Actors

- `Token` - `OTC` Otcrit token ethereum contract.
- `Token owner` - `Private key (PK)` holder of address from which Token contract deployed.
- `Investor` - An identified person who bought at least minimal allowed amount of tokens.
- `Priveleged holders` - partners, team members, bounty participants.
- `Website` - `otcrit.org` website including private investor's web-zone.

Token

Before ICO and Pre-ICO a production ready ERC20 compliant OCR Token must be deployed.

Token features

- Token has fixed supply and not mintable
- Total supply: `65e6` tokens
- Token id: `OTC`
- `18` decimals
- Token/ETH exchange rate: `4000`
- Token can be in locked/unlocked states:
- `Locked` state - tokens cannot be transfered outside from investor.
- `Unlocked` state - tokens can be transfered 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

- `52e6` Sold to public
- `5.5e6` Team members
- `3.25e6` Bounty
- `3.25` Partners and advisors

Token distribution among privileged holders

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

- Public
- Team
- Bounty
- Partners

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

General rules

- Pre-ICO managed by a separate smart contract allowed to distribute tokens for `OTC` token. Pre-ICO contract controlled by `Token Owner`.
- Low-cap: 100 ETH If low-cap is not reached until end of pre-ico all invested eths allowed to withdraw by investors. Pre-ico state will be `Not completed`
- Hard-cap: 1500 ETH If hard-cap reached pre-ico state will be `Completed`

Pre-ICO phases

- `Inactive` - pre-ico is not started and pre-ico `start date` in the future.
- `Active` - pre-ico is in progress and investors can buy tokens. Pre-ico start date in the past.
- `Suspended` - pre-ico temporarily suspended, cannot accept buy requests. Can be resumed to `Active` state.
- `Terminated` - pre-ico terminated, cannot accept buy requests, cannot be resumed. Inverstors are able to returns theirs 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 returns theirs funds.
- `Completed` - When one of the following is true:
- Low cap funded and pre-ico `end date` in the past
- Hard cap funded

Pre-ICO dates

- Pre-ICO `Start date` can be changed by `Token Owner` only if pre-ico in `Inactive` state.
- Pre-ICO `End date` can be changed only in `Inactive` or `Suspended` states.
- Pre-ICO distribution rules can be changed only in `Inactive` or `Suspended` states.

Pre-ICO distribution rules

- `6.75e6` Tokens distributed in pre-ico phase
- `1 ETH == 4000 OTC`
- `12.5%` Bonus as percent of investment during first week of pre-ico
- `10%` Bonus as percent of investment from second week up to end of pre-ico
- Hard-cap `1500` ETH
- Low-cap `100` ETH
- Investor can return his initial funds only if `pre-ico` in `Terminated` or `Not completed` states

Pre-ICO investment workflow

1. Investor must read then accept rules and conditions of pre-ico phase.
2. Investor must identify himself by registering on `otcrit.org` website using `auth0.com` service
3. `Website` generates unique ID for investor
4. Upon request `Website` generates eth address (using BIP32 HD wallet) dedicated to `investor` used as endpoint for investment payments from this particular investor.
   NOTE: `Investor` does not own generated endpoint address. `PK` of this address owned by `token owner`.
   NOTE: `Website` software signs endpoint address by token owner private key and store signature hash in `DB`. We have the following tables in website `DB`:

```
INVESTORS:
 investor id,
 investor email,
 endpoint eth address,
 signature hash of endpoint address (signed by token owner),

INVESTMENTS:
 investor id,
 sender eth address,
 amount wei,
 ethereum block number,
 stage: 'pre-ico' | 'ico'
 registered: true|false (true if investment registered in pre-ico contract)
```

1. All funds paid to `endpoint address` controlled by `token owner` (by definition).
2. `Website` software listens eth network (using parity client) for investment transactions and calls pre-ico contract updating amount of tokens belonging to investor. `Pre-ico` contract received the following data:
   - endpoint address
   - signature of endpoint address (signed by token owner)
3. pre-ico contract updates token distribution for investor using endpoint balance.

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. `CLI tool` must have access to `website DB` in order to access `INVESTORS` and `INVESTMENTS` tables.

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 other operations.