Термины

1. Множественная подпись (мультиподпись) - требование заверения управляющего воздействия на контракты кворумом электронных подписей (M из N, напр. 2 из 3). Сами подписи и параметры кворума также изменяемы посредством М.П.
2. Crowdsale-контракт - контракт, принимающий средства инвесторов в криптовалюте и выдающий токены взамен.
3. Fallback-режим (пауза для непредвиденных обстоятельств) - режим минимальной функциональности crowdsale-контракта, когда прием инвестиций приостановлен и допустимы лишь некоторые управляющие воздействия.
4. Soft cap - минимальный порог сбора инвестиций, при недостижении которого средства возвращаются вкладчикам.
5. Hard cap - максимальный порог сбора, при достижении которого crowdsale досрочно успешно завершается.

Контракты

1. Токен (ERC20, до 18 знаков после запятой).
   Токен выдается и сжигается (при возврате инвестиций при недостижении soft cap) в ходе crowdsale'ов. Оставляем возможность доп. эмиссии после ICO.
   минорное: какой код токена (напр. “”)?
   минорное: какое название токена (напр. “”)?
2. Хранилище эфира (Funds)
   Контракт, обеспечивающий прозрачную и гарантированную блокчейном реализацию soft cap: если soft cap не собран, средства могут быть извлечены инвесторами и только ими; если soft cap собран, средства могут быть извлечены владельцами crowdsale и только ими.
3. Crowdsale pre ICO 1 – контракт первого этапа pre ICO
4. Crowdsale pre ICO 2 – контракт второго этапа pre ICO
5. Crowdsale ICO
   Crowdsale-контракт этапа ICO

Параметры

- Pre ICO 1 – первый этап pre ICO
  - дата начала: делаем устанавливаемой владельцами до ICO

    - дата окончания: две недели от даты начала
    - soft cap – не устанавливаем
    - Hard cap – не устанавливаем
    - Курс токенов задается владельцами до ICO вызовом метода
    - В первую неделю цена токена не меняется. Во вторую неделю цена токена повышается на 5%.
    - Используем хранилище эфира
    - Не используем аналитику
- Pre ICO 2 – второй этап pre ICO
    - дата начала – 00:00 часов дня следующего за днем окончания pre ICO 1
    - дата окончания: две недели от даты начала
    - soft cap – не устанавливаем
    - Hard cap – не устанавливаем
    - В первую неделю цена токенов – цена последней недели pre ICO 1 + 5%
    - Во вторую неделю – цена первой недели pre ICO 2 + 5%.
    - Используем хранилище эфира
    - Не используем аналитику
- ICO
    - дата начала – 00:00 часов дня следующего за днем окончания pre ICO 2
    - дата окончания: два месяца от даты начала
    - soft cap: делаем устанавливаемой владельцами до pre ICO 1
    - Hard cap: делаем устанавливаемой владельцами до pre ICO 1
    - Цена токенов – цена второй недели pre ICO 2 + 5%
    - 20% токенов генерятся для владельцев
    - Первый месяц цена токена не меняется. Во второй месяц каждую неделю цена токена повышается на 5%.
    - Используем мультиподпись
      Минорное: нужны адреса, участвующие в мультиподписи
    - Используем хранилище эфира
    - Не используем аналитику

Безопасность

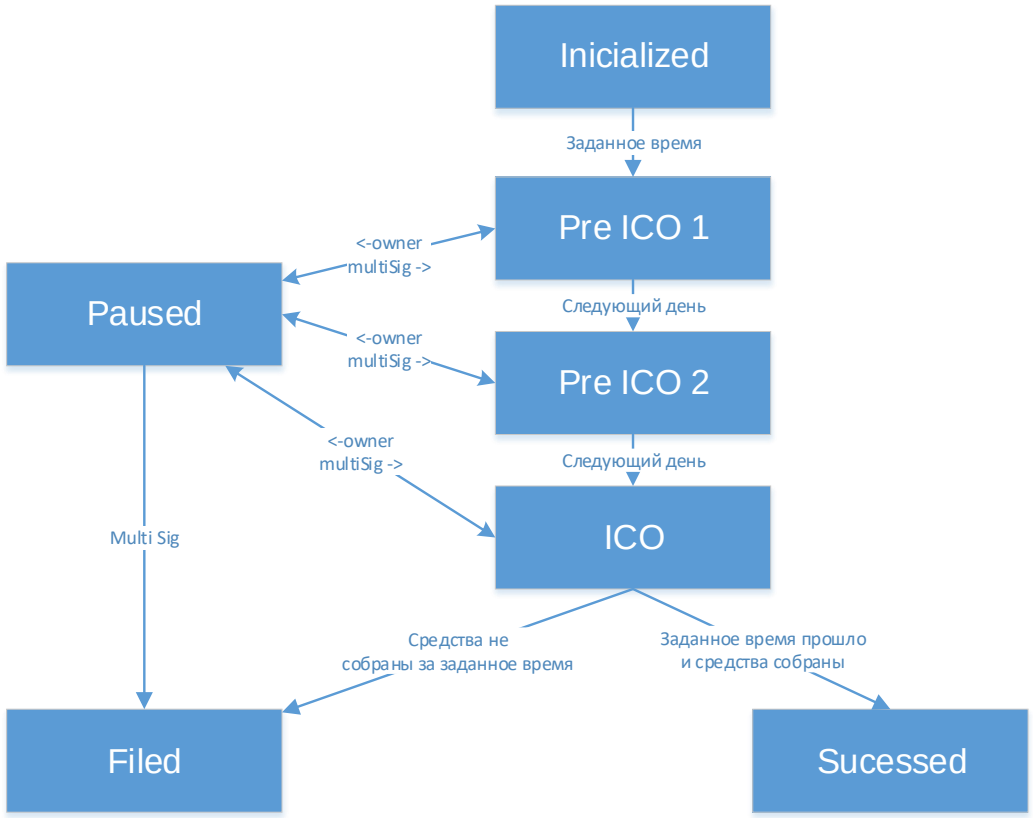
1. Во время pre ICO 1 и pre ICO 2 вывод/перевод средств владельцами и инвесторами запрещен

2. Во время ICO используем мультиподпись 2/3 (всего 3 подписи, кворум составляют любые 2 из них). Любое управляющее воздействие на контракты ICO (за исключением паузы), токена и Funds требует множественной подписи.
3. Во время ICO владельцы с помощью мультиподписи могут задавать контракту токена т.н. контракт-контроллер.
4. Переход в fallback-режим по решению владельцев (достаточно одной подписи). Автоматический переход в fallback-режим при обнаружении утечки эфира. Выход из fallback-режима требует мультиподписи. Несмотря на использование паузы, никакие времена контракта (окончания crowdsale, бонусы на основе времени, и т.д.) не корректируются.
5. Любые выводы эфира из crowdsale, имеющего soft cap, возможны только после необратимого перехода в состояния успеха либо неудачи.

Прочее

1. Передача токенов между владельцами заблокирована до окончания ICO.
2. Для владельцев crowdsale оставляем возможность пробной инвестиции вне временных рамок - для теста в mainnet.
3. В случае недостижения soft cap вместе с возвратом средств сжигаем соотв. токены инвестора.
4. Периоды crowdsale вычисляются с точностью +-1 минута.

Граф состояний crowdsale-контракта ICO



Этапы работы

1. Согласование техпроекта
2. Написание кода Solidity
3. Покрытие кода unit-тестами
4. Внутренний аудит
5. Деплой контрактов и эмуляция в testnet
6. Деплой контрактов в mainnet
7. Верификация байт-кода контрактов на etherscan.io
8. Bug baunti (внешний аудит)
9. Доработка по результатам Bug baunti
10. Тестирование
11. Передача управления контрактами Заказчику
12. Проверка связей и владельцев контрактов
13. Пробная инвестиция в mainnet
14. Оперативная поддержка и устранение багов