### Pikabu ICO

### 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.

Код токена: PKB

Название токена: PIKABU BROVASTIK TOKEN

1. 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.
2. Crowdsale ICO  
   Crowdsale-контракт этапа ICO
3. Вывод токенов

Контракт, обеспечивающий честное использованеи собранных средств: владельцы могут выводить не более 20% собранных средств в год, что дает некоторую защиту от скама.

#### Параметры

* ICO
  + дата начала: делаем устанавливаемой владельцами до ICO
  + дата окончания: делаем устанавливаемой владельцами до ICO
  + soft cap: делаем устанавливаемой владельцами до ICO
  + Hard cap: делаем устанавливаемой владельцами до ICO
  + Курс токенов задается владельцами до ICO вызовом метода
  + 20% токенов генерятся для владельцев
  + Цена токена определяется текущей стоимостью токена на бирже
  + Используем мультиподпись
  + Используем хранилище эфира

### Безопасность

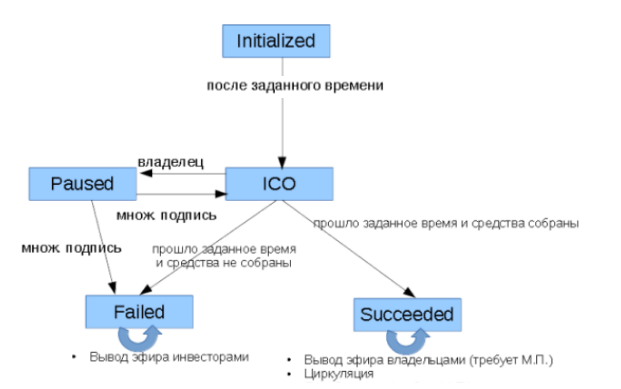
1. Во время ICO используем мультиподпись 2/3 (всего 3 подписи, кворум составляют любые 2 из них). Любое управляющее воздействие на контракты ICO (за исключением паузы), токена и Funds требует множественной подписи.
2. Во время ICO владельцы с помощью мультиподписи могут задавать контракту токена т.н. контракт-контроллер.
3. 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.
4. 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. Передача управления контрактами Заказчику
9. Проверка связей и владельцев контрактов
10. Пробная инвестиция в mainnet
11. Оперативная поддержка и устранение багов