Bancor プロトコル

スマートコントラクトを通じて、トークンの継続的な流動性を確保し、非同期的な価格発見を可能にするスマートトークンについて

Eyal Hertzog, Guy Benartzi & Galia Benartzi

May 30, 2017

訳者: 栗林 健太郎
原本: Draft Version 0.99

「欲求の二重一致問題」は、Jevons (1875) によって提起された。

> 取引は二者間で、かつ、その二者において処分可能な所有物がお互いの欲求を満たす場合に可能となる。欲求を抱く多くの人々が存在し、そして、欲求されるべき多くの所有物が存在する。しかし、現に取引が行われるためには、まれにしか起こらない、欲求の二重一致が必要になる。

目次

1 Bancor プロトコル

要約： *Bancor*（バンコール）プロトコルには、スマートコントラクト上のトークンのための、価格発見[*1]と流動性を担保するメカニズムが備わっている。スマートトークンはひとつ以上のトークンを準備金として保有し、その準備トークンと交換することで、誰もが即座にスマートトークンを購入したり、精算したりすることができる。 そしてそれは、スマートコントラクトを直接的に通じて行われ、継続的に計出される価格において取引される。その計算は、売買をバランスする公式に基づいて行われる。

Bancor プロトコルは、第二次世界大戦後、国際的な通貨の換算をシステム化するための、Bancor と呼ばれる超国家的な準備通貨の導入に関する、ケインズ経済学者（たち）の提案[*2] に敬意を表して名付けられた。

1.1 背景

我々は、誰もが記事・歌あるいは動画を公開し、ディスカッションのためのグループを形成し、さらにはオンラインのマーケットプレイスを運営できるような、そんな世界に住んでいる。いまや我々は、一般の人々によって生成された通貨の発生をも目の当たりにし始めている。様々な形で貯蔵された価値（以下、通貨と呼ぶ）が、何世紀にもわたって発行され、流通してきた。それらは、紙幣、債権、株式、ギフトカード、ポイント、コミュニティ通貨など、様々な形態をなしてきた。ビットコインは、初の**非中央集権的な**デジタル通貨であり、その後には暗号通貨発行の流行が続いた。また近頃では、資産の新しい形としての「トークン」の隆盛があり、それらは典型的にはクラウドセール（ICO）において、スマートコントラクトを通じて発行されている。

しかしながら、通貨とは本質的にはネットワークの価値を示すものであり、情報のネットワークにおいて行われるようには、お互いにつながったりはしないものである。情報のネットワークにおいては、インターネット上の情報の交換地点であるスイッチが情報を連結する一方で、通貨においては、取引所にいる活発なトレーダーが通貨を連結する。

現在の通貨あるいは資産の交換モデルには、致命的な障壁がある。それは、市場の流動性を得るためにある程度の量の取引が必要になるということである。この生来の障壁は、コミュニティ通貨[*3] やポイント、あるいはその他の特別仕様のトークンのような小規模な通貨が、市場において決定される交換レートに基づいて、その他の人気のある通貨と交換されることをほとんど不可能にする。

スマートコントラクトブロックチェーンの時代においては、発行やふるまいを制御する不変のコードによって、トークンは自動的に管理される。このことは、トークンの製作者によって設計され、自動的に管理されるスマートコントラクトを直接的に通じて、トークンが他のトークンの残高を保有する（すなわち、備えておく）ことができるということである。これらの新しい技術的な可能性は、あり得べき通貨交換のソリューションや市場価格の決定について再考する、十分な理由となる。

[*1] *https://en.wikipedia.org/wiki/Price_discovery*
[*2] *https://en.wikipedia.org/wiki/Bancor*
[*3] *https://en.wikipedia.org/wiki/Community_currency*

1.2 スマートトークンの導入：流動性問題の解決策

スマートトークンは、標準的な ERC20 トークンであり、Bancor プロトコルを実装することで、継続的な流動性と自動的かつ円滑な価格発見を両立する。スマートトークンのコントラクトは、即座に**売り注文**と**買い注文**とを処理し、そのことで価格発見のプロセスが駆動される。この能力により、スマートトークンは流動性の確保において、取引所での取引を必要としない。

スマートトークンは、少なくともひとつ、それ自身以外のトークンを**準備トークン**として保有する。それは、(現在のところ) 別のスマートトークンや、ERC20 に準拠したトークン、あるいは Ether でもあってもよい。スマートトークンは、購入された際に発行され、流動した際に破棄される。したがって、それはいつでも準備トークンによってその時点の価格で購入され得るし、同様に、準備トークンへと精算され得る。

1.3 価格発見の新手法

スマートトークンは価格発見において、「不変の準備率（*Constant Reserve Ratio: CRR*)」に基づく新しい方法を用いている。CRR は、スマートトークンの作成者により、準備トークンのそれぞれに対して設定される。また、スマートトークンの現在の供給量と準備トークンの残高とともに、価格の計算に使われ、それは以下の通り示される：

$$Price = \frac{Balance}{Supply \times CRR}$$

この計算によって、準備率が、準備トークン残高をスマートトークンの時価総額の間に収まることが保証される。そしてそれは、価格を決定するトークンの供給となる。時価総額がトークンの供給割合になるで、スマートトークンが、スマートコントラクト通じた売買のどちらになるかにしたがって価格が決定することになる。スマートトークンの価格は、準備トークンによって示されることになり、また、都度都度の売買をなすスマートコントラクトによって調整されることにもなる。それは、準備残高およびスマートトークンの供給を(すなわち、その価格を)、詳細については後述の通り、増減させることになる。

スマートトークンが、準備通貨のいずせかによって購入された際、その購入に対する支払いは準備残高に付加されることになる。そして算出された価格に基づいて、購入者に対して**新しいトークンが発行される**ことになる。上述の計算方法により、CRR が 100% 以下である状況下でのスマートトークンの購入は、価格の上昇をもたらす。なぜなら、トークンの供給は比において掛け算されると同時に、準備残高と供給のどちらもが増加するからである。

同様に、スマートトークンが精算される際、それらのトークンは**供給量から削除される**、すなわち破棄される。そして、現在の価格にもとづいて、準備トークンは清算人に譲渡されることになる。この場合、CRR が 100% 以下のスマートトークンにとっては、すべての精算が価格の減少をもたらすことになる。

この非同期的な価格発見のモデルは、売買量の平衡状態に対して、現在価格を調整する作用をもたらす。古典的な交換のモデ 2 者間の**リアルタイムな**マッチング順によって決定されていた一方で、スマートトークンの価格は、以下の順序により、**ひとりでに**算出されることになる。

上述の公式は現在価格を計算するが、売買が実行された時、実効価格はトランザクションのサイズの関数として決定される。その算出は、あたかもすべてのトランザクションが無限に小さな増分に帰されて記述されているようであり、その際、それぞれの増分がスマートトークンの供給、準備残高、すなわちトークンの価格に

変化をもたらしている。このことは、同じ量のスマートトークンを、単一あるいは複数のトランザクションを通じて購入することが、同じ価格の合計を保証する。さらには、この方法は、CRR が不変であり続け、また、準備トークンが決して枯渇しないことも保証する。本質的には、スマートトークンの供給と準備残高を変化させることによる、その価格におけるトランザクションのサイズの効果は、あらゆるトランザクションにとって実効的な価格に含まれることになる。トランザクションサイズごとの価格算出の数学的な定式化については、本ドキュメントにおいて後述する。

この手法を用いることにより、Bancor プロトコルは、**既存の標準的なトークンについて**、流動性と非同期的な価格決定をともに可能にする。それは、後方互換製を保ちつつ、準備残高として保有されるスマートトークンを通じて実現される。このスマートトークンのユースケース他については、後述する。

1.4 スマートトークンのユースケース

1.4.1 ユーザ作成通貨のロングテール

ロングテール現象は、ブログのような出版、YouTube のような動画、Reddit や Facebook のようなフォーラムなど、様々なオンラインのエコシステムにおいて観察される。これらの例のいずれにおいても、ロングテールはその前方よりも著しく大きくなり続けてきた。障壁が取り除かれるや否や、ロングテールの形成は始まる（例えば、YouTube は誰もがユーザ作成による動画をアップロードし、共有することを容易にした)。

ユーザ作成通貨には、グループ通貨（コミュニティ志向の通貨)、ポイント（ビジネス志向の通貨)、そして最近のものとしては数百もの暗号通貨（プロトコル志向の通貨）など、たくさんの実例がある。しかし、これらの小規模な、あるいは、新しい通貨が流動性を獲得し維持することは、通貨の発展にとっていまも重大な障壁であり続けている。

スマートトークンは、単一の当事者のみにより購入・精算が可能で、計出される価格を用い、**ふたつの逆向きの欲求を同時に満たす必要をなくす**という点において、ユニークである。このことは、Bancor プロトコルを用いることで、取引量が少ないであろう小規模な通貨が、継続的な流動性を提供することができることを説得的に示す。すなわち、それらの通貨がグローバル経済につながるに際しての障壁を取り払うことを意味する。

通貨のロングテールが可能になることで、新世代のクリエイティブなユースケースがもたらされることがあり得る。それらすべての未来を予測することは不可能であるにしても、以下に示すとおり、有望なユースケースはいくつかある。

1.4.2 プロジェクトのクラウドファンディング

クラウドファンディングが急速に広がっている。スマートトークンは、暗号通貨によるクラウドファンディングの提起に使うことができる。そこで参加者は、流動的で、市場において価格の決まるトークンを受け取ることになる。一例として、ミュージシャンがアルバムを収録するための資金を集め、発行されたトークンによってのみオンラインで購入できるアルバムを作ることが考えられる。アルバムが成功すれば、トークンに対する需要が高まり、価格が高騰し、トークンの所有者への報奨となる。他にも、ベンチャーキャピタルの資金をクラウドファンディングによって集めたり、信用創造機能を持つ地域通貨の初期資本を募ったりという例もある。

1.4.3 トークンチェンジャー

トークンチェンジャーは、複数の準備トークンを持ち、全体の CRR が 100% であり、準備トークンとして保有しているどの ERC20 準拠トークン間でも取引できるようなスマートトークンである。トークンチェンジャーは、ひとつの準備トークンによってスマートトークンを購入する 2 段階のプロセスを通じて、準備トークン間において取引できるサービスを提供するべく設計されている。そのことで、即座にトークンを他の通貨へ精算することができる。

価格計算の公式により、ある準備トークン X を別の準備トークン Y へ変換するたびに、 X の価格は下がり Y の価格は上がる。取引が大きくなると、価格はより急激に動くことになる。しかし、準備高が多くなれば、価格の変動率は減少していく。

既述の通り、ERC20 準拠トークンはいずれも、たとえそれが他の取引所においてやり取りされていたとしても、準備トークンとして使うことができる。そのような事態においては、外部の取引所における価格と計算された価格との間に隔たりが起こり得る。この状況は、裁定取引の機会を生み出し、**鞘を取ることで経済的均衡を回復するインセンティブを人々にもたらす**。すなわち、他の取引所でのトークンの取引価格と、トークンチェンジャーでの価格とが同期され続けることになる。

トークンチェンジャーの作成者は、購入あるいは精算ごとに適用される手数料を設定できる。手数料は準備トークンとして充当することもでき、そのことによってスマートトークンの価格は変換によって得られる金額により増加することになり、そのことでスマートトークンの価値も増加する。この増加は、そのスマートトークンを保有している者に利益をもたらす。このスマートトークンの保有者は、スマートトークンの作成時に準備トークンに最初の入金をした者や、スマートトークンの発行後に準備トークンのいずれかによって購入をした者である。

MtGox や Bitfinex のようなポピュラーな交換所は、その管理するアカウントから数億ドル相当の資産を、ハッキングにより盗まれてしまった。トークンチェンジャーによりあるトークンを別のトークンに変換することは、取引所に資金をあらかじめ入金することを要しない。したがって、カウンターパーティリスクを取り除くことができる。もうひとつ重要な利点として、スマートトークンの非中央集権的な性質により、他の即時取引のソリューションとは違い、トランザクション数の制約を適用する必要がないことがあげられる。非中央集権的な取引所がこのような利点をもたらす一方で、スマートトークンは流動性を提供するに際して、取引量の多寡に頼らずに済む。

1.4.4 非中央集権的なトークンのバスケット取引

スマートトークンは、非中央集権的なトークンのバスケット取引にも用いることができる。それは、ETF やインデックスファンドと機能的には類似しており、全体の CRR が 100% である準備トークンのポートフォリオを保有することで簡単に実現できる。準備トークンの価格が上下するにしたがって、スマートトークンの価値も同様に上下する。トークンチェンジャー同様に、市場価格と変換レートを再調整する裁定取引をするインセンティブが存在し、そのことで、リアルタイムな市場価値に基づき、準備トークン間における適切な交換比率が保証される。これらのスマートトークンにより、金融サービスの提供者の媒介なしに、人々は直接に資産のバスケット取引を行うことが可能となる。

1.4.5 ネットワークトークン

同一の準備トークンを集合的に用いるスマートトークンは、**トークンのネットワーク**を成す。共有される準備トークンは**ネットワークトークン**として表現することができ、それは準備トークンを保持するトークンのネットワーク全体の価値を表す。それらネットワークに属するスマートトークンのいずれに対しても、需要の増加がネットワークトークンへの需要の増加をもたらす。なぜなら、それらのトークンを購入するにはネットワークトークンが必要であり、準備トークン内に保有されているからである。需要の増加は、ネットワークトークンの価格を上昇させ、準備トークン残高の価値も増えるている間はずっと、ネットワーク全体にとって利益となる。すなわち、CRR を維持するために、スマートトークンの価値もまた上昇する。ネットワークトークンは、「トークンのためのトークン」としての機能も果たす。それは、ネットワーク内のすべてのスマートトークンを、互いに交換可能なものにする。

ネットワークトークンは、別個の目的のために、複数の、関連するスマートトークンを作成しようとする人々にとって有用であり得る。地域ネットワークにおけるコミュニティ通貨、複数のゲーム製作者からなるスタジオ、共同の顧客向けプログラムを実施する独立した事業者のグループなどが例としてあげられる。このネットワークトークンのモデルは、ネットワークに参加するスマートトークンの相互作用関係を生み出し、単一のイーサリアム上のサービスが Ether の価値を向上させ**保有者のすべて**に利する仕組みと比較検討してみることができる。

さらに考えられるネットワークトークンのユースケースとしては、互いに準備トークンをネットワークトークンとして保有し、他方に二つ目の準備残高を標準的なトークンとして保有するようなトークンチェンジャー同士を連結することである。この構造は、新たなトークンチェンジャーが作られ、価値が向上する時はいつでも、ネットワークトークンに対する需要が高まると同時に、ネットワークトークンを別のネットワークトークンと交換することを可能にする。

1.5 スマートトークンの利点

スマートトークンには、伝統的な取引モデルと比べて、複数の利点がある。

1. **継続的な流動性**　購入と精算がスマートコントラクトを通じて行われるため、スマートトークンには常に、取引量に関わらず流動性が備わっている。
2. **追加の手数料が不要**　スマートトークンに適用されるただひとつ必要な手数料は、ブロックチェーンプラットフォームで必要なもの（gas）のみである、それは相対的に低額である。
3. **スプレッドがないこと**　価格計算はスマートトークンによってアルゴリズム的に計算されるため、スマートトークンの購入と精算に対して同額が適用される。
4. **予見可能な価格低下**　スマートトークンは、トランザクションのサイズに基づいて、取引する前に、正確な価格低下の計算が事前に可能である。
5. **比較的小さな価格変動率**　たとえば 10% の CRR を持つスマートトークンは、全期間の板情報におけるトークンの**供給全体**との交換と比べてみることができ、それは実質的な市場の深さを形成する。典型的な暗号通貨交換所では、任意の時点における市場への通貨供給率は、せいぜい 1% 以下である。CRR が高くなればなるほど、スマートトークンの価格変動率は低くなる。CRR が低くなればなるほど、当初の準備量に比べて「新しい信用」が創造される。

1.6 Bancor プロトコルのエコシステム

Bancor ネットワークのエコシステムにおいては、様々な当事者が異なる役割を引き受けることがあり得る。最初の参加形態は以下の通りである。

エンドユーザー スマートトークンの受け取り、保有、送信、要求、購入、精算を行う。

スマートトークンの作成者 常に流動性を持つスマートトークンを新規に発行する。そのトークンは、バスケット取引やネットワークトークンの仕組みを通じて、取引やトークン交換に使われることもある。

資産をトークン化する者 Tether と US ドル Digix と金（ゴールド）の関係のように、外部の資産を表す ERC20 トークンを発行する。そのことで、スマートトークンはそれらの資産を準備トークンとして利用することができる。

裁定取引をする者 暗号通貨取引所と Bancor ネットワークとの間の価格差を継続して解消するよう、有機的に動機づけられている。スマートトークンには、購入により価格が上昇し、売ることにより価格が減少する取引所に似た作用を持つため、同様の裁定取引メカニズムとインセンティブがあてはまる。

1.7 「欲求の二重一致問題」への解決策

1.7.1 スマートトークンの初期化とカスタマイゼーション

2 Bprotocol ファウンデーション

2.1 Bancor Network Token (BNT)：初めてのスマートトークン

2.2 BNT をクラウドセールスする目的

3 トランザクションごとの価格計算

4 要約

5 謝辞