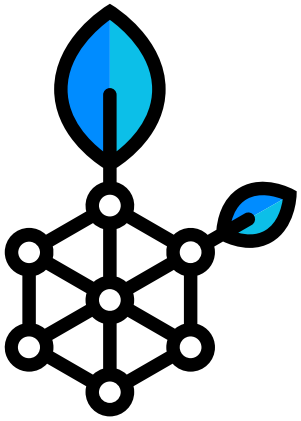


rif

RSK Infrastructure Framework

RIF Identity Protocol

为下一代分布式应用程序构建基础架构

V 1.21

摘要

我们相信加密货币将在未来十年呈指数级增长。但是，要真正实现大规模采用，不仅是精通技术的社区，任何人都需要能够管理数字钱包和资产。因此，采用的主要障碍之一是区块链技术固有的复杂性。

易用性是取得无银行账户和非技术用户的关键。仅举一个例子，如果用户必须复制并粘贴十六进制长的地址传输或接收数字资产，那么很难期望广泛采用。此外，手动输入地址是一个容易出错的过程，而且简单的拼写错误可能会导致资金损失。通过添加名称解析服务（也称为“别名”或“域”），可以大大降低错误概率以及系统的显著复杂性。技术越简单，则越快采用。

RIF目录协议（RDP）的目标是通过简单的资源名称查找不同类型的资源。示例资源如下：RSK地址、个人加密公钥、社交网络句柄等。

此外，集中访问与人类可读名称相关联的多个资源可改善平台的用户体验。由于资源名称可能会随时间而变化，因此系统需要灵活支持频繁更改。最后，该系统使用户能够通过RIF代币轻松购买、出售和拍卖名称。

简介

万维网的支柱之一是域名系统（DNS）。该系统负责将人类可读的名称映射到IP地址。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规则，确保网络运营。ICANN执行DNS根区域注册表的实际技术维护。

这些服务是信任和失败的中心点[1][2]；它们可以通过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能够在不容易检测的情况下审查名称。

RIF目录旨在成为一个去中心化且安全的类DNS系统。在金融包容性和个人自由的背景下的命名服务用例是无穷无尽的。名称服务可以首先用于通过识别交易终点来简化资产转移识别：人们可能有别名与朋友分享，以便安全联系或获得付款。基金会也可以透明地使用别名，并安全地确定捐赠地址，或者向其他机构提供资金的内部资金流。名称服务可以用于为去中心化的互联网站点提供资源定位器，将页面存储在去中心化的存储网络上。名称还用于标识收集公开的信誉代币的任何实体。

RIF目录和金融包容性

导致加密货币目前无法快速大规模采用这一问题的关键是处理用户地址的难度。如果用户必须复制并粘贴十六进制长的地址以传输或接收数字资产，那么很难期望广泛采用。例如，一个随机的RSK地址是“06f1b66ffe49df7fce684df16c62f59dc9adbd3f”，这个在手动转抄时非常容易出错，而一个简单的拼写错误可能导致资金损失。此外 ，这也很难记住。

另一个相关用例是银行账户别名。在银行金融系统中，银行账户有唯一编号。 例如在阿根廷的银行系统中，账号称为CBU，其长度为22位。由于其复杂性，银行提供了构建CBU别名的可能性，这是一个长度在6到20个字符之间的字母数字唯一名称。别名字符必须来自英文字母，并且允许的唯一特殊字符是点（.）和短划线（ - ）。它在银行用户之间的交易中很有用。例如，Bob只需向Alice发送他的人类可读的别名。然后，她在收件人的地址字段中输入Bob的别名并执行交易。 由于使用别名作为账户名时可以简化银行交易，因此其已被所有社区采用。

总而言之，RDP是一项允许用户获取可以与网页等分散或集中资源相关联的商业域的协议，或者可以是一个与个人资源（例如钱包、存储或通信地址）独特关联的别名。使用人类可读地址的一个优点是减少了区块链技术对于最终用户的显著复杂性。

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

RIF目录实施

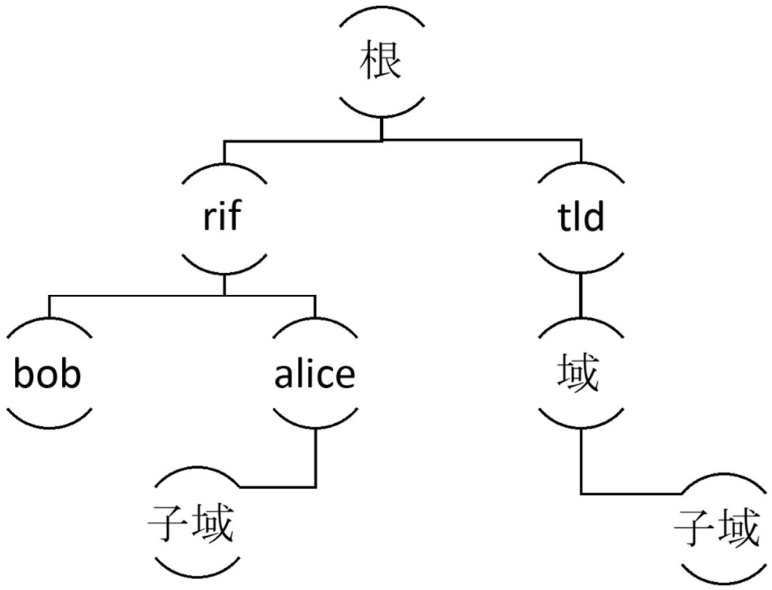
RIF实验室已经为RDP实施了第一个服务提供商，称为RIF名称服务。RNS使用RSK区块链维护和控制对名称信息的访问。因此，RNS确保了RSK区块链的分散性和安全性。虽然其他RDP服务提供商可能会在未来进行注册，但我们认为命名本质上是一种极大地受益于网络效应的服务，因此我们期望RIF和RSK社区长期选择单一提供商。

RIF目录协议的设计

RIF目录协议定义了一个简化地址使用的接口。
这对于实现将方便用户使用的域名映射到资源（例如RSK地址）的机制至关重要。系统应是透明的：用户应能够证明其拥有某个域名，其已经支付了规定的费用，并且有明确的失效日期，从而他们可以提前付款，以减少意外丧失名称权利的风险。此外，设计应考虑不同用户希望获取相同域名的常见情况，并尽力在获得名称之前解决此问题，从而避免代价高昂的争议解决阶段。最后，该设计应尽量减少名称审查和名称抢注风险。对RDP设计非常重要的是RIF代币，这是首次获取名称的首选代币。RIF代币在名称拍卖中用作支付保证金的代币，也用于支付名称的维护租金。

获取域名

域名数据库被解释为树。树的根（称为根节点）控制所有可能的顶级域名（TLD ）。顶级域名（TLD）的下级称为域。此外，域的下级称为子域。
任何RDP名称必须符合以下格式：“子域（n） .... 子域（1）.domain.tld”。名称由一系列以点分隔的标签组成。最后一个标签对应于顶级域，下级域总是在上级域之前。此外，每个标签必须是UTS46[3]中所述有效的标准化标签，使用选项transitional = false并使用STD3AsciiRules = true。



通过盲拍获取域名

首次获得域名的机制通过使用RIF代币的Vickrey盲拍[4]进行。 “Vickrey拍卖是一种密封拍卖。投标人在不知道拍卖中其他人出价的情况下提交书面投标。出价最高的人获胜，但支付的价格为第二高出价”[4]。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，同时也增加了卖家取得最高价格的可能性。
例如，如果“.rif”是顶级域名并且用户Alice希望获得域名“alice.rif”（如上图所示），她可以对此域名进行拍卖，进行出价；如果她的出标最后是最高出价，她将成为“alice.rif”域名的新所有者。

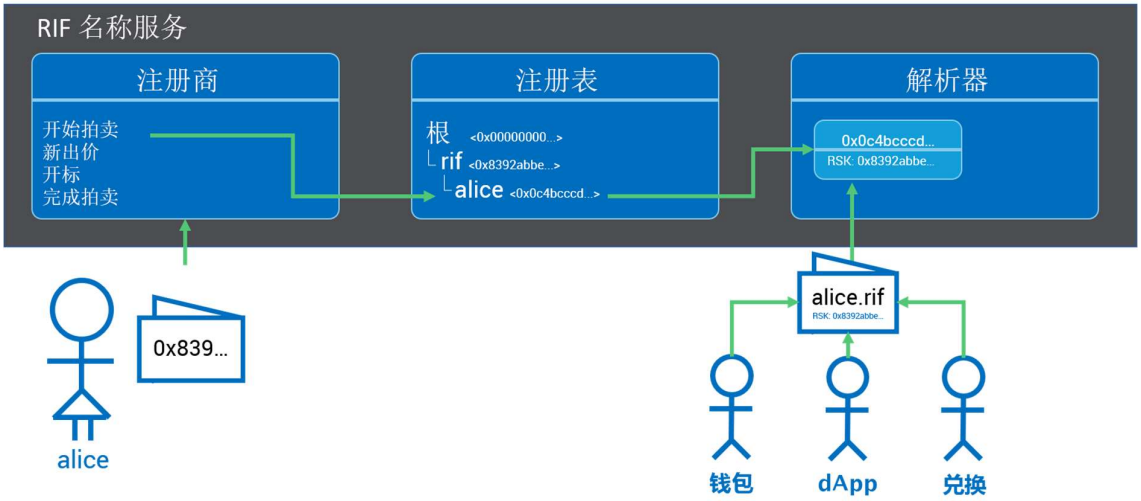
通过转授获取域名

域的所有者可以将子域的所有权转授给买方，无需经过拍卖流程。例如，如果用户Bob是“bob.rif”的所有者并且Alice想要子域“subdomain.bob.rif”，Bob则可以不通过拍卖流程将子域所有权转授给Alice。
从域级别来看，可以通过所有权转移执行转授。一旦Alice获得域，她应设置一个解析器，该解析器将进行新域和所需资源之间的解析（如下节所述）。

域名地址解析

域的解析是系统在数据库中查找名称的过程，检查该名称是否存在；如果存在，则返回相关信息。此项解析可用于钱包、兑换或dApp，以处理便于用户了解的名称，而不

是复杂的地址。例如，为使Alice能够向Bob汇款，Bob首先将他的注册别名发送给Alice，然后Alice可以通过在钱包应用程序中输入别名以查找Bob的地址，钱包将在RDP数据库中查找此名称， 并使用与别名相关联的解析器获得的地址信息继续进行。



二级市场

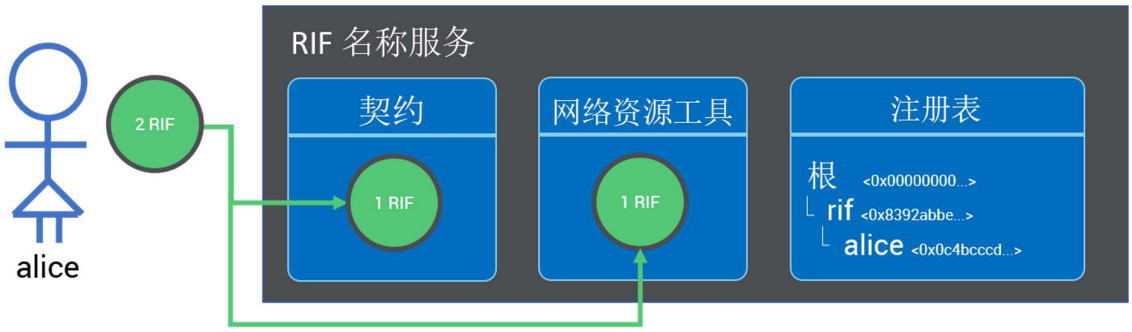
虽然RIF目录没有指定一旦取得域名后用于出售域名的特定二级市场，但已经有去中心化的第二市场解决方案供人们买卖域名。如果需求很高，我们预计RIF社区将创建专门针对域名出售的新二级市场。二级市场可以接受以其他加密货币支付的域名价款，也可以支持其他类型的拍卖，或简单的先到先得转让。域名的二级市场也可以使用RIF代币，但不限于仅使用该代币。

服务提供商的收入

服务提供商可以从名称拍卖和租金中收取费用。他们可以选择没收费用、捐赠费用或使用费用获利。RIF代币收费还可用于防止名称抢注，因为所有者必须为每个取得的域名支付年度维护租金。

锁定的代币

当用户参与拍卖时，提供的RIF代币被锁定在契约中，如下图所示。



获胜出价的一部分（对应于第二高出价的金额）被锁定以换取域名所有权。对应于失败出价而锁定的其他金额将在合法所有者要求时退还给其合法所有者。
当域名发放时，RIF锁定代币将在扣除服务提供商规定的费用后退还给所有者。

年度付款

要获得并保留域名的所有权，所有者必须支付经常性的年费，称为租金。自支付上次年租金起9个月后，域名所有者可以选择支付费用以续展所有权一年或放弃域名的所有权。
如果所有者不支付年租金，则意味着所有者选择放弃所有权，在这种情况下，其原先的锁定代币将在扣除服务提供商规定的费用后退还给用户。

未来

我们已经创建了一个公平有用的协议，以激励用户交易其名称，并减少滥用行为。但是，我们认为协议可能会发展，或者将来可能会被其他更好的RIF协议取代。我们简要讨论协议可以采取的方向。

升级

RDP的服务提供商可以启用代码升级以添加功能或纠正错误。这些升级将由服务提供商的所有者控制。　服务升级应回溯兼容。换言之，不得变更域的所有权（DNS域除外，见下一节所说明）。收费结构、拍卖模型和其他功能可以变更。

DNS 域和 Oracles

通过将DNS域名和顶级域名与RDP域名和顶级域名相匹配，RDP可以将常规DNS地址迁移到RDP。为了公平对待DNS域名所有者，DNS域名所有者应能够在RDP中主张域名并证明其是使用oracles或数字证书链的合法所有者。如果与ICANN域名发生冲突，将使用RDP域名（一种仲裁制度）解决冲突。该仲裁制度可通过oracles或以去中心化的方式实

施。虽然当前版本的RIF目录没有为此提供特定的接口，但我们预计协议可能会在未来版本中取得发展以允许此功能。

匿名

用户可能希望隐藏其别名所映射的支付地址。可以使用加密资源完成此操作。所有者需要通过可能由RIF通信服务提供商提供的链外通信信道将解密密钥传送给用户。此外，加密地址可以是隐秘地址。隐秘地址允许付款人为每笔付款获得新的唯一地址，从而降低付款关联的可能性。

创建新的顶级域名

RIF实验室作为RDP的一个服务提供商。他们已部署了顶级域名的初始注册商。在此提供商中，RIF实验室可能会在未来让用户创建和买卖其自己的顶级域名。

总结

RIF目录协议的构建利用了许多以前从事名称服务的组织所收集的知识，并提供了一个简单且与现有名称服务提供商兼容的统一接口。该接口允许用户获取域名，在域名拍卖中进行出价，管理子域名，并使用RIF代币轻松支付所需费用，以获得可由去中心化和无审查的网络提供的服务。

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] NPM Library https://www.npmjs.com/package/idna-uts46
[4] "Vickrey Auction" https://en.wikipedia.org/wiki/Vickrey_auction