Formulas for Bancor system

Meni Rosenfeld*

December 12, 2016
Latest version: June 11, 2017

Abstract

The Bancor system allows a smart contract to handle the purchase and sale of tokens, without a 2nd party. The tokens are traded for coins of a parent currency that are held in reserve. This document will derive the formulas required to determine the amount of tokens received for a given amount of coins.

Contents

1 Basic Formulas

Let R be the current reserve of the parent currency (say, Ether). Let S be the current outstanding supply of tokens. Let F be the constant fractional reserve ratio, and finally let P be the current price of a token.

The total market cap of the tokens is SP, and by definition the amount in reserve is F times that, $R = FSP$. This means that the price at any time can be calculated as $P = \frac{R}{SF}$.

When a user buys an infinitesimal amount of coins dS (selling simply means $dS < 0$), the supply of tokens increases by this amount. The user pays $P\ dS$ for them, which are added to the reserve, meaning $dR = P\ dS$. Additionally, since $R = FSP$, we have $dR = d(FSP) = Fd(SP) = F(S\ dP + P\ dS)$. So we have:

$$P\ dS = dR = F(S\ dP + P\ dS)$$

$$P\ dS(1 - F) = FS\ dP$$

[*] The author can be contacted at meni@bitcoin.org.il. If you would like to support this research, you can send bitcoins to 18Vftuz74RnVdMM1boN69oW59FagBNSvo4.

$$P\ dS\left(\frac{1}{F}-1\right)=S\ dP$$

Letting $\alpha=\frac{1}{F}-1$ we have

$$P\ dS\alpha=S\ dP$$
$$\alpha\frac{dS}{S}=\frac{dP}{P}$$
$$\alpha\ d\log S=d\log P$$
$$\alpha\log S+A=\log P$$
$$e^{A}S^{\alpha}=P$$
$$P=\left(\frac{S}{S_0}\right)^{\alpha}P_0$$

This allows calculating the current price, given the current supply of tokens, and the initial price and supply.

If a user buys a total of T tokens, bringing the total supply from S_0 to S_0+T, the total paid amount is

$$\begin{aligned}
E &= \int_{S_0}^{S_0+T} P\ dS=\int_{S_0}^{S_0+T} P_0\left(S/S_0\right)^{\alpha}\ dS= \\
&= P_0S_0\frac{(S/S_0)^{\alpha+1}}{\alpha+1}\Bigg|_{S=S_0}^{S_0+T}=P_0S_0\left(\frac{((S_0+T)/S_0)^{\alpha+1}}{\alpha+1}-\frac{(S_0/S_0)^{\alpha+1}}{\alpha+1}\right)= \\
&= \frac{P_0S_0}{\alpha+1}\left(\left(1+\frac{T}{S_0}\right)^{\alpha+1}-1\right)=FP_0S_0\left(\left(1+\frac{T}{S_0}\right)^{1/F}-1\right)= \\
&= R_0\left(\left(1+\frac{T}{S_0}\right)^{1/F}-1\right)=R_0\left(\sqrt[F]{1+\frac{T}{S_0}}-1\right)
\end{aligned}$$

From this we can deduce the amount of tokens T obtained by paying E:

$$E=R_0\left(\sqrt[F]{1+\frac{T}{S_0}}-1\right)$$
$$1+\frac{E}{R_0}=\sqrt[F]{1+\frac{T}{S_0}}$$
$$\left(1+\frac{E}{R_0}\right)^{F}=1+\frac{T}{S_0}$$
$$T=S_0\left(\left(1+\frac{E}{R_0}\right)^{F}-1\right)$$

2 Multiple Reserve Currencies

A Bancor-based smart contract can also have reserves consisting of several parent currencies. If there are m different reserve currencies, then for each currency $i \in \{1, 2, \ldots, m\}$ we have amount in reserve R_i, fractional reserve ratio F_i, and price P_i (where $\sum_i F_i \leq 1$). The outstanding supply of tokens S is global. As before, we have for every i, $R_i = F_i S P_i$, which also means that $dR_i = F_i(S\, dP_i + P_i\, dS)$. Tokens can be bought and sold for any combination of currencies, so in general $dS = \sum_i \frac{dR_i}{P_i}$.

If tokens are bought or sold for a specific reserve currency i, we have $dR_i = P_i\, dS$ and $dR_j = 0$ for $j \neq i$. This case is identical to the one in the previous section. Note that trades using one currency affect the token price in terms of the other currencies - since R_j, F_j are fixed and S changes, the price of the token changes in inverse proportion to S.

Buying and selling tokens for different currencies commutes - if a single trader performs several such operations, the end result is the same regardless of the order in which they are carried out (of course, if there are multiple traders, value can be transferred from one to the other depending on the order of operations). In particular, if at some point there are S_0 outstanding tokens and reserve R_{i0} of each currency i, the following invariant holds:

$$S = S_0 \prod_{i=1}^{m} \left(\frac{R_i}{R_{i0}} \right)^{F_i}$$

Which means that if a user spends a total of $E_1, E_2, \ldots, E_m$ coins of currency $1, 2, \ldots, m$ respectively (where any combination of the E_i can be negative), the amount of tokens obtained is

$$T = S_0 \left(\left(\prod_{i=1}^{m} \left(1 + \frac{E_i}{R_{i0}} \right)^{F_i} \right) - 1 \right).$$