Crowbar token contract specifications

Crowbar Project

v0.0.4a

1. Symbol - CWBR

   Is free according to search as of 6/16/2018
2. Contract returns tokens immediately to backers
3. Participation currency - ETH
4. Soft cap is 200 ETH, no hard cap, projected cap is 10000 ETH equals to 5M tokens
5. Contract collects and stores received ETH (total amount) from backers to predefined address (wallet) minus operational amount, used by the team, so that
   a. $A_B = W_F + O_F$, where $A_B \geq 200$ ETH is total amount sent to contract address.
   b. $P_O = 100 \times A_B^{-0.42}$ is operational percent, applied to total amount

      Suggested value of P_O is 10% to 2% and below depending on A_B from power curve formula
   c. $W_F = (1 - \frac{P_O}{100}) \times A_B = (1 - \frac{100 \times A_B^{-0.42}}{100}) \times A_B = A_B - A_B^{0.58}$ is amount of wallet funds to be distributed after the test
   d. $O_F = \frac{P_O \times A_B}{100} = \frac{(100 \times A_B^{-0.42}) \times A_B}{100} = A_B^{0.58}$ is operational amount used by team.

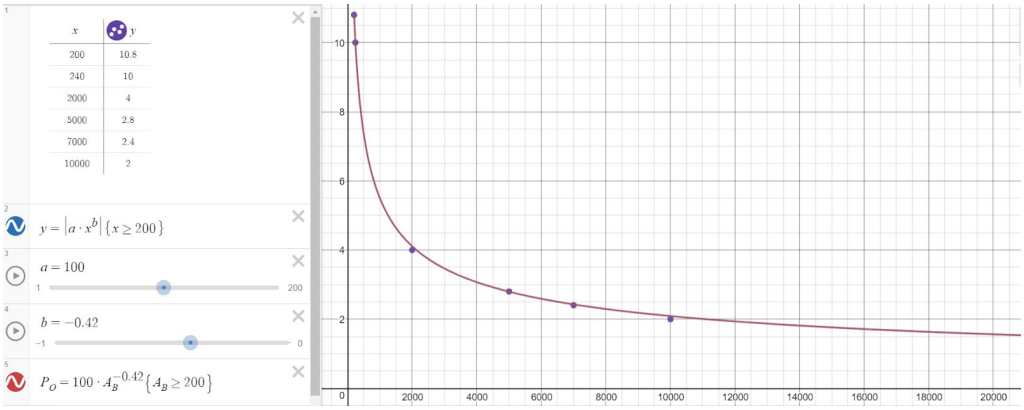

Figure1. Operational percent dependency of total amount backed

6. Price is approx equivalent of ~1$ in ETH as of 6/16/2018 = 0.002ETH
7. Participants - minimum 200 backers (sceptics camp)

8. Depending on input parameter R (has to be enumerable of constants representing set N_R of possible output from oracle smart contract), token contract has to distribute from wallet to accounts of group that are holding token proportionally to amount of holdings at the moment of result distribution t_{RD}
    a. $N_R := [T, S, C]$ is a set of constants representing (T)raders, (S)ceptics, (C)ancel
    b. $S_A := \{a_0 .. a_n | \forall A_a > 0\}$ is a set of all addresses holding tokens with amount greater then 0 at t_{RD}
    c. $S_S := \{a_k .. a_{k+j}\}, S_S \subseteq S_A$ is a set of all addresses of skeptics (initial backers)
    d. $S_T := \{a_m .. a_{m+l}\}, S_T \subseteq S_A$ is a set of all addresses of traders
    e. $S_C := S_A$ is a set of all addresses holding tokens at t_{RD} in case of cancel
9. At t_{RD} is $a_i \in S_S \Rightarrow a_i \notin S_T$ - any address in sceptics list can not be considered trader address.
10. Address $a \in S_S$ only if it held tokens before t_0 - time of test start. If $A_{t_m a}$ - is amount of tokens at address a for time $t_m \leq t_0$ and $A_{t_j a}$ - is amount of tokens at address a for $t_j > t_0$ then $a \in S_S \Rightarrow A_{t_j a} \leq A_{t_m a} \Rightarrow A_{t_m a} > 0$ - token amount of skeptic address after tests starts has to be lower or equal to the initial backing deposit. This is done to prevent attack vector described in section **3.3.5.1 Skeptics win.**

    $$A = F_{SA}(a)$$

    is a function of amount eligible for payout for skeptic address $a \in S_S$
11. $P = F_P(a)$ is a function of payout for address a at t_{RD}. Address is eligible for payout if

    $$P > 0 \Rightarrow A_a > 0$$

12. t_r is time when test result is decided and t_m is any time so that $t_r > t_m > t_{RD}$ and $A_{a_l} > 0$ - is amount of tokens at address $a_l \in S_T$. One trade cycle (TC) for amount A_{a_l} is set of two transactions (one for buy T_B followed by sell T_S).

    $$A = F_{TA}(a)$$

    is a function of amount eligible for payout for trader address $a \in S_T$. Number of trade cycles N_{TC} for amount A_{a_l} is

    $$N_{TC} = 1 \Leftrightarrow N_{TC} := \{T_B, T_S\} \Rightarrow t_{T_B} < t_{T_S} and A_{T_B} = A_{T_S} = A_{a_l}$$

    If n_{t_m} is number of trade cycles for amount $A_{a_l} > 0$ for address a_l then

    $$A_{a_l} = F_{TA}(a_l) > 0 \Leftrightarrow n_{t_m} > 1$$

This is required to prevent attack vector described in section **3.3.5.2 Traders win**

13. For A_P - total amount eligible for payout and test outcome $R \in N_R$ so

$$A_P = F_A(a, R)$$

Then

$$R = T \Leftrightarrow A_P = \sum_{i=m}^{i=l} F_{TA}(a_i) \; and \; \forall a_i \in S_T$$

with

$$R = S \Leftrightarrow A_P = \sum_{i=k}^{i=j} F_{SA}(a_i) \; and \; \forall a_i \in S_S$$

14. P_a payout for address a then will be $P_a = F_p(a) = Q \times F_A(a, R)$ where $Q = \frac{A_P}{W_F}$ is payout price per token.