

MATRIX 网页钱包手册

版本: V1.1

作者: MATRIX 基金会北京研究院

日期: 2018.12.27



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	į	录······	1
变	更i	记录	3
1	į	引言	4
	1.1	1 文档用途	4
	1.2	2 术语	4
2	1	创建新钱包账户	5
3	ī	在线交易	8
(3.′	1 即时交易	8
	3	3.1.1 一对一即时交易	8
	3	3.1.2 一对多即时交易 1	11
;	3.2	2 定时交易1	12
	3	3.2.1 一对一定时交易 1	12
	3	3.2.2 一对多定时交易 1	12
;	3.3	3 可撤销交易1	13
	3	3.3.1 一对一可撤销交易 1	13
	3	3.3.2 一对多可撤销交易 1	14
(3.4	4 撤销交易1	14
4	ì	离线交易1	17



5	授权委托	18
6	取消委托	20
7	CHECK TX STATUS	23
8	抵押交易	24
9	AI 交易	28
10	合约	. 错误!未定义书签。



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		
2018.12.27	交易类型划分为即时交易、定时交易和可撤销交易(均支持一对一和一对多)	郝林		
2018.12.28	交易类型增加 '授权 委托'交易	郝林		
2018.12.28	 1.抵押交易部分更新, 去除 nodelD 2.合约部署与交互 3. AI 交易 	郝林		
2019.1.28	委托交易界面更新	郝林		
2019.2.25	增加多币种创建	郝林		
2019.3.28	1. 委托交易增加按 次数委托 2. 多币种创建更新 3. 账户黑名单交易	郝林		



1 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: https://wallet.matrix.io/

1.1 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。

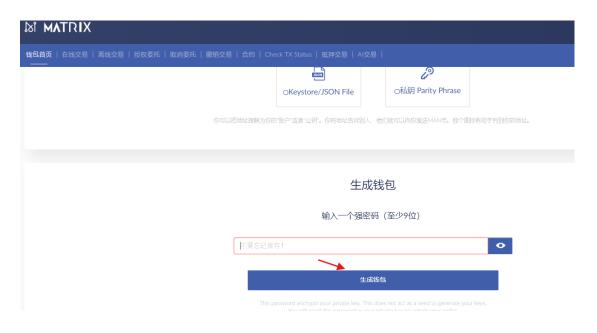
1.2 术语

术语	备注



2 创建新钱包账户

1. 输入密码:点击"生成钱包",这个密码一定要记住



2. 保存 `Keystore File(UTC/JSON)` 文件

保存你的Keystore或者私钥。

不要忘记你的密码



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":"de4ce30a9



abc138408509c7628681fd08d931586","Crypto":{"ciphertext":"099827b94d7c64e4aa54b ccbad342db7a375d558987c79ae921c9d7223b44bdc","cipherparams":{"iv":"07adb85fcf b94f487f4381fdc47e79b4"},"cipher":"aes-128-ctr","kdf":"scrypt","kdfparams":{"dklen":32 ,"salt":"1d57cfc8fc5cb9a03a30ddc2cbe4949e17e220949a582ad8be10b41c02be9021","n ":8192,"r":8,"p":1},"mac":"c85427a2d62b10d24647e06d2cda99c5576828d655a3d4382c4 9fa478fafebbb"}}

重要: Keystore 文件务必妥善保存!

下图是点击 'I understand. Continue' 后的效果:

Save Your Private Key.

不要忘记密码

6f9ec31a9b443a951c6c58e63ff942b446e3cfaff87e639295c37ed201e37812

Do not lose it! It cannot be recovered if you lose it.

Do not share it! Your funds will be stolen if you use this file on a malicious/phishing site

Make a backup! Secure it like the millions of dollars it may one day be worth.

保存你的地址

- 3. 点击 `保存你的地址`
- 4. 加载账号,选择和打开之前下载的`Keystore File(UTC/JSON)`文件或者输入秘钥:





5. 如果选择 keystore 文件 ,还需要输入密码。钱包解锁后,可以看到自己的账户信息,如下:



上面的账户地址就是`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。此外,您可以看到,除了主账户外,还有其他几个账户类型,它们分别展示不同场景下的账户余额,下文会有介绍



3 在线交易

进入在线交易界面,如上方式解锁钱包:

战包首页 在线交易 离线交易	授权委托 取消委托 撤销交易 合约 Check TX Status 抵押交易 AI交易				
发送交易					
发送至地址:	谱输入地址				
交易金额:	清輸入全额				
	+添加多笔交易				
® 自付gas ○ 委托gas	® 自付gas ◎ 委托gas				
◉ 即时交易	® 即叶本层				
○ 定时交易 ○ 可撤销交易					

3.1 即时交易

顾名思义,即时交易为实时转账,包括一对一转账和一对多转账

3.1.1 一对一即时交易

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

- 输入交易金额
- gas 支付方式选择'自付 gas'(代付会在下面介绍)
- 点击 `即时交易`



- 可以选择在普通文本框、富文本框和分布式存储中输入内容
- 点击 `生成交易`



点击生成交易按钮后, 会分两列展示未生效交易和签名交易, 如下所示:





点击发送交易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:

确认交易信息

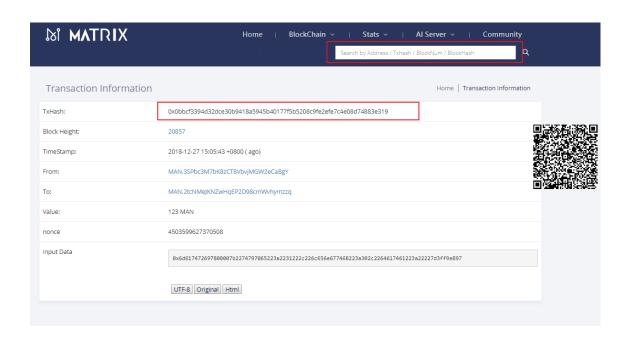


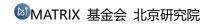
成功后会看到网站底部出现一个绿色框,显示发送成功,并产生了一个 `TX ID`,如果大家发送 MAN 或其他代币到交易所,过了一段时间对方还没收到的话,可以直接将这个 TX ID 给对方检查,或者可以直接到区块链浏览器查看交易细节



Your TX has been broadcast to the network. This does not mean it has been mined & sent. During times of extreme volume, it may take 3+ hours to send. 1) Check your TX below. 2) If it is pending for hours or disappears, use the Check TX Status Page to replace. 3) Use [MAN Gas Station] to see what gas price is optimal. 4) Save

your TX Hash in case you need it later:
0x0bbcf3394d32dce30b9418a5945b40177f5b5208c9fe2efe7c4e08d74883e319





3.1.2 一对多即时交易

MATRIX 网页钱包支持一对多交易(点击 '+添加多笔交易'添加多个新地址),同时向多个地址转账(添加的地址也可以删除):

发送交易

发送至地址:	MAN.2tcNMeJKNZwHqEP2D98cmWvhymzzq	address1		
交易金额:	交易全额: 123			
发送至地址:	MAN.2n9Qx5ehJNonZVGUDuUKYefbTqacS	address2		
交易金额:	456			
		○ 删除此笔交易		
		+添加多笔交易		

其他操作同一对一交易,不再赘述。



3.2 定时交易

定时交易是指,在指定时间(高度)真正完成转账

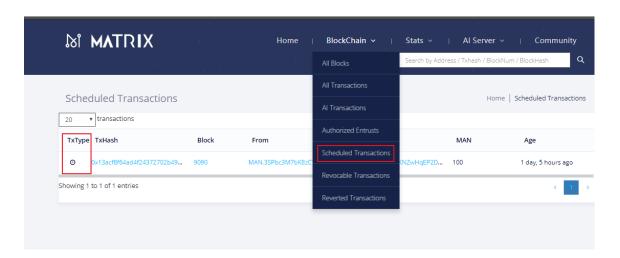
请注意: 交易会在当时上链, 而交易双方账户的余额变动会在指定时间完成

3.2.1 一对一定时交易

钱包解锁及交易发起步骤同'3.1.1 一对一即时交易',交易类型需要选择'定时交易'



发起的定时交易可以在浏览器 Scheduled Transactions 中查询



3.2.2 一对多定时交易

钱包解锁及交易发起步骤同'3.1.2一对多即时交易',交易类型需要选择'定时交易'



3.3 可撤销交易

可撤销交易在 24 小时内都可以撤销,交易发送后,主账户余额会减少,可撤销账户余额会相应增加。如果 24 小内不撤回,可撤销账户中的余额会转到交易的接收方账户。如果撤回,则返回自己的主账户

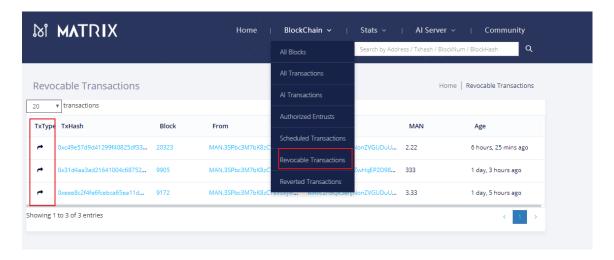
3.3.1 一对一可撤销交易

钱包解锁及交易发起步骤同 '3.1.1 一对一即时交易', 交易类型需要选择 '可撤销交易'



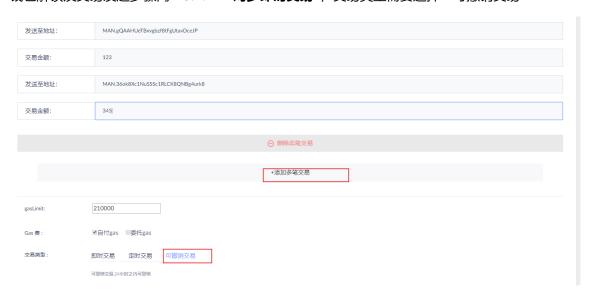


发起的可撤销交易可以在浏览器 Revocable Transactions 中查询



3.3.2 一对多可撤销交易

钱包解锁及交易发起步骤同 '3.1.2 一对多即时交易', 交易类型需要选择 '可撤销交易'



3.4 撤销交易

对可撤销交易进行撤销,撤销后,可撤销账户的余额会返回主账户。

注意:

1. 撤销交易只可以撤销可撤销类型的交易,其他类型的交易不能撤销成功



2. 撤销交易只可以撤销自己发送的可撤销交易,不可以撤销别人发送的可撤销交易

首先进入撤销交易页面,解锁钱包

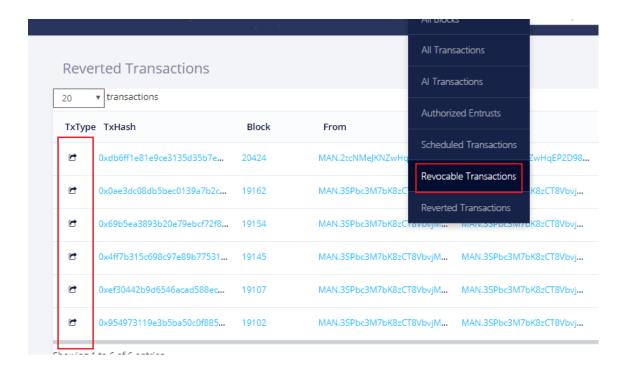
输入要撤销交易的 hash, 点击 '生成交易', 然后点击 '发送交易'





通过生成的 hash,可以在浏览器中查询到这笔交易;或者在 Reverted Transactions 查询

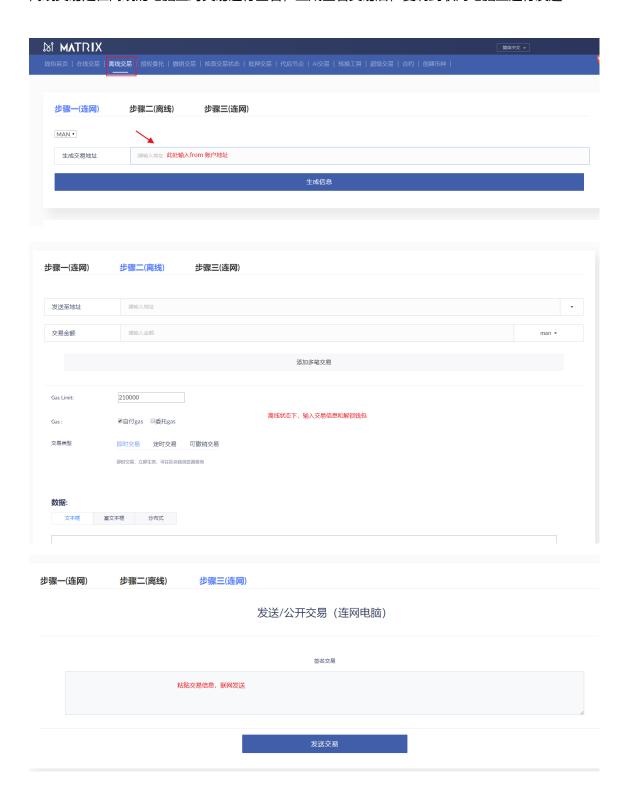






4 离线交易

离线交易是在离线的电脑上对交易进行签名,生成签名交易后,复制到联网电脑上进行发送





5 授权委托

委托交易是两个账户之间的委托行为,委托账户可以委托:

- 代扣 gas:被委托账户发起交易时,gas费由委托账户支付
- 1. 点击授权委托, 并解锁钱包进入授权委托页面

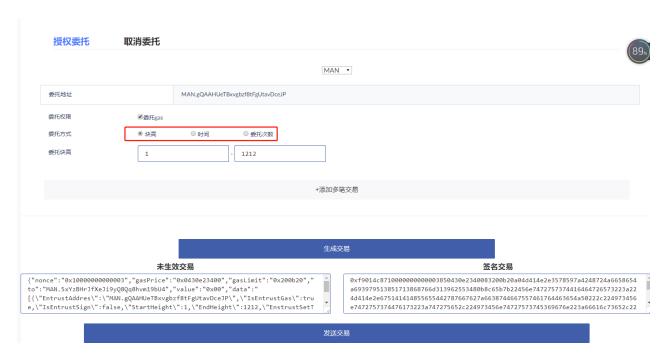


如下图填写必要的信息



委托方式可以选择"按块高"委托,可以选择"按时间"委托,也可以限制委托次数





请注意,如果选择块高或时间,那么只有在指定的块高或时间范围内,委托是生效的。

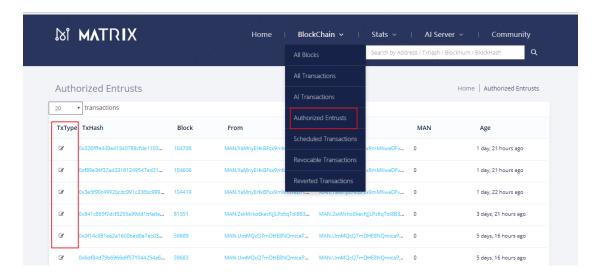
对于委托次数来说,每完成一笔代扣 gas 的交易,委托次数就递减一次,直至用完。



2.点击生成交易和发送交易

交易上链以后,可以通过区块链浏览器 Authorized Entrusts 来查询





完成委托后,即可在在线交易中选择 "委托 gas"



6 取消委托

取消委托是对前一部分的委托交易进行取消操作

点击"取消委托"并进入取消委托界面

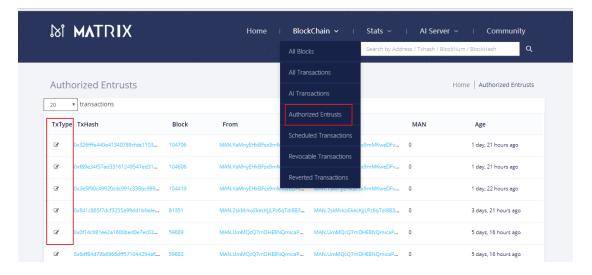




勾选方框,然后点击生成交易和发送交易,委托的权限即被取消



交易上链以后,可以通过区块链浏览器 Authorized Entrusts 来查询



完成委托后,即可在在线交易中选择 "委托 gas"





7 Check TX Status

通过 'Check TX Status' 可以通过交易 hash 查询这笔交易的状态和详细信息

Check TX Status

During times of high volume (like during ICOs) transactions can be pending for hours, if not days. This tool aims to give you the ability to find and "cancel" / replace these TXs. ** This is not typically something you can do. It should not be relied upon & will only work when the TX Pools are full

0xd18b1acc860e4b08d75a896b2ac81f3eb586ac2e6f336a7fc8604b277ffa188d

Check TX Status

Transaction Found

our transaction was successfully mined and is on the blockchain.

- If you see a red (1), a BAD INSTRUCTION or OUT OF GAS error message, it means that the transaction was not successfully sent. You
 cannot cancel or replace this transaction. Instead, send a new transaction. If you received an "Out of Gas" error, you should double the
 sas limit you specified originally.
- If you do not see any errors, your transaction was successfully sent. Your ETH or Tokens are where you sent them. If you cannot see this ETH or Tokens credited in your other wallet / exchange account, and it has been 24+ hours since you sent, please contact that service. Send them the link to your transaction and ask them, nicely, to look into your situation.

Transaction Details

 TX Hash
 Oxd18b1acc860e4b08d75a896b2ac81/3eb586ac2e6/336a7/c8604b277ffa188d

 茨自地址:
 MAN.2nRsUetjWAaYUErkgBxGETimfUUs

 茨往地址:
 MAN.5m2XU6yGoSJIAmFFkKKM5cdURUF

 数額
 0.4403723035 MAN

 按往地址:
 MAN.9HE223J2nC8HYjEBecdB1xGXFETG

 数額
 0.4403723035 MAN

 按往地址:
 MAN.CrsrQSJI/Gxpb2taGhChLuyZwZJo

 数額
 0.4403723035 MAN



8 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。

抵押交易分矿工节点抵押和验证节点抵押,抵押金额介于 1w 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。

> 矿工抵押



首先输入抵押金额和账户地址,解锁钱包,提交





生成并发送交易, 即完成抵押

查询抵押状态

查询抵押 輸入抵押账户地址				
MAN.3Ugik7ZsLoaNgX51kCJEWz1ZjxQgW				
man.sugik/2stodingAsikeJcw212jxQgw				
查询抵押				
抵押金额(V	/EI) 10006482041616466643284			
节点地址 MAN.3Ugik7ZsLoaNgX51kCJEWz1Zj×QgW				
抵押状态	Set to mining node			

▶ 验证者抵押

抵押竞选类型选择 Validator Deposit,其他步骤同"矿工抵押"



查询抵押状态



查询抵押

输入抵押账户地址

MAN.2skMrkoEkecKjJLPz6qTdi8B3NgjU		
	查询抵押	
抵押金额(WEI)	400258281034465847554944	
节点地址	MAN.2skMrkoEkecKjJLPz6qTdi8B3NgjU	
抵押状态	Set to validator node]

▶ 退选

如果用户想退出抵押,可以选择退选



解锁钱包完成交易

▶ 查询退选后的抵押状态:展示在多少块高退选

查询抵押

输入抵押账户地址





▶ 退款

退款后等待 600 块即可执行退款交易

抵押交易 © 退选抵押交易 Dease select deposit withdrawal deposit refund

退款即时生效,抵押状态消失



9 AI 交易

用户在交易中上传自己的图片或医疗影像资料,会自动通过 AI 服务器进行分析处理,然后用户可以在区块链浏览器中按照 html 格式显示这笔交易及 AI 分析处理结果。

通过钱包发起交易时,请求处理的图片资源不同,AI 服务器收到交易信息后就会提供不同的处理服务,包括:AI 姿态识别、AI 物体识别和 AI 医疗诊断

> AI 姿态识别: 人体姿态智能检测, 对图片中人体的不同部位进行检测和标识

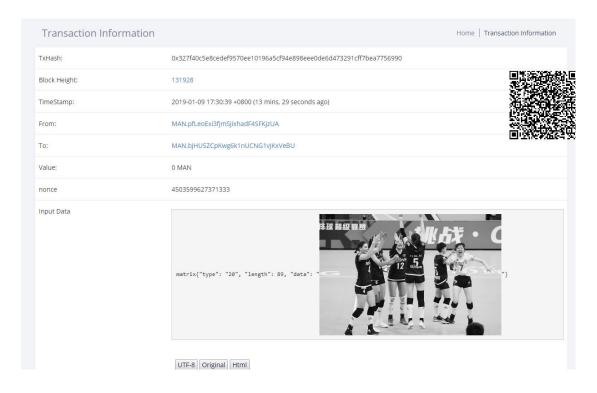
登录网页钱包进入 AI 交易界面,选择姿态识别

钱包首页 在线交易	离线交易 授权委托 取消委托 撤销交易 Check TX Status 抵押交易 代启节点 Al交易 转换工具
AI交易	
AI交易类型:	※姿态识別 物体识别 医疗诊断
上传数据:	请选择上传文件*
	0%

选择图片文件上传

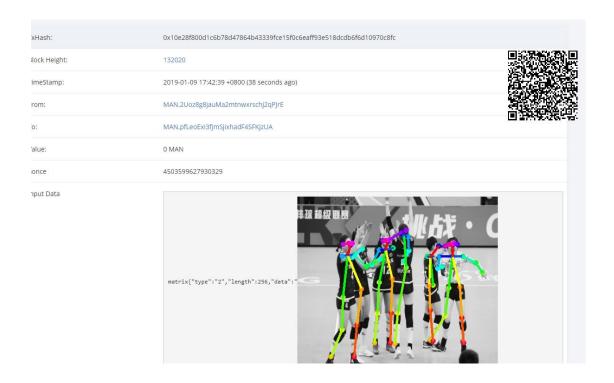
生成并发送交易,记住交易 hash 在浏览器中查询





等待数秒钟后, AI 服务器会返回处理结果

可以看到,处理后的图片是通过另一个自动触发的交易实现的。而这个交易的 from 地址是 AI 服务器的统一地址, to 地址则是原始交易中的 from 地址





AI 物体识别:智能对象识别,对图片中物体进行检测,并提供与其他物体的相似度

发起交易方式同"姿态识别", 交易类型要选择"物体识别"

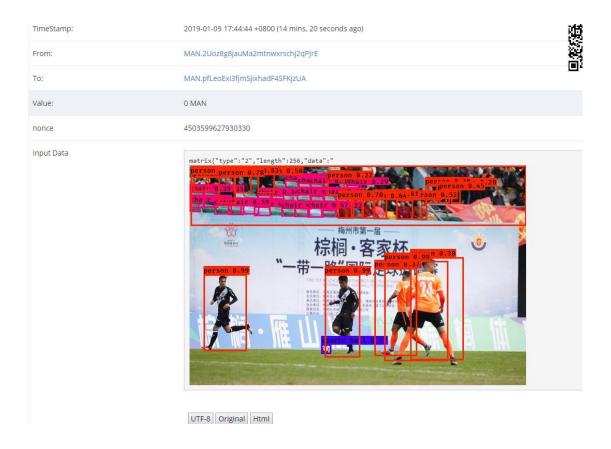
AI交易				
AI交易类型:	□姿态识别	☑物体识别	□医疗诊断	

处理前的图片



处理后的图片





➤ AI 医疗诊断

登录网页钱包,选择 AI 交易

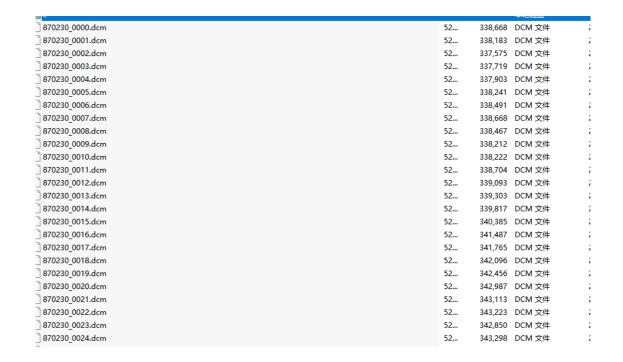


选择一种方式解锁钱包

钱包解锁后进入交易界面后,选中"医疗诊断"



选取并上传指定格式的压缩文件 (文件要包含完整的一套医疗影像的 dcm 文件)



生成并发送交易,复制生成的 hash



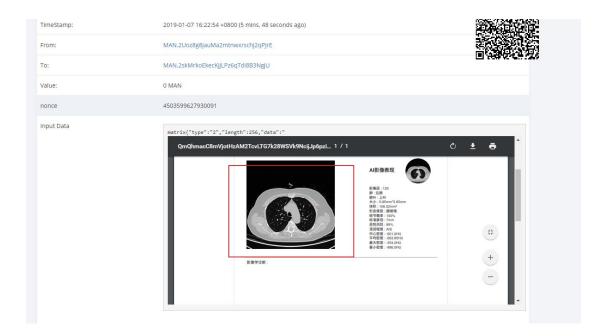
Your TX has been broadcast to the network. This does not mean it has been mined & sent. During times of extreme volume, it may take 3+ hours to send. 1) Check your TX below. 2) If it is pending for hours or disappears, use the Check TX Status Page to replace. 3) Use [MAN Gas Station] to see what gas price is optimal. 4) Save your TX Hash in case you need it later:

| Ox182dbfd03a40c45fdb9e6f6ff945199d3e9ba2b4592071cdb05e2cbd81872e7b



等待 15 分钟左右, 会返回处理结果 (可以通过 hash 查询 – 与姿态识别和物体识别一样, 交易发送方是 ai 处理交易的接收方; 也可以在浏览器的 AI 交易分类下查询)

Hash: 0xff6f8034a9ed524f0c8ca1421c12359d2346ab5d53c28732b2a7396c93eafedd



注:目前支持肺部诊疗影像的处理



10 创建多币种

1. 首先在"转换工具"下,输入 MAN 地址和币种名称,点击转换



- 2.记下生成的新币种地址,进入"创建币种"界面
- 3.创建币种需要余额大于 10 万 MAN 币 (如果系统中币种超过 100,则需要 9.5 万,依次衰
- 减)的钱包地址进行解锁,10万自动转给指定账户
 - 4.输入刚刚生成的币种名称和地址,填写交易金额进行创建



5. 创建完成后,可以在交易界面币种下拉列表中看到刚刚生成的币种







11合约

通过钱包的合约功能, 您可以在 MATRIX 主链上创建 token

进入"合约"模块,从您实现编译好的合约代码中复制出 byte code 部分, 粘贴到 Byte Code 框中 (合约交易附带的数据很多, gas limit 尽量设置大一些):

\$6115\$\$57600886f35b601860008473ffffffffffffffffffffffffffffffffffff	
s Limit:	
99999	

选择一种钱包解锁方式来解锁钱包,然后点击"签名交易",然后点击"部署合约"

Gas Limit:	
3000000	
	签名交易
未生效交易	签名交易
{"nonce":"0x1000000000000000", "gasPrice":"0x0430e23400", "gasLimit":"0x2dc6 c0", "value":"0x00", "data":"0x60806040526012600255600254600a0a60035560126 00a0a60045573698022a4b9245f58b8da4161ab6c7a4226dc9d11600560006101000a815 48173ffffffffffffffffffffffffffffffffffff	0xf91d928710000000000006859430e23400832dc6c08080b91d2d608060405260126002 55600254600a0a6003556012600a0a60045573698022a4b9245f58b8da4161ab6c7a4226 dc9d11600560006101000a81548173ffffffffffffffffffffffffffffffffffff
	部署合约

交易成功后会返回一个合约地址,记录这个地址



Your TX has been broadcast to the network. This does not mean it has been mined & sent. During times of extreme volume, it may take 3+ hours to send. 1) Check your TX below. 2) If it is pending for hours or disappears, use the Check TX Status Page to replace. 3) Use [MAN Gas Station] to see what gas price is optimal. 4) Save your TX Hash in case you need it later:

0x15bab63acb0aaed9237959bf0bb8695558acfd80a195aca8t7192ad18ddf0366
View your transaction & Contract Address MAN.39mZaejH7jHUt3MTTrkjiXCTmQS47

返回首页点击添加 token,填入合约地址,代币符号(代币名称),小数点位数(默认填写 18),



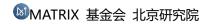
点击 "保存"。会提示 token 添加成功



进入交易页面,可以选择刚刚创建的 token

发送交易





12黑名单

MATRIX 有权对违规的账户、需要特殊对待的账户加入黑名单中做特殊处理。被加入黑名单的账户无法发送交易,但仍可以接受转账

有资格加黑名单的账户地址会提前写在配置文件 man.json 中

点击"黑名单"进入



生成并发送交易后,指定地址即被添加到黑名单中,禁止发起交易