THE ROOT INFRASTRUCTURE FRAMEWORK

V 1.21

RIF Directory Protocol

Building the infrastructure for the next generation of distributed applications

Abstract

We believe that cryptocurrencies will grow exponentially in the next decade. However, to genuinely enable mass adoption, not only the tech-savvy community, anyone needs to be able to manage digital wallets and assets. So, one of the principal barriers for adoption is the inherent complexity of the blockchain technology.

Ease of use is key for reaching the unbanked and non-technical users. It's difficult to expect a broad adoption if users must copy and paste long hexadecimal addresses to transfer or receive digital assets, just to mention one example. In addition, manually typing addresses is an error-prone process, and a simple typo may cause loss of funds. By adding a name resolution service, also known as "aliases" or "domains", the probability of errors is much reduced, as well as the apparent complexity of the system, the easier the technology is, the faster the adoption.

The RIF Directory Protocol (RDP) goal is to find different types of resources by simple resource names. Example resources are: RSK addresses, personal encryption public keys, social network handles, and so forth.

In addition, centralizing the access to multiple resources associated with a human-readable name improves a platform user experience. As resource names may change over time, the system needs to be flexible to support frequent changes. Lastly, the system enables users to easily buy, sell and auction names, through the RIF token.

Introduction

One of the pillars of the World Wide Web, is the Domain Name System (DNS). This system is responsible for mapping human-readable names to IP addresses. The Internet Corporation for Assigned Names and Numbers (ICANN) is a corporation responsible for coordinating the maintenance and rules of several databases related to the namespaces and numerical spaces of the Internet, ensuring the Network's operation. ICANN performs the actual technical maintenance of DNS root zone registries.

These services are central point of trust and failure[1][2]; they can be taken offline by DDoS attacks and mappings for domains can be changed by either forcing changes to the DNS servers or by spoofing replies from them. In addition, there are some security concerns such as ISPs being capable of censoring names without easy detection.

RIF Directory aims to become a decentralized and secure DNS-like system. The use cases for naming in the context of financial inclusion and individual freedom are endless. Name services can first be used to simplify the transfer of assets identify by identifying transaction endpoints: people may have aliases to share with friends in order to contacted securely or be paid. Also foundations may use aliases to transparently and securely identify donation addresses, or internal flows of funds to other institutions. Name services could be used to provide resource locators for decentralized Internet sites, storing pages over decentralize storage networks. Names are also used to identify any entity that collects reputation tokens that are public.

RIF Directory and Financial Inclusion

A problem that slows down mass cryptocurrency adoption is the difficulty of dealing with user addresses. It's difficult to expect a broad adoption if users must copy and paste long hexadecimal addresses to transfer or receive digital assets. For example, a random RSK address is "06f1b66ffe49df7fce684df16c62f59dc9adbd3f", which is notoriously error-prone to manually transcribe and a simple typo may cause loss of funds. Moreover, it's also difficult to remember.

Another related use case is the Bank Account Alias. In the bank financial system, a bank account has a unique number. For example in Argentina's bank system, the account number is named CBU and it has a length of 22 digits. Due to its complexity, the banks provide the possibility of building a CBU Alias, an alphanumeric unique name with a length between 6 and 20 characters. The Alias characters must be from the english alphabet, and the only specials characters allowed are dot (.) and dash (-). It is useful in transactions between bank users. For example, Bob simply sends to Alice his human-readable Alias. Then, she puts in the recipient's address field Bob's Alias and performs the transaction. Due to the increased

simplicity of bank transactions when using an Alias as account, they have been adopted by all community.
To summarize, RDP is a protocol that allows users to acquire commercial domains that can be associated with decentralized or centralized resources such as webpages, or an alias that can be uniquely associated with personal resources (e.g. wallet, storage, or communication addresses). The advantage of using human-readable addresses is the reduction of the apparent complexity of Blockchain technology for the end- user.

The initial guidelines provided in this protocol may be subject to further changes, as the ideas and architecture will be discussed and improved by the ecosystem in the future.

A RIF Directory Implementation

RIF Labs has implemented a first service provider for the RDP, called RIF Name Services. RNS uses the RSK blockchain to maintain and control access to the name information. Therefore, RNS ensures the decentralization and security of the RSK blockchain. Although other RDP service providers may register in the future, we think that naming is inherently a service that greatly benefits from network effects, and therefore we expect a single provider to be chosen by the RIF and RSK community in the long run.

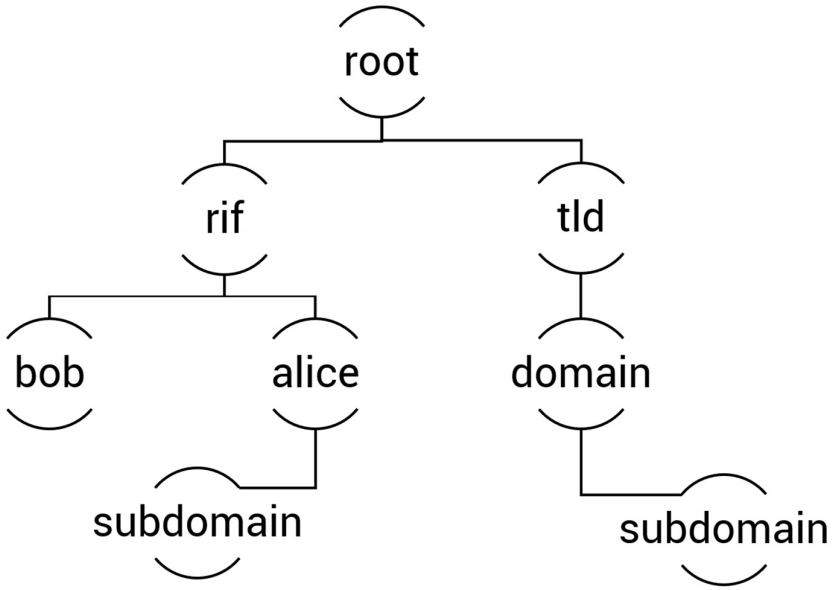
The Design of RIF Directory Protocol

The RIF Directory Protocol defines an interface to simplify the use of addresses.
This is essential to implement a mechanism which maps a user-friendly domain name to a resource (e.g. an RSK address). The system should be transparent: users should be able to attest that they own a certain domain, that they've paid the required fees, and the expiration date is clear so they can make payments in advance to reduce the risk of accidental loss of name rights. Also the design should consider the frequent case which different users want to acquire the same domain name, and try to resolve this before the name is acquired, avoiding costly dispute resolution stages. Last, the design should minimize the risk of name censorship and name squatting. Important to the design of RDP is the RIF token, which is the preferred token for first-time name acquisition. The RIF Token is used as a mean to stake tokens at name auctions and also for paying a name's maintenance rent.

Acquiring Domains

The Domain name database is interpreted as a tree. The root of the tree (called Root node) has control of all possible top-level domain names, or TLDs. The children of the TLDs are called Domains. In addition, children of Domains are called subdomains.

Any RDP name must conform to the following format: “subdomain(n)....subdomain(1).domain.tld”. Names consist of a series of labels separated by dots. The last label corresponds to the TLD, and childs always precede parents. Moreover, each label must be a valid normalized label as described in UTS46 [3] with the the following restrictions: transitional must be false and use STD3AsciiRules must be true.



Obtaining a Domain by Blind Auctions

The mechanism to obtain a domain for the first time is through a blind Vickrey auction [4]. “A Vickrey auction is a type of sealed-bid auction. Bidders submit written bids without knowing the bid of the other people in the auction. The highest bidder wins but the price paid is the second-highest bid” [4]. The practice has shown that human psychological quirks and not just supply and demand drive auctions. Vickrey auction mechanism reduces the likelihood that a bidder will overpay for an item as well as it also increases the likelihood that the seller will get the most he can get for it.
For example, if “.rif” is the TLD and a user Alice wants to get the domain “alice.rif” (as shown in the previous figure), she can open an auction to this domain, make a bid, and if her bid turns out to be the highest, she will become the new owner of the “alice.rif” domain.

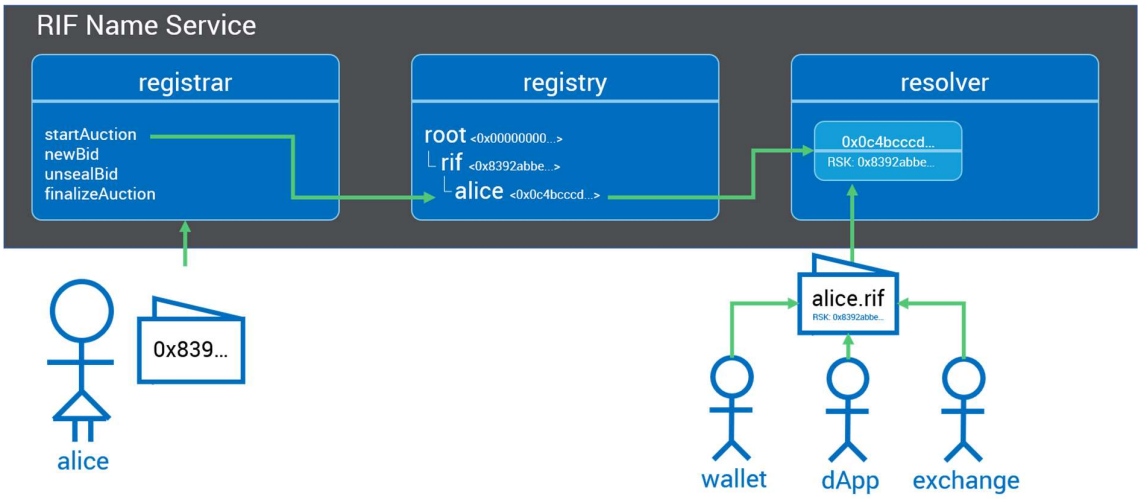
Obtaining a Domain by Delegation

A domain owner can delegate subdomain’s ownership to a buyer without going through an auction process. For example, if a user Bob is the owner of “bob.rif” and Alice wants the subdomain “alice.bob.rif”, Bob can delegate the subdomain ownership to Alice without an auction process.
From the domain level perspective, delegation can be executed through a transfer of ownership. Once a Alice gets a domain, she should set a resolver that will make the

resolution between the new domain and the desired resource, as we will explain in the next section.

Domains Address Resolution

The resolution of a domain is the process where the system looks up the name in the database, checks if it present, and, if so, returns the associated information. This resolution can be used in wallets, exchanges or dApps, to handle user-friendly names instead of complex addresses. For example, for Alice to send money to Bob, Bob first sends his registered alias to Alice, and then Alice can lookup Bob's address, by typing the alias in the wallet application, and the wallet will look up this name in the RDP database and proceed by using the address information obtained by the Resolver associated with the alias.



Secondary Markets

While RIF Directory does not specify a particular secondary market to be used to sell domains once they have been acquired, there are already decentralized second market solutions for people to buy and sell them. If the demand is high, we expect the RIF community to create new secondary markets specifically tailored for domain sells. Secondary markets may accept paying for domains with other cryptocurrencies, and also they may support other kinds of auctions, or simple first-in first served transfers. Secondary markets for domain names may use also the RIF token, but are not limited to use only the token.

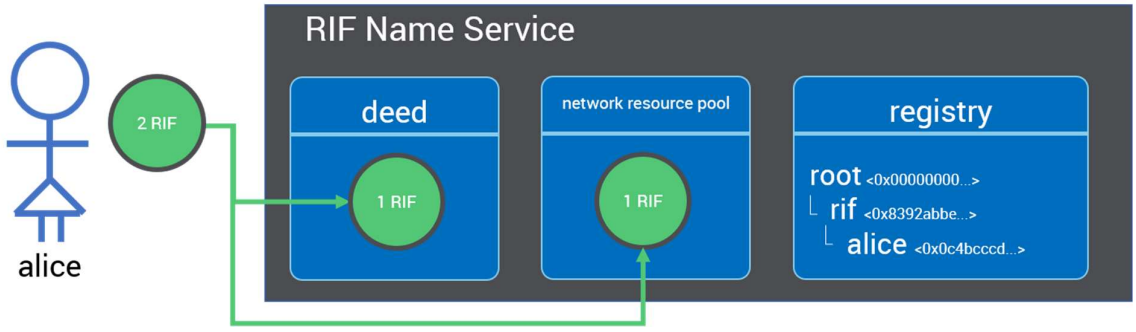
Service Provider's Revenues

Service Providers may collect fees from name auctions and rents. They may choose to either burn the fees, donate them, or use them for profit. The RIF token fees also serve to prevent

name squatting, because owners must pay an annual maintenance rent for every domain acquired.

Locked Tokens

When a user participates in an auction, the RIF tokens offered are locked in the Deed as shown in the following diagram.



A part of the winning offer, corresponding to the amount of the second winning offer, is locked in exchange for the domain ownership. The other amounts locked corresponding to losing bids are refunded to their rightful owners on request.
The RIF locked tokens will be refunded to the owner when the domain is released, minus fees that are defined by Service Providers.

Annual Payments

To obtain and retain ownership of the domain, an owner must pay a recurrent annual fee called rent. After nine months from the last annual rent paid, the domain owner will have the option to pay for the fee to keep ownership for another year or relinquish ownership over the domain.
If the owner doesn't pay the annual rent, it means the owner is opting to relinquish ownership, in this case his originally locked tokens will be returned to the user, minus a fee defined by the Service Provider

The Future

We have created a protocol that is fair and useful providing incentivizes for users to trade names but reducing abuse. However, we think that the protocol may evolve or other better RIF protocols may replace it in the future. We briefly discuss what directions the protocol could take.

Upgrades

A Service Provider of the RDP may enable code upgrades to add functionality or to correct bugs. These upgrades would be commanded by the service provider owners. Service upgrades should be backward compatible. In other words, the ownership of domains should not be altered (with the exception of DNS domains, as explained in the next section). Fee structures, auction models and other functions could be altered.

DNS Domains and Oracles

RDP opens the possibility for the migration of regular DNS addresses to the RDP, by matching DNS domains and TLDs with RDP domains and TLDs. For this to be fair with DNS domain owners, a DNS domain owner should be able to claim a domain in the RDP and and prove he is the legit owner using either oracles or digital certification chains. In case of collision between an ICANN name domain, and a RDP domain, an arbitrage system may be used to resolve the conflicts. Said arbitrage system could be implemented through oracles, or in a decentralized manner. Although the current version of RIF Directory does not provide a specific interface for this, we foresee the protocol could evolve in future versions to allow this functionality.

Anonymity

Users may want to hide the payment address their alias maps to. This can be done with encrypted resources. The owner would need to transfer the decryption key to a user on request through an off-chain communication channel, possibly offered by a RIF Communications service provider. Also, the encrypted addresses can be a stealth address. Stealth addresses allow the payer to derive new unique address for each payment, reducing the likelihood payments can be linked.

Creating New Top-level Domains

RIF Labs acts as a Service Provider for RDP. They have deployed an initial Registrar for TLD. Within this provider, RIF Labs may, in the future, let users create, buy and sell their own TLDs.

Summary

The RIF Directory Protocol was build leveraging the knowledge collected by many prior organizations that have worked on name services and provides a single unified interface that is both simple and compatible with existent name service providers. The interface allows users acquire domains, make a bid in a domain auction, manage subdomains, and pay the required fees using RIF Tokens easily, for a service that can be provided by a decentralized and uncensored network.

References

[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