# RICO - Responsible Initial Coin Offering

Yuseku Senga

Decentralizedtech Research Institute

senga@dri.network

ver 1.0 (2017/10/10)

**概要**

Responsible Initial Coin Offersing (以下 RICO) は Initial Coin Offering において、先進的な ICO プロジェクトのトークン設計手法を、素早く自分のプロジェクトに取り入れられるフレームワークである。また、RICO 独自の ICO 手法を用いることで、プロジェクト支援者とプロジェクトオーナーにとってより公平で責任のある ICO を行うことが可能である。さらに、RICO のアプリケーションスタックはトークンの自律生成と分散型の責任ある公開買い付けアプローチを採用することで、よりコードベースのガバナンス体制を強化する。プロジェクトオーナーの行動を制限し、同時にプロジェクト支援者にとって公平な支援機会を提供することを目指す。

## 1 問題提起

EIP-20 Token Standard(1) は Etheruem エコシステム上において、トークンフォーマットとして機能する。分散型アプリケーション (以下 Dapps) において、システム全体がトラストレス状態を維持しながら異なる Dapps 間を接続するためには、EIP-20 のように共通化されたトークンフォーマットを利用する必要がある。

このトークンフォーマットを利用したアプリケーションを開発するにあたり、我々は伝統的に Initial Coin Offering(以下 ICO) 手法に頼らざるを得ない。ICO はプロジェクト単位で寄付を受け付け、それに対してトークンを生成する。そして従来の ICO では、トークンの生成プロセスや、調達した資金の管理がプロジェクトオーナー側に一任されることが多い。これは支援者にとって極めて不利となる問題があるだけでなく、以下のようなリスクが発生しやすいことが報告されている。

- トークンロックの正当性の欠如によるトークンの不正利用
- 運営資金の過大な設定と、利己的利用
- 大量ホールダーの偏りによる市場での潜在的売り圧力の上昇と流動性の低下とそれに伴うトークン価格の下落

また従来の ICO を用いたプロジェクトのほとんどが、トークンを生成した段階において、プロジェクトの支援者よりもプロジェクトオーナー側が多くの保有割合を得ていることも問題となっている。なぜなら、プロジェクトオーナーが初期に大量保有するトークンは、潜在的売り圧力を上昇させ、極めて安定性が低い状態を作り出すためである。これにより、トークンを保持することがリスクとなるため、買われづらい状態が発生する。これは、流動性の低下と、ボラティリティの増大に繋がることが知られている。これらのリスクを放置すると、トークンを求めるプロジェクト支援者が極めて不利な状況に置かれる可能性がある。

## 2　解決のアプローチと方法

我々はこれらの問題が、トークンの生成プロセス全てにおいて、プロジェクトオーナーの権利を最小化した仕組みを採用することで解消されると考えている。そこで、Ethereum のスマートコントラクト機能を用いて、トークンの生成プロセスを非中央集権化するアプローチを提案する。

以下の節では、このアプローチによる具体的な解決方法を示す。

### 2.1　トークン生成の厳密化と予約

従来の ICO の場合、トークンの生成プロセスはプロジェクトオーナー側が自由に決定できる。つまり、トークンの設計とトークンの保有構成比率は、プロジェクトオーナーによって決定される。トークンの販売は発行後に行われ、プロジェクト支援者は発行されたトークンを購入する。RICO 独自のアプローチでは、トークン発行のすべての実行プロセスは Ethereum Virtual Machine(EVM) 上で厳密に定義され、自動的に実行される。また、トークン生成の速度を自動的にコントロールすることで、システムの分散化を進めるためのより公平な配布を実行できる。

トークンの発行は以下のステップを経て行われる。

- トークンの初期化（プロジェクトオーナーは公開買い付けの条件とトークンの生成規定を決定）
- トークンの自動公開買い付け（プロジェクトオーナーは公開買い付けを行う）
- トークン生成予約（プロジェクト支援者は Proof of Donation によって生成の予約を行う)
- トークン生成（ある一定期間の期間を設け、その期間が終了または発行上限に到達後、発行規定に従い、自動生成される）

### 2.2　トークンの生成規定

トークンの生成規定はプロジェクトオーナーが規定し、プロジェクト支援者がトークンの生成を行う。生成規定には以下の条件を規定する。

- トークンの最大生成上限
- トークンの生成タイミングとそのタイミングでの量、宛先
- トークンの自動買い付けの量
- トークンの自動買い付けの ETH/Token のレート

### 2.3　トークンの自動公開買い付け (TOB)

プロジェクトオーナーは、トークン生成予約開始より前に、トークンの公開買い付けを自動的に行うことが可能である。このアプローチが意図するのは公開買い付けによってプロジェクトチームにプロジェクトの成功に責任を持たせることで、モチベーションの維持させるためである。また、買い付けに用いられた ETH は生成されたトークンのマーケットメイキングの費用として期限付きでマーケットメイカーに寄付される。賛同するプロジェクトオーナーは必ず 6 ヶ月間以上のトークンロックを行う必要がある。公開買い付けの要件は以下の通りである。

- 公開自動買い付けの時の ETH/Token のレート
- 公開自動買い付けのトークン割合

### 2.4　Proof of Donation (PoD) によるトークン生成の予約

トークンの公開自動買い付け (TOB) が成功した場合、プロジェクトオーナーは寄付を受け付けることが可能である。プロジェクトオーナーは寄付を受けつけ、プロジェクトの原資とすることが可能である。プロジェクトに寄付を行う者はプロジェクト支援者としてトークンの新規発行予約に自動的に登録される。このときのトークンの発行価格は DutchAuction 形式の価格決定を行うことが可能である。また、従来のように、調達時の価格を明示的に固定にすることも可能である。

### 2.5　DutchAuction によるトークン発行価格の決定

トークンの発行価格の決定方式は、Raiden-Network(2) や Gnosis-Project(3) が採用した、DutchAuction 方式を採用することが可能である。

DutchAuction 方式とは、せり下げの競売の方法であり、不特定多数の投票者がトークンの価格に Bet することでトークンの競売価格を決定する方法である。これを採用する利点として、プレディクションマーケット（群衆の知恵）作用によって、トークン価格が市場で取引される前の段階で需要と供給が均衡するため、市場価格に近くなることが知られている。RICO は、この手法によってトークンの価値決定を市場の公平な判断に任せることを目指す。

トークン価格のモデルを以下に示す。

$$Price_{token}(t, eth) = \begin{cases} \frac{priceFactor * 10^{18}}{st - t + 7500 + 1} & (1) \\ \frac{received_{eth} * 10^{18}}{supply_{max} + 1} & (2) \end{cases}.$$

$t = BlockTime, eth = ReceivedETH, st = staringTime$ である。この式によってトークンプライスは (1) または (2) の状態を取ることが決定されている。イーサリアム上での時間はマイナーの決定する block.timestamp が用いられる。寄付募集期間がスタートすると st = t となり、$\lim_{t \to \infty} Price_{token}(t, eth) > (2)$ となるように価格は決定される。このことは $\frac{d \sum_{t=st}^{\infty} received_{eth}}{dt}$ がより低い場合、トークンプライスはゼロに近くため、トークンプライスは市場の注目度に応じてプライスは定量的に決定されることが導かれる。

### 2.6 0ETH 送信によるトークンの生成

トークンの新規生成は、トークンの生成規定に定める期間を過ぎた場合、プロジェクト支援者自身の操作によってトークンを生成することが可能である。プロジェクト支援者は、コントラクトアドレスに 0ETH を送信することによって、自身に対して予約されていたトークンが自動的に生成され入手できる。トークンは生成された時点から送受信が可能である。

## 3 コアモジュール

### 3.1 Contract Diagram

以下にコントラクトのダイアグラムを示す。

トークンの発行、プロジェクトオーナーへの寄付の送信はすべて RICO コントラクト内で実行される。そのため、プロジェクト支援者の資金は中間者

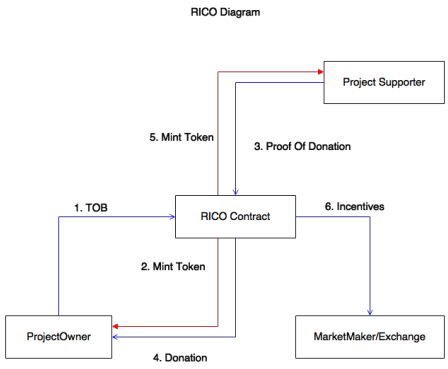


図 1　ContractDiagram

を挟まずにプロジェクトオーナーに直接送金される。また、プロジェクトオーナーは TOB によって消費した ETH を直接マーケットメイカーに寄付することが明示的に決定される。これはマーケットメイカーのインセンティブとして利用される。

### 3.2 ApiFunctions

#### 3.2.1 init()

RICO を初期化する。

#### 3.2.2 initTokenData()

EIP-20 フォーマットのトークン情報を初期化する.

#### 3.2.3 addRound()

トークンの生成量と生成タイミングを入力しラウンドを生成する.

#### 3.2.4 addMarketMaker()

TOB された ETH のインセンティブ配布プログラムの登録（マーケットメイカー）.

#### 3.2.5 strategyConfirm()

プロジェクトオーナーはトークンの生成規定の確認してロックする。

#### 3.2.6 deposit()

プロジェクトオーナーが TOB を行うために ETH をデポジットする。

#### 3.2.7 execTOB()

プロジェクトオーナーが TOB を行うための ETH を確認し、ToB を実行する。

#### 3.2.8 execMarketMaker()

プロジェクトオーナーはマーケットマイカーに対し、寄付を実行する。

#### 3.2.9 widthdraw()

プロジェクトオーナーがもし余剰の ETH を入れてしまった場合、reFund することができる。

#### 3.2.10 donate()

プロジェクト支援者はプロジェクトオーナーに対し、寄付を実行する.

#### 3.2.11 mintToken()

プロジェクト支援者はトークンを PoD に従って生成する。

## 4 まとめ

現状の ICO での問題、特にプロジェクトオーナーと支援者のトークン発行権利の歪みは、プロジェクトオーナーが一方的に一般投資家を搾取するといった社会問題にも発展している。プロジェクトの支援のあり方はよりフェアでなければならない。RICO は、プロジェクトオーナーによる公開買い付け手法と、トークンの厳密な発行規定、マーケットメイカーへのインセンティブの導入というアプローチを用いた RICO 独自の手法をはじめ、さまざまな先進的な ICO プロジェクトのトークン設計手法を、誰でも簡単に自分のプロジェクトに取り入れることができるようになるフレームワークである。これらの組み込みによって、ICO 時のリスクを大幅に低減できる可能性がある。さらに、RICO は今までよりも公平性が高く、プロジェクトオーナーが責任のある、良質なプロジェクトを迅速に支援するフレームワークとして社会実装することを可能にするものである。

## 5 脚注


1. EIP-20 TokenStandard.
https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20-token-standard.md.
2. Raiden Network https://raiden.network.
3. Gnosis Project https://gnosis.pm.