

Actors

- Token owner - `Private key (PK)` holder of address from which Token contract deployed.
- Investor - Identified person who bought at least minimal allowed amount of tokens.
- Privileged holders - partners, team members.

Token

Before ICO and Pre-ICO we need to create a production ready ERC20 compliant OCR Token.

Token features

- Token has fixed supply and is not mintable
- Total supply: 65e6 tokens
- Token id: `OTC`
- 18 decimals
- Token/ETH exchange rate: 4500
- Token can be in locked/unlocked states:
 - Locked state - tokens cannot be transferred outside from investor.
 - Unlocked state - tokens can be transferred from investor. Unlocked state is only allowed when main ICO successfully completed and all available tokens (65e6) are distributed.
- Token distribution can be managed from selected ETH addresses controlled by `Token Owner`

Token distribution table

- 1.3e6 Distributed among partners before
- 3.25e6 Bounty distributed tokens
- 5.85e6 Distributed among team members
- 54.6e6 Public available tokens

Token distribution among privileged holders

Token contract has separate counters (number of available tokens) for all token distribution classes:

- Partners
- Bounty
- Team
- Public

Token distribution for `privileged holders`:

- `Privileged holder` provides its ETH address to the `Token owner`
- `Token owner` has the ability to call protected `Token contract` (via `CLI manager tool`) method assigning tokens to `PH` ETH address then decrement token counter for the specified distributions

class.

- `Token owner` cannot assign more tokens than allowed in token distribution table.

Pre-ICO

Remaining questions:

- What is the minimal amount of tokens `investor` can buy?

General rules

- Pre-ICO performed by a separate smart contract allowed to distribute tokens for `OTC` token.
Pre-ICO contract controlled by `Token Owner`.
- Pre-ICO contract has a `Team Walled` address in order to collect investors ETHs if pre-ico finished successfully.
- Low-cap: 100 ETH
- Hard-cap: 1500 ETH

Pre-ICO phases

- `Inactive` - pre-ico is not started
- `In-progress` - pre-ico is in progress and investors can buy tokens.
- `Suspended` - pre-ico temporarily suspended, cannot accept buy requests. Can be resumed to `in-progress` state.
- `Terminated` - pre-ico terminated, cannot accept buy requests, cannot be resumed. Investors are able to return their funds. `Token Owner` can terminate pre-ico at any time.
- `Not completed` - pre-ico goals not completed. Low-cap not funded and pre-ico finish date in the past. Investors are able to return their funds.
- `Finished` - When one of the following is true:
 - Low cap funded and pre-ico finish date in the past
 - Hard cap funded

Pre-ICO dates

- Pre-ICO has its `start date` (can be changed by `Token Owner`). Start date cannot be changed if pre-ico not in `Inactive` or `Suspended` state.
- Pre-ICO `end date` can be changed if pre-ico in `Inactive` or `Suspended` states.

Pre-ICO distribution rules

- Extra 10% tokens bonus if investment greater or equal 0.5 ETH
- Investor can return his initial funds only if pre-ico in `Terminated` or `Not completed` calling specific pre-ico contract method.
- Invested ETHs can be transferred to `Team Walled` only if pre-ico in `Finished` state.

Ways to invest:

Simple

- `Pre-ICO` contract can accept payments from any ETH address. Investor is `PK` owner of this address.
- `Investor` cannot be identified.

Pros

- Significantly faster and cheaper to implement comparing to `Advanced`

Cons

- Allows anonymous investors

Advanced

- `Pre-ICO` investor must register in private zone at `otcrit.org` using `auth0.com` service
- Web site generates unique investor ID
- Web site allows to create ETH address on behalf to investor, payings to this address will transfer to `pre-ico` contract. In the `pre-ico` contract investor identified by its investor ID.

Pros

- Investors are not anonymous and forced to accept service `terms of usage`
- Investors can easily control their fundings on website

Cons

- More dev resources to implement comparing `Simple` case
- Single point of failure - if website DB will lost then all investor identifiers will
- Investor do not control their investments from cryptographically point of view. (This restriction can be resolved.)

How to control/admin Token and ICO?

I propose to write a simple command line tool helping to manage `Token` and `ICO` smart contract. This cmd tool will use `PK` of `Token Owner`. It more cheap in development and convenient than a custom web based admin panel.

For example get general token info:

```
otcrit token status
Token name: OTC
Status: locked
Distributed tokens: 650000 (10%)
```

Add a team member to `privileged` holders and give him 10000 team privileged tokens:

```
otcrit team allow John 0xe486581929055dd2C6eF7B92dD4Cfd83f6Ef26d1 10000
```

List of all privileged groups:

```
otcrit show privileged

team (remaining: 100000):
  Bob 0xe486581929055dd2C6eF7B92dD4Cfd83f6Ef26d1 55000
  John 0xe999581929055dd2C6eF7B92dD4Cfd83f6Ef26a1 10000

partners (remaining 45000):
  Alice 0xe943881929055dd2C6eF7B92dD4Cfd83f6Ef26a1 3000
```

and many other operations

otcrit.org website integration

Website will show pre-ico/ico status and dates in real time

Estimation of Develepment resources:

- OTC Token with support of privileged users: 14h
- Pre-ICO contract: 26h
- Token/Pre-ICO contract test cases: 30h
- Command line management tool: 30h
- otcrit.org website integration: 8h

Total 108h. 14-18 days to implement.

- Web private zone for investors: we need to discuss all features