**MATRIX 网页钱包手册**

**版本: V1.0**

**作者：MATRIX 基金会北京研究院**

**日期：2018.09.28**

任何情况下，与本系统及其衍生产品，以及与之相关的全部文件（包括本文件及其任何附件中的全部信息）相关的全部知识产权（包括但不限于版权、商标和技术秘密）皆属于 MATRIX 基金会所有。

本文件中的信息是保密的，且仅供用户指定的接收人内部使用。未经 MATRIX 基金会事先书面同意，本文件的任何用户不得对本产品和本文件中的信息向任何第三方（包括但不限于除用户指定接收人以外的管理人员、员工和关联公司）进行披露、出借、许可、转让、出售、分发、传播或进行与本产品和本文件相关的任何其他处置，也不得使该等第三方以任何形式使用本产品和本文件中的信息。

未经 MATRIX 基金会事先书面允许，不得为任何目的、以任何形式或任何方式对本文件进行复制、修改或分发。本文件的任何用户不得更改、移除或损害本文件所使用的任何商标。

本文件按“原样”提供，就本文件的正确性、准确性、可靠性或其他方面，MATRIX 基金会并不保证本文件的使用或使用后果。本文件中的全部信息皆可能在没有任何通知的情形下被进一步修改，MATRIX 基金会对本文件中可能出现的任何错误或不准确之处不承担任何责任。

在任何情况下，MATRIX 基金会均不对任何因使用本软件产品和本文件中的信息而引起的任何直接损失、间接损失、附带损失、特别损失或惩罚性损害赔偿（包括但不限于获得替代商品或服务、丧失使用权、数据或利润；或商业中断），责任或侵权（包括过失或其他侵权）承担任何责任，即使 MATRIX 基金会事先获知上述损失可能发生。

MATRIX 基金会保留所有权利

# 目 录

[目 录 1](#_Toc527648499)

[变更记录 2](#_Toc527648500)

[1 引言 3](#_Toc527648501)

[1.1 文档用途 3](#_Toc527648502)

[1.2 术语 3](#_Toc527648503)

[2 创建新钱包 4](#_Toc527648504)

[3 在线交易 7](#_Toc527648505)

[3.1 一对一交易 7](#_Toc527648506)

[3.2 一对多交易 9](#_Toc527648507)

[4 离线交易 11](#_Toc527648508)

[5 抵押交易 14](#_Toc527648509)

[6 退选交易 16](#_Toc527648510)

[7 退款交易 17](#_Toc527648511)

# 变更记录

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 修订日期 | 修订内容 | 作者 | 评审者 | 评审日期 |
| 2018-09-28 | 初版 | 郝林、黄志 |  |  |
| 2018-10-8 | 更新‘抵押交易’、‘退选交易’和‘退款交易’部分 | 郝林、黄志 |  |  |

# 引言

网页钱包使用非常简便，打开网页即可使用。而且网页钱包是去中心化的钱包，不会存储用户的钱包信息账号。即使钱包网站挂掉，一样可以通过钱包的私钥和密码在其他钱包上找回钱包账号，MATRIX 网页钱包绝对安全，请放心使用

钱包官网地址：http://testnet.matrix.io/

## 文档用途

本文档针对 MATRIX 网页钱包的使用做了详细说明，方便用户快速入门和掌握。

## 术语

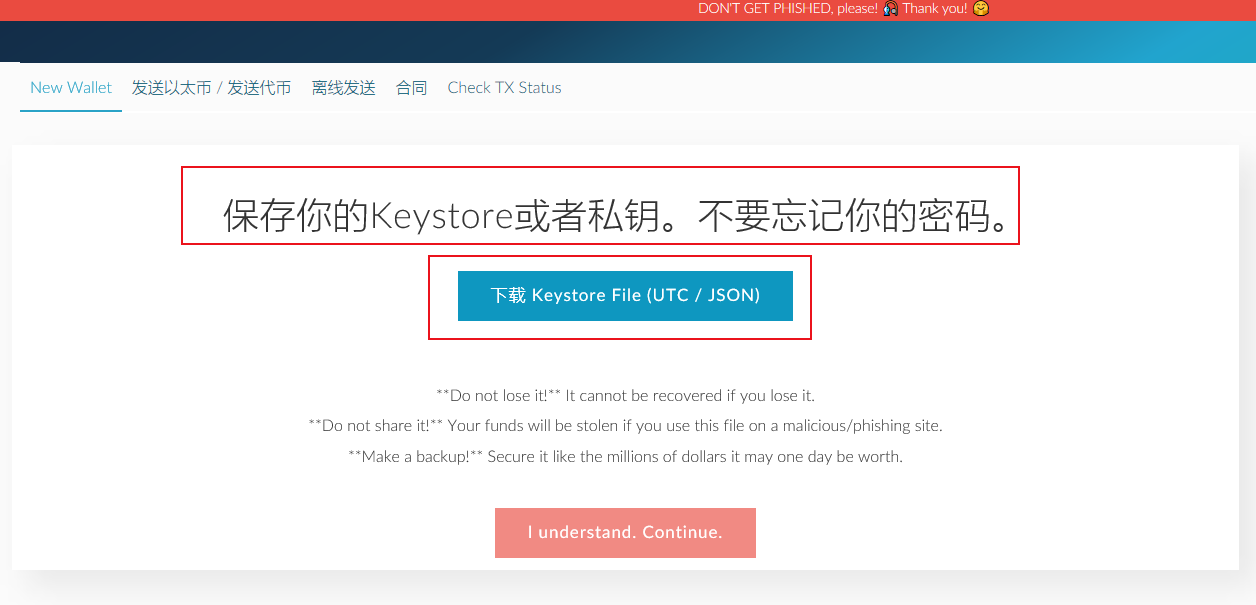
| **术语** | **备注** |
| --- | --- |
|  |  |

# 创建新钱包

1. 输入密码：点击“生成钱包”，这个密码一定要记住



1. 保存 **`Keystore File(UTC/JSON)`** 文件

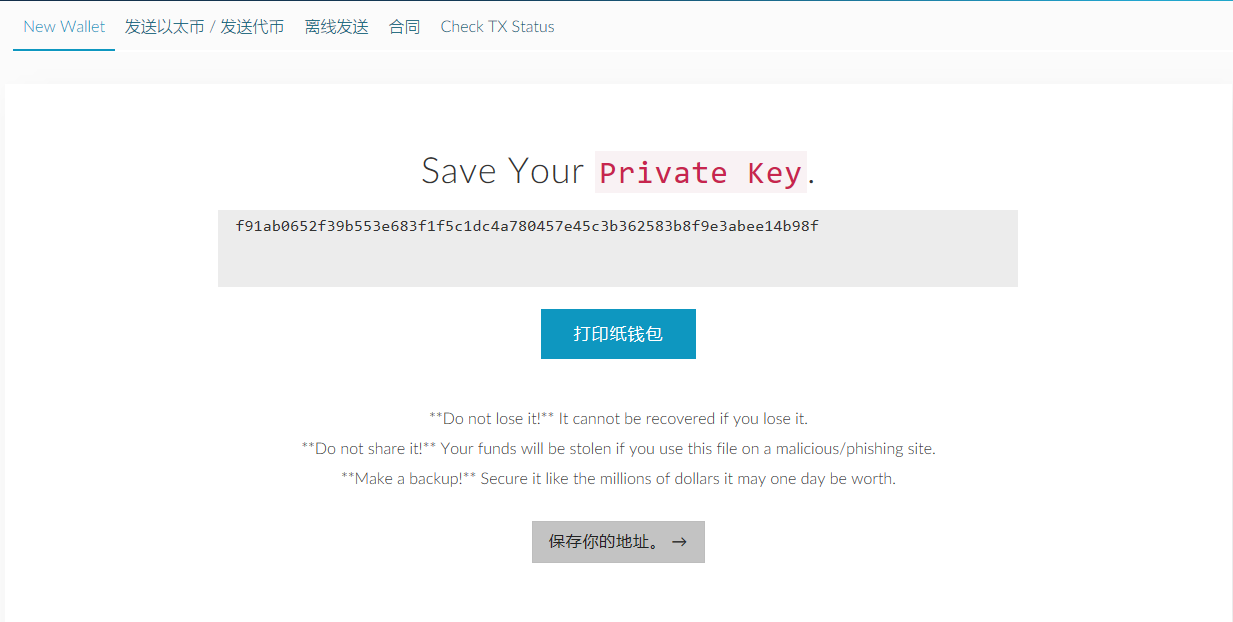


下面是保存的 `Keystore File(UTC/JSON)` 文件的JSON数据：

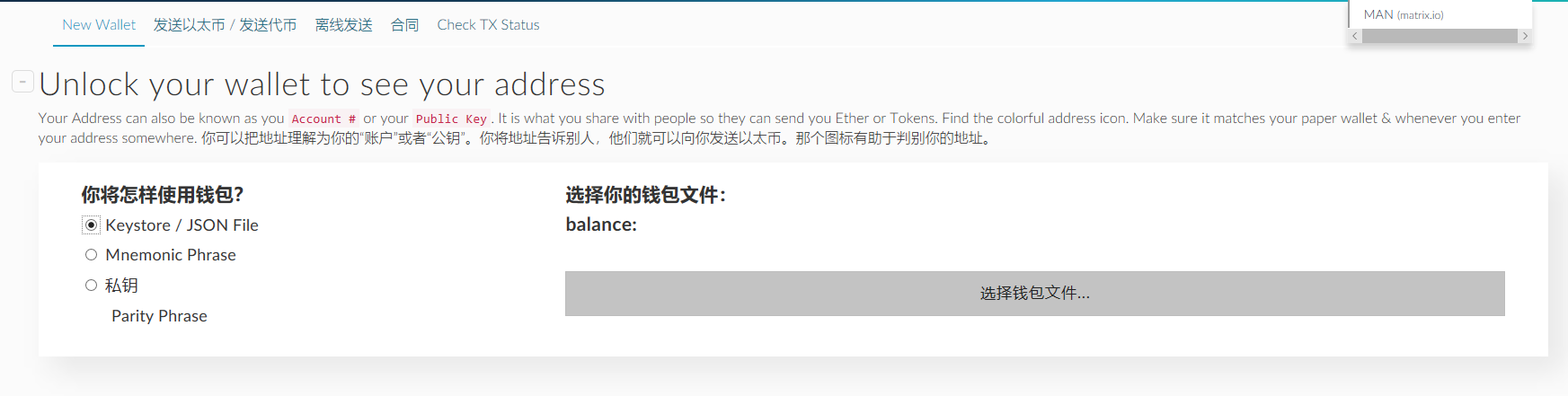
 {"version":3,"id":"69dfbc60-7221-4f05-853d-749046b685bb","address":"de4ce30a9abc138408509c7628681fd08d931586","Crypto":{"ciphertext":"099827b94d7c64e4aa54bccbad342db7a375d558987c79ae921c9d7223b44bdc","cipherparams":{"iv":"07adb85fcfb94f487f4381fdc47e79b4"},"cipher":"aes-128-ctr","kdf":"scrypt","kdfparams":{"dklen":32,"salt":"1d57cfc8fc5cb9a03a30ddc2cbe4949e17e220949a582ad8be10b41c02be9021","n":8192,"r":8,"p":1},"mac":"c85427a2d62b10d24647e06d2cda99c5576828d655a3d4382c49fa478fafebbb"}}

**重要：Keystore 文件务必妥善保存！**

下图是点击 `I understand. Continue` 后的效果：



1. 点击 `打印纸钱包`，将这张图片打印收藏起来（保存Private Key，用来生成keystore 和密码，也可以修改密码)
2. 点击 `保存你的地址`



1. 加载账号，选择和打开之前下载的`Keystore File(UTC/JSON)`文件：



6. 输入密码，点击`已联网并解锁钱包`



上面的地址就是 `你的钱包地址`，如果别人给你转账，直接把这个地址提供给对方即可。

# 在线交易

如上正确输入密码后，即可进入在线交易界面：



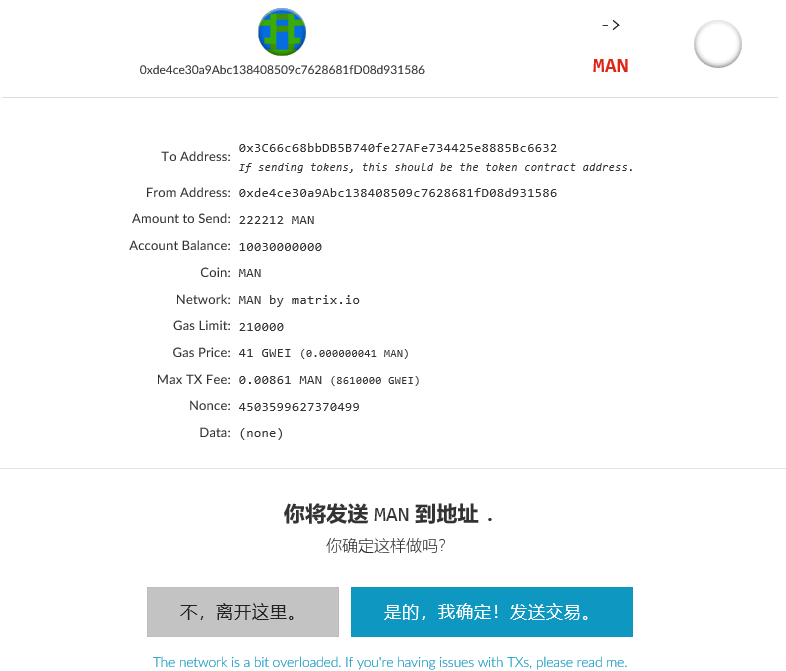
## 一对一交易

向单个账户地址进行转账交易：

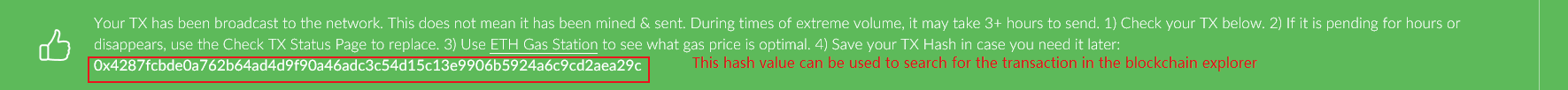
- 选择`发送至地址`：到账地址可选择本地地址和添加新地址。添加新地址后可以在地址下拉框中选择  
- 输入转账金额  
- gas limit 可以无需理会  
- 点击 `生成交易`  
- 点击 `发送交易`

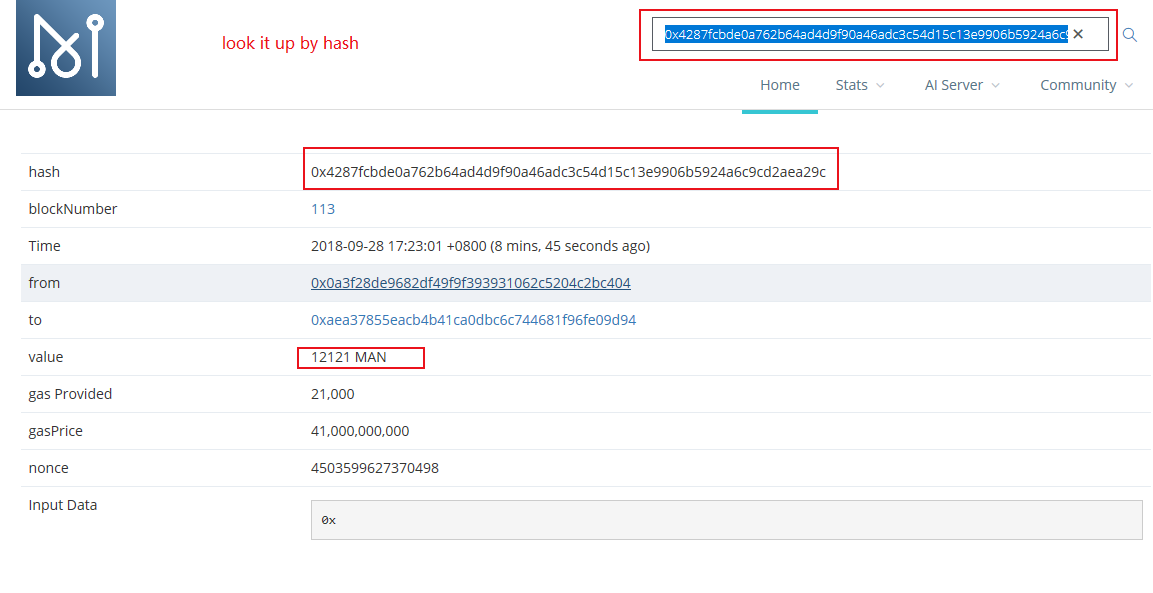


点击发送交易按钮后，会弹出一个确定按钮，核对信息无误后，点击 `是的，我确定！发送交易`，如下图所示：



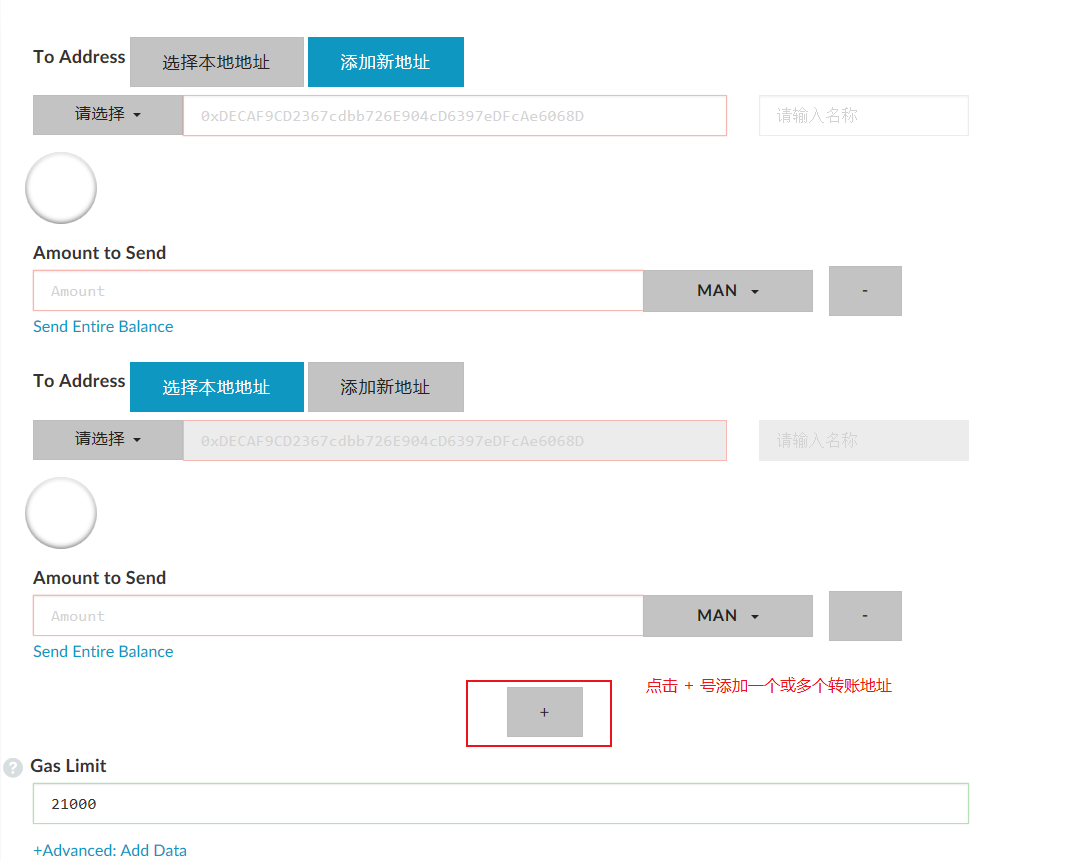
成功后会看到网站底部出现一个绿色框，显示发送成功，并产生了一个 `TX ID`，如果大家发送MAN或其他代币到交易所，过了一段时间对方还没收到的话，可以直接将这个TX ID给对方检查，或者可以直接到交易记录浏览器查看交易细节





## 一对多交易

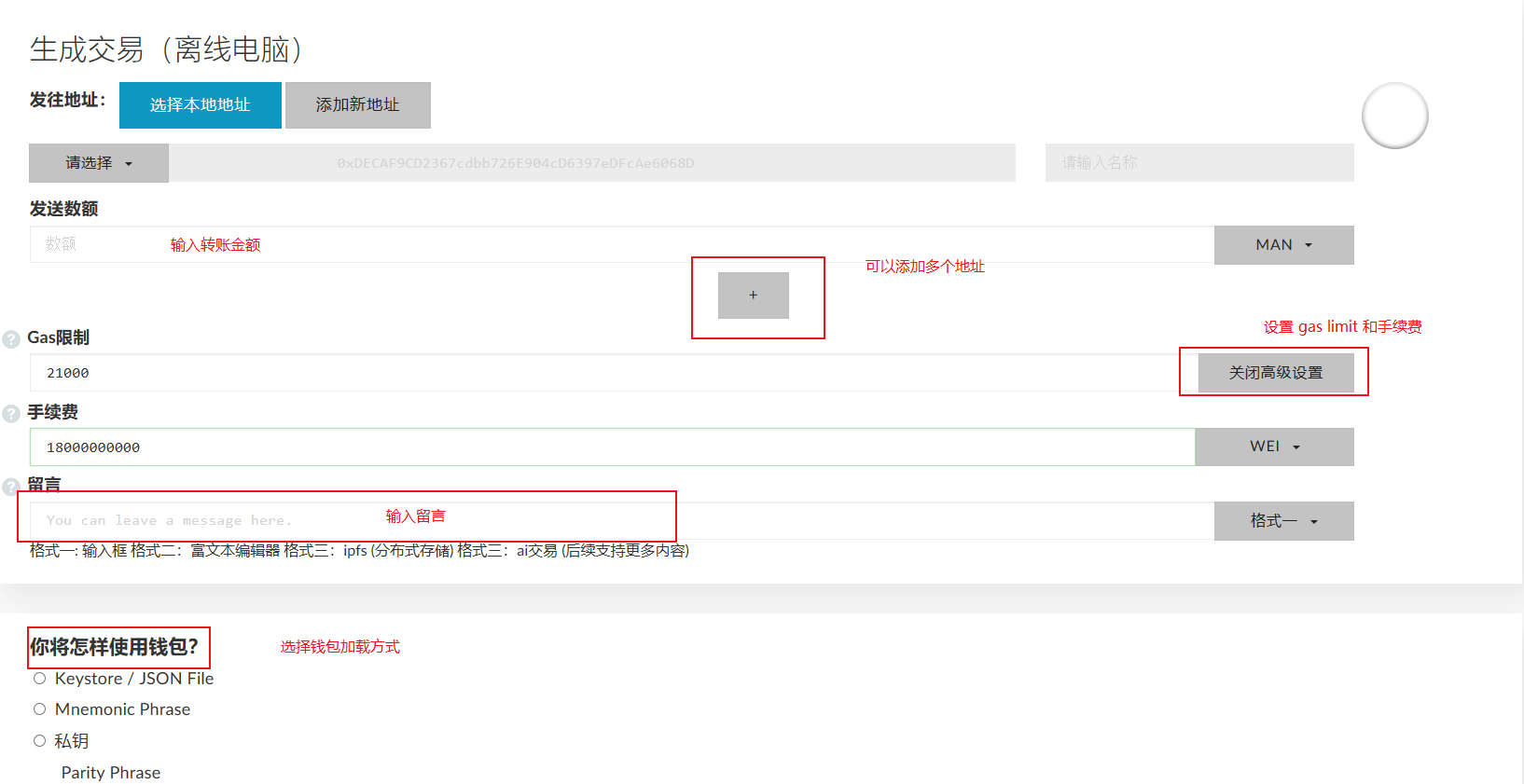
MATRIX 网页钱包支持一对多交易（点击 + 号添加多个新地址），同时向多个地址转账：



其他操作同一对一交易，不再赘述。

# 离线交易

**富文本**：相比在线交易，离线交易的最大特点是支持留言功能  
留言内容包括文字、图片、视频（长度限制在480字节内）。留言支持文本、图片、视频内容上传



**IPFS 格式交易：**

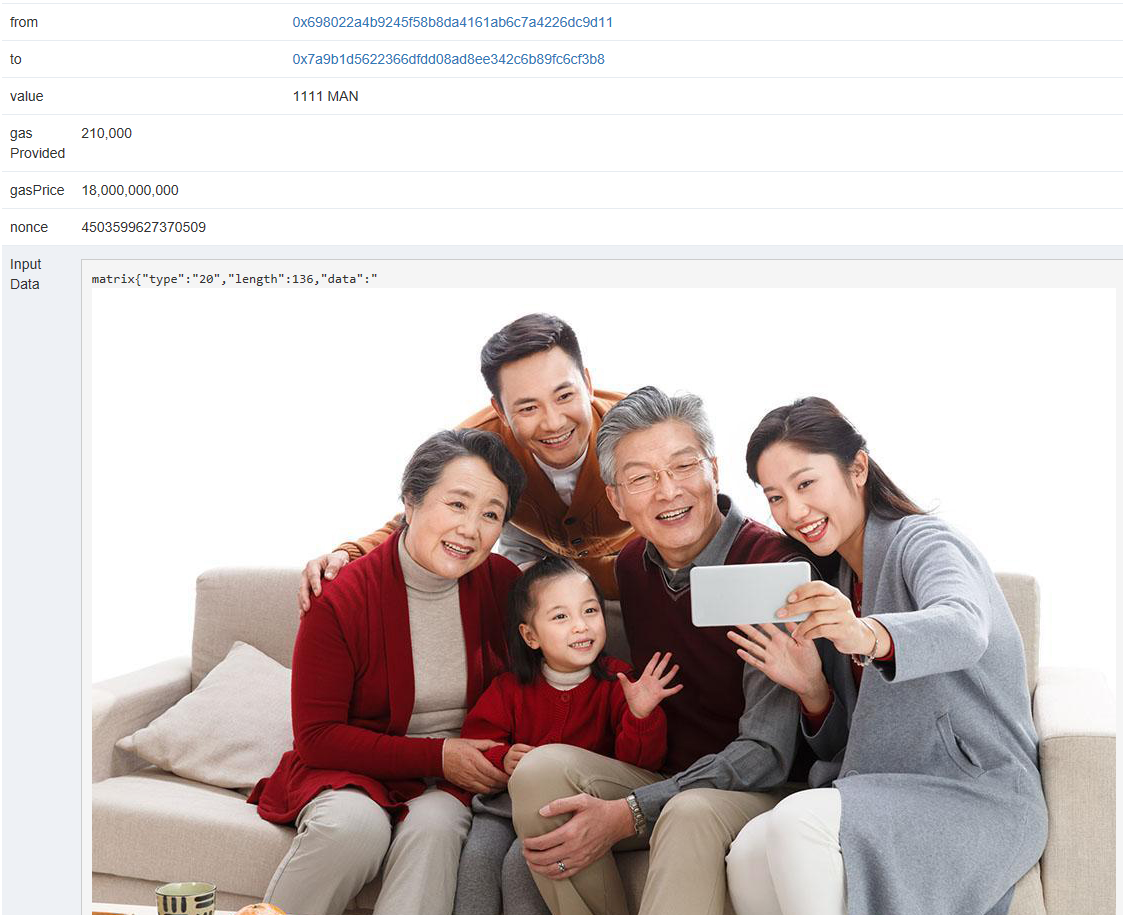
首先根据离线交易中的格式四（AI 人脸识别）或格式五（AI 物体识别）做一笔上传图片的通用交易，同时生成交易hash。

原始图片会上传到IPFS，IPFS服务器进行处理生成处理结果（索引信息），将处理结果上传到MATRIX区块链上，同时也将结果传送给AI服务器，AI服务器处理该交易进行图片识别处理，AI服务器处理完后，将触发另一笔交易，该交易的接收账户是原始交易的发送账户，转账金额为0。

通过查询原始交易的账户交易流水即可确认原始交易图片和AI处理过的图片的两笔交易。

**AI 人脸识别：**

处理前通过区块浏览器查看：

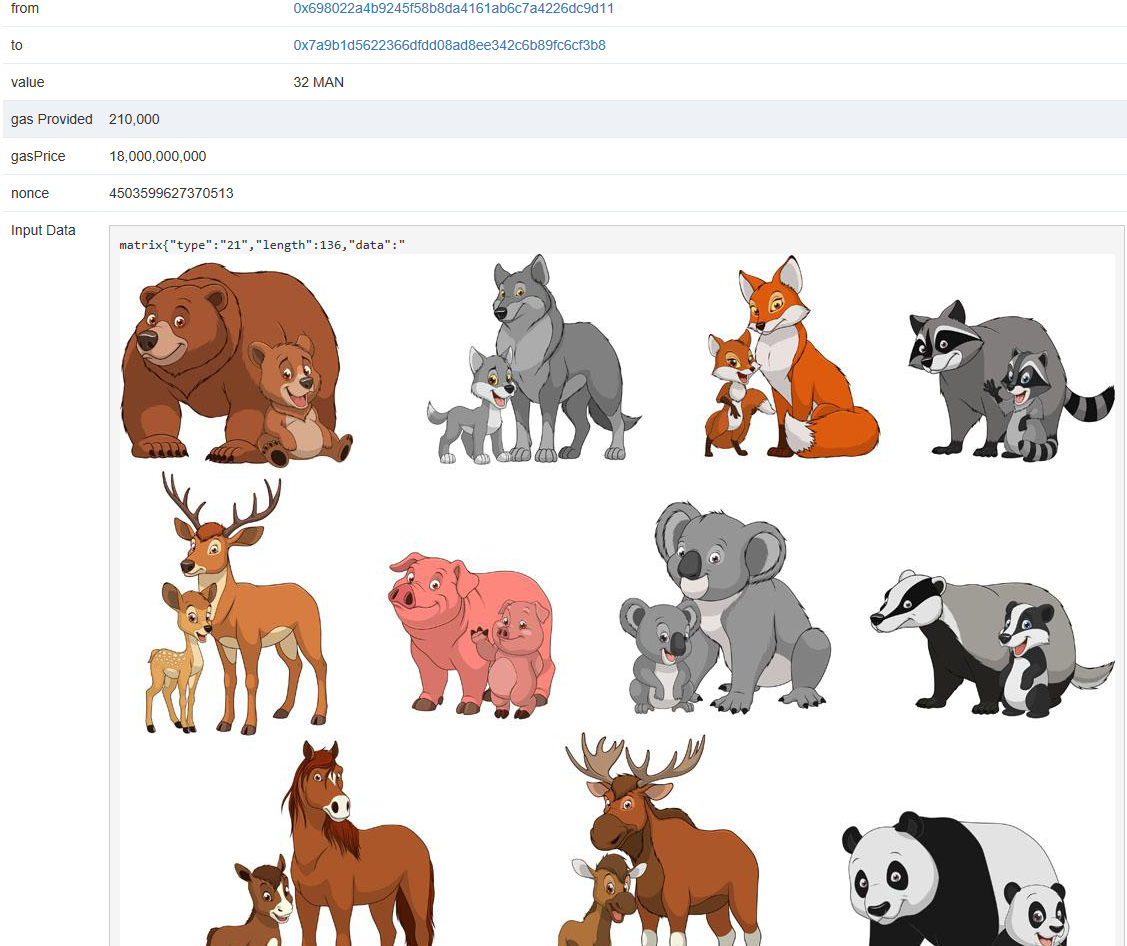


处理后通过区块链浏览器查看：

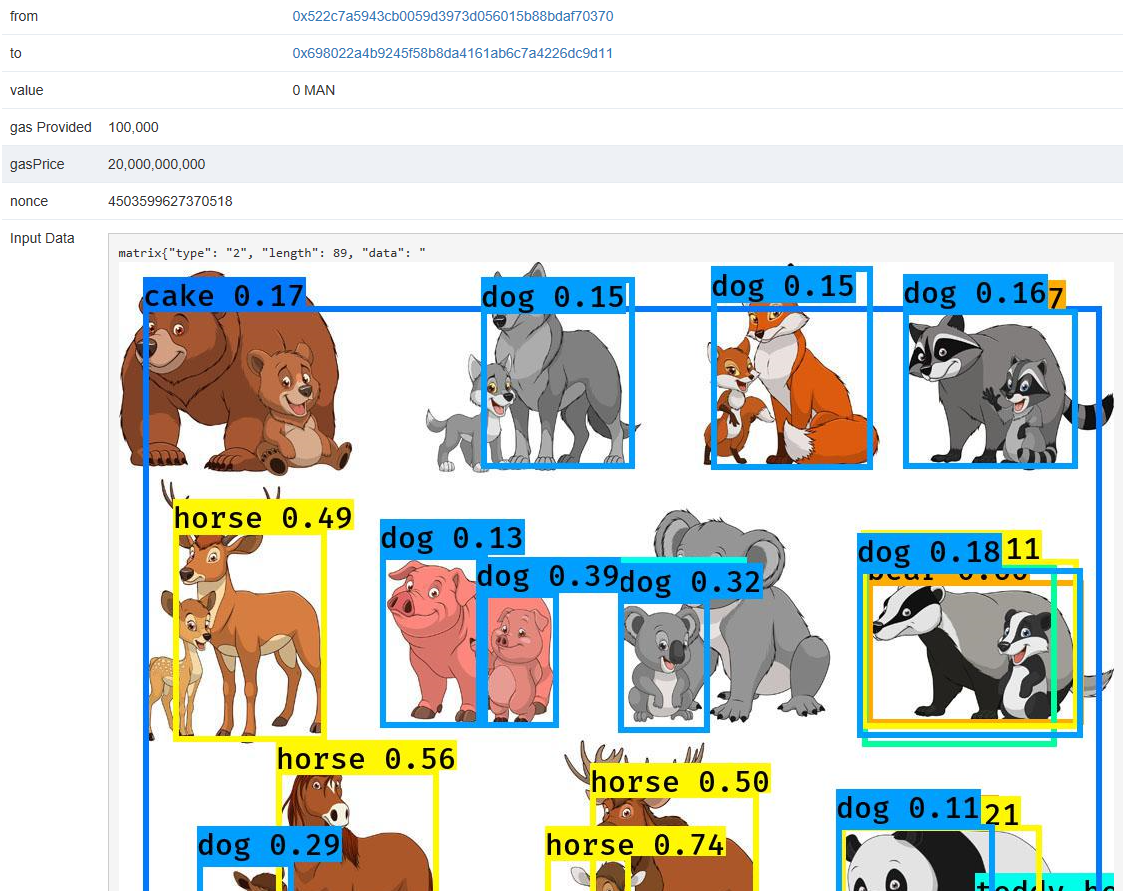


**AI动物和物体识别：**

处理前通过区块链浏览器查看：



处理后通过区块链浏览器查看：



# 抵押交易

申请成为 MATRIX 区块链的矿工或验证者，需要抵押一定的 MAN 币。这一般通过智慧合约来实现

抵押交易分矿工节点抵押和验证节点抵押，抵押金额介于 1 w和10w MAN 币的抵押交易为矿工节点抵押交易，>= 10w的为验证节点抵押交易。

当退出抵押流程时需要执行退选和退款，退选执行成功时查询状态栏中显示退选节点高度，退款成功后会将抵押金额返还至原交易账户。

注意：抵押交易中的gasprice 和gaslimit不需要用户填写，已经设置成默认值，正常情况下足够抵押交易使用。

* + - 1. 查询抵押交易状态：输入交易抵押账户地址进行查询



* 抵押金额：金额单位为WEI，除以1+e18（10 的 18 次方）得出正常金额值；
* 抵押节点ID: 拥有抵押参选资格的节点ID（节点ID 是需要参加抵押的节点ID，测试时需要运行gman, 通过命令获取NodeID - 具体见gman操作说明)
* 抵押状态：节点已处于抵押状态；节点在xx高度退出抵押，但是还未退款
  + - 1. 执行抵押交易

矿工抵押交易：1w<抵押金额<10w



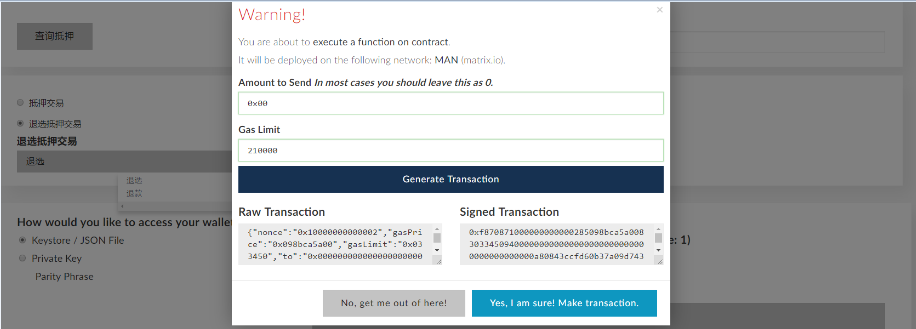
验证抵押交易：抵押金额>=10w



# 退选交易

退选抵押交易以及查询退选后抵押账户的抵押状态

**注意：**退选后该账户依然在抵押列表中但不参与收益，直到达到指定的确认数（最新高度 - 该交易所在高度 = 该交易的确认数）并且退款成功后才完全退出竞选





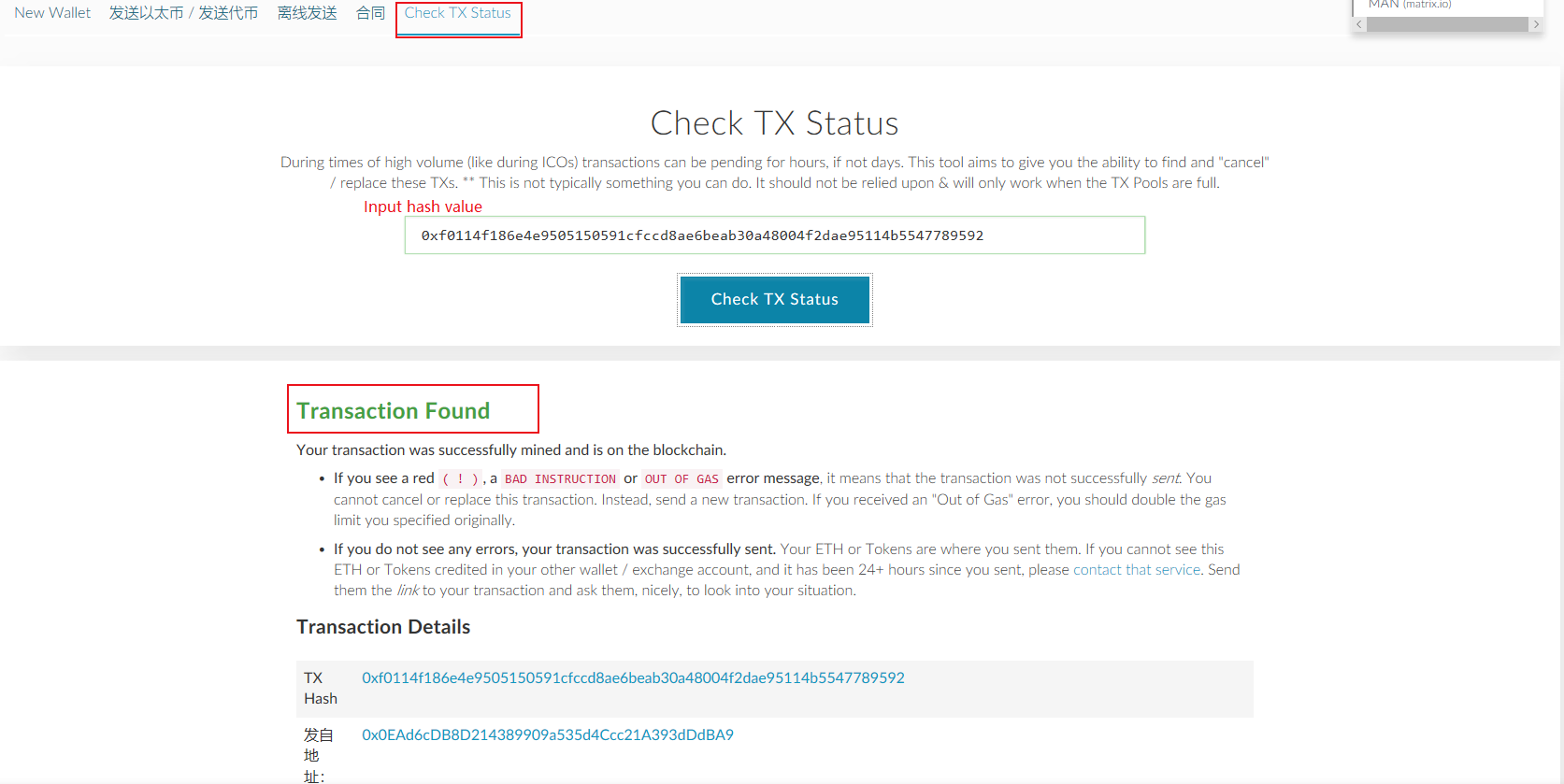
# 退款交易

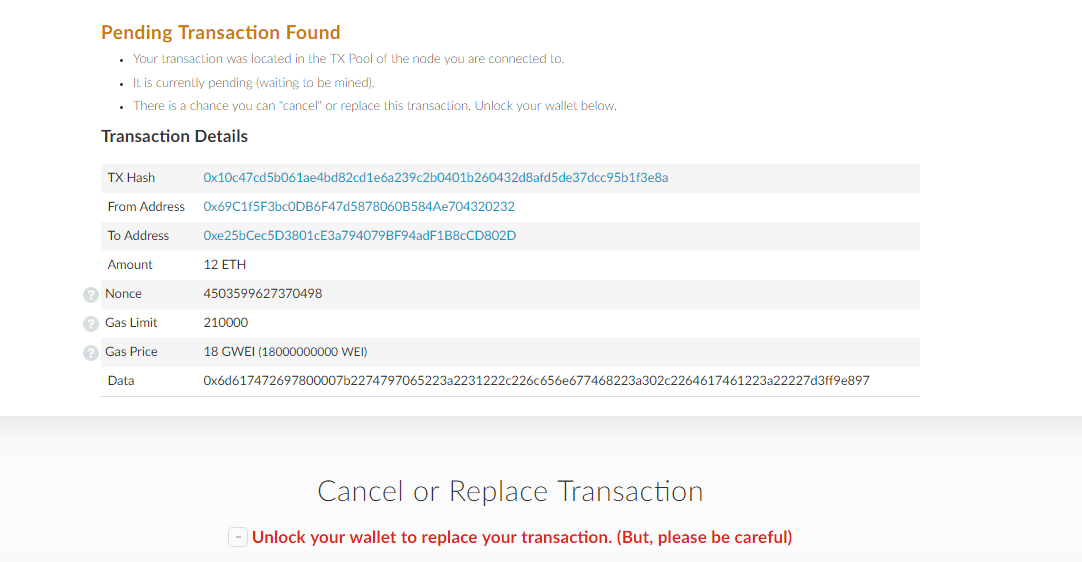
退款抵押交易：当达到指定确认数之后，退款抵押交易才能执行成功。退款成功后抵押金额会返还给参与抵押的账户，同时关于该账户的抵押交易信息会完全消失，查询为空



8交易状态查询

查询交易状态，输入交易hash显示“Transaction Found”说明该交易已经上链，显示“Pending Transaction Found”说明该交易已经在交易池中可撤回。





当该交易处在交易池中时可覆盖该交易，以达到撤销交易的效果，点击“Cancel or Replace Transaction”构建交易即可完成替换