**Смарт-контракт голосования Ростелеком 2022**

Список транзакций, которые должен обрабатывать блокчейн (контракт RTK версии voting-contract:v1.5.2) приведен в табл. 1 – 13.

Таблица 1 – Транзакция 103 "operation = initiateVoting"

| Параметр | Описание | Тип | Пример, примечание |
| --- | --- | --- | --- |
| bulletinHash | Хэш бюллетеня | string | 5ec3f6a79frgwqgrgeetqgd339d4d135f3dba |
| dimension | Размерность бюллетеня | string | [[1,1,3],[1,5,8]] |
| blindSigModulo | Модуль протокола выдачи слепой подписи | string | base64:lRTl6mS6ql16vNPY3Z... |
| blindSigExponent | Публичная экспонента протокола выдачи слепой подписи | string | base64:AQAB |
| dateStart | Дата и время начала приема бюллетеней (UTC по часам контракта) | Integer | Поле опциональное |
| servers | Список серверов, от которых могут быть обработаны транзакции c operation = "addMainKey" | updateServerList | finishVoting | decryption | commissionDecryption | results | string | ["pubkey1", "pubkey2"] |
| votersListRegistrators | Список участников уполномоченных загрузить список избирателей | string | ["pubkey1", "pubkey2"] |
| blindSigIssueRegistrator | Участник, уполномоченный отправить транзакцию blindSigIssue | string | "pubkey1" |
| pollId | Id голосования в системах РТК | string | uid |
| isRevoteBlocked | Опциональный признак, отвечающий за возможность переголосований.  isRevoteBlocked = false – переголосования разрешены,  isRevoteBlocked = true или признак отсутствует – переголосование запрещено | Boolean | True |

Список проверок для транзакции 103 "operation = initiateVoting":

1. Проверить что обязательные поля не пустые

Запись информации на ключи контракта:

1. Значения ключей bulletinHash, dimension, blindSigModulo, blindSigExponent, dateStart, isRevoteBlocked из транзакции, pollId и basePoint сохранить на ключ VOTING\_BASE (в соответствующий параметр). Если параметр isRevoteBlocked в 103 транзакции отсутствует, то установить isRevoteBlocked в значении = true
2. Список публичных ключей серверов (SERVERS) сохранить в массиве на ключе SERVERS
3. Ключ участника уполномоченного на загрузку списка избирателей (votersListRegistrator) записать на ключ VOTERS\_LIST\_REGISTRATOR
4. Ключ участника уполномоченного на отправку транзакции blindSigIssue записать на ключ BLINDSIG\_ISSUE\_REGISTRATOR
5. Ключ участника уполномоченного на отправку транзакции startIssueBallots, stopIssueBallots записать на ключ ISSUE\_BALLOTS\_REGISTRATOR
6. Ключ участника jwtTokenRegistrator записать на ключ JWTTOKEN\_REGISTRATOR

Таблица 2 – Транзакция 104 "operation = updateServerList"

|  |  |  |  |
| --- | --- | --- | --- |
| Параметр | Описание | Тип | Пример, примечание |
| servers | Список серверов, от которых могут быть обработаны транзакции c operation = "addMainKey" | updateServerList | finishVoting | decryption | commissionDecryption | results | string | ["pubkey1", "pubkey2"] |

Список проверок для транзакции 104 "operation = updateServerList":

1. Проверить, что отправитель указан в ключе SERVERS
2. Проверить, что кол-во указанных в транзакции серверов не менее 1

Запись информации на ключи контракта:

1. Перезаписать ключ SERVERS списком ключей активных серверов.

Таблица 3 – Транзакция 104 "operation = addMainKey"

| Параметр | Описание | Тип | Пример, примечание |
| --- | --- | --- | --- |
| mainKey | Ключ шифрования бюллетеней | string |  |
| commissionKey | Ключ комиссии | string |  |
| dkgKey | Ключ системы ПТК ДЭГ | string |  |

Список проверок для транзакции 104 "operation = addMainKey":

1. Проверить что отправитель указан в ключе SERVERS
2. Проверить что обязательные поля не пустые
3. Проверить что VOTING\_BASE.dateStart позже текущего времени (UTC по часам смарт-контракта) или dateStart не заполнено и VOTING\_BASE.status равно active

Запись информации на ключи контракта:

1. Сохранить значение mainKey в ключ MAIN\_KEY стейта контракта
2. Сохранить значение commissionKey в ключ COMMISSION\_KEY стейта контракта
3. Сохранить значение dkgKey в ключ DKG\_KEY стейта контракта

Таблица 4 – Транзакция 104 "operation = addVotersList"

|  |  |  |  |
| --- | --- | --- | --- |
| Параметр | Описание | Тип | Пример, примечание |
| votersCount | Количество избирателей в списке | Integer | 2 |
| userIdHashes | Массив хэшей userId избирателей | String | [\"123123123\", \"123123123\"] |
| PrimaryUikRegionCode | Идентификатор региона | string |  |
| PrimaryUikNumber | Номер избирательного участка | Integer |  |

Список проверок для транзакции 104 "operation = addVotersList":

1. Проверить, что отправитель указан в ключе VOTERS\_LIST\_REGISTRATOR
2. Проверить, что обязательные поля не пустые

Запись информации на ключи контракта:

1. Сохранить значение userIdHashes, PrimaryUikRegionCode, PrimaryUikNumber на ключ VOTERS\_LIST\_<txId>

Таблица 5 – Транзакция 104 "operation = removeFromVotersList"

|  |  |  |  |
| --- | --- | --- | --- |
| Параметр | Описание | Тип | Пример, примечание |
| userIdHashes | Массив хэшей userId избирателей | String | [\"123123123\", \"123123123\"] |
| PrimaryUikRegionCode | Идентификатор региона | string |  |
| PrimaryUikNumber | Номер избирательного участка | Integer |  |

Список проверок для транзакции 104 "operation = removeFromVotersList":

1. 1.Проверить, что отправитель указан в ключе VOTERS\_LIST\_REGISTRATOR
2. 2.Проверить, что обязательные поля не пустые

Запись информации на ключи контракта:

1. 1.Сохранить значение userIdHashes на ключ VOTERS\_LIST\_REMOVE\_<txId>

Таблица 6 – Транзакция 104 "operation = addToVotersList"

|  |  |  |  |
| --- | --- | --- | --- |
| Параметр | Описание | Тип | Пример, примечание |
| userIdHashes | Массив хэшей userId избирателей | String | [\"123123123\", \"123123123\"] |

Список проверок для транзакции 104 "operation = addToVotersList":

1. Проверить, что отправитель указан в ключе VOTERS\_LIST\_REGISTRATOR
2. Проверить, что обязательные поля не пустые

Запись информации на ключи контракта:

1. Сохранить значение userIdHashes на ключ VOTERS\_LIST\_ADD\_<txId>

Таблица 7 – Транзакция 104 "operation = startVoting"

|  |  |  |  |
| --- | --- | --- | --- |
| Параметр | Описание | Тип | Пример, примечание |
| dateStart | UTC Время запуска голосования | Integer | Поле опциональное |

Список проверок для транзакции 104 "operation = startVoting":

1. Если в транзакции указан dateStart, проверить что dateStart > now, в случае успеха:
   1. Cохранить dateStart на ключ VOTING\_BASE.dateStart
   2. Сохранить значение 1 на ключ VOTING\_BASE.ready
2. Если в транзакции НЕ указан dateStart и VOTING\_BASE.dateStart пустое:
   1. Cохранить текущее время на ключ VOTING\_BASE.dateStart
   2. Сохранить значение 1 на ключ VOTING\_BASE.ready
3. Если в транзакции НЕ указан dateStart и VOTING\_BASE.dateStart НЕ пустое:
   1. Сохранить значение 1 на ключ VOTING\_BASE.ready

Таблица 8 – Транзакция 104 "operation = blindSigIssue"

|  |  |  |  |
| --- | --- | --- | --- |
| Параметр | Описание | Тип | Пример, примечание |
| data | Факт выдачи слепой подписи | string | [{ /"userId/": /"userId1/", /"maskedSig/": /"maskedSig1/"},  { /"userId/": /"userId2/", /"maskedSig/": /"maskedSig2/"}] |
| PrimaryUikRegionCode | Идентификатор региона | string |  |
| PrimaryUikNumber | Номер избирательного участка | Integer |  |

Список проверок для транзакции 104 "operation = blindSigIssue":

1. Проверить что VOTING\_BASE.dateStart раньше текущего времени (UTC по часам смарт-контракта) и VOTING\_BASE.status равно active
2. Проверить, что отправитель указан в ключе BLINDSIG\_ISSUE\_REGISTRATOR

Запись информации на ключи контракта:

1. Для каждого значения из массива userId сохранить ключ BLINDSIG\_<txId> = [{ /"userId/": /"userId1/", /"maskedSig/": /"maskedSig1/", /"idToken/": /"idToken"/ }
2. Если смарт-контракт отклоняет транзакцию, сохранить на ключ FAIL\_<txId>\_blindSig причину отклонения транзакции. Например, для валидации подписи "signature validate by blindSigIssueRegistrator invalid"

Таблица 9 – Транзакция 104 "operation = vote"

| Параметр | Описание | Тип | Пример, примечание |
| --- | --- | --- | --- |
| vote | Зашифрованный голос | binary | Байтовое представление |
| blindSig | Слепая подпись избирателя | binary | Байтовое представление |

Список проверок для транзакции 104 "operation = vote":

1. Проверить что VOTING\_BASE.ready == 1
2. Проверить, что это не повторный голос избирателя. Т.е. ключа VOTE\_<publicKey> НЕ существует. Если ключ существует и VOTING\_BASE.isRevoteBlocked = true, то отклонить транзакцию
3. Проверить корректность слепой подписи. FDH - СТРИБОГ-256
4. Если на стейте контракта уже есть ключ VOTE\_<publicKey>, проверить что VOTE\_<publicKey>.blindSig на стейте совпадает с blindSig транзакции
5. Проверить что обязательные поля не пустые
6. Проверить что VOTING\_BASE.dateStart раньше текущего времени (UTC по часам смарт-контракта) и VOTING\_BASE.status равно active

Запись информации на ключи контракта:

1. Если все проверки успешно пройдены, сохранить на ключе VOTE\_<publicKey> объект {"vote": "txId", "blindSig": "blindSig1"}
2. Если смарт-контракт отклоняет транзакцию, сохранить на ключ FAIL\_<senderAddress>\_<txId>\_vote публичный ключ отправителя и причину отклонения транзакции

Таблица 10 – Транзакция 104 "operation = finishVoting"

|  |  |  |  |
| --- | --- | --- | --- |
| Параметр | Описание | Тип | Пример, примечание |
| Параметры транзакции отсутствуют | | | |

Список проверок для транзакции 104 "operation = finishVoting":

1. Проверить, что отправитель указан в ключе SERVERS
2. Проверить что VOTING\_BASE.status равно active

Запись информации на ключи контракта:

1. Если VOTING\_BASE.dateStart позже текущего времени (UTC по часам смарт-контракта) или пустой, установить VOTING\_BASE.status в значение halted
2. Если VOTING\_BASE.dateStart ранее текущего времени (UTC по часам смарт-контракта), установить VOTING\_BASE.status в значение completed
3. Сохранить текущее время в параметр VOTING\_BASE.dateEnd

Таблица 11 – Транзакция 104 "operation = decryption"

|  |  |  |  |
| --- | --- | --- | --- |
| Параметр | Описание | Тип | Пример, примечание |
| decryptions | Результат частичной расшифровки ключом ЦИК России | binary | Байтовое представление |

Список проверок для транзакции 104 "operation = decryption":

1. Проверить, что отправитель указан в ключе SERVERS
2. Проверить что обязательные поля не пустые
3. Проверить что VOTING\_BASE.status равно completed

Запись информации на ключи контракта:

1. Если все проверки успешно пройдены, сохранить id транзакции на ключ DECRYPTION\_<publicKey>

Таблица 12 – Транзакция 104 "operation = commissionDecryption"

|  |  |  |  |
| --- | --- | --- | --- |
| Параметр | Описание | Тип | Пример, примечание |
| decryptions | Результат расшифровки ключом комиссии | binary | Байтовое представление |

Список проверок для транзакции 104 "operation = commissionDecryption":

1. Проверить, что отправитель указан в ключе SERVERS
2. Проверить что обязательные поля не пустые
3. Проверить что VOTING\_BASE.status равно completed
4. Если приватный ключ commisionSecretKey присутствует, то проверить его на публичном ключе записанном на ключе COMMISION\_KEY контракта

Запись информации на ключи контракта:

1. Если все проверки успешно пройдены, сохранить id транзакции на ключ COMMISION\_DECRYPTION
2. Если смарт-контракт отклоняет транзакцию, сохранить на ключ FAIL\_<txId>\_commisionDecryption причину отклонения транзакции

Таблица 13 – Транзакция 104 "operation = results"

|  |  |  |  |
| --- | --- | --- | --- |
| Параметр | Описание | Тип | Пример, примечание |
| results | Итоги голосования в расшифрованном виде | string | [[25,23,11,11,6,3,1,0]] |

Список проверок для транзакции 104 "operation = results":

1. Проверить, что отправитель указан в ключе SERVERS
2. Проверить что обязательные поля не пустые
3. Проверить что VOTING\_BASE.status равно completed

Запись информации на ключи контракта:

1. Сохранить значение results в ключ RESULTS стейта контракта