

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	3
1.1	背景	3
1.2	スマートトークンの導入：流動性問題の解決策	4
1.3	価格発見の新手法	4
1.4	スマートトークンのユースケース	5
1.5	スマートトークンの利点	5
1.6	Bancor プロトコルのエコシステム	5
1.7	「欲求の二重一致問題」への解決策	5
2	Bprotocol ファウンデーション	5
2.1	Bancor Network Token (BNT)：初めてのスマートトークン	5
2.2	BNT をクラウドセールスする目的	5
3	トランザクションごとの価格計算	5
4	要約	5
5	謝辞	5

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、準備通貨のいずれ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ル 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 ユーザにより作成される通貨のロングテール

1.4.2 プロジェクトのクラウドファンディング

1.4.3 トークン交換所

1.4.4 非中央集権的なトークンバスケット

1.4.5 ネットワークトークン

1.5 スマートトークンの利点

1.6 Bancor プロトコルのエコシステム

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