**说明**

**改动内容**：

1. 冷热钱包创建和登录钱包跳转页面不同，需要进行判断。
2. 导航大栏进行改动，冷热钱包的逻辑进行了分离。总共分成六部分，Account/Vote/Tokens/是热钱包的功能，里边转账投票等功能都是热钱包对应的地址完成的；Offline transaction和Watching wallet是冷热钱包交互的部分；Cold wallet是冷钱包部分的功能。用户进入程序后系统自动判断联网状态，联网五项可用，未联网则只能使用冷钱包功能。
3. 冷热钱包默认都是一个地址，暂时不添加多地址功能。
4. 第4项、第6项功能进行了简化，只走热钱包流程；新增加离线交易、监视钱包、冷钱包功能需要重新梳理流程。
5. 投票和转账均需要冷钱包授权，具体过程参考教程—如何使用冷钱包签名交易和授权投票
6. 余额列表页面增加了冻结功能，冻结仅限于TRX，冻结TRX带来两个效果：获得股权和带宽，股权是投票使用，带宽用来进行转账（包括TRX和其他Token）、投票、冻结、发行通证和参与通证发行。发生解冻操作时，以前的投票会失效，可以通过重新冻结并投票来避免失效。解冻后带宽不会清空，下次冻结时，新冻结部分带宽将进行累加。
7. 新增加了带宽功能，执行上述提到的各项操作均需要消耗带宽，每次执行消耗10^5个带宽。带宽计算规则如下：冻结资金\*冻结天数\*常数=带宽，例如冻结2个TRX（1TRX=10^6drop）,时间为3天，带宽=10^6\*3\*2=6\*10^6，如果距离上次执行操作超过一定时间（10s），则本次操作不需要消耗带宽。距离上次合约（投票、转账、转移资产和冻结）超过10s则不需要消耗带宽。
8. 查询带宽接口在查询余额列表页面。
9. 查询冻结金额（股权）接口在查询列表页面，冻结可以分多次完成，需要将每次冻结操作的金额加和得到总冻结金额。当临时需要更多的股权或带宽时，可以追加冻结资金，从而获取追加部分的股权与带宽。此时解冻时间推迟到最后一次冻结操作的3天后。

**钱包需求windows**

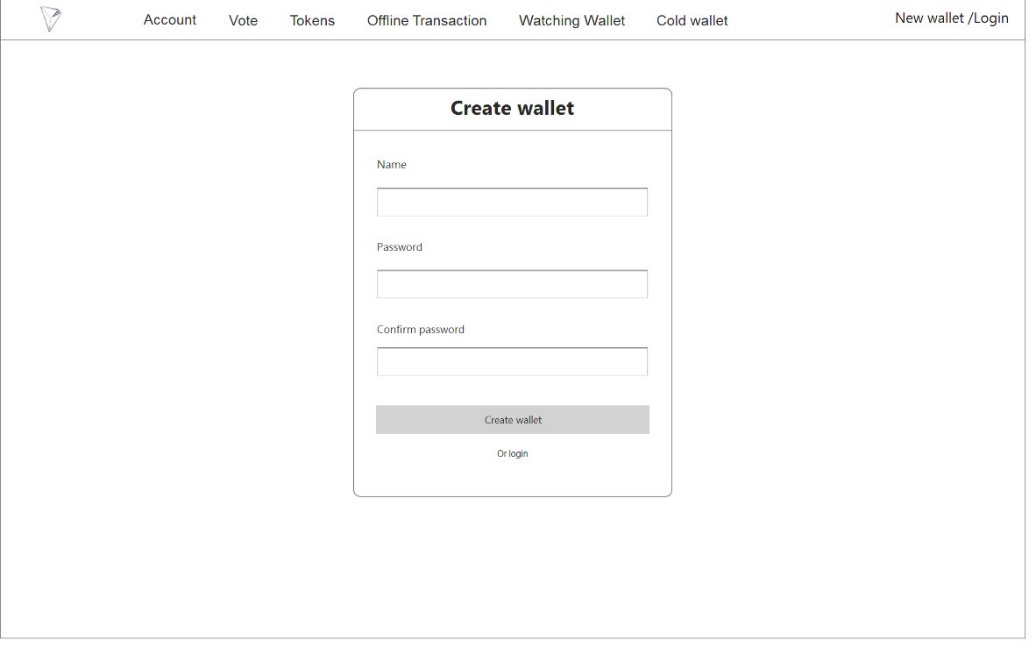
开发一个英文版本的windows钱包，包括冷钱包和热钱包两部分，冷钱包负责存储私钥和签名授权，热钱包负责发起和广播交易。具体功能如下：

热钱包部分：

# 创建/登录钱包

1. **创建钱包**

用户设置钱包名称和密码，用户确认一遍密码，并将密码记录保存。需要用户记录密码，暂不提供密码找回功能。

跳转成功直接登录然后跳转到投票页面(8-1)。****

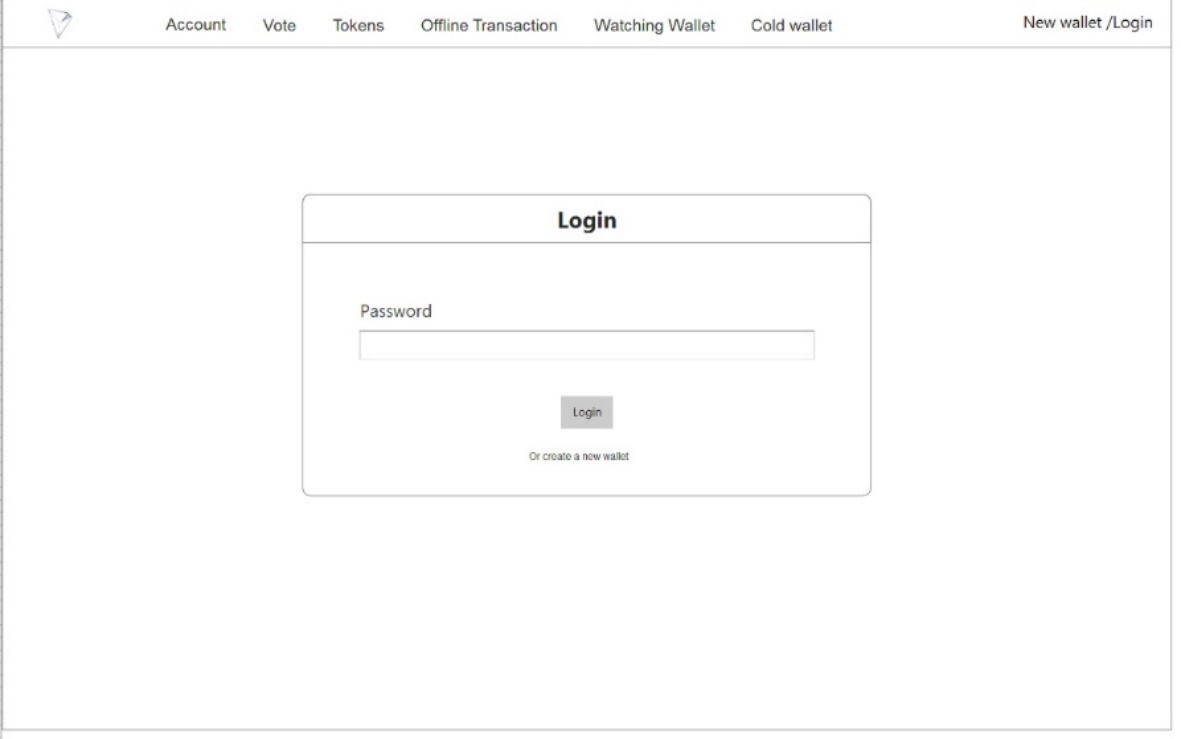
页面1-1

采用以太坊的keystore机制：本地存储ECDSA的公钥密钥信息，以本地文件的形式提供对账户信息和数字签名公钥私钥的存储和读取。

**密码参考链接：**[**https://blog.csdn.net/teaspring/article/details/78350888**](https://blog.csdn.net/teaspring/article/details/78350888)

**不需要调用接口**

1. **登录**

输入密码登录，钱包的所有功能需要登录才能使用，登录成功跳转到投票页面（8-1）****

页面2-1

**不需要调用接口**

1. **注销**

点击注销回到登录页面(2-1)。

**调用接口--获取账户信息**

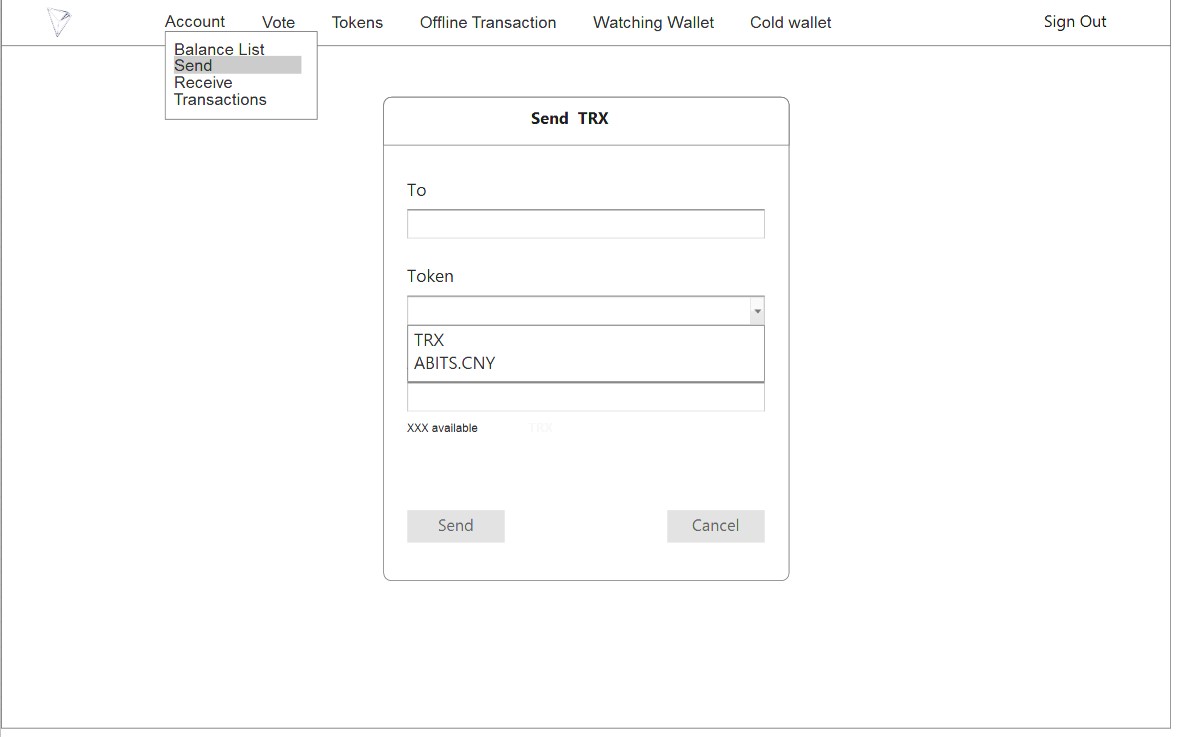
|  |  |
| --- | --- |
| 接口声明 | rpc GetAccount (Account) returns (Account) {}; |
| 提供节点 | fullnode、soliditynode |
| 参数说明 | Account：只需要输入address即可 |
| 返回值 | Account：返回账户所有的详细信息 |
| 功能说明 | 查询余额列表。从返回的Account中可以展示所有的资产信息 |

# 账户

导航栏包括四部分，账户余额，转账，收款，交易记录。转账只是热钱包转账。

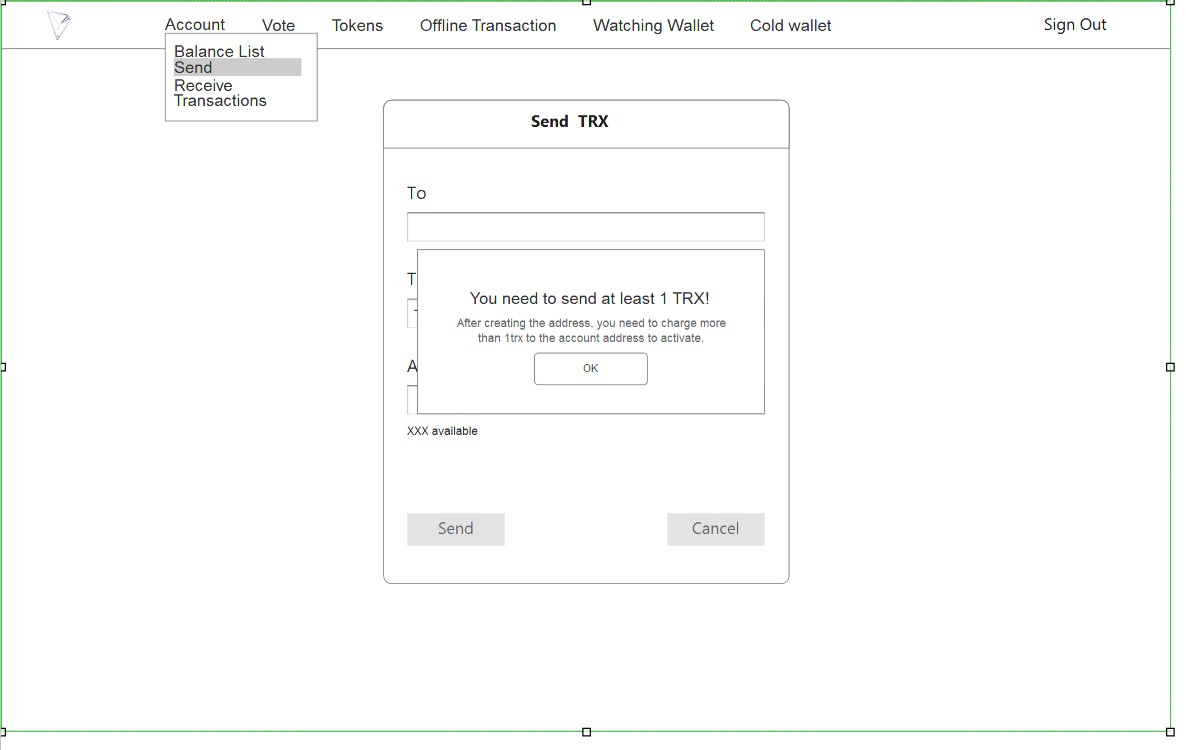
1. **转账**

点击Send按钮转账，转账需要输入目标账户的地址，转账的币种（TRX或者其他Token）和数目。可以提示用户最大的转账额度（xxx is available），也就是当前币种的余额。转账需要消耗带宽，执行一次转账操作需要消耗10^5个带宽，转账完成跳转至余额列表页面（6-1）。



页面4-1

用户在创建地址后，需要向该地址转账1TRX以上，地址才会激活。转账小于1TRX出现提示框提示页面（4-2）,判断账户是否激活需要调用查询账户信息接口（接口在余额列表页），如果返回的信息中有创建时间，则为已经存在，不限制转账额度；反之不存在，限制转账额度。此举是为了限制无效的创建账户。



页面4-2

**调用接口--转让波场币**

|  |  |
| --- | --- |
| 接口声明 | rpc CreateTransaction (TransferContract) returns (Transaction)　{}; |
| 提供节点 | fullnode。 |
| 参数说明 | TransferContract：包含提供方地址、接收方地址、金额，其中金额的单位为drop。 |
| 返回值 | Transaction：返回包含转账合约的交易，钱包签名后再请求广播交易。 |
| 功能说明 | 转账。创建一个转账的交易。 |

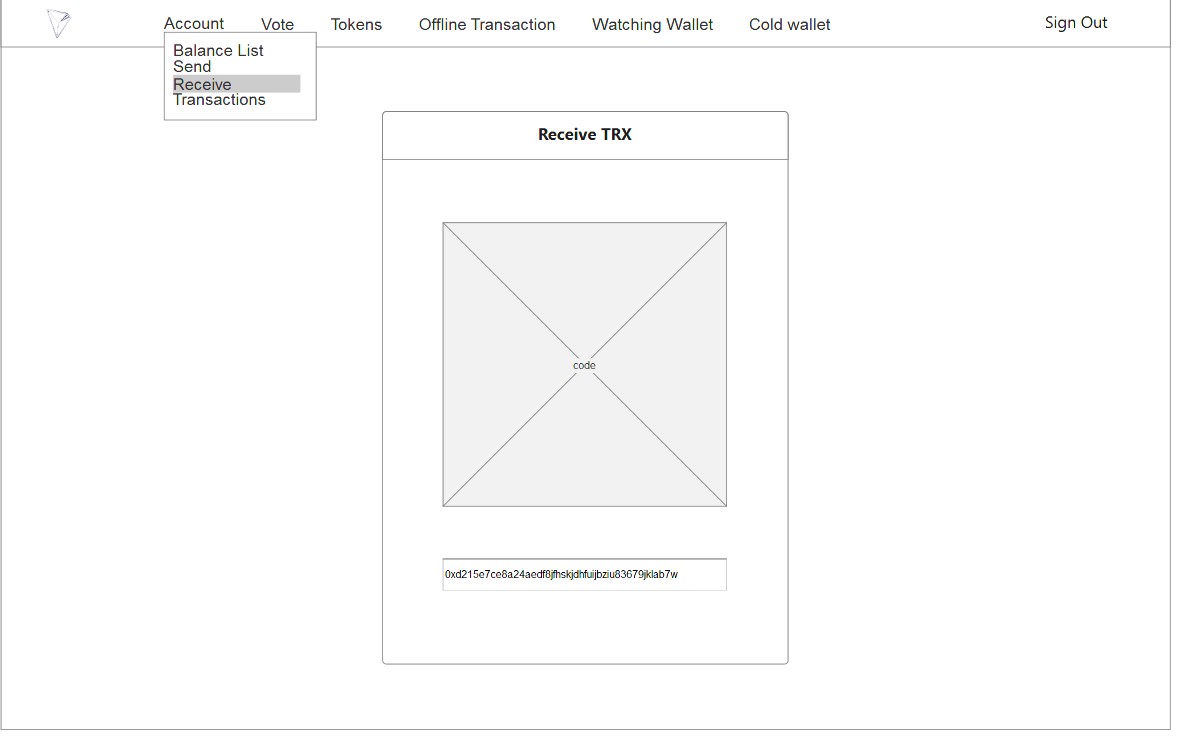
**调用接口--转让其他token**

|  |  |
| --- | --- |
| 接口声明 | rpcTransferAsset (TransferAssetContract) returns (Transaction){}; |
| 提供节点 | Fullnode。 |
| 参数说明 | TransferAssetContract：包含通证名称、提供方地址、接收方地址、通证数量。 |
| 返回值 | Transaction：返回包含转让通证的交易，钱包签名后再请求广播交易。 |
| 功能说明 | 转让通证。创建一个转让通证的交易。 |

**调用接口--广播交易**

|  |  |
| --- | --- |
| 接口声明 | rpcBroadcastTransaction (Transaction) returns (Return) {}; |
| 提供节点 | fullnode |
| 参数说明 | Transaction：已经由钱包签名的交易。波场中需要改变区块链状态的操作都封装在交易中 |
| 返回值 | 成功或失败。广播交易前会预执行交易，返回其结果。注意：返回成功不一定保证交易成功。 |
| 功能说明 | 转账、投票、发行通证、参与通证发行等。将已签名的交易信息，发送到节点，由节点验证后广播到网络中。 |

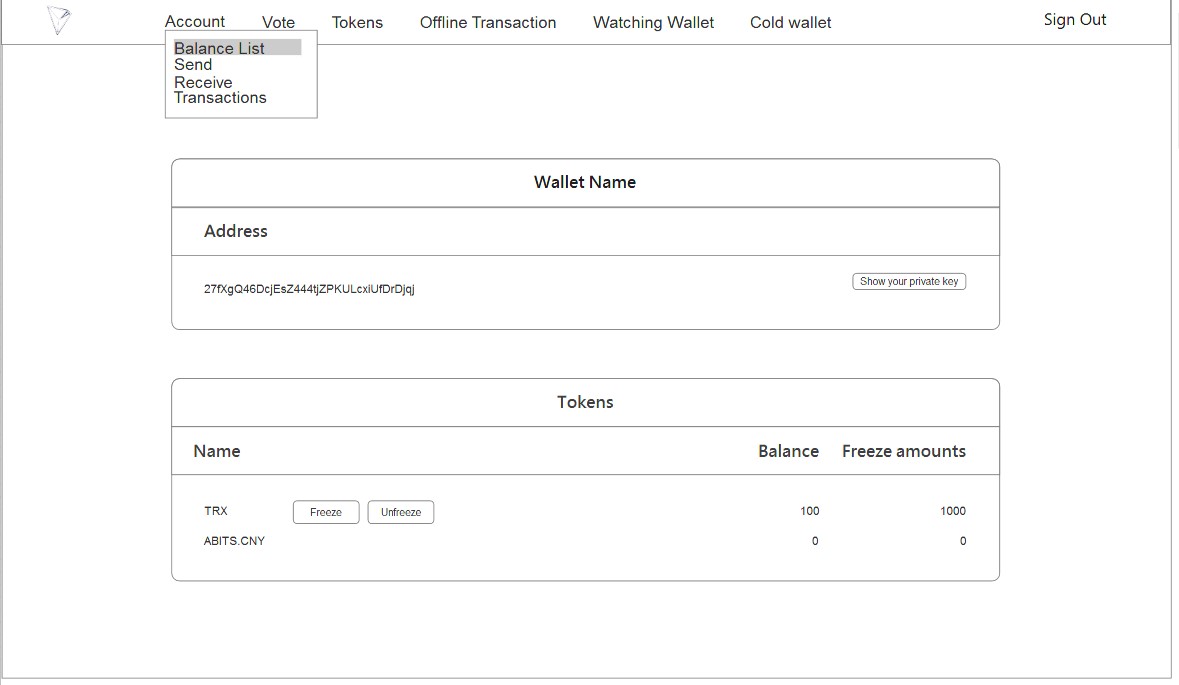
1. **收款**

显示收款的二维码地址。

页面5-1

**地址是本地算出来的，不需要调用接口。**

1. **查询余额列表**

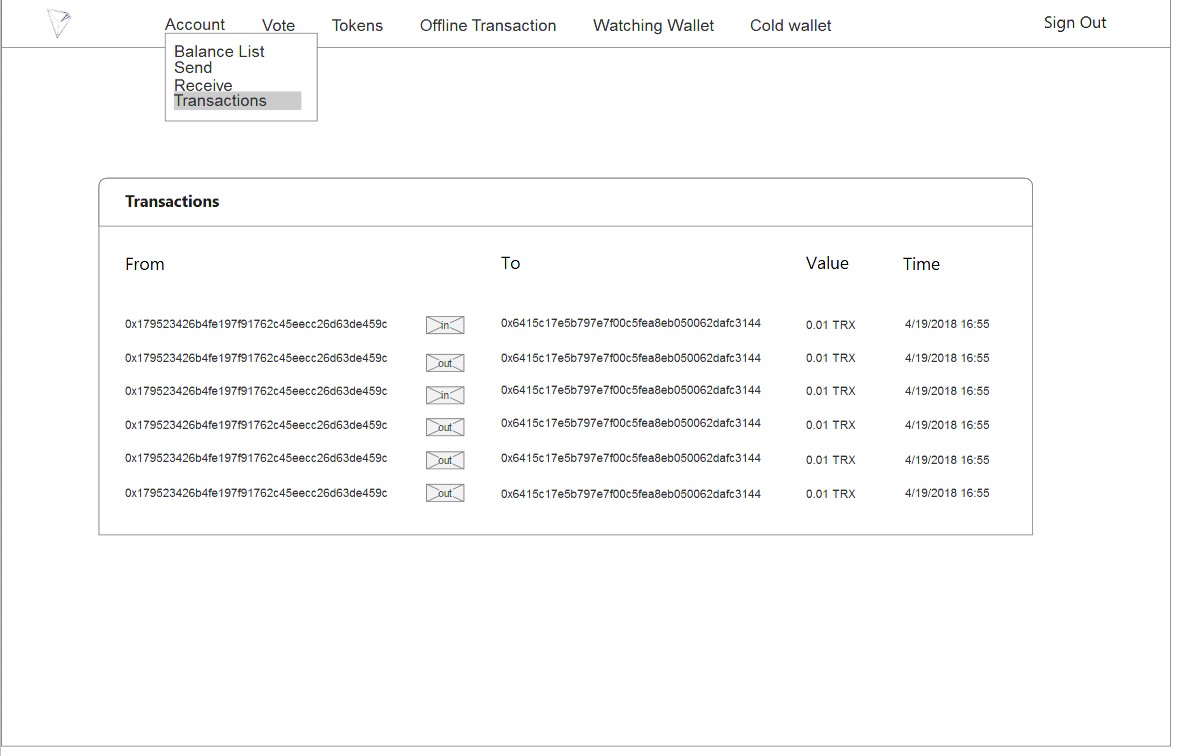
余额列表页面显示地址和该地址对应的TRX余额和其他token的列表，包括币种和数目以及冻结的金额。点击Show your private key可以显示地址对应的私钥。 

页面6-1

**调用接口--获取账户信息**

|  |  |
| --- | --- |
| 接口声明 | rpcGetAccount (Account) returns (Account) {}; |
| 提供节点 | fullnode、soliditynode。 |
| 参数说明 | Account：只需要输入address即可。 |
| 返回值 | Account：返回账户所有的详细信息。 |
| 功能说明 | 查询余额列表。从返回的Account中可以展示所有的资产信息。 |

**7.查询钱包交易记录**

交易记录展示转账的地址，收款的地址和TRX金额，如果转账的是Token，需要展示Token的单位和数量。in和out表示是进账还是出账。

页面7-1

**调用接口--通过地址查询所有发起交易**

|  |  |
| --- | --- |
| 接口声明 | rpcgetTransactionsFromThis (Account) returns (TransactionList) {}; |
| 提供节点 | soliditynode。 |
| 参数说明 | Account：发起方账户，只需要地址。 |
| 返回值 | TransactionList：交易列表。 |
| 功能说明 | 通过账户地址查询所有发起的交易。 |

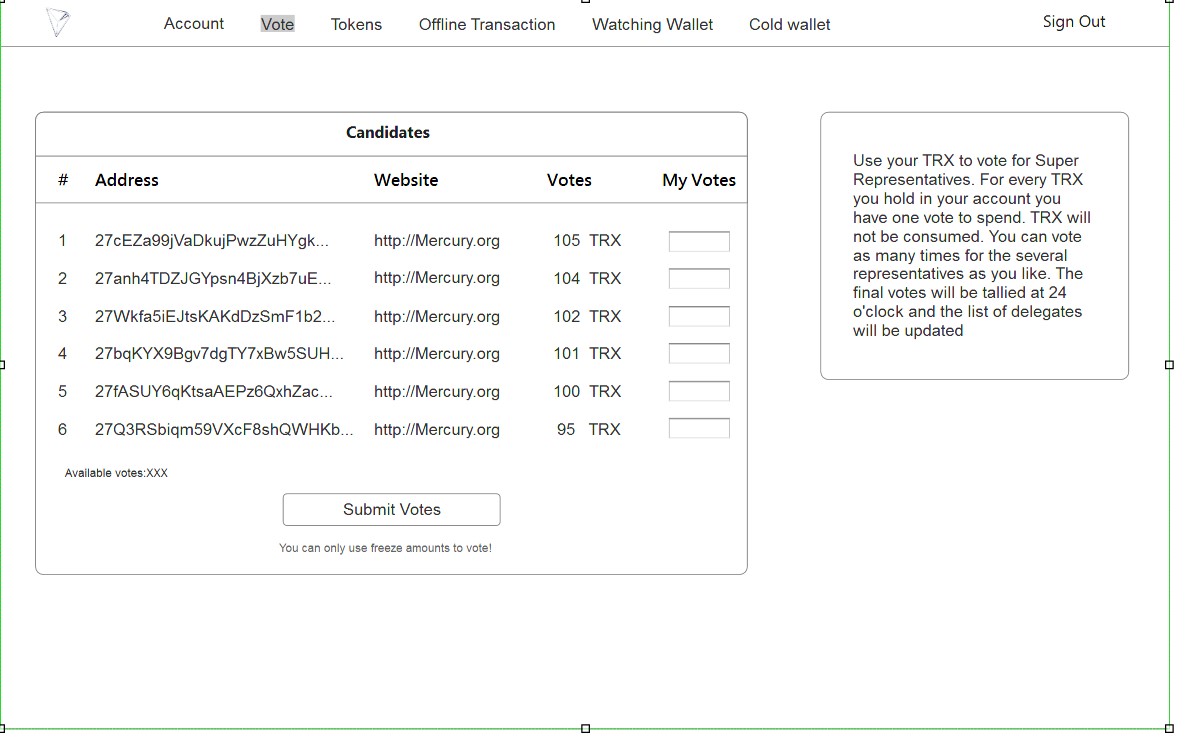
**调用接口--通过地址查询所有接收交易**

|  |  |
| --- | --- |
| 接口声明 | rpcgetTransactionsToThis (Account) returns (NumberMessage) {}; |
| 提供节点 | soliditynode。 |
| 参数说明 | Account：接收方账户，只需要地址。 |
| 返回值 | TransactionList：交易列表。 |
| 功能说明 | 通过账户地址查询所有其它账户发起和本账户有关的交易。 |

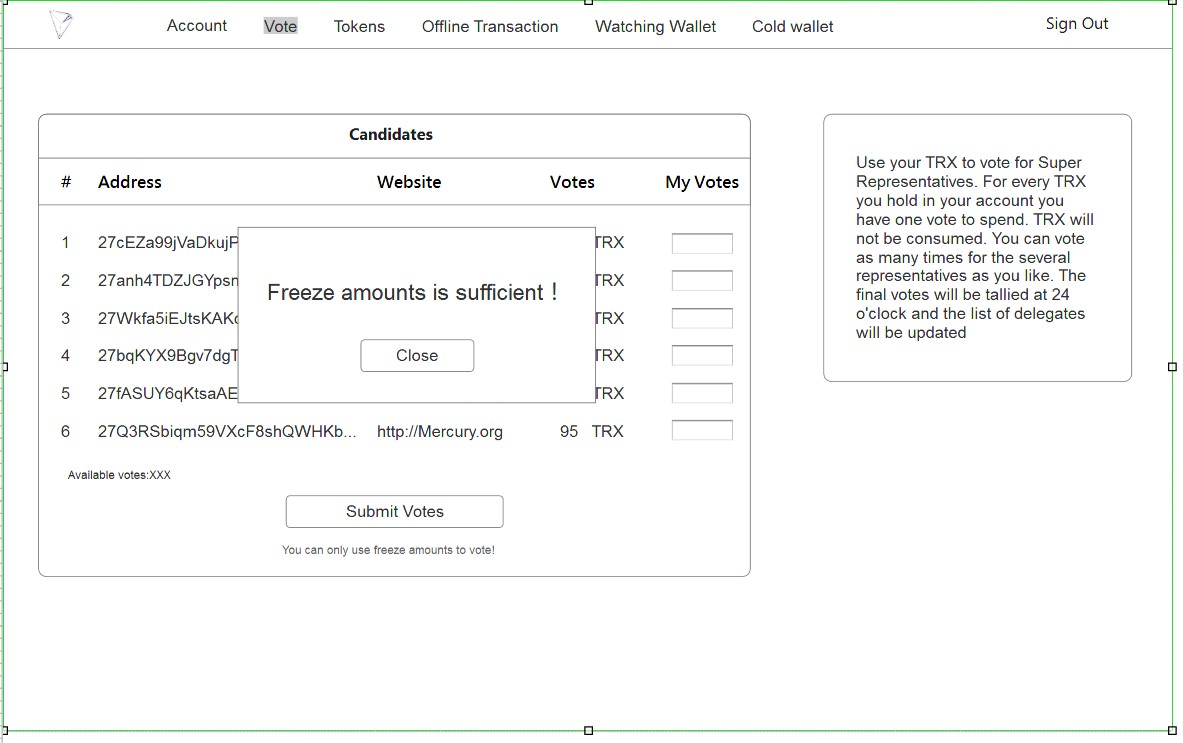
# 投票

1. **投票功能**

输入投票数量就可以投票，投票需要冻结资金，每冻结1TRX可以获得1 票。在解冻后，以前的投票会失效，可以通过重新冻结并投票来避免失效。投票数不超过总股权即可投票成功（接口在查询余额列表页面），对单个代表的投票数没有限制，投票成功消耗10^5带宽，若冻结金额不足跳转提示账户冻结金额不足（11-2）。只记录最后一次投票，（最后一次投票会覆盖之前的所有投票），投票页面实时显示用户的可用票数（available votes）。点击Vote投票成功，停留在投票页面。点击OK按钮停留在投票页面（8-1）。股权不足按钮置灰，点击会出现提示框。（8-2）

****

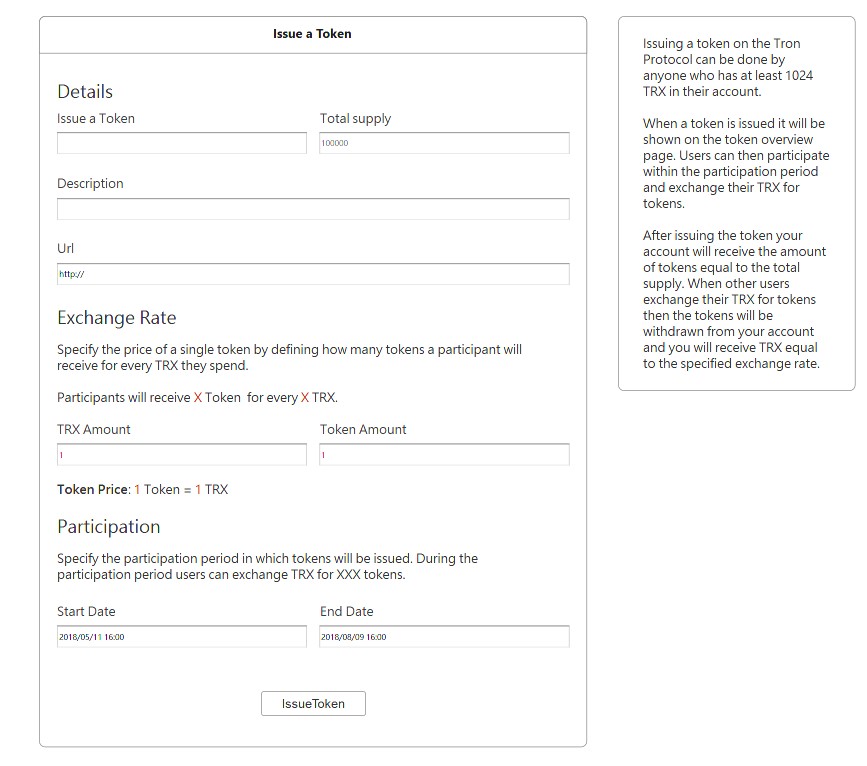
页面 8-1



页面 8-2

# 通证

1. **发行通证**

发行通证每次会消耗1024个TRX，可以发行代币。需要填入代币名称，发行数目，代币描述，网页介绍，以及和TRX兑换比例。操作需要消耗10^5带宽，距离上次合约（投票、转账、转移资产和冻结）超过10s则不需要消耗带宽。通证发行成功后跳转到全部通证列表页（10-1）。

页面9-1

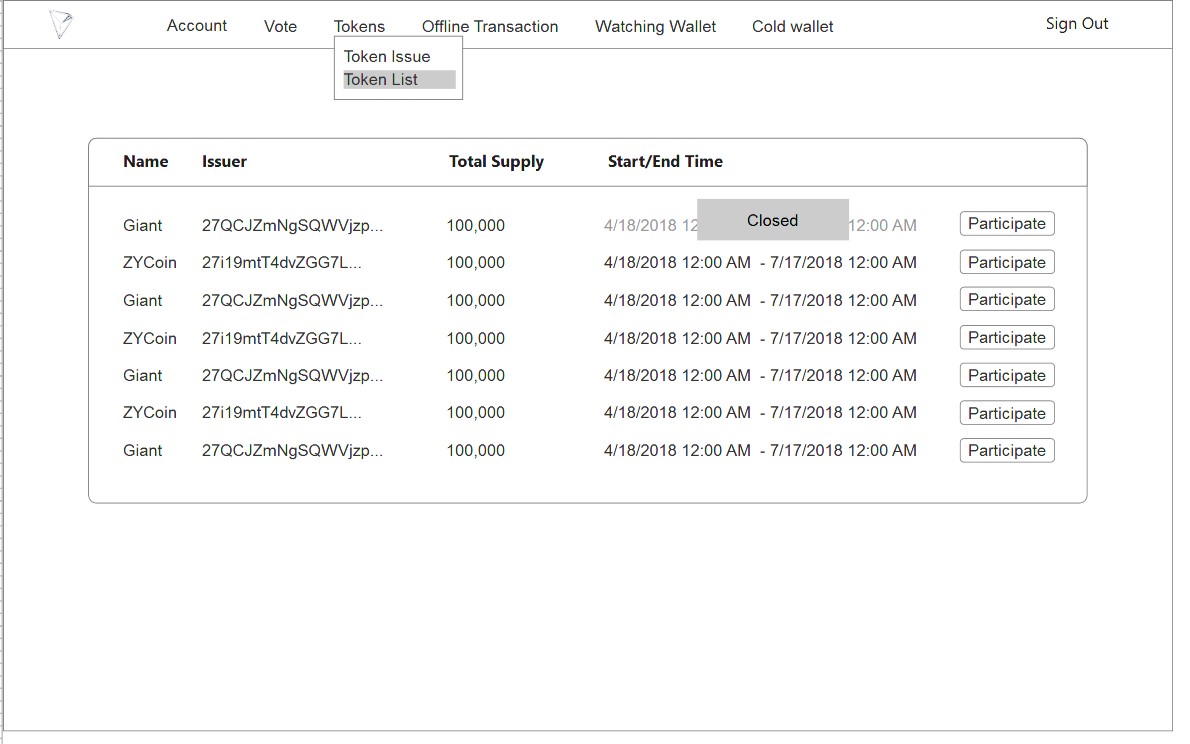
**调用接口--通证发行**

|  |  |
| --- | --- |
| 接口声明 | rpc CreateAssetIssue (AssetIssueContract) returns (Transaction) {}; |
| 提供节点 | fullnode。 |
| 参数说明 | AssetIssueContract：包含发行人地址、通证名称、总发行量、波场币vs通证汇兑比例、开始时间、结束  时间、衰减率、投票分数、详细描述、url等。 |
| 返回值 | Transaction：返回通证发行的交易，钱包签名后再请求广播交易。 |
| 功能说明 | 发行通证。所有人都可以发行通证，发行通证会消耗1024个trx。发行通证后，在有效期内任何人都可以参与通证发行，用trx按照比例兑换通证。 |

**调用接口--广播交易**Transaction

|  |  |
| --- | --- |
| 接口声明 | rpcBroadcastTransaction (Transaction) returns (Return) {}; |
| 提供节点 | fullnode。 |
| 参数说明 | Transaction：已经由钱包签名的交易。波场中需要改变区块链状态的操作都封装在交易中。 |
| 返回值 | Return：成功或失败。广播交易前会预执行交易，返回其结果。注意：返回成功不一定保证交易成功。 |
| 功能说明 | 转账、投票、发行通证、参与通证发行等。将已签名的交易信息，发送到节点，由节点验证后广播到网络中。 |

1. **全部通证列表**

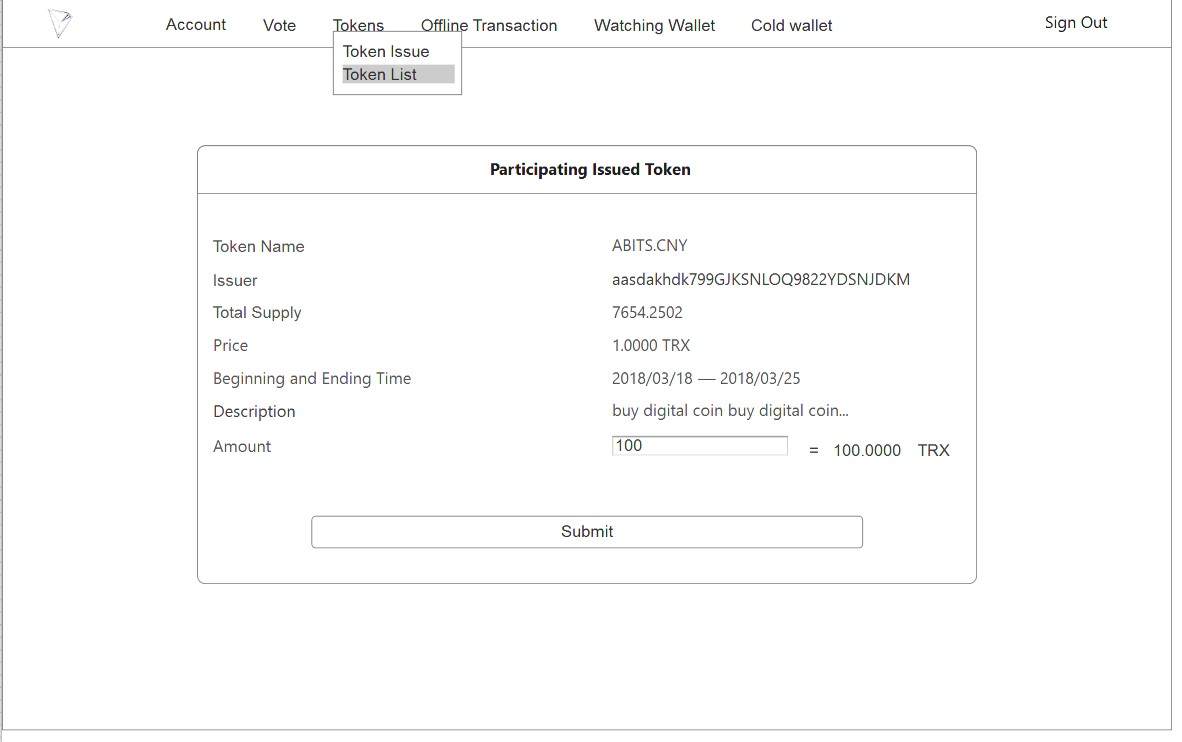
展示全部通证的列表，包括名字，发行商地址，总供应量，开始结束时间（如果发行截止，会显示已经截止），剩余量，用户可以点击参与来参与资产发行。点击参与跳转到参与通证发行页面（10-1）。

页面10-1

**调用接口--查询所有通证列表**

|  |  |
| --- | --- |
| 接口声明 | rpcGetAssetIssueList (EmptyMessage) returns (AssetIssueList) {}; |
| 提供节点 | fullnode、soliditynode。 |
| 参数说明 | EmptyMessage：空 |
| 返回值 | AssetIssueList： AssetIssueContract的列表。所有已发行通证详细信息。 |
| 功能说明 | 全部通证列表。展示所有通证，供用户选择参与。 |

1. **参与通证发行**

点击通证列表页中的某一个通证可以参与通证发行，需要输入参与通证的数目，会扣除相应数量的TRX换成通证。操作消耗10^5个带宽，距离上次合约（投票、转账、转移资产和冻结）超过10s则不需要消耗带宽。参与通证发行成功会跳转到余额列表（6-1）。

页面11-1

**调用接口--参与通证发行**

|  |  |
| --- | --- |
| 接口声明 | rpcParticipateAssetIssue (ParticipateAssetIssueContract) returns (Transaction){}; |
| 提供节点 | fullnode。 |
| 参数说明 | ParticipateAssetIssueContract：包含参与方地址、发行方地址、通证名称、参与金额，其中金额的单位为drop。 |
| 返回值 | Return：成功或失败。广播交易前会预执行交易，返回其结果。注意：返回成功不一定保证交易成功。 |
| 功能说明 | 参与通证发行。 |

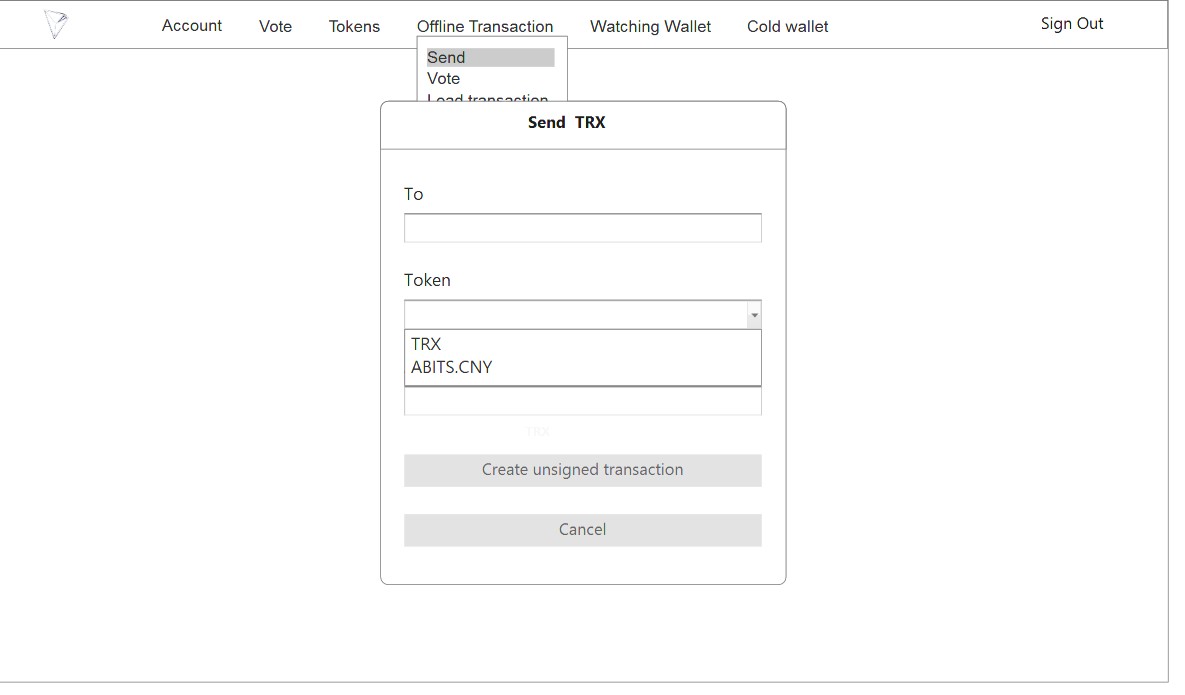
**调用接口--广播交易**

|  |  |
| --- | --- |
| 接口声明 | rpcBroadcastTransaction (Transaction) returns (Return) {}; |
| 提供节点 | fullnode。 |
| 参数说明 | Transaction：已经由钱包签名的交易。波场中需要改变区块链状态的操作都封装在交易中。 |
| 返回值 | Return：成功或失败。广播交易前会预执行交易，返回其结果。注意：返回成功不一定保证交易成功。 |
| 功能说明 | 转账、投票、发行通证、参与通证发行等。将已签名的交易信息，发送到节点，由节点验证后广播到网络中。 |

# 离线交易

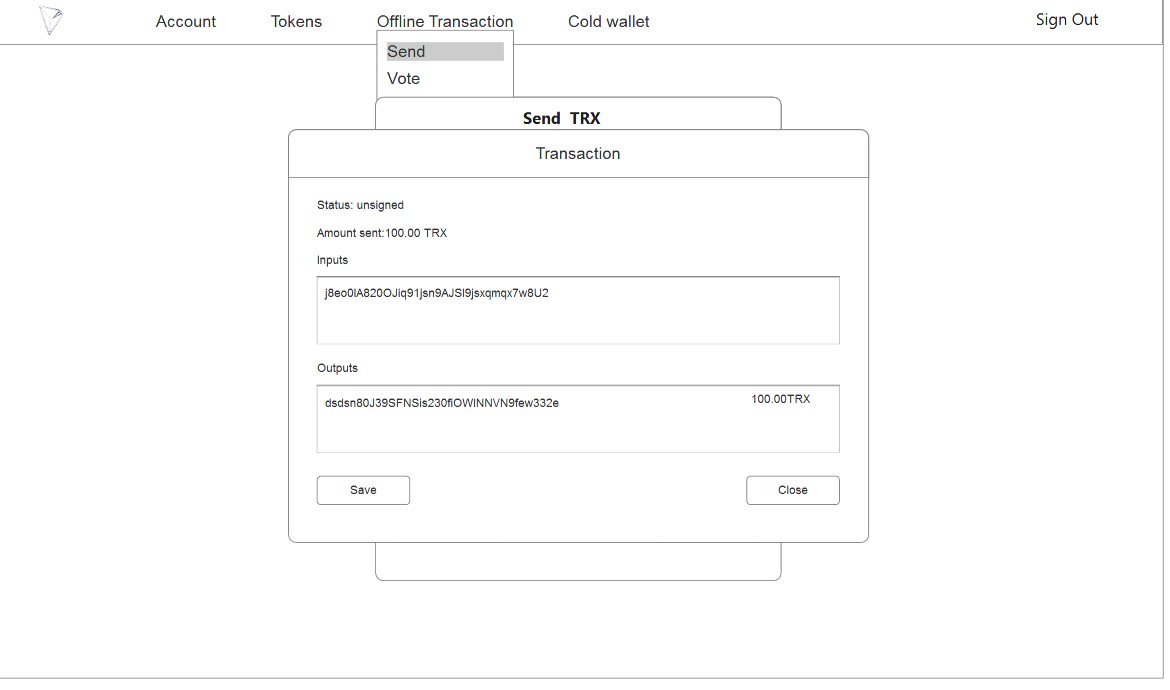
1. **发送**

发送需要输入目标账户的地址，转账的币种（TRX或者其他Token）和数目，点击“Create unsigned transaction”跳转至页面（12-2）。



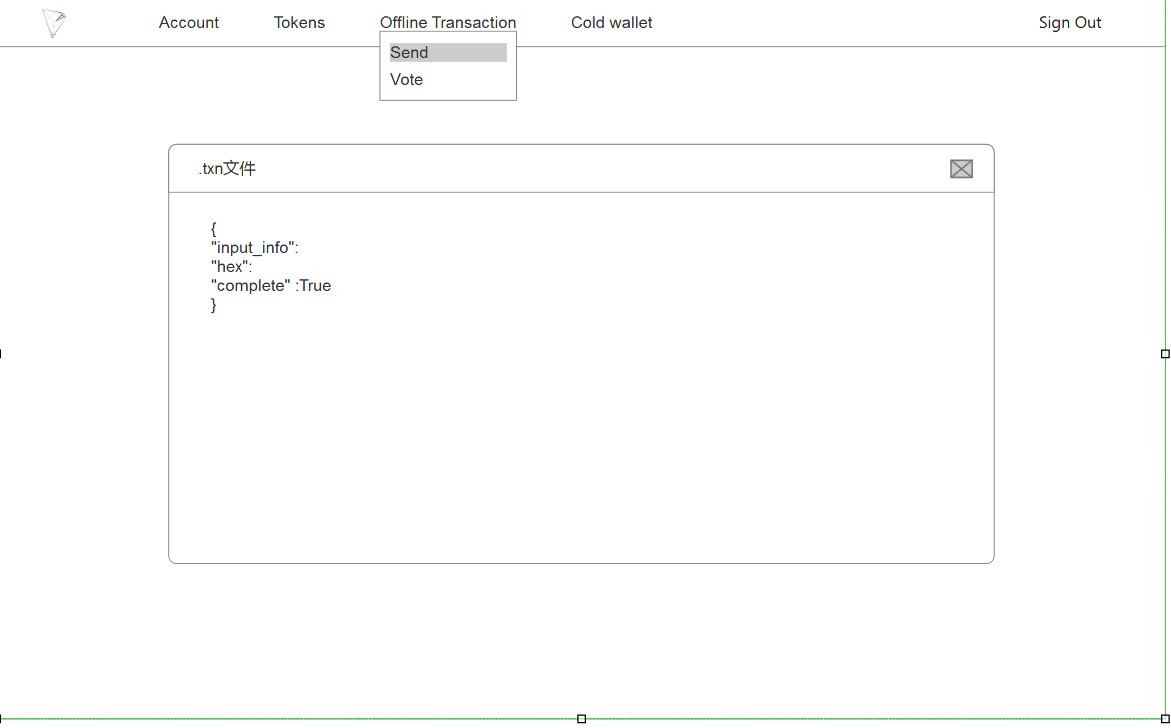
页面12-1

生成未签名交易，点击Save保存成 .txn文件（12-3）。



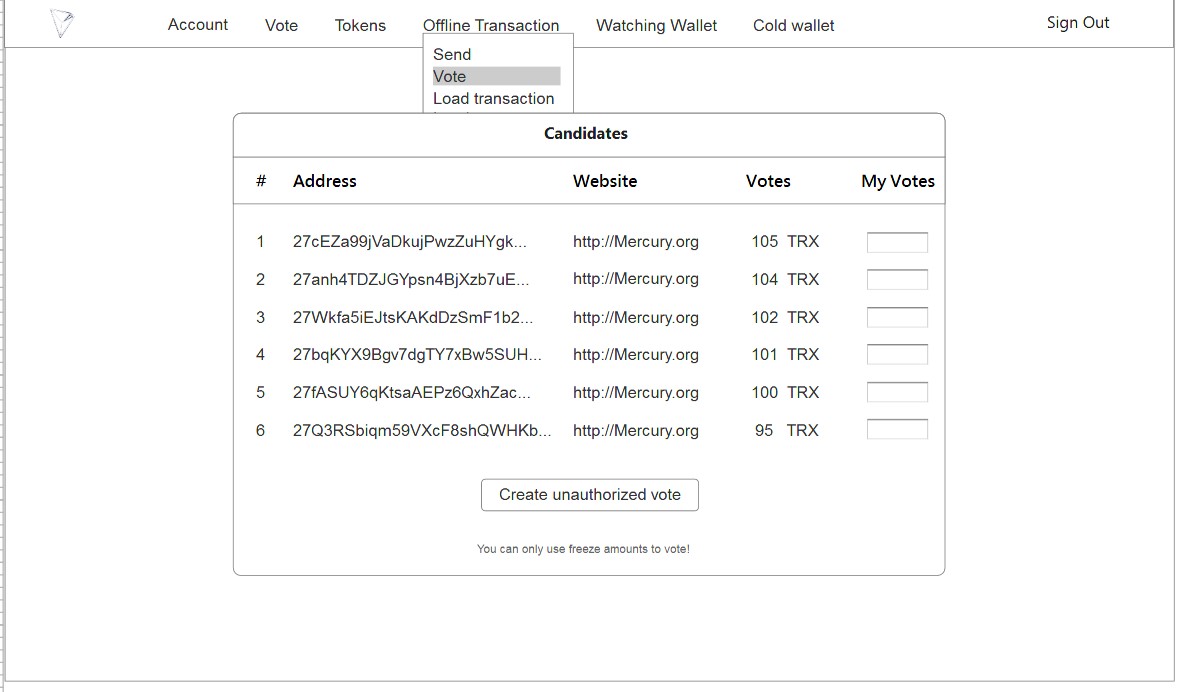
页面12-2

将此文件拷入冷钱包中。



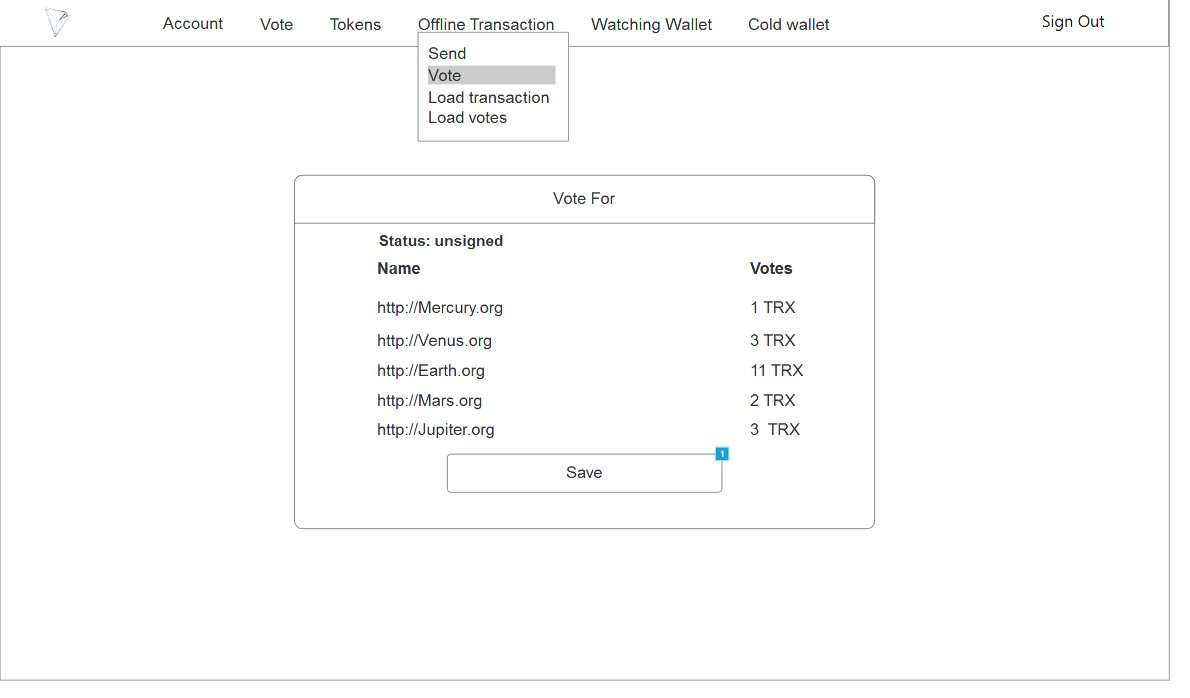
页面12-3

1. **投票**

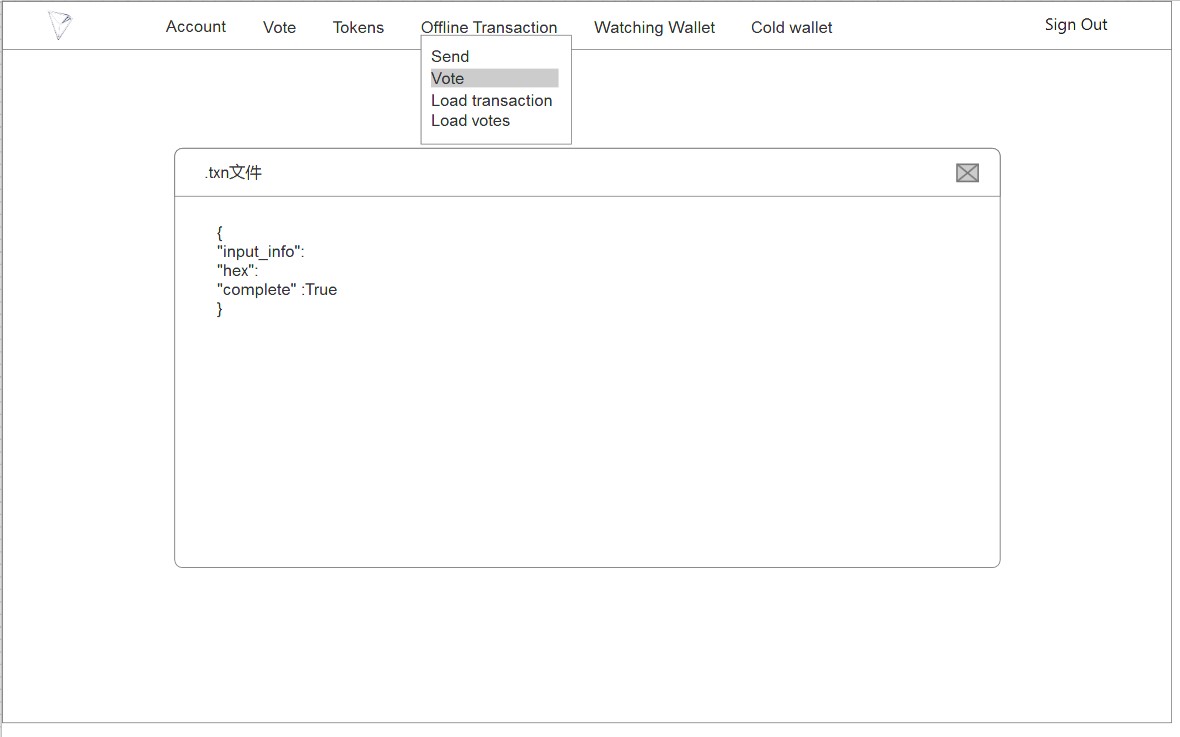
输入投票数量就可以投票，点击Create unsigned vote创建未授权投票，跳转至页面(13-2)

页面 13-1

点击Save生成.txn文件，页面（13-3）。



页面13-2



页面13-3

**调用接口--获取账户信息**

|  |  |
| --- | --- |
| 接口声明 | rpc GetAccount (Account) returns (Account) {}; |
| 提供节点 | fullnode、soliditynode |
| 参数说明 | Account：只需要输入address即可 |
| 返回值 | Account：返回账户所有的详细信息 |
| 功能说明 | 查询余额列表。从返回的Account中可以展示所有的资产信息 |

**调用接口--投票**

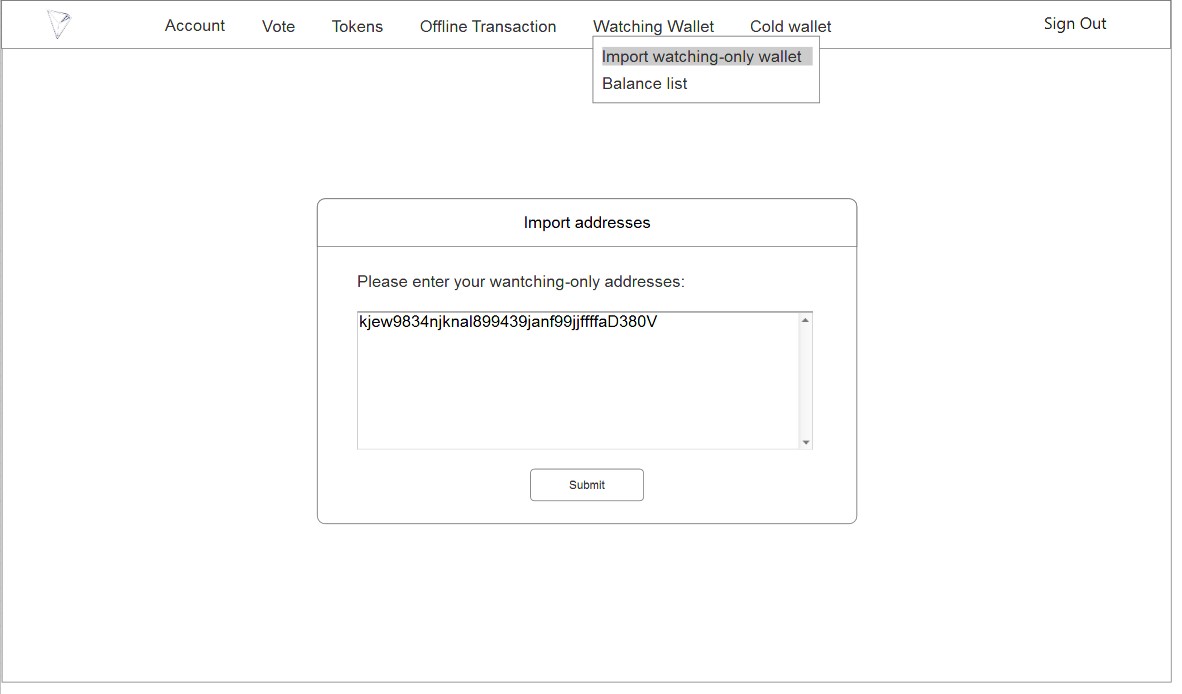
|  |  |
| --- | --- |
| 接口声明 | rpcVoteWitnessAccount (VoteWitnessContract) returns (Transaction){}; |
| 提供节点 | fullnode。 |
| 参数说明 | VoteWitnessContract：包含投票人地址和一个投票对象列表，包含候选人地址和投票数。 |
| 返回值 | Transaction：返回包含投票的交易，钱包签名后再请求广播交易。 |
| 功能说明 | 投票功能。只能对超级代表候选人进行投票，投票总数量不能大于投票人拥有的波场币数量。  给“超级代表候选人”投票，填写好投票数目，点击“提交投票”。 |
| 规则 | a.用户的最高投票数必须少于或者等于手持TRX的数量。  b.每个用户可多次投票给多个候选人。  c.每6小时更新超级代表列表。  d.投票操作均不消耗TRX。 |

**调用接口--广播交易**

|  |  |
| --- | --- |
| 接口声明 | rpcBroadcastTransaction (Transaction) returns (Return) {}; |
| 提供节点 | fullnode。 |
| 参数说明 | Transaction：已经由钱包签名的交易。波场中需要改变区块链状态的操作都封装在交易中。 |
| 返回值 | Return：成功或失败。广播交易前会预执行交易，返回其结果。注意：返回成功不一定保证交易成功。 |
| 功能说明 | 转账、投票、发行通证、参与通证发行等。将已签名的交易信息，发送到节点，由节点验证后广播到网络中。 |

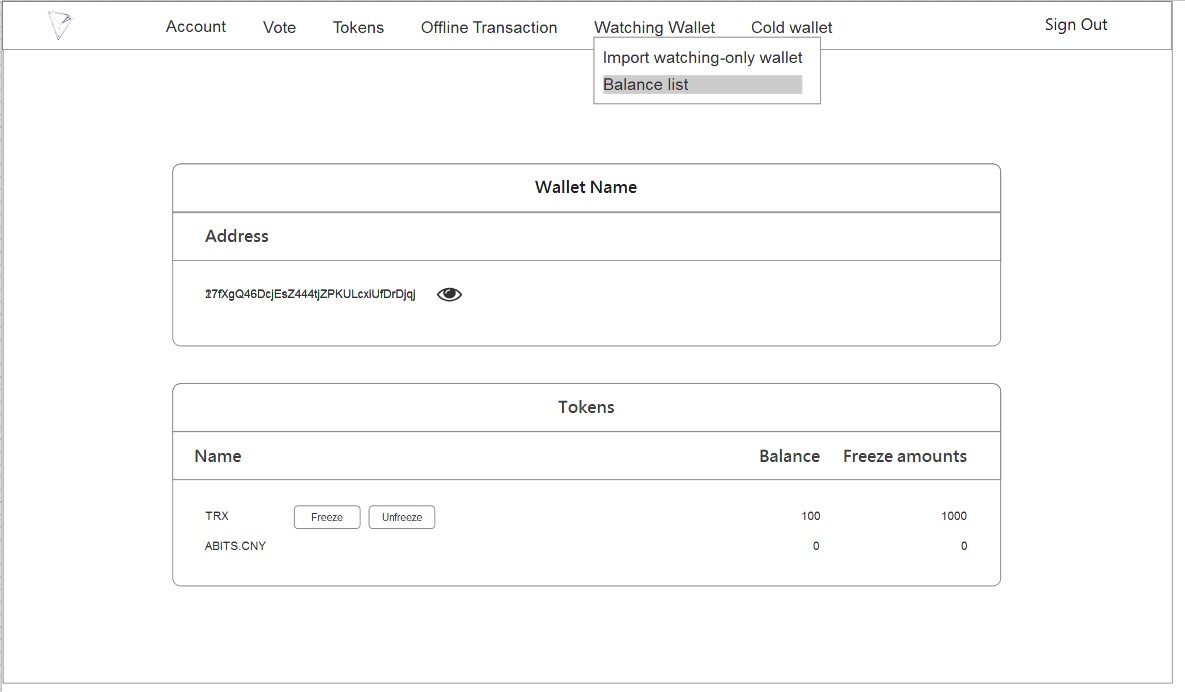
# 监视钱包

1. **导入监视钱包**

将只看钱包的地址输入进添加框中，默认添加一个地址，点击Submit成功添加地址跳转至余额列表界面（15-1）****

页面 14-1

1. **余额列表**

余额列表界面展示只看地址和对应的Token信息，包括Token的种类、数目。****

页面 15-1

# 创建/登录钱包

1. **创建钱包**

注册完直接登录然后跳转到地址页面（18-1）

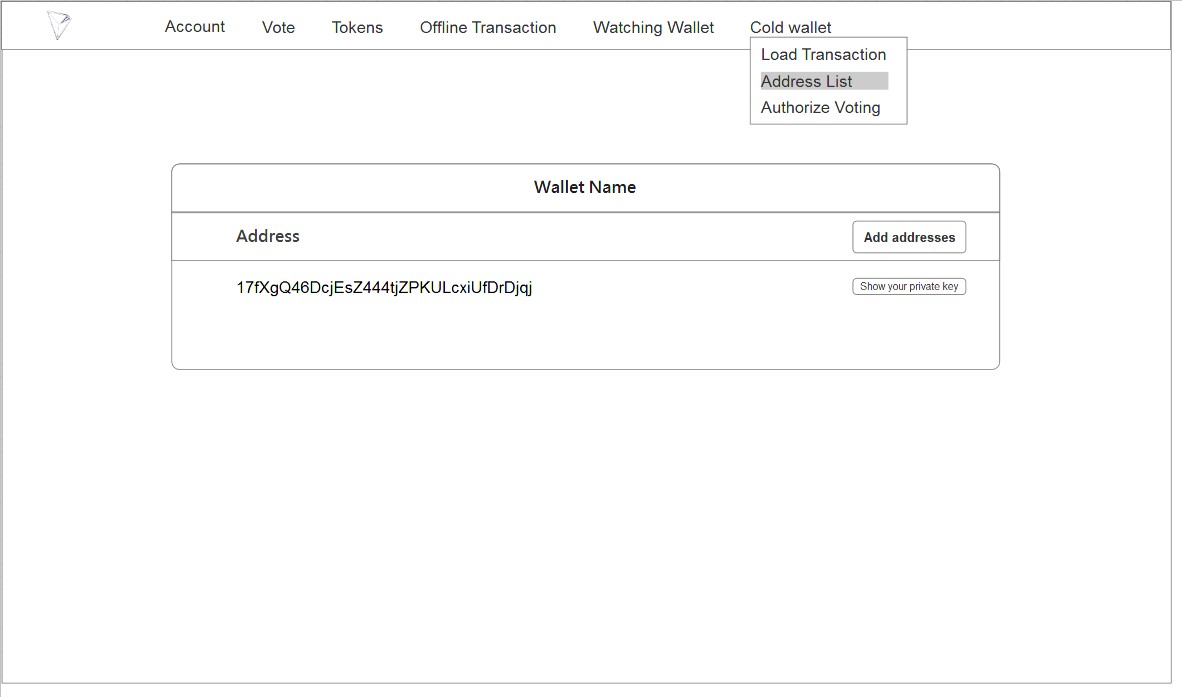
1. **登录**

输入密码登录，钱包的所有功能需要登录才能使用，登录成功跳转到地址页面（18-1）

# 账户

1. **查询地址列表**

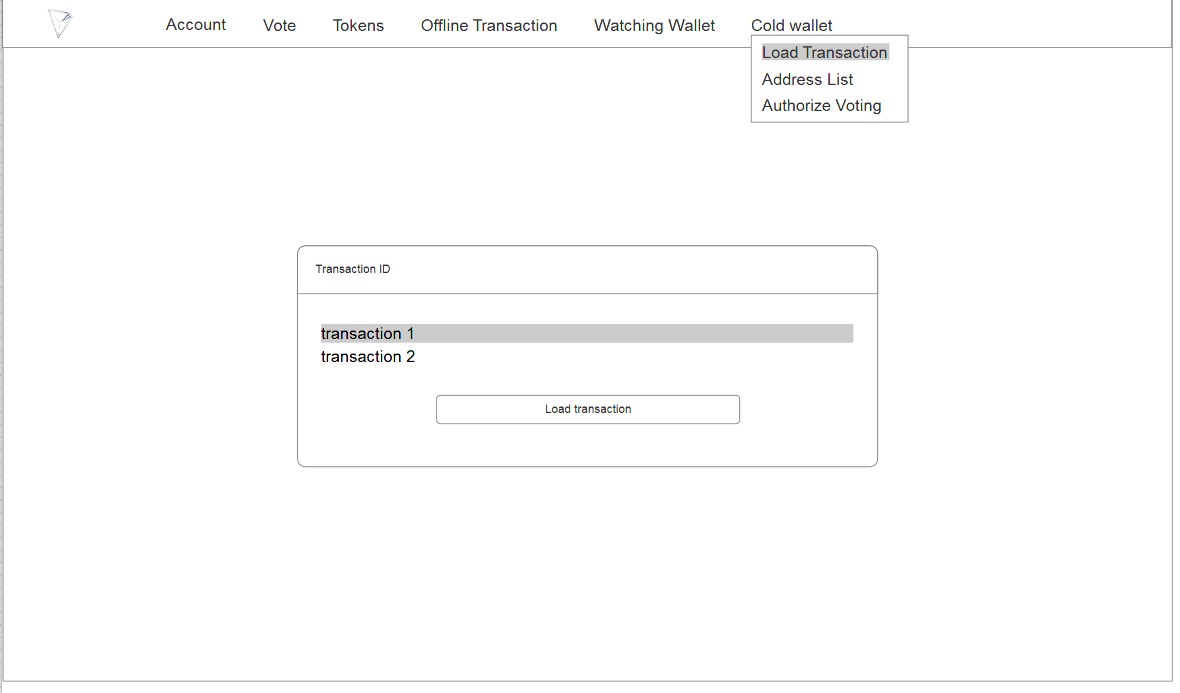
账户余额列表只显示地址和私钥，不显示Token数目等。一个冷钱包默认一个地址。



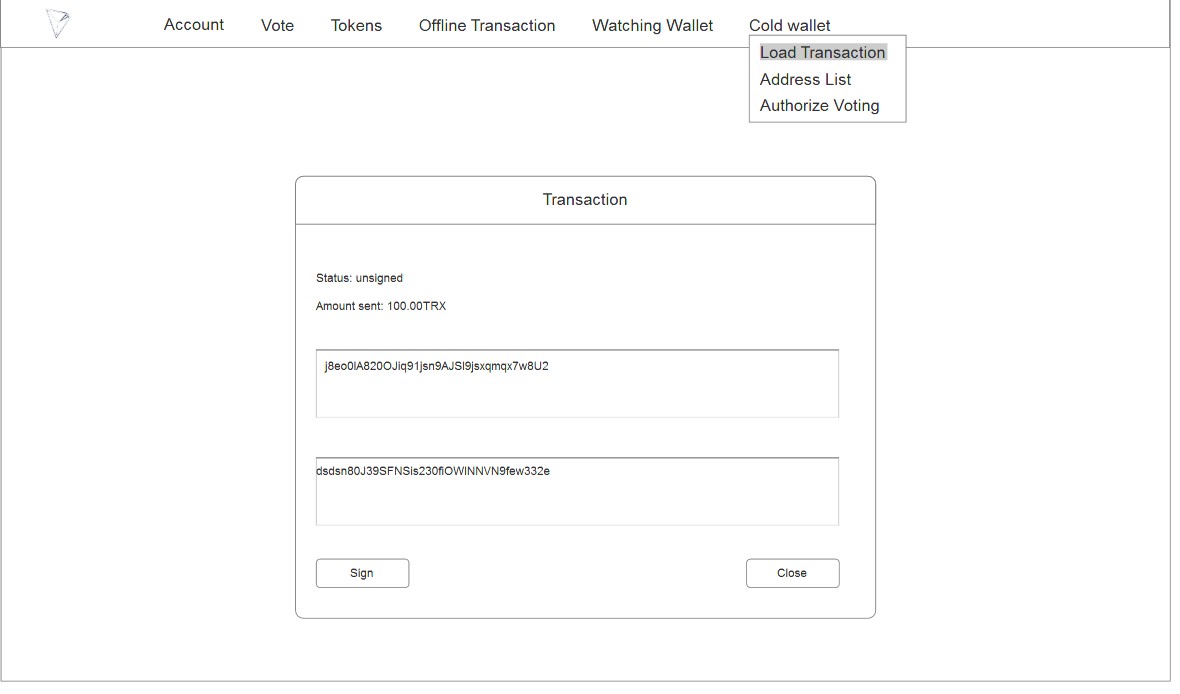
页面18-1

1. **加载交易**

点击冷钱包加载交易，出现文件选择框，选择要签名的交易并签名。

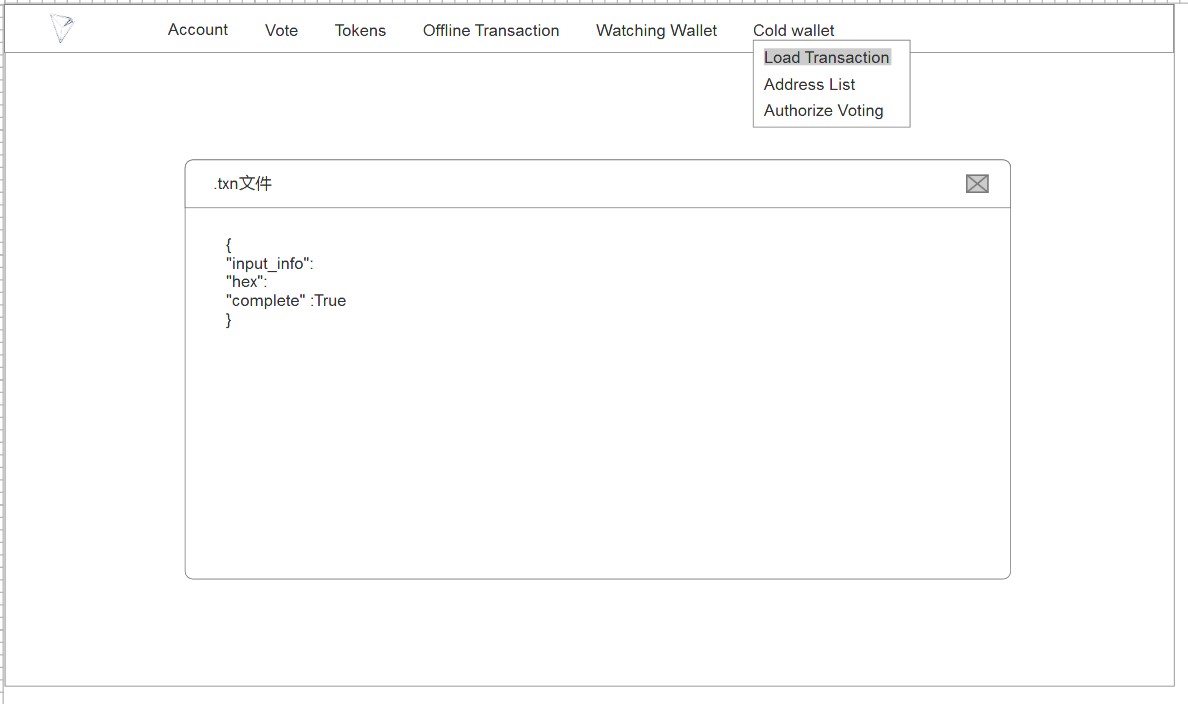


页面16-1



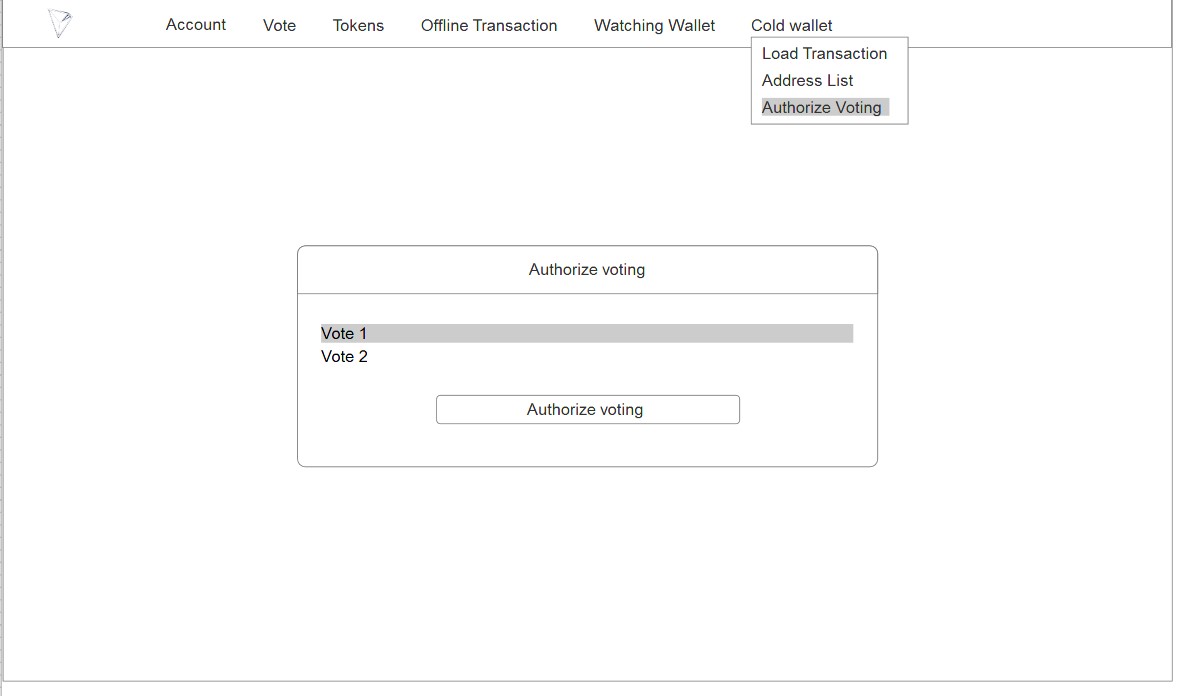
页面16-2

签名之后自动生成.txn已签名文件。将文件用U盘拷入热钱包。

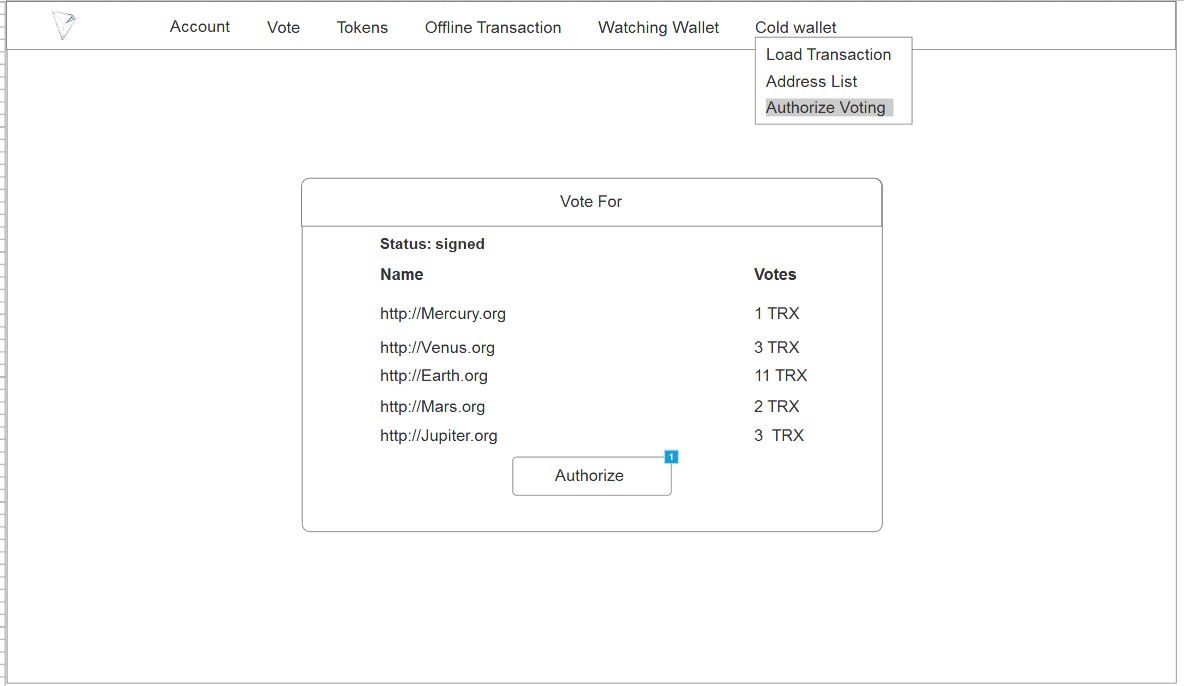


冷钱包部分均不需要调用接口。

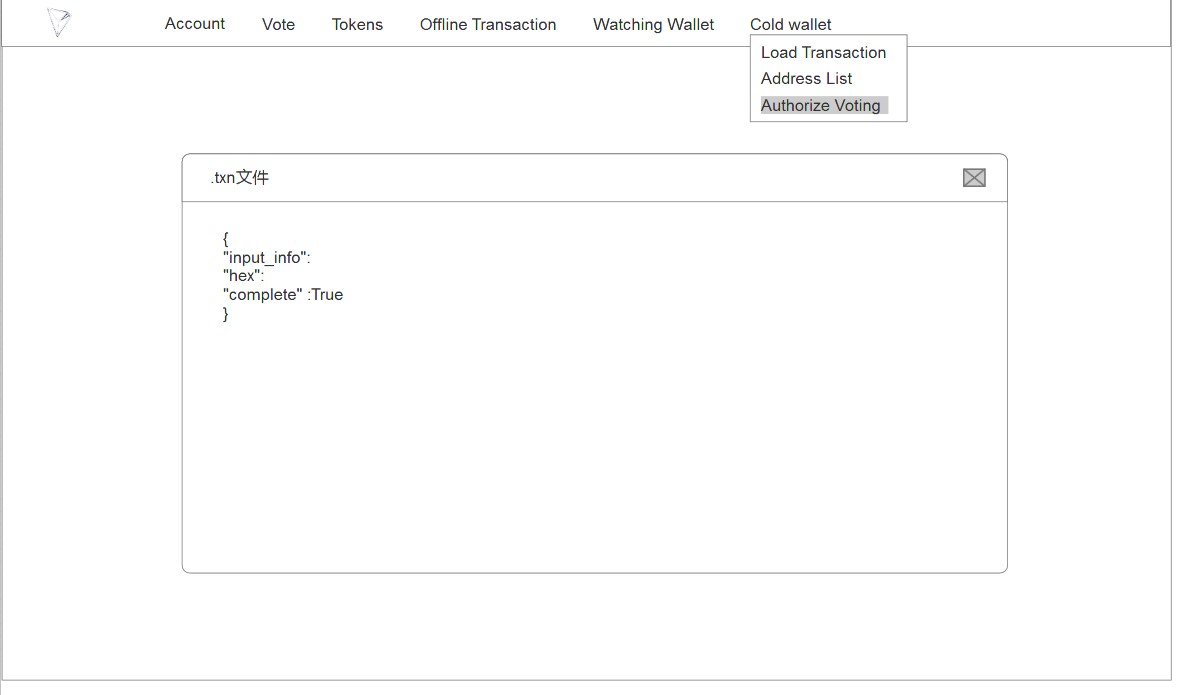
1. **授权投票**

热钱包部分的待授权文件拷入到冷钱包中，冷钱包点击授权投票，选择要载入的授权文件，点击授权。跳转至页面（20-2）

页面 20-1

页面显示投票的代表和票数，点击授权自动生成.txn文件****

页面 20-2

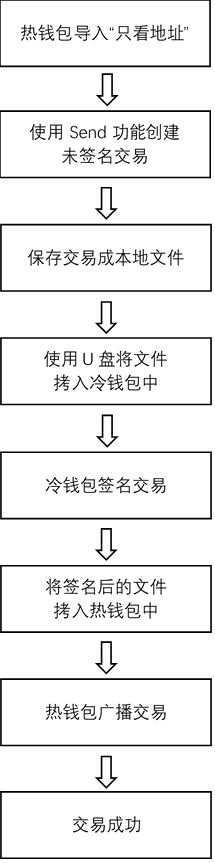


页面 20-3

# 交互过程

在进行转账交易之前要建立冷热钱包的监控关系。使用热钱包余额列表界面的Add addresses功能，导入“只看地址”。转账过程是：热钱包发起交易🡪冷钱包签名授权🡪热钱包广播交易。

交易流程图如下：



参考资料：

1. 可参考web版本的钱包：[https://trxscan.org/#/](https://trxscan.org/" \l "/)
2. 参考的PB协议链接：

<https://github.com/tronprotocol/protocol/blob/master/Chinese%20version%20of%20TRON%20Protocol%20document.md>

1. 1 TRX= 10^6 drop后台的单位是drop
2. http://47.254.18.49:18890/wallet/listwitnesses 这是测试网的一台机器，这个接口是把grpc的转成json的，所有接口查看protobuf定义
3. https://tronscan.org/#/blockchain 这是区块链浏览器，这里可以申请账户和测试用的钱。
4. <https://github.com/tronprotocol/protocol/blob/master/api/api.proto>
5. https://github.com/tronprotocol/protocol 这里是全部protocol定义， wallet-cli项目里有java版的使用方法
6. 比特币冷钱包到底应该怎么做？

<http://www.8btc.com/cold-wallet>

1. 关于比特币的“冷存储”和Armory的使用

<http://www.cnblogs.com/liuhaitao/p/4920549.html>

1. <https://github.com/tronprotocol/wallet-cli/blob/master/src/main/resources/static/js/cryptohash/crypto.js> 是密码算法相关
2. <https://github.com/tronprotocol/wallet-cli/blob/master/src/main/resources/static/js/cryptohash/lib/code.js> 是编码相关
3. <https://github.com/tronprotocol/wallet-cli/tree/master/src/main/resources/static/js/cryptohash>这里面有各种hash 签名 编码的函数