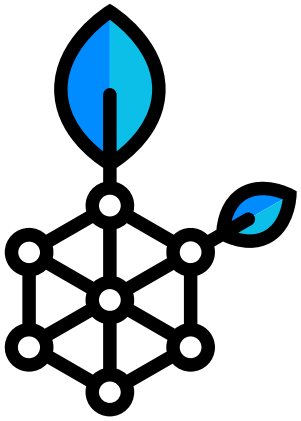


rif

RSK Infrastructure Framework

RIF Identity Protocol

次世代分散型アプリケーション向けインフラストラクチャの構築

V 1.21

概要

仮想通貨は今後 10 年で急成長すると考えられています。しかしながら、大量導入を実際に可能にするためには、テクノロジーに精通しているコミュニティだけではなく、誰もがデジタルのウォレット（財布）とアセット（資産）を管理できるようにならなければなりません。導入の主な障壁の 1 つにブロックチェーン技術特有の複雑性が挙げられます。

銀行口座を持っておらず技術に詳しくないユーザーに到達するうえでの鍵となるのは使いやすさです。これはあくまで 1 つの例ですが、ユーザーがデジタルアセットの譲渡または受領時に 16 進数の長ったらしいアドレスをコピーして貼り付けなければならないとしたら、幅広い導入は期待できません。そのうえ、アドレスの手動入力は間違いやすく、1 文字でも間違うと資金の損失につながりかねません。名称解決サービス（「エイリアス」や「ドメイン」とも呼ばれます）を追加することで、エラーの可能性が大幅に軽減されるだけでなく、システムの明白な複雑性も薄れてテクノロジーが簡易化されるため、導入が加速します。

RIF ディレクトリ・プロトコル（Directory Protocol：RDP）の目的は、簡単なリソース名を付けることで様々な種別のリソースを検索できるようにすることです。リソースの例：RSK アドレス、個人の暗号化パブリックキー、ソーシャルネットワークのハンドル名等。

さらに、人間が読み取れる名称に関連付けられた複数のリソースへのアクセスを中央集中化することで、プラットフォームのユーザーエクスペリエンスが向上します。リソース名称は時間の経過とともに変わる可能性があるため、システムは頻繁な変更に対応できるような柔軟性を備えている必要があります。最後に、このシステムによって、ユーザーは RIF トークンを通じて名称の売買やオークションを簡単に実行できるようになります。

はじめに

ワールド・ワイド・ウェブの柱の 1 つはドメイン名システム（DNS）です。このシステムは人間が読み取れる名称を IP アドレスにマッピングするものです。Internet Corporation for Assigned Names and Numbers（ICANN）は、ネットワーク運営が保証されるように、インターネットの名称スペースと数字スペースに関連する複数のデータベースのメンテナンスとルールを調整する組織です。ICANN は DNS ルート・ゾーン・レジストリの技術的なメンテナンスを実際に実行しています。

これらのサービスは信頼性と障害の中心ポイントです[1][2]; DDoS 攻撃によってオフラインで盗まれる可能性があり、DNS サーバーの強制変更または DNS サーバー応答のなりすましのいずれかによってドメインのマッピングが変更される恐れがあります。さらに、容易に検出されることなく名称を検閲できる IPS など、セキュリティに関する懸念がいくつかあります。

RIF ディレクトリ（Directory）は分散型の安全な DNS のようなシステムとなることを目指しています。金融包摂と個人の自由という文脈でのネーミングの使用事例は無限です。名称サービスは、本来、取引エンドポイントを特定することで、資産の譲渡を簡素化するのに用いることができるものであり、人は安全な方法で連絡を受けたり、支払を受けたりする目的で友人とエイリアスを共有する場合があります。さらに、財団法人がエイリアスを用いて透明かつ安全に寄付の住所、もしくは他の機関への内部の資金の流れを特定することがあります。名称サービスは、分散型インターネットサイトにリソースのロケーションを提供して分散型のストレージ・ネットワークにページを保存するのに使用することが可能です。また、名称を使用してパブリックである評判トークンを収集する組織が特定されています。

RIF ディレクトリと金融包摂（Directory and Financial Inclusion）

仮想通貨の大量導入を遅滞させている問題とはユーザーのアドレスを処理する困難さです。ユーザーがデジタルアセットの譲渡または受領時に 16 進数の長ったらしいアドレスをコピーして貼り付けなければならないとしたら、幅広い導入は期待できません。例えば、無作為の RSK アドレスが「06f1b66ffe49df7fce684df16c62f59dc9adbd3f」だとしたら、手動で入力する際にきっと間違えやすく、ちょっとした入力ミスが資金喪失につながりかねません。そのうえ、覚えるのが困難です。
もう 1 つの関連した使用事例は銀行口座のエイリアスです。銀行の金融システムでは、銀行口座には一意の番号が付されています。 例えば、アルゼンチンの銀行シス

テムでは、口座番号は CBU と呼ばれ、22 桁の数字から成ります。こうした複雑性を理由に、銀行は 6〜20 字の長さのアルファベットの一意の名称である CBU エイリアスを構築するという動きにシフトしています。エイリアス文字は英語のアルファベット表記とし、唯一認められている特殊文字はドット（.）とダッシュ（-）です。これは銀行利用者間の取引において便利です。例えば、Bob は Alis に人間が読み取れるエイリアスを送信するだけで済みます。その後、Alis は受領者のアドレス欄に Bob のエイリアスを入力して取引を実行します。 口座としてエイリアスを利用する際に銀行取引の簡潔性が向上することから、全てのコミュニティによって導入されてきました。
つまり、RDP は分散型またはウェブページ等の中央集中型リソースに関連付けることが可能な営利的なドメイン、あるいは個人的なリソース（例：ウォレット、ストレージ、コミュニケーションのアドレス）に独自に関連付けることができるエイリアスをユーザーが取得するのを可能にするプロトコルなのです。人間が読み取れるアドレスを使用することの利点は、エンドユーザー側には、ブロックチェーン技術の見掛け上の複雑さが緩和されることです。

このプロトコル内の初期のガイドラインは変更されることがあり、そのアイデアとアーキテクチャについては今後考察されたうえでエコシステムにより改良されます。

RIF ディレクトリ実行（Directory Implementation）

RIF Labs は RIF 名称サービス（Name Services）と呼ばれる RDP の初のサービスプロバイダです。RNS は RSK ブロックチェーンを用いて名称情報へのアクセスの保守管理と制御を行います。よって、RSN は RSK ブロックチェーンの分散化と安全を保証します。その他の RDP サービスプロバイダが今後登録することが考えられますが、ネーミングは本質的に、ネットワークの効果に伴う大きな恩恵を享受するサービスであると当社は考えていることから、長期的には RIF および RSK コミュニティによって選ばれる唯一無二のプロバイダとなることを目指しています。

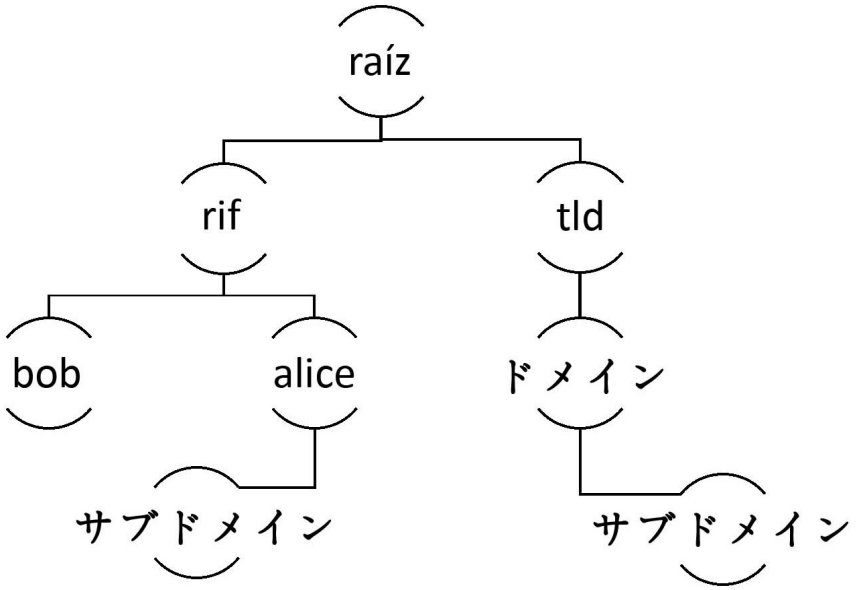
RIF ディレクトリ・プロトコル（Directory Protocol）の設計

RIF ディレクトリ・プロトコル（Directory Protocol）はアドレスの利用を簡素化するインターフェースを定義します。
このことはリソースにユーザーフレンドリーなドメイン名をマッピングするメカニズムを実行するうえで不可欠です（例：RSK アドレス）。システムは透明であるべ

きです：ユーザーは、特定のドメインを保有すること、必要な手数料を支払済みであること、ならびに有効期限が明確であることを立証でき、結果として、名称権の予期せぬ喪失というリスクを縮減するために前払いを行うことができることが不可欠です。設計も、様々なユーザーが同じドメイン名を取得したいと考えるような頻出事例を勘案し、名称が取得される前にこうした問題の解決に取り組み、費用のかさむ紛争解決に発展するのを回避すべきです。最後に、設計は名称の検閲や無断占有というリスクを最小化すべきです。RDF の設計にとって重要なのは RIF トークンであり、初回の名称取得にあたっての推奨トークンです。RIF トークンは名称オークションの場でのトークン付与の手段として用いられると同時に、名称の保守管理レンタル料の支払にも使用されます。

ドメインの取得

ドメイン名データベースはツリーとして解釈されています。ツリーの根っこ（ルートノードと呼ばれます）は全ての考えられるトップレベルのドメイン名、または TLD を支配します。TLD の子供たちはドメインと呼ばれます。加えて、ドメインの子供たちはサブドメインと呼ばれます。
RDP 名は以下のフォーマットに適合する必要があります：「サブドメイン（n）.... サブドメイン（1）.domain.tld」。名称はドットで区切られた一連のラベルで構成されます。最後のラベルが TLD に対応し、子供は常に親の前に来ます。さらに、各ラベルは、UTS46 [3]で説明されている通り、正規化された有効なラベルとし、以下の制約事項が伴います：transitional=false で、STD3AsciiRules = true とすること。



ブラインドオークションによるドメイン取得

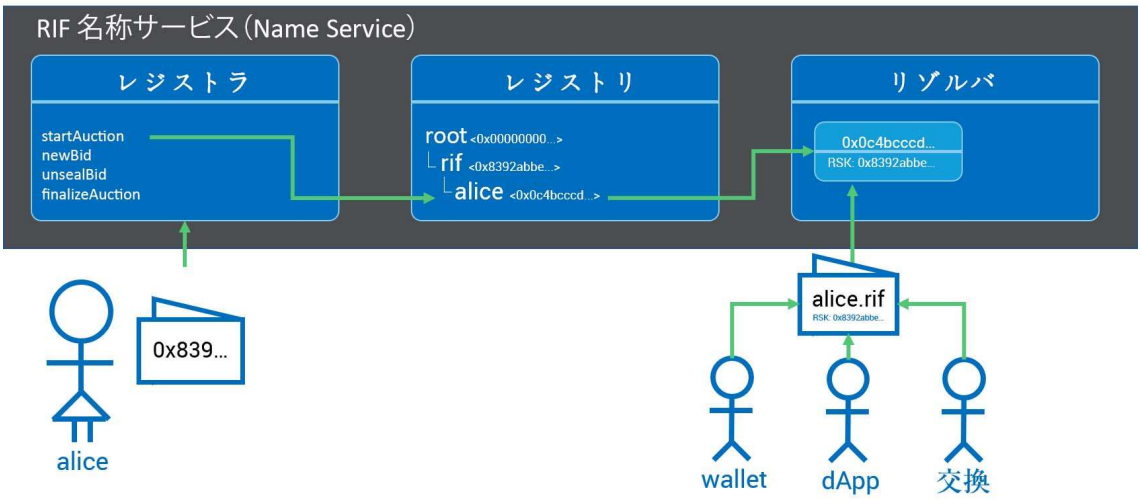
初めてドメインを取得するにあたってのメカニズムは Vickrey オークション[4]経由です。 「Vickrey オークションは秘密入札オークションの 1 つです。入札者はオークションにて他人の入札のことは認識せずに書面形式の入札を行います。最高値を付けた入札者が選ばれますが、支払う価格は 2 番目に高い値とします」[4]。その慣例は、人間心理学的なねじれを示しており、単にドライブオークションの需要と供給ではありません。Vickrey オークションのメカニズムにより、入札者がアイテムに対して過剰に支払う可能性が減ると同時に、売り手側がそのために入手できるものの大半を入手する可能性が増します。
例えば、「.rif」が TLD であり、ユーザーであるドメイン「alice.rif」（前の図のように）を取得したい場合、彼女はこのドメインに対してオークションを開いて、ドメインに値を付け、自身の値が最高値であれば、彼女は「alice.rif」ドメインの新しい所有者になります。

委譲によるドメインの取得

ドメインの所有者はオークションのプロセスを踏むことなく、購入者にサブドメインの所有権を委譲することができます。例えば、ユーザーである Bob が「bobb.rif」の所有者で、Alice がサブドメイン「“alice.bob.rif”」を欲しがっている場合、Bob はオークションのプロセスを経ることなく、そのサブドメインの所有権を Alice に委譲することができます。
ドメインレベルの視点に立つと、委譲は所有権の移転を通じて実施可能です。Alice がドメインを入手したら、次のセクションで説明しますが、新しいドメインと希望するリソースを照会して割り出すリゾルバを設定すべきです。

ドメインアドレスの割り出し

ドメインの割り出しとは、システムがデータベース内の名称を検証し、存在するかどうか検証し、存在する場合、付随情報を返還するシステムです。この割り出し処理はウォレット、エクスチェンジ、または dApp 内で使用でき、複雑なアドレスではなく、ユーザーフレンドリーの名称を扱うことができます。例えば、Alice が Bob に送金するのに、Bob は最初に自身の登録エイリアスを Alice に送信することで、Alice はウォレットのアプリケーションにエイリアスを入力して Bob のアドレスを検索し、ウォレットが RDP データベース内でこの名称を検索し、エイリアスに関連付けられたリゾルバによって取得されたアドレス情報を使って処理することができます。



流通市場

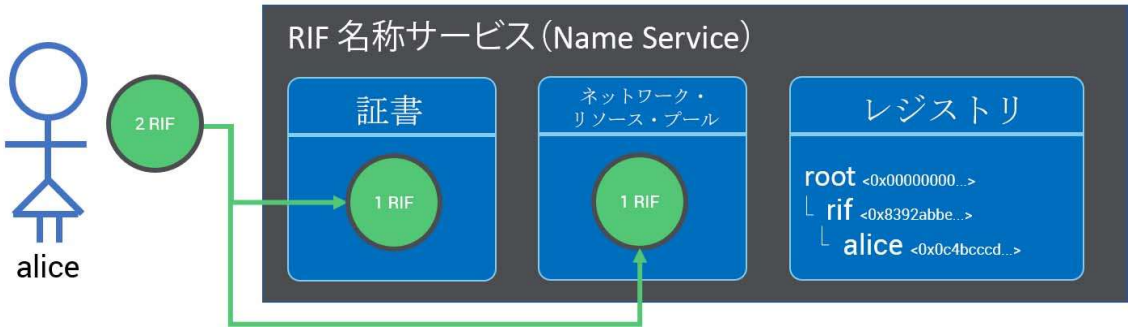
RIF ディレクトリ（Directory）は取得された時点でドメインを販売するのに用いられる特定の流通市場を指定しませんが、ドメイン売買にあたってすでに分散型流通市場ソリューションが存在します。需要が高いと、RIF コミュニティがドメイン販売に特化した新たな流通市場を創造することになることが期待されます。流通市場は他の仮想通貨によるドメイン支払を受諾する場合があり、また、他の種類のオークションあるいは単に先着順の譲渡や移転に対応するかもしれません。ドメイン名の流通市場はさらに RIF トークンを使用しますが、そのトークンの利用に限定されるわけではありません。

サービスプロバイダの収益

サービスプロバイダはオークションや賃料にて手数料を収集すると考えられます。そして、手数料の償却、寄付あるいは営利目的の使用のいずれかを行うと考えられます。また、RIF トークン手数料は名称の無断占有を防止する役割を果たしますが、なぜなら、所有者は取得した各ドメインの年間メンテナンス料を支払う必要があるからです。

ロックされたトークン

ユーザーがオークションに参加する際、申し出られる RIF トークンは以下のダイアグラムにて確認できるように、証書としてロックされます。



落札オファーの一環として、2 番目に高い金額相当がドメイン所有権の対価としてロックされます。落札者以外の入札に相当するその他の金額は、要請を受けた時点で、正規の所有者に返還されます。
ロックされた RIF トークンですが、ドメインが解除されると、サービスプロバイダ規定の手数料を差し引いて所有者に返還されます。

年間の支払

ドメインの所有権の取得と保持にあたっては、所有者は賃料と呼ばれる年間手数料を継続して支払う必要があります。直近の年間賃料の支払から 9 か月後、ドメインの所有者は次年度も保有を継続するために手数料を支払うか、ドメインの所有を放棄するか選択することになります。
所有者が年間賃料を支払わない場合、所有者は所有権を放棄したものと見なされ、この場合、自身の当初ロックされたトークンはサービスプロバイダ規定の手数料を差し引いて返還されます

今後の見通し

当社はユーザーが名称を売買するインセンティブを供与しつつも悪用を縮減する公正で有用なプロトコルを創造しています。ただし、プロトコルが進化してゆく、または他のより優れた RIF プロトコルが今後取って代わることになるかもしれません。プロトコルが歩みうる方向性について手短に検証します。

アップグレード

RDP のサービスプロバイダはコードのアップグレードによって機能性の追加やバグの修正を行うことがあります。こうしたアップグレードはサービスプロバイダ所有者によって制御されます。 サービスのアップグレードは後方互換であることとします。言い換えれば、ドメインの所有権は改ざんされるべきではありません（次のセ

クションにて説明される、DNS ドメインの例外は除きます）。手数料体系、オークションのモデル、その他の機能は改訂される可能性があります。

DNS ドメインと Oracles

RDP は DMS ドメインならびに RDP ドメインを有する TLD を適合させることで、TLD 通常の DNS アドレスの RDP への移行という可能性の扉を開きます。このことが DNS ドメイン所有者にとって公正であるよう、DNS ドメイン所有者は RDP にてドメインを申請し、自身が Oracles またはデジタル認証チェーンのいずれかを使用して正当な所有者であることを証明できることが不可欠です。ICANN のドメインと RDP ドメインがぶつかる場合は、裁定システムが使用されてこの衝突が解消されることがあります。上記の裁定システムは Oracles、または分散型の方法により実装されている可能性があります。現行版の RIF ディレクトリ（Directory））はこれについて特定のインターフェースを提供しませんが、今後のバージョンでプロトコルが進化してこの機能性が実現することが期待されます。

匿名性

ユーザーは自らのエイリアスがマッピングする決済アドレスを非表示にしたいと思う場合があります。それは暗号化されたリソースで実現できます。所有者は RIF Communications サービスプロバイダによって提供されるような、オフチェーンのコミュニケーション経路にて、要請に応じ、ユーザーに暗号解読キーを譲渡する必要があります。また、暗号化されたアドレスはステルスアドレスの可能性があります。ステルスアドレスは支払者が各決済の新規の一意のアドレスを得るのを可能にし、決済がリンクされる可能性を低減します。

トップレベルのドメインの新規作成

RIF Labs は RDP のサービスプロバイダの役割を果たします。そして、TDR の初期のレジストリを展開しています。このプロバイダ内で、RIF Labs は、今後、ユーザーが独自の TLD の生成、購入、売却を行うのを可能にすることになるかもしれません。

要約

RIF ディレクトリ・プロトコル（Directory Protocol）は名称サービスに取り組んできた数々の先行組織によって収集された知識を活用すべく構築され、シンプルで、かつ、既存の名称サービスプロバイダと互換する単一の統合インターフェースを提供します。そうしたインターフェースは、ユーザーによるドメイン取得、ドメインの

オークションでの入札、サブドメインの管理、分散型で無検閲のネットワークによって提供可能なサービスに係る RIF トークンを使った必要な手数料の簡単決済を可能にします。

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