Описание

Система смарт контрактов предназначена для проведение лотерей и создания столов для игры бинго. Для обеспечения случайных результатов используется отдельный смарт контракт с генерацией псевдослучайных чисел в нужном формате. Для покупки билетов и выплат выигрышей используется ERC20 токен, который работает только в нашей системе и привязывается к используемым нами стейбл коинами. При розыгрыше лотереи расчет результатов обеспечивается с помощью бекенда, так как подобные расчеты на стороне блокчейна являются очень дорогостоящими и неэффективными.

Token

Смакт контракт реализован на основе openzeppelin ERC20Upgradeable контракта. Контракт является обновляемым. Токен используется для расчетов внутри системы лотереи. Все трансферы могут проводится только между нашими контрактами и участниками лотереи.
Контракт имеет систему ролей, в которой есть три роли:

- **DEFAULT_ADMIN_ROLE** - дефолтная роль суперадмина, которая выдает и убирает все остальные роли. Выдается овнеру при инициализации контракта.
- **TOKEN_ADMIN_ROLE** - роль админа токена, которая имеет право минтить и бернить токены на любых адресах. Для использования при конвертации стейбл коинов на внутренние токены и наоборот.
- **CONTRACT_ROLE** - роль контракта которая выдается используемым контрактам системы. Все трансферы в которых нет адреса с этой ролью блокируются. Сейчас такая роль выдается контракту Лотереи.

DataFeeds

Смарт контракт для генерации псевдослучайных чисел. Контракт не является обновляемым так как не содержит в себе никаких данных, только методы для генерации результатов для лотереи и бинго. Может быть в любой момент заменен на другой контракт и установлен в контрактах лотереи и бинго.
Контракт имеет основные методы:

- **getRandomLotto_6_49** - возвращает 6 неповторяющихся рандомных чисел от 1 до 49 в формате bytes6. В функцию передается соль - параметр типа bytes32 который учитывается при генерации чисел.
- **getRandomBingoNumbers** - возвращает набор неповторяющихся рандомных чисел от 1 до указанного значения максимального числа при вызове функции. Максимальное число которое можно передать - 96, то есть максимальный набор будет состоять из 96 чисел. В функцию передается соль - параметр типа bytes32 который учитывается при генерации чисел.

- **getNumbersFromBytes** - вспомогательная функция для конвертации bytes любого размера в массив чисел, где каждый byte из bytes соответствует числу в массиве.

Lottery

Смарт контракт для проведения лотерей с возможностью обновления. Каждая лотерея инициализируется, разыгрывается и рассчитывается администратором лотереи. Все лотереи и их результаты сохраняются в контракте. При инициализации администратор указывает тип лотереи и время розыгрыша. Время розыгрыша это таймштамп, до которого включительно регистрируются билеты и после которого можно разыграть и рассчитать лотерею. До времени розыгрыша нельзя разыграть лотерею а после нельзя зарегистрировать билеты. При розыгрыше лотереи с контракта DateFeeds берутся 6 чисел и записываются в лотерею как выигрышные. После розыгрыша лотереи у каждого билета этой лотереи показывается тип выигрыша для билета. При расчете лотереи на бекенде анализируются все билеты, рассчитывается пул лотереи и в результаты лотереи записываются данные розыгрыша - количество билетов и сумма выигрыша на один билет для каждого типа выигрыша. После расчета для каждого билета этой лотереи также показывается сумма выигрыша и если он выигрышный, то возможность забрать выигрыш. Билеты покупаются за внутренние токены привязанные к стейбл токенам в любое время и средства сразу засчитываются в джекпот, за вычетом комиссии. Цена билета устанавливается при инициализации контракта и может быть изменена в любое время администратором лотереи. Регистрировать билеты можно только на активную лотерею, указывая набор чисел при этом. Все билеты и их результаты сохраняются в контракте.

Типы лотерей: **Weekly**, **Monthly**, **Quarter**, **Yearly**.

Проценты для расчета пула лотереи в зависимости от типа:
- **Weekly** - **3,5%** от джекпота.
- **Monthly** - **10%** от джекпота.
- **Quarter** - **25%** от джекпота.
- **Yearly** - **100%** от джекпота.

Типы выигрышей билетов: **None**, **ThreeNum**, **FourNum**, **FiveNum**, **SixNum**.

Проценты для расчета части пула лотереи для каждого типа выигрыша:
- **None** - 0, 1 или 2 угаданных числа - **0%** от пула лотереи.
- **ThreeNum** - 3 угаданных числа - **5%** от пула лотереи.
- **FourNum** - 4 угаданных числа - **10%** от пула лотереи.
- **FiveNum** - 5 угаданных чисел - **20%** от пула лотереи.
- **SixNum** - 6 угаданных чисел - **65%** от пула лотереи.

Часть пула для каждого типа выигрыша равномерно распределяются на количество билетов с данным типом выигрыша. Если билетов какого то типа выигрыша нету то часть пула лотереи для этого типа выигрыша возвращается в джекпот.

При расчете каждой лотереи джекпот уменьшается на значение рассчитанного пула лотереи а значение не выплаченных выигрышей соответственно увеличивается. При продаже билетов в джекпот засчитывается сумма покупки токенов минус комиссия лотереи, которую в любой момент может снять администратор лотереи. Комиссия может быть установлена в диапазоне от 0(комиссия не будет взиматься) до 20% включительно. Размер комиссии устанавливается при инициализации контракта и может быть изменена в любое время администратором лотереи.
Контракт имеет основные методы:

- **getLottery** - возвращает массив данных лотереи по указанному id, где
  [
  LotteryStatus - статус лотереи (**NotExist**, **Init**, **Drawn**, **Calculated**),
  LotteryType - тип лотереи (**Weekly**, **Monthly**, **Quarter**, **Yearly),**
  uint - таймштамп времени розыгрыша,
  uint - количество зарегистрированных билетов,
  uint - размер джекпота на момент расчета(заполняется при расчете),
  bytes6 - набор выигрышных чисел (заполняется при розыгрыше),
  [][] - масив результатов(количество билетов и размер выигрыша на билет, заполняется при расчете)
  ]
- **getTicket** - возвращает массив данных билета по указаннім id лотереи и билета, где
  [
  bool - true если билет активный(зарегистрированный)
  bool - true если билет оплачен
  address - адрес владельца билета
  bytes6 - числа указанные для билета
  WinType - тип выигрыша билета(**None**, **ThreeNum**, **FourNum**, **FiveNum**, **SixNum**), показывается после розыгрыша лотереи
  uint - выигрыш билета, показывается после расчета лотереи
  ]
- **setTicketPrice** - установка новой цены билета, только для администратора лотереи
- **setDataFeeds** - установка адреса контракта для получения рандомных значений, только для администратора лотереи
- **initLottery** - инициализация лотереи, только для администратора лотереи
- **drawnLottery** - розыгрыш лотереи, только для администратора лотереи
- **calculateLottery** - расчет лотереи, только для администратора лотереи
- **buyTickets** - покупка билетов
- **registerTickets** - регистрация билетов
- **claimTickket** - снятие выигрыша выигрышных билетов
- **setFee** - установка новой комиссии, только для администратора лотереи
- **withdrawFee** - снятие комиссии, только для администратора лотереи

Bingo

Смарт контракт для добавления столов игры бинго с возможностью обновления. При добавлении стола с контракта DateFeeds берется набор рандомных чисел и записываться в контракт с id стола. Id для столов начинаются с нуля и увеличиваются по мере добавления. Добавлять столы меет право администратор бинго. Максимальное число для стола, которое равно количеству чисел в наборе, может быть в диапазоне от 1 до 96. Контракт имеет основные методы:

- **addTable** - добавляет стол с набором рандомных чисел указанного размера.
- **setDataFeeds** - устанавливает контракт для получения данных рассчитываемых с помощью псевдорандома.

Vesting contracts

Список контрактов

- ***RoomCoin.sol*** - Смарт-контракт реализован на основе открытого контракта ERC20 Zeppelin с добавленной логикой управления.
- ***vesting/StrategicRoundLock.sol*** - Смарт контракт для предпродажи и вестинга для StrategicRoundLock раунда.
- ***vesting/SeedRoundLock.sol*** - Смарт контракт для предпродажи и вестинга для SeedRoundLock раунда.
- ***vesting/PrivateRoundStage1Lock.sol*** - Смарт контракт для предпродажи и вестинга для PrivateRoundStage1Lock раунда.
- ***vesting/PrivateRoundStage2Lock.sol*** - Смарт контракт для предпродажи и вестинга для PrivateRoundStage2Lock раунда.
- ***vesting/TGELock.sol*** - Смарт контракт для предпродажи и вестинга для TGE (IDO) раунда.
- ***vesting/FoundersAndTeamLock.sol*** - Смарт контракт с вестингом для FoundersAndTeam команды.
- ***vesting/AdvisorsLock.sol*** - Смарт контракт с вестингом для Advisors команды.
- ***vesting/MarketingLock.sol*** - Смарт контракт с вестингом для Marketing команды.
- ***vesting/GamersRewardsLock.sol*** - Смарт контракт с вестингом для GamersRewards.
- ***vesting/DevelopmentLock.sol*** - Смарт контракт с вестингом для Development команды.
- ***vesting/TreasuryLock.sol*** - Смарт контракт с вестингом для Treasury команды.

RoomCoin

Название - ***Room Coin***
Символ - ***RMC***

Общее количество токенов - ***10.000.000***
Максимальная комиссия - ***5%***

- В смарт-контракте есть белый список. Если один из адресов в белом списке присутствует в трансфере, трансфер происходит как обычный трансфер ERC20 без обработки.
- В смарт-контракте есть черный список. Если один из адресов в черном списке присутствует в трансфере, трансфер запрещен.
- Белый список имеет приоритет над черным списком. Это означает, что если в передаче присутствуют адреса с обоих списков, трансфер происходит без ограничений.
- В смарт-контракте установлено ограничение на максимальное количество токенов в транзакции, которое устанавливается владельцем контракта.
- Адреса с ролью ***RMC_PAIR_ROLE***, считаются пулами, предоставляются владельцем контракта.
- В смарт-контракте установлено ограничение на торговлю с пулами. После покупки токенов в пуле продать их можно только после определенного количества блоков, установленного владельцем контракта.
- В смарт-контракте есть антибот-механизм, который работает в начале торговли на определенное количество блоков и добавляет в черный список адреса, пытающиеся взаимодействовать с зарегистрированными пулами.
- В смарт-контракте есть комиссия, которая сжигается во время передачи, если комиссия не отключена для адреса отправителя. Максимальное значение комиссии составляет 5% и устанавливается владельцем контракта.

Контракты с предпродажей и вестингом

(***StrategicRoundLock***, ***SeedRoundLock***, ***PrivateRoundStage1Lock***, ***PrivateRoundStage2Lock***, ***TGELock***)

Смарт контракт обеспечивает продажу токенов после начала продаж и распределяет токены владельцам на протяжении определенного периода для вестинга. Для каждого из раундов устанавливаются индивидуальные параметры в соответствии с токеномикой. Начало и конец торговли и вестинга устанавливаются владельцем контракта и могут быть произвольными.

Контракты на разблокировку

(***FoundersAndTeamLock***, ***AdvisorsLock***, ***MarketingLock***, ***GamersRewardsLock***, ***DevelopmentLock***, ***TreasuryLock***)
Смарт контракт обеспечивает распределение токенов на указанный адрес на протяжении определенного периода. Для каждого контракта устанавливаются индивидуальные параметры в соответствии с токеномикой. Начало и конец разблокировки устанавливаются владельцем контракта и могут быть произвольными.

Токеномика

https://docs.google.com/spreadsheets/d/e/2PACX-1vSdn3Xkp0iyfvctGtM1iLuasP6KB157AGjt9hEutDuSvp_ZQlZboSWx0cnkNFk-P8h6nrTWCzHBfKic/pubhtml#