RIGOBLOCK: ファンド・インフラストラクチャ向けのプロトコル

アセットマネージャーのための新たなパラダイム

GABRIELE RIGO
RIGOBLOCK創業者
GAB@RIGOBLOCK.COM

要旨.　　資産運用業界は、ファンド流通ネットワークや大手企業によって支配されてしまっています。長年の経験や投資家からの資産、独自の資金を持たない新興のマネージャーにとって、自らのファンドを立ち上げるということは難しく、非常に面倒なことになっています。しかし、大手ヘッジファンドは才能溢れる人材を常に探し求めており、若い専門家たちにリスクを委譲し、最新の研究とデータ分析手法を活用して優れた収益を得ることを目標に掲げています。軽量な運用体制(マネージド・アカウント)も存在してはいますが、管理に負担がかかるため、ポートフォリオの管理やリバランスに多くの時間を費やす必要があります。

ブロックチェーンは、これまでは想像の世界のものでしかなかったコストの低さとプロセスの革新性という2つの性質を備えた理想的な技術であり、短期間でファンドを設立することを可能にします。当社では、新興のマネージャーの皆様でも独自の投資商品を構築することができるような技術的な枠組みを提供します。本ホワイトペーパーでは、その技術的な枠組みのデザイン、実装のビジョン、概念実証、より高い透明性を提供するという機会、運用の効率性、プロセスの刷新などについて考察しています。また、才能に溢れた人やそのような人の懸命な働きに対して見返りを与えるような代替パラダイムの提案も行なっています。

1. イントロダクション

この10年間で、資産運用業界はより大きな企業体制へと向けた統合の道を歩み続けてきています。特に、ヘッジファンド業界は標準化と規制化の進んだ部門へと発展を遂げています。多額の設立コストや最低5,000万ドルという要件だけでなく、それよりもはるかに大きな初期運用資産(Assets Under Management, AUM)などの条件によって、小規模のプレイヤーは自動的に市場から除外される結果となってしまっています。そのような高額のAUM要件の裏には、プライムブローカーサービスをファンドに提供するにはコストが高くついてしまうという理由があります。そのようなコストには、純資産総額(Net Assets Value, NAV)の見積もりや、担保勘定、運用会社のコスト、法務および顧問費用などが含まれています。さらに、投資ファンドや運用会社は多くの場合ただの私書箱のような存在に過ぎません。つまり、そのような企業では実際には誰も雇用しておらず、ただ会社組織をオフショアしているだけに過ぎないのです。

イーサリアムプロトコルは、投資商品を素早く作成するのに最適な技術を提供します。この技術により、リアルタイムな募集や償還が可能となり、管理者や管理人を必要とせずにトラストレスに分散型取引所で取引を行うことが可能となります。その結果、業界でこれまで目にすることができなかったような高い水準の効率性と透明性が実現されることになります。当社の提案するモデルの正の外部性の1つとして、AUMの規模への非依存性によって、大手投資ファンドで職を得るための実績作りのツールとして使用することができるという点があります。これにより、トレーダーの認知度を高めることが可能となります。いずれにせよ、私たちは資産運用の方法を変える道を切り拓いていくことを目指しています。

1.1. 原動力

規制というものは、ファンドマネージャーたちが自らのファンドを立ち上げるのを妨げ、中小企業の買収や合併、望ましくない顧問委員会の導入などを通して他の企業との統合を余儀なくさせている主な要因の1つであり、これにより資産運用業界に内在する利害の衝突を増大させる結果となっています。規制の範囲は、このような利害の衝突の監視と管理を行うためのものであり、マネーロンダリングや不正行為(マネージャーが資金を持ち逃げしたり、不当な費用をファンドに入力したりすることなど)を防止します。当社のモデルの説明を行うことで、いかなる規制も必要としない(あるいは、少なくとも非常に高い自己規制基準を達成する)ような高い透明性と効率性の水準で自己規制を行う1つの枠組みを提供したいと私たちは考えています。当社の提供する仕組みの効率性の水準は、これまでに見たこともないようなレベルのコンプライアンスを提供します。

当社では、あらゆる個人の方が独自の投資商品をシームレスに作成・展開できるようにすることを主な目標としています。当社のビジョンは、取引目的以外の理由で個人の資金にアクセスすることなく、人々に自らの才能を発揮し、情熱を共有し、グローバルに競争できるような技術を提供することです。これにより、ビジネスの運用面での作業量を削減することが可能となり、マネージャーは投資家のためにリスク調整済みの優れたリターンを生み出すことにだけフォーカスすることができるようになります。

利益の衝突は、しばしばファンドの「不十分な」運用実績の原因の1つとなっており、多くの精神的バイアス(近視眼的な損失回避やAUMが大幅に上昇したときに優れたリターンを再び上げることができないことなど)によって不十分な運用実績がもたらされる可能性があります。場合によっては、そのような構造の中で繰り返し起こる利益の衝突に疲れ切ってしまい、優れたマネージャーがファンドを去ってしまうことさえあります。私たちは、利益の衝突を完全に失くすことこそが、投資家とマネージャーの両者にとっての最高の利益になると考えています。

全体として、私たちはマネージャーのことを一番に考え、投資家に最高クラスの技術を提案するような完全分散型のフレームワークを提供したいと考えており、それにより両者の相互利益を一致させようとしています。さらに、私たちは才能に満ちた人向けの競争力と透明性の高い実力主義の市場を構築することを目指しています。

これまで他の人たちによって提案されてきた資産運用向けのブロックチェーンモデルの多くは、非常に中央集権的なアプローチをとっており、規制を比較的受けていない組織に対してある程度の信頼性を必要としています。

1.2. 市場概況

現在までのところ、ブロックチェーン上に構築された資産運用プラットフォームをまだ目にすることはありませんが、私たちは取引や資産運用の分野で過去に行われた試みを再認識する必要があります。例えば、Stellarネットワークでは、取引や株式発行の効率化、募集や償還業務などで使用されているトークン発行のためのプラットフォームを提供していますが、そのアプローチは中央集権化

されており、トークン発行を行う主体が資産の管理を行っているため、依然としてユーザーの信頼性を要求しています。

Iconomiプロジェクトは暗号通貨関連資産の取引用プラットフォームになることを目指しており、*中央集権型のサーバーベースのアプローチ*で株式発行や募集、償還などのプロセスをデジタル化しようとしています。Iconomiプロジェクトでは、ユーザーフレンドリーなフロントエンドプラットフォームが提供されており、ブロックチェーンブラウザとのやりとりを必要としていません。Iconomiプロジェクトではユーザーの秘密鍵の管理を行っているため、資金の管理人(技術と流動性スタックのみを提供するために、現在はイギリスのアセット・マネージャーとパートナーシップ締結済み)として機能しており、そのためインフラである程度の信頼性を必要としています。また、Iconomiプラットフォームでは、プロのマネージャーを対象としています。Iconomiのような企業の文脈では、RigoBlockの技術はファンドをオンチェーンで構築するために容易にプラグイン可能な分散型エンジンとみなすことができます。

民間銀行で分散型アプローチを正式化するという初の試みは、EtherPlanというプロジェクトで提案されています。しかし、そのアイデアにも高いレベルの信頼性が必要となっており、既存の軋轢の多くをより新しい技術的に高度なものへと置き換えています。そのため、少なくともこのような技術開発の初期段階においては、急激な変化のための基礎を築くことができなくなっています。このプロジェクトは、現在停止状態となっています。その一方で、最近になって同様のアプローチがSwissborgプロジェクトによって採用されており、そのプロジェクト自体は見込み顧客とみなすことができます。*完全に分散した形*でブロックチェーン技術を使用するという初の試みは、Melonportによって行われました。このプロジェクトは、当社初の分散型ヘッジファンドというコンセプトであるDrango(現在はRigoBlock Drango)と同じ時期に誕生しました。どちらのプロトコルも同じ問題を解決することを目指していますが、それぞれ異なる方法論を採用しています。そのため、Melonportは当社に最も近い競合他社であるとみなすことができます。技術的な初期段階にあるとはいえ、この2つのプロジェクトは互いに補完しあうものとみなすこともできます。また、Melonportは分散型資産運用のオープンプロトコルの技術的枠組みおよびコンセプトのための初の正式な使用を提供しており、「モジュール」の一部を提供していくために外部開発者を活用しています。RigoBlockは、より抽象的かつ自由な形で同じようなコンセプトを採用しており、開発者が「独自バージョンの資産運用」を持ち込み、当社のプロトコルを活用できるようにしようとしています。

ShapeshiftによるPrismは、分散型取引所とハイブリッド型の資産運用プラットフォームという2つの性質を備えたプロダクトです。Prismは金融仕組み商品に相当するものであり、ブロックチェーン上で構築が行われています。現時点で、Prismはまだクローズドアルファテスト段階にあります。RigoBlockにとって、Prismは分散型トークンプール(Dragos)で取引可能な資産として扱うことができます。

しかし、現在の技術水準では、イーサリアムのメインネットワーク上にはまだ資産運用プラットフォームは実現されていません。その理由として、分散型取引所そのものが現在はアルファ版の形でのみ*テストネットワーク*上に存在しているという点を挙げることができます。お気づきの方もいらっしゃるかもしれませんが、いくつかの問いにはまだ回答が与えられていません。答えはまだ見つかっていないと謙虚に述べることもできますが、プロジェクトの方向性が経営と技術的な進歩によって決定されるということもあります。そのため、この後のパラグラフでも可能な限りそのような問いに対する回答を行っていくよう取り組んでいきます。

2. ブロックチェーンとファンド

ブロックチェーン上にファンドを作成するというプロセスを説明するために、ここでスマートコントラクトという概念を思い出す必要があります。スマートコントラクトにより、特定のプロセスを管理するというダイナミクスを直接ブロックチェーンにコーディングすることが可能となり、作成プロセスと管理を他のあらゆるものから分離することができます。そして、ブロックチェーン上にデプロイされたコードからファンクションの呼び出しが行われるたびにユニークなコードやトランザクションの一意のハッシュを作成することによって、そのプロセスを分離させることもできます。これはつまり、同じ性質を備えつつ独自の固有識別コードを持つ商品を作成するために、誰でも同じ*Solidityソースコード*[1]を使用することができる可能性があるということを意味しており、事前に定義したさまざまな範囲でパーソナル化させることが可能となります。これは、完全にトラストレスな環境から信頼性に依存する環境に至るまで、さまざまなレベルの信頼性に対応するものとなります。

2.1. **信頼性**　価値の交換は、互いに相手を信頼する必要なく、ブロックチェーン上で行われます。これこそがブロックチェーン技術の美しさであり、この利点をスマートコントラクトにも利用することが可能となっています。実際、*エスクロー口座(Escrow Account)*を慎重に扱うことにより、ファンド内でトラストレスな形で資金の移転を行うことが可能となります。実際、エスクロー口座を慎重に扱うことにより、ファンド内でトラストレスな形で資金の移転を行うことが可能となります。より正確に言うと、価値の一部がファンド内にある場合、その価値はマネージャーが取引目的でのみ使用することが可能であり、それ以外では決してアクセスすることができません。マネージャーは、分散型取引所のエスクロー口座に対して入金の指示だけ行うことができます。ブロックチェーン上から資金が移動することは決してなく、常にファンドの管理下にあります。マネージャーもプラットフォームも、資金にアクセスすることはできません。不変性こそがブロックチェーンの大きな特性であり、この性質によってプログラムされていることだけをコードに実行させ、それ以外のことを決して行わせないということを保証することができるようになります。

2.2. **Dragoの作成** Dragosは私たちのファンドとでも言うべき存在であり、通称分散型トークンプールと呼ばれています。RigoBlockプラットフォームは現在アルファ版であり、Parity DAppストアで利用可能となっています。Parity UIをローカルで稼働させている世界中のユーザーから確認することが可能です。つまり、バックグラウンドでソフトウェア(Parityクライアント)を稼働させ、通常のウェブブラウザインターフェースを通してストアにアクセスすることになります。RigoBlockは、「Applications」タブから確認することができます。KovanテストネットでParityを稼働させている場合には、実際に使用することもできます。
また、pool.rigoblock.comで閲覧専用のWebアルファ版を提供しており、rigo.networkではIPFS DAppも提供しています。分散型トークンプールは1クリックでアプリケーション上に作成され、プラットフォームにより1つのトランザクションを通じてブロックチェーン上にコードがデプロイされます。ファンドの名前とシンボルを入力すると、ポップアップが表示され、ユーザーはトランザクションを実行するよう求められます。トランザクションが作成されると、ユーザーは新しいファンドが作成されたことを確認し、自動的なトークン作成プロセスを通じてすぐにファンドの株式の募集を行うことができるようになります。ユーザーの株式の残高がプラスの場合、反対取引を行うことによって株式をEtherに交換することができます。つまり、トークンは破棄され、それと引き換えにEtherを受け取ることになります。

[1] Solidityとはイーサリアムブロックチェーンの用のJavascriptベースの言語であり、バックエンド(ブロックチェーン)に関連するすべてのコードを他のものから完全に分離することを目的として利用されています。

当社のアプローチではソフトウェアの実装を完全にオンチェーンで行っているため、トラストレスな環境とサーバレスなインフラストラクチャを構築することができます。しかし、NAVの計算のような機能はオフチェーンで行われることになるため、最も効率的かつ効果的な形でブロックチェーンを利用することができます。権利や金銭に関わる全てのことがオンチェーンで分散的に行われるということを私たちは強調したいと考えており、提供される情報を信用することなく、ただファンドのコードを知るだけで誰でも分散型ファンドの存在や行動に関するすべての機能をリアルタイムで監査することが可能となります。

3. ソーシャルトレーディング

ファンドマネージャーたちは投資に関する情報を非公開にしなければならないという話をよく耳にしますが、これはそうしなければ競合他社によって彼らのポジションがコピーされてしまい、市場の非効率性を活用することができなくなってしまうからです。このような未解決の問題に対して、当社では2つの異議を提案しています。まず1つ目として、マネージャーたちにポートフォリオの公開を余儀なくさせるソーシャルトレーディングプラットフォームには経験豊富なマネージャーの積極的な参加が促進されるという観察結果があります。そして、2つ目として、金融市場全般の縮小とその効率性に基づいているという点があります。秘密主義というコンセプトの根本的な変化を通して、金融の世界にはオープンソースソフトウェア開発の(比較的)斬新なアプローチが反映されることになるため、私たちは情報がより効率的に市場価格に反映されるようになると予測しています。マネージャーには、自らの調査作業に対して能力主義に基づいた報酬の提供が行われるようになります。非効率性が長期間にわたって市場に当たり前のように存在してしまっているということを明らかにしたいと私たちは考えています。さらに、金融市場の存在理由は、同じ問題に対して人々の意見が食い違うという点にあります。多くの場合、同じようなスキルを持った資産運用管理者でもデータ分析を行うモデルは異なっており、同じ入力要因を分析した場合でも反対の結果が生み出されることもあります。また、それとは別のケースとして、アマチュア(十分な情報を持たないプレイヤー)とプロのマネージャーの違いという点もあります。その最も極端な例が、政治家(中央銀行または政府)とプロのマネージャー集団になります。いずれにしても、人々の意見は食い違っており、個人は合理的な期待行動が経験的に観察されないことの多い囚人のジレンマに常にとらわれてしまっています。特に、資産の運用に関しては、人間の精神の美しさと複雑さによって客観的に見て合理的ではないような過ちを犯してしまうということを理解していますが、効率性の道に向けて金融市場を動かしていくのに私たちの取り組みを役立てることができることを願っています。プロのマネージャーに管理を委任して平均的な投資家の方たちでも自らの金融ポートフォリオで良いリターンを得られるようにできれば、私たちはこの業界に大きな変化をもたらすことができると信じています。

4. トレーディング用ダッシュボード

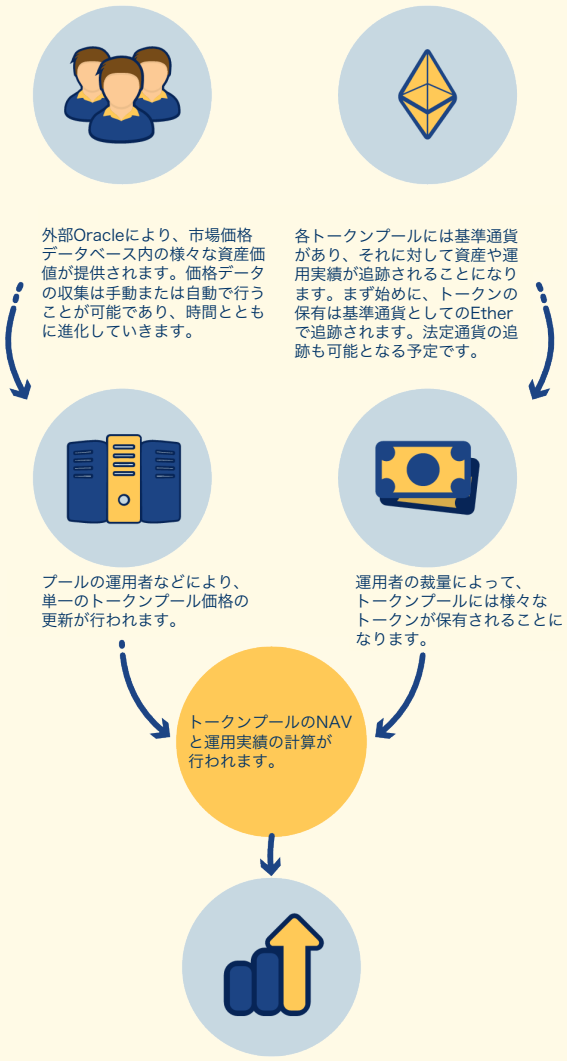
当社では、トレーディング向けの統合ツールセットを提供することを目標の1つに掲げており、その範囲は営業部門の業務から事務管理部門の調整にまで渡ります。そのため、私たちはプラットフォームをポートフォリオ用のオフチェーンダッシュボード専用のセクションと統合し、様々な時間枠の運用実績やポートフォリオ内のポジションを表示したり、一つ一つのポジションに関連した取引全体の可視化を行ったりすることができるようにしたいと考えています。その中には、リスクのモニタリングや時間経過に伴うポートフォリオのリスクの評価なども含まれています。これらはすべて非常にパワフルなツールであり、普段はプロのマネージャーにのみ利用可能なものであり、小規模な企業のマネージャーや新興企業のマネージャーには利用できないものとなっています。これこそが、プラットフォームの進化に向けて進むための道となります。私たちは、APIや他のフロントエンドプラットフォームとの使い勝手の良いインターフェースを通してクオンツトレーディング戦略の自動化を可能にするようなJavaScriptライブラリの提供にも取り組んでいます。当社のモジュール式アーキテクチャにより、外部サービスプロバイダの方でも当社のプロトコルの上に独自のダッシュボードを構築したり、当社のプロトコルやRigoトークン(GRGトークンとも呼ばれる)のインセンティブメカニズムをベースとしたモジュールの一部のみを使用して独自フォーク版の分散型資産運用プラットフォームを作成したりすることもできます。

5. NAVの見積もり

ブロックチェーンから資産が離れるようなことは決してないため、資産の追跡は非常に容易になります。さらに、口座とポジションがリアルタイムで利用可能であり、残高も自動でリアルタイムに更新されます。つまり、ファンドの運用担当者にとっては、ファンドの営業部門やプライムブローカーの事務管理部門と手動でポジションの調整を行う必要がなくなるということを意味しています。ミスやタイポの心配もありません。取引が営業部門で執行されると、誰でも監査できるようにオンチェーンで自動的にリアルタイムで調整が行われます。これにより、リアルタイムでNAVを見積もることが潜在的に可能となります。NAVの見積もりとオンチェーンでの登録にはEthereum Virtual Machine(EVM)の計算を利用することが必要となるため、当社ではオフチェーンでのNAVの見積もりをリアルタイムでユーザーに提供することを決定しました。ユーザーは、必要な場合にのみブロックチェーン上の公式のNAV価格を更新することができるようになるため、不必要に計算リソースやストレージリソースを浪費することがありません。当社では、誠実な行動のための条件を提供するインセンティブの仕組みを作成します。NAVの見積もりを提供するために外部Oracleに頼るのではなく、マネージャー自らが価格を公表できるようにします。

5.1. 公平なユーザーの行動とNAVの公表 当社のアプローチでは、ユーザーは自らのファンドの株式に対するビッド価格とアスク価格を公表することになります。この2つの価格で、ファンドは任意の数の株式の売買を行うことを余儀なくされます。そのため、常に2つの条件が満たされる必要があります。リアルタイムでリクエストに応えられるように、ファンドは常に最低額のEtherを償還用に利用可能にしておく必要があります。マネージャーは実際のNAV値を公表する必要があり、公表しなかった場合にはアービトレージャーの潜在的なターゲットになってしまいます。最終的には私たちはただの人間にすぎないため、賢明な読者の方であれば、操作や不正行為といった要因を方程式から取り除くべきでないとお考えになるかもしれません。1つの可能性として、すべてのことをコードに解決させるということがあります。これは十分に実行可能なアプローチであり、今後もこの道に向けてさらに発展させていくことを検討しています。当社の現在の代替手段は、良い行動が報われ、悪い行動が罰せられるというインセンティブの仕組みを作り出すことであり、そのためNAVの見積もりは中央集権的な関係者に依存することがありません。まず第一に、インフラストラクチャ全体が透過的に構築され、すべての情報が公開されます。NAVの見積もりがオンチェーンで行われなかった場合でも、各個人はリアルタイムでポートフォリオのデューデリジェンスを行うことができます。第2に、優れたマネージャーたちが「ファンド・オブ・ファンズ」の市場を利用できるようにすることによって、最適なマネージャーに対して誠実な行動と飛躍的な成長のための基礎を築いていきます。最後に、トレーダー自らの実績こそがトレーダーのキャリアにおいて最も重要な保証の1つであるということを再認識させたいと考えています。しかし、以前の雇用者との秘密保持契約(NDA)や単一運用口座により、実際の実績を提供することは難しくなっています。第三者による監査も非常に高額なものとなっています。

当社の提案するパラダイムでは、リアルマネーの取引によって得られる監査済みのリアルタイムの実績は、トレーダーによって公表され得るNAVを通して利用可能になるだけでなく、ブロックチェーンから直接データを要求する人であれば誰でも計算可能となります。そのため、いかなる仲介者も必要とすることがありません。世界的に有名なアメリカの金融ジャーナリストであり、トレーダーでもあるJack D. Schwager氏は、そのような商品の必要性を証明するために、トレーダーの従来型のマネージド・アカウントの計算および監査を行うためのスタートアップを最近立ち上げました。



現在の資産は、イーサリアムブロックチェーン上で作成されるトークンとなっています。将来的には、トークン化有価証券やトークン化株式・債権、トークン化資産も含まれる予定となっています。

6. 運用報酬

数多く存在する投資家の中でも、特に伝説的な投資家として知られるウォーレン・バフェット氏は、既存の手数料体系によって顕著になっている資産運用やヘッジファンドのリスク志向のカルチャーを公に批判しています。実際、20%という典型的な運用報酬は、短期的な運用実績を重視して過度のリスクを取るようにマネージャーたちを駆り立てるということで批判を受けています。多くの場合、高額の運用報酬の存在によって、大手ファンドの運用実績は精彩を欠いてしまっています。ファンドの成長に伴って観察される経験的な現象として、創業時に得られていた優れたリターンを再現することができなくなるというものがあります。その時点で運用報酬は非常に高くなっているため、ヘッジファンドのコスト構造では正当とみなすことができなくなってしまっています。

6.1. 利害を調整させるための新しい方法

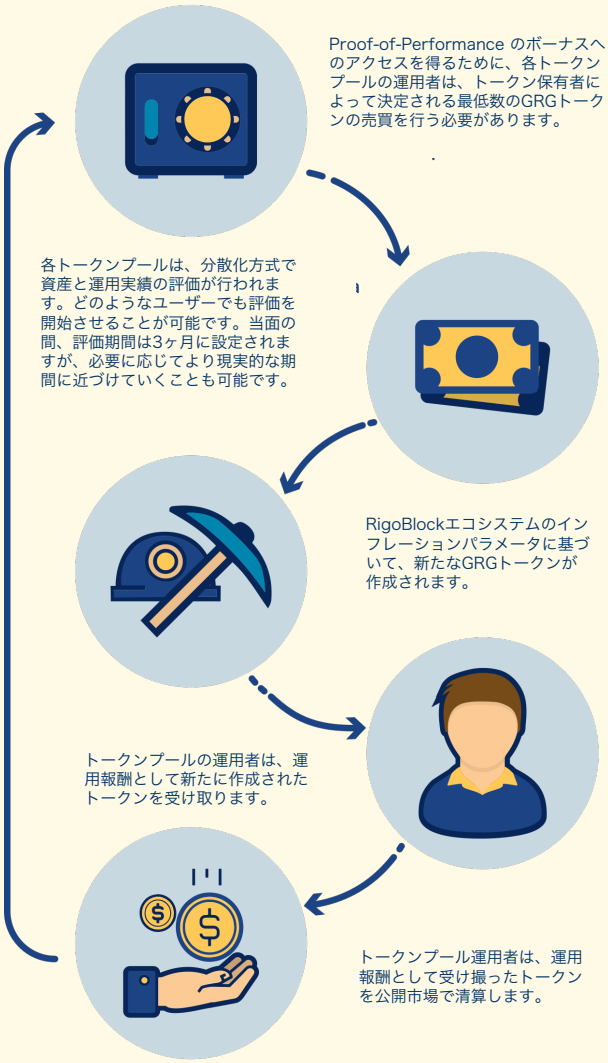
当社では、運用報酬に対して根本的な変化を提案しようとしており、それには2つの理由があります。まず第1に、私たちは運用の質の向上を目指しています。さらに、オンチェーンでの管理や運用報酬の計算が高額になる一方で、当社のモデルでは取引ごとの報酬の計算を非常に容易にするブロックチェーン技術の重要な特徴を活用しているため、手動での調整や支払いを必要とすることなく正しい口座に対して自動的に報酬を割り当てることが可能となります。管理や運用報酬がファンドに直接請求されるのではなく、当社のプロトコルには手数料は存在せず、プロトコルの上に構築されたProof-of-Performanceと呼ばれるアルゴリズムによってマネージャーはRigoトークンで報酬を受け取ることができます。Proof-of-Performanceモジュールは、各サブ期間ごとにファンドの資産と実績の計算を行い、この2つの要因に基づいて四半期ベースでトレーダーに報酬を提供します。各期間の終わりに、トレーダーは報酬を請求することができます。Proof-of-Performanceアルゴリズムのパラメータは Rigoトークン保有者によって設定されており、公平な報酬率を決定することが可能となっています。

6.2. モジュールの配布

ファンドのためのエコシステムを構築するためのもう1つの方法として、モジュール配布というコンセプトがあります。サードパーティ製のプラットフォームは、当社の配布するモジュールを活用するだけでなく、当社のプロトコルの上に独自のモジュールを作成することもでき、取引ごとの手数料を設定することも可能となっています。手数料はディストリビューターによって任意に設定や修正が行われますが、その内容は一般に公開されることになります。そのため、ディストリビューターは競争の激しい市場で独自の手数料を透明性の高い形で設定することができ流ようになります。通常、この種の手数料の利用には手動によるエラー(計算や支払いなど)がつきものですが、ブロックチェーンを利用することによってこれを自動的かつシームレスに実行することが可能となります。そのような運用を従来型の運用会社が行おうとした場合、その手続きを実行するには非常に高額な費用がかかってしまいます。

6.3. 過度のリスク負担

過度にリスクを取ろうとすることは、最大のリターンを生み出すために可能な限り多くのリスクを取ることによって20%の運用報酬を得ようとする慣習に由来しています。これにより、マネージャーは短期的な利益に集中することが可能となります。Rigoトークン保有者は運用報酬のために正しいパラメータを設定することができるため、私たちはProof-of-Performanceモデルによって運用のフォーカスをより長期的な利益へとシフトさせると同時に、優れたマネージャーの受け取る事のできる金額の上限を外すことができると考えています。そして、この方法論によってマネージャーの報酬が下がるということはありませんが、フォーカスが長期的なリターンへと移るために、リターンの質が長期的には向上することになると考えています。



GRG価格が上下に変動した場合、トークン保有者はProof-of-Performance報酬へのアクセスを得るために必要なGRGトークンの枚数を増減させることができます。

7. Vault

これまでに立てられた仮説の多くを排除することによって、結果として得られる製品は完全にトラストレスでシンプルなものとなります。それこそがVaultなのです。これは、イーサリアムコミュニティにとってのXapoのトラストレス版とみなすことができます。Xapoは、個人や法人顧客向けの安全なビットコインストレージを可能にするサービスです。これにより、非常にセキュアなビットコインストレージ保管庫を備えたアカウントを必要な数だけ作成することが可能となります。Xapoでは、中央集権型のサービスを提供しており、顧客の資産とも言える顧客の鍵にアクセスすることができます。当社では、Xapoとは異なるアプローチをとります。当社はサービスが完全に分散化され、顧客の鍵に対するアクセスや知識を決して持たないことを望んでいます。究極的には、顧客自らが鍵に対して責任を負うことになります。完全に分散型かつトラストレスなサービスを実現するために、トークンとEtherの交換だけを可能にするためのスマートコントラクトがコーディングされており、Etherの送信者に対してトークンを作成し、Etherと引き換えに送信されたトークンを破棄します。これは、Xapoの非常にセキュアなコールドストレージとは明確に異なるアプローチとなっています。オンチェーン上で転送を直接規定する機能をコード化できるようにすることによって単純化が行われており、スマートコントラクトのデザインによってセキュアにされています。当社のアプローチでは、たとえどのような顧客であっても常に顧客が自らの資産を管理することになります。さらに、コードはオンチェーンで展開されることになるため、プラットフォームを稼働している企業に何か問題が起きたとしても、コードによってトークンの保有者はいつでもEtherとトークンの交換を行うことが可能となります。その結果、不正や検閲の証明が保証されることになります。設計上、当社のプロダクトは、Etherの安全なホットストレージを提供するためにXapo(すなわち、暗号通貨ウォレット)のようなサービスで使用することが可能であり、それと同時に鍵のコールドストレージも実現します。鍵はオフチェーンに保管されますが、各ユーザーごとの入金総額をリアルタイムで可視化するために、ユーザーはブロックチェーンに問い合わせを行うことも可能です。私たちが無くそうとしている1つ目の仮説は、マネージャーによって資金がエスクロー口座に移動されてしまうというものです。これはもはや不可能なこととなります。私たちは、ファンド内からのEtherの送金を防止します。この場合、マネージャーはEtherをエスクロー口座に移転することができなくなります。さらに、私たちが無くそうとしている2つ目の仮説が、NAVの見積もりです。この場合、NAVは株式あたりにつき1　Etherで固定されることになります。ファンドではEtherのみを保有するため、いかなる管理または運用手数料も存在せず、1つの株式の価値は常に同じになります。現在、当社には独自の分散型トークンプールを作成したり、既知の価格でリアルタイムでトークンの売買を行ったりすることのできるプロダクトがあります。これにより、自分の望む数のファンドを作成することができるようになるため、家族や友人、さらには機関の投資を管理するための効率的なツールを手にすることになります。トークンの購入のたびに取引手数料を設定することも可能であり、第三者と調整を行ったり、手数料の計算に時間を費やしたりする必要なく自動的にトークンを受け取ることができます。Vaultは、1つの場所に安全にEtherを保管したいと考える人を対象としたプロダクトであり、そのような人は多かれ少なかれ同じような問題を経験しています。その問題とは、Etherの購入や長期保有の際に、他の人の代理でEtherを保有したり、それに対してあらゆる責任を負ったり、いつでも資金にアクセスしたりする必要があるという問題です。Vaultは、イーサリアムのメインネットで稼働している当社初のプロダクトであり、RigoBlockプロトコルやProof-of-Performanceインセンティブメカニズムを活用していますが、外部サービス(分散型取引所やOracle)の運用には依存していません。Vaultへの現在の取り組みとして、Proof-of-Stakeマイニングのプールを可能にするために、イーサリアムベースマイニングの次のフロンティアであるCasperとの相互作用の事前設定を行っています。Vaultは、2018年第3四半期中にイーサリアムのメインネット上で稼働を開始する予定となっており、Proof-of-Stakeマイニングのプールは Ethereum Constantinople(2018年第4四半期に予定されているProof-of-Stakeへのイーサリアムの移行)と同時に立ち上げられる可能性があります。

8. RigoBlock Registry

RigoBlock Registryは、性質的にはENS(Ethereum Name Service)と似ており、承認された資産運用企業であればオンチェーンで資産の登録を行い、現在オンチェーンで転送を行うのに必要となっているHEXアドレスの代わりに名前を使って資金のやり取りを行うことができるようになります。外部関係者の利用を促進するために、当社ではRigoBlock Registryを単独のコンポーネントとして分離しています。現在、当社のモジュールインフラストラクチャを活用して下さる外部サービスプロバイダの方を求めています。RigoBlock Registryを使用すると、独自のレジストリの作成と管理を行わずに、ただRegistryアプリケーションに接続するだけでやり取りを行うことが可能となります。

9. RigoBlock Exchange

RigoBlock Exchangeは、Dragosから取引を行えるような分散型取引所を提供するという目的で構築されています。これは、レバレッジ暗号通貨スワップ取引のための完全分散型取引所となります。この取引所により、ユーザーはロングサイドとショートサイドの両方でETHUSD(現時点では取引所にはこの1つの資産のみ存在)でレバレッジ取引を行うことが可能となります。そのため、トレーダーは購入によって価格が上昇した場合に利益を得ることができるだけでなく、ショートポジションでも利益を得ることができ流ようになります。デリバティブとは、ブロックチェーン上に存在しない資産を表す契約のことです。RigoBlock Exchangeは、今日のあらゆる分散型取引所が直面している問題(ほとんどの場合はレイテンシによる執行の遅れや予期しない注文のガス手数料)による制約を受けますが、それでも非常にユニークなものとなっています。また、分散型取引所が金融取引の新たなフロンティアになると信じているため、私たちはRigoBlock Exchangeをさらに改善していくことができると期待しています。RigoBlock Exchangeは長期的なプロジェクトであり、現在は主に分散型取引所とDragosの統合に取り組んでいることもあり、近日中に実稼働させる予定はありません。

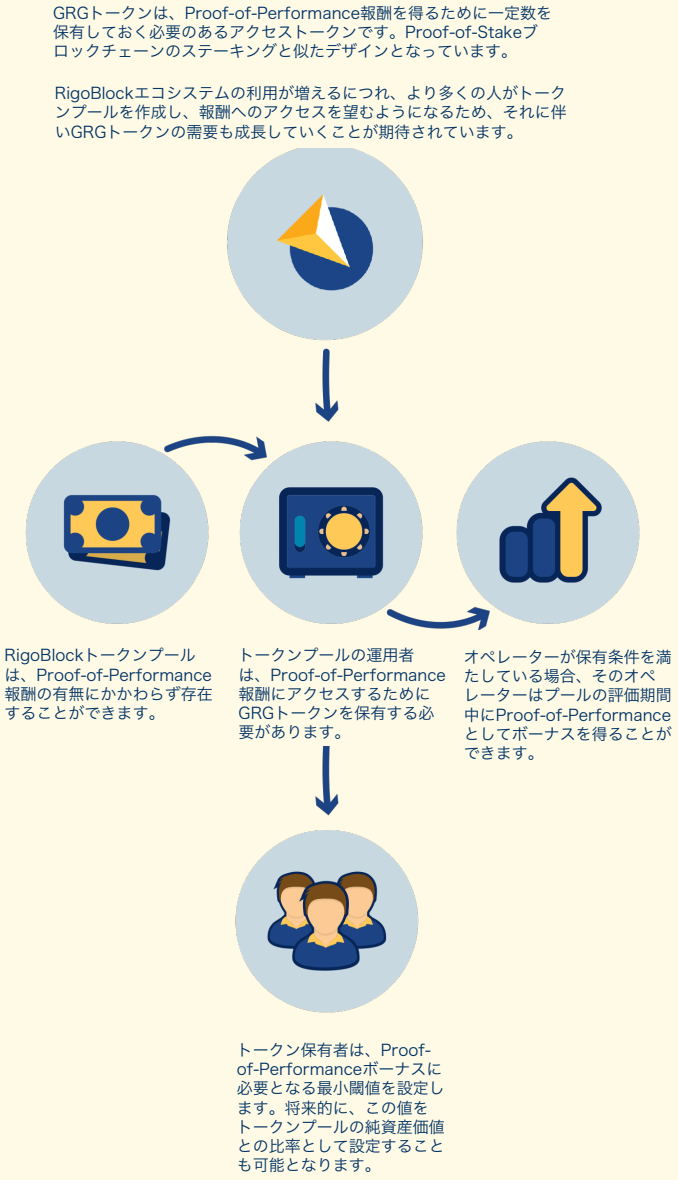
10. Proof-of-Performance

Proof-of-Performanceは、マネージャーの運用報酬のための新たなパラダイムです。前述の通り、当社は管理報酬と運用報酬という従来型のコンセプトに破壊をもたらそうとしています。Proof-of-Performanceにより、トレーダーはリスク調整後の運用実績に基づいてGRGトークンをマイニング(技術的にはミンティング)することができます。トークンプールが大きければ大きいほど、トレーダーにはより多くのGRGトークンをミンティングする資格が与えられます。独自の分散型トークンプールを稼働させるために、マネージャーは最低限のGRGトークンを保有する必要があります。GRGトークンには本質的価値が備わっておらず、実際の活動や有価証券に相当するものではないため、いかなる配当や配当を得る資格も生み出さず、その利益も資産によって裏付けられていません。その唯一の目的は、トレーダーの運用実績に対して報酬を提供し、当社のインセンティブメカニズムの基本とすることです。特に、「適格」や「専門的」といったステータスや規制の対象となる恐れのあるステータスを必要とするような活動では、ユーザーは最低限のGRGトークンを保有する必要があります。

10.1. **資産という要素** Proof-of-Performanceの1つ目の要素は、トークンプールのサイズとなります。トークンプールマネージャー用の新しいGRGトークンの枚数は、その資産に比例します。これは、従来型の運用報酬の代用となります。

10.2. **運用実績という要素** 2つ目の要素として、前回の観測期間に対するトークンプールの運用実績の絶対値の計算があります。この計算はデフォルトでは四半期ごとに行われますが、時間枠を短くしたり長くしたり調整することも可能となっています。

10.3. **ハイウォーターマーク** 各トークンプールに対して、その最高水準値に対するベンチマークが取られ、プラスの運用実績のみで構成されることが保証されます。トークンプールの純資産価値が少なくともその最高水準値に達していない場合、前述のトークンプールに対してProof-of-Performanceトークンはミンティングされません。



上の図は、Proof-of-Performanceインセンティブシステムの概略図を示したものとなります。この図では、ウォレット内に最低限のGRGトークンを保有しているかという状態に基づいて報酬を受け取るトークンプールマネージャーが示されています。プレミアム機能をアンロックする場合にも、標準的なユーザーはGRGトークンを保有する必要があります。そうでない場合には、デフォルトでその機能はロックされています。

10.4. **動的パラメータ設定** 資産と運用実績は、市場の均衡が最適な組み合わせを決定できるように、トークン保有者の設定する動的な方法で組み合わされます。各マネージャーの報酬は、資産と運用実績をトークンプールの属するクラス(またはアプリケーション)の報酬係数と掛け合わせることによって得られます。報酬係数は、トークン保有者によって動的に設定されます。

この新しいパラダイムシフトは、トークンプールマネージャーの報酬を従来型の管理・運用報酬からネットワークによるボーナスへと移行させます。その後、これは適度なインフレーションの形(1%から2%の間の予想総計)で支払われることになり、これがRigoBlockエコシステムに外部開発者だけでなく、ユーザーを呼び込むメリットとなります。

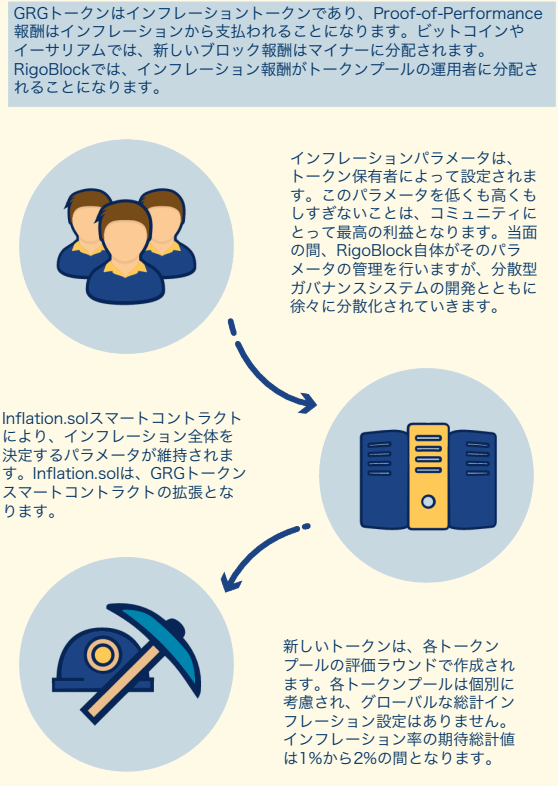
要約すると、Proof-of-Performanceインセンティブシステムは、マイナス以外の運用実績の場合にマネージャーに報酬を提供します。そして、資産をスタンドアプリケーションに保持させておくのではなく、RigoBlockエコシステムに資産を持ち込むことに対してインセンティブを生み出します。

10.5. **需要と供給の要素**　GRGトークンはインフレーショントークンです。新しいトークンの作成と割り当ては、Proof-of-Performanceアルゴリズムによって自動的に行われ、スマートコントラクトによって執行されます。その後、新しいトークンはトークンプールマネージャーへと配布されます。

そのような報酬が、管理・運用報酬の代わりとなります。配布は、完全に監査可能で透明性の高い方法でGRGトークンと結びついたProof-of-Performanceモジュールから自動的に行われるため、手動による介入や中央集権型の関係者に依存する必要はありません。

報酬を受け取るために、マネージャーは最低限のトークンを保有しておく必要があります。その最少額は動的であり、トークン保有者によって設定されるため、エコシステム内のインフレーションと需要の間の比率に対してバランスが取られることになります。標準的なユーザーの場合、プラットフォームのプレミアム機能をアンロックするためにGRGトークンを保有する必要があり、これによって追加の需要が生み出されることになります。

RigoBlockプロトコルの上でアプリケーションを作成する外部開発者への報酬を可能にする継続的な資金調達モデルを形成するために、RigoBlockプロトコルは作成された新しいトークンのうちの5%をロイヤルティとして保持します。GRGトークン保有者によってインフレーションパラメータの設定が行われることになるため、継続的な資金調達モデルは無価値な新しいトークンを生成するというよりもポジティブなインセンティブをターゲットとするインセンティブを提供します。



11. 今後の方向性

私たちは、2016年初頭から概念実証の作成を行ってきており、2016年8月頃には分散型投資商品向けのスマートコントラクトをリリースしています。その後ずっと、コンセプトの改良や機能の追加、セキュリティのチェック、「スマートコントラクトエンジン」と呼ばれるコードのモジュールプロトコル化などに取り組み続けており、より抽象化を進め、外部サービスプロバイダがRigoBlock上に独自の分散型運用会社を構築できるようにしています。当社のプラットフォームはKovanテストネット上でのアルファテストを経て、2017年5月以来Parity　UI内で一般公開されています。より従来型のUX体験へと移行していく前に、安全な環境内でテストできるような選択を行いました。UX/UIの改善にはかなりの取り組みが行われており、プラットフォームは2018年第1四半期にベータ版へとアップグレードし、ウェブから利用可能となっています。現在、早期テスターグループでより進化したベータ版が使用されています。当社のチームはすでに大きく成長しており、現在は10名以上の人々(そのうちの3名は資産運用や法律、暗号通貨、ブロックチェーンなどの分野で関連する経験と能力を備えた顧問の方です)で構成されています。チームは、インターフェースの改善を行ったり、平均的なユーザーに使い勝手の良いプラットフォームを提供できるよう取り組みを行っています。そして、この数ヶ月の間にも分散型取引所にはかなりの進展がありました。例えば、0xプロトコルはハイブリッドな分散型取引所を作成するためにブロックチェーンを利用する際の効率性の標準を定めており、多くのリレーがその上に構築されています。これにより、分散型取引所には組織的な流動性がもたらされています。さらに、ファンド同士の相互作用を可能にする0xのアップグレードが、2018年第3四半期中旬にイーサリアムメインネットで稼働することが期待されています。当社のDragosは、PoCの実演を行えるようにするために、すでにRigoBlock Exchangeとの統合およびテストを終えています。Dragosはリリース時には限られた機能のみ動作可能となる予定であり、2018年第4四半期に外部取引所がプロトコルに接続される予定となっています。RigoBlock Exchangeは外部Oracleに依存しているため、デリバティブにより適した分散型取引所を見つけることができた場合には本稼働を行わない予定となっています。また、当社では分散型Oracleシステムへの取り組みのために他社との協力も行っており、これによりオンチェーンのOracleを維持するコストを削減することが可能となります。当社では独自のOracleの構築も行っており、これは単なる最適化以上のものとなります。当社では、誰にでも無料価格を提供できるような効率的な方法を常に模索し続けています。また、当社では、当社の技術をイーサリアムのメインネット上で完全稼動させた後に、RigoBlockプラットフォームをトレーダーのためのエコシステムにしていくことを究極の目標としています。これにより、どれほど奇妙でおかしなものであっても、お好みの投資ストラテジーを実行することが可能となります。そのようなエコシステムを構築するためのツールの1つが、ファンドから他のファンドへの投資(専用のファンド・オブ・ファンズの仕組み)を可能にし、最適なトレーディング戦略に投資を行うことをタスクとする自律型ファンドプールを構築し、前例のないほどの水準の多様化によって大衆からより簡単に資金提供を行えるようにするツールです。この場合、RigoBlockプールは数千または潜在的には数百万ものトレーダーを擁するグローバルなトレーダーのファンドとして機能し、また保証人としてあらゆる規制を負担することになるため、そのようなプール・オブ・プールズにはトレーダーたちを規制の負担から解放する力が備わることになります。

11.1. **サードパーティの統合**　当社のモジュラー式のブロックチェーンソリューションにより、既存の市場でも独自のプラットフォームやウォレットアプリケーション上で独自のファンドを提供できるようになります。当社のJavaScript APIを使ってやりとりを行うことによって、サードパーティーの方でもファンドを提供することができます。

当社ではファンドの資産へのアクセスを有しておらず、また顧客の鍵へのアクセスの管理や所有も行っていないため、サードパーティープラットフォームは当社のブランドまたは独自のブランドの下でユーザーの鍵の管理や既存サービスの統合に焦点を当てることができるようになります。当社のプロトコルの上で手数料の請求を行うことも可能であり、当社のディストリビューションモジュールを使えば配布手数料を請求することも可能となっています。

11.2. **分散型ガバナンス**　当社特有のトピックとして、不正行為の可能性に関するものがあります。スキャムトークンが外部の分散型取引所に上場され、当社プラットフォーム上に展開された分散型トークンプールを通してそのトークンのクリエイターによって購入された場合、どうなるでしょうか？当社ではすでに、オーソリティメカニズムとガバナンスメカニズムの構築によってこの問題に取り組んでいます。このメカニズムでは、承認済みのトークンプールから承認済みのトレーダーまたは承認済みの取引所に対してのみ取引が可能であり、取引所のトークンでさえ承認される必要があります。これは、RigoBlockエコシステムのコンプライアンスを改善するために構築されています。このことが分散化の制限とみなされる可能性もありますが、将来的にはアップグレード可能となっています。また、分散型ガバナンスのパラメータの設定を行うのは、技術によって安全な分散型ガバナンスが可能になった時にRigoBlockが完全分散型組織になるというビジョンを持った、Rigoトークンの保有者なのです。

私たちは、世界の価値がトークン化されていくというビジョンを共有しており、トークンとトークン化された資産という価値を体系化するためのリファレンスツールになることを目指しています。また、安定通貨建てのファンドとシェアクラス(ヘッジありのものとヘッジなし)を心に思い描いています。長期的には、お金に関連するあらゆるものがブロックチェーンを通して取引され、さまざまなプロトコルが互いに通信し合い、給料や税金がデジタルトークンで支払われるような世界を思い描いています。今のところ、ブロックチェーン非依存のフレームワークを提供するために可能な唯一の方法は、互いに異なるブロックチェーンや転送方式を処理する中央集権型の仲介者による中央集権型のアプローチを取るということです。リレー(BitcoinRelay)を使用することによって、サイドチェーンを通したソリューションの提案を行っている優れたプロジェクト(HyperLedger)もあります。また、大事なことを言い忘れていましたが、他のブロックチェーンが何を行っているのかをあらゆるブロックチェーンが認識できるようにし、それによってあるチェーンから別のチェーンへの転送を可能にするためにバリデーターの利用を提案しているPlkadotは、自らをパブリックブロックチェーンやプライベートブロックチェーン、コンソーシアムブロックチェーンとして位置付けようとしています。

11.3. **スケーラビリティ**　プラットフォームのスケーラビリティは、基盤としているブロクチェーンのスケーラビリティに直接関係しています。さらに、アプリケーション用の分散型ストレージは、DDoS攻撃に対する費用対効果の高い非常にスケーラブルなソリューションを提供し、検閲体制の高いプラットフォームになっていくと考えられています。IPFSやイーサリアム向けの分散型ストレージソリューションであるSwarmは、そのようなソリューションを提供しています。また、ファンドの構造は、取引が行われる市場と同じくらい拡張性が高くなっています。マネージャーはすぐに見通しとグローバルリーチを得ることができるようになるため、国境はなくなりつつあります。提案されているファンド・オブ・ファンズの仕組みにより、ビジネスを専門的に拡大するだけでなく、さらには法人顧客のみをターゲットにすることも可能となります。リアルマネーに適用しようとした場合、スケーラビリティがソーシャルトレーディングの現在の限界の1つとなっています。この限界によって、たくさんのフォロワーを持つトレーダーは自らの取引価格に対する価格の影響を認識できない可能性があります。その影響を認識していた場合、トレーダーは自らの顧客にフリー・ライディングできることになり、共通の利益と個々の利益を完全に一致させなくても済むようになります。これとは対照的に、RigoBlock Dragoでは、マネージャーが取引を行う市場と同じくらい取引の拡張性が高い非常にスケーラブルなインフラストラクチャを提供します。さらに、単一口座の定期的なリバランシングを行う必要なく、トレーダーは投資家をまとめてプールすることからあらゆる恩恵を享受することができます。最終的に、規制に関するトピックは、RigoBlockプロトコルを使用する個人の責任となります。投資家の顧客をプールすることは、特定の条件下ではほとんどの国で規制の対象となります。ターゲットとする顧客やビジネスモデルに応じて、規制は異なります。規制が非常に限定的な場合もあれば、負担が大きい場合もあります。当社が提案しているのは、自動的に自己規制を行い、従来型のファンドの仕組みよりもより高いコンプライアンスの保証を課すような枠組みなのです。そのため、運用に必要となる業務を大幅に軽減することが可能となります。特定の条件下であれば、当社のプール・オブ・プールズモデルと同様に、一部のマネージャーたちは完全に規制の範囲の対象外となると私たちは考えています。私たちの仕事は、仕事を効率的に行えるようにするための技術的なツールを個人の方に提供し、そのような方たちが自らのコアビジネスに集中できるようにすることです。トレーダーのためのエコシステムを構築するということは、私たちにとってそのような個人の方の抱える問題を一つ一つ解決していくことを意味しています。

12. 結論

本稿では、RigoBlockプロトコルの紹介、説明、正式な定義を行ってきました。当社のスマートコントラクトエンジンによって、トレーダーの方はイーサリアムネットワーク上にあるRigoBlockプラットフォームに分散型ファンドプールを展開し、リアルタイムでファンドの株式の募集や償還を行うことが可能となります。コントラクトは自律的かつ変更不可能なものであり、マネージャーの方はそれらの管理を行うだけで済みます。このような水準の透明性や効率性、説明責任によって、これまでどのような規制環境でも目にすることのできなかった自己規制機関を構成することができるようになります。新しいトークンミンティング用のアルゴリズムであるProof-of-Performanceによって、私たちはこれまでとは異なる運用報酬のパラダイムをご提案します。

13. 謝辞

本稿の執筆にあたり、数多くの方々にフィードバックのご提供や改善の支援を行って頂きました。紙面の都合上、全ての方々のお名前を挙げることはできませんが、この場を借りて感謝の意を表します。特に、Hanna Keskin氏、Sharif Tarver氏、David Fava氏には、本稿に貴重なフィードバックをお寄せ下さったことに感謝致します。また、視覚的に分かりやすい方法でProof-of-Performanceシステムの説明をご支援下さったMikko Ohtamaa氏にも感謝致します。当社のビジョンの推進と実現を可能にするオープンアーキテクチャを構築して下さったイーサリアムコミュニティとコミュニティ向けのツールを構築して下さったParityチームの皆様にも感謝致します。最後に、テスターの皆様にも感謝致します。今後もRigoBlockプラットフォーム上でのエクスペリエンスを改善していくために、懸命に取り組みを行ってまいります。