

# MATRIX 网页钱包手册

版本: V1.2

作者: MATRIX 基金会北京研究院

日期: 2019.4.1



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	ā	₹	1
变	更证	<b>己录</b>	3
1	3	言	1
	1.1	文档用途4	1
	1.2	术语4	1
2	铥	<b>浅包概貌</b>	5
3	ê	<b>]建新钱包账户</b>	3
4	3	Σ易11	1
	4.1	即时交易1 <sup></sup>	1
	4	.1.1 一对一即时交易11	1
	4	.1.2 一对多即时交易1:	3
	4.2	定时交易15	5
	4	.2.1 一对一定时交易15	5
	4	.2.2 一对多定时交易16	3
	4.3	撤销交易16	3
5		<b>号线转账18</b>	3
6	ĭ	设置2′	1



(	6.1	关联钱包	21
(	6.2	地址转换	24
(	6.3	私钥备份	25
(	6.4	KEYSTORE 备份	25
7	绿(	色挖矿	26
-	7.1	挖矿收益	26
-	7.2	竞选节点	26
-	7.3	二次秘钥	29
8	ΑI	应用	30
9	创系	建多币种	36
10	合约	约	38



# 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	<ol> <li>1.抵押交易部分更新, 去除 nodelD</li> <li>2.合约部署与交互</li> <li>3. AI 交易</li> </ol>	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		
2019.4.1	新版钱包	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

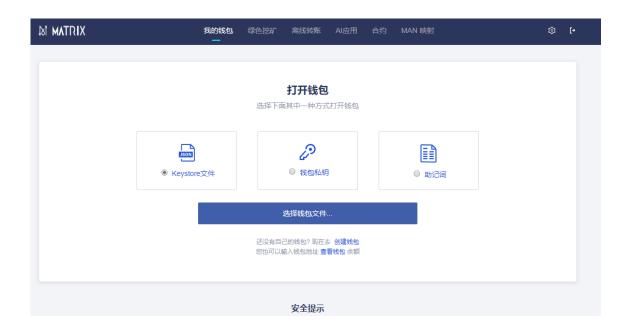
本文档针对 MATRIX 网页钱包的使用做了详细说明,方便用户快速入门和掌握。

### 1.2 术语

术语	<b>备注</b>



## 2 钱包概貌



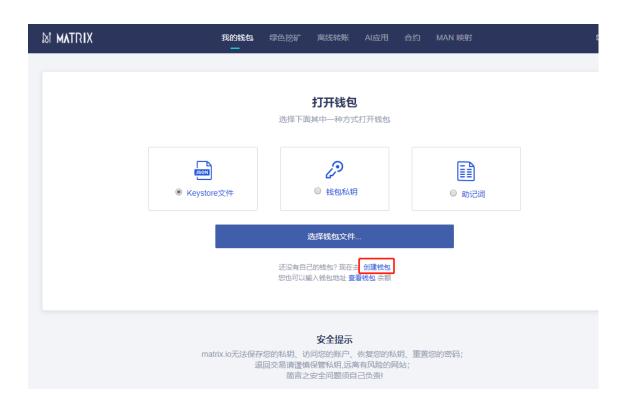
#### 可以看到,新版钱包有六大部分组成

- 我的钱包:可以创建新钱包或者查看自己的钱包信息。想发起一笔交易,需要进入我的钱包后进行操作
- 绿色挖矿:完成节点抵押、二次秘钥、查看挖矿收益等
- 离线转账: 支持您在离线状态下解锁钱包(上传私钥或 keystore), 这样您的私钥或 keystore
   不会暴露在网络中,提高资产安全
- AI 应用:上传图片进行 AI 处理,支持肺癌诊断、姿态识别和物体识别
- 合约:在 MATRIX 主链上部署智能合约,例如,发币等
- MAN 映射:支持将您的 MAN 资产从以太坊映射到 matrix 主链
- 设置:可以进行地址关联 (账户间代付 gas)、地址转换、私钥备份、keystore 备份等



## 3 创建新钱包账户

1. 如果您第一次使用我们的网页钱包,请先点击"创建钱包"+"一键创建钱包"



#### 创建钱包

MATRIX钱包是一款去中心化网页版钱包, 我们不会存储您的任何信息及密码, 所以创建成功后请妥善保管您的keystore或私钥, 若丢失无法找回!



目前提供了三种创建钱包的方式: Keystore 文件、私钥和助记词

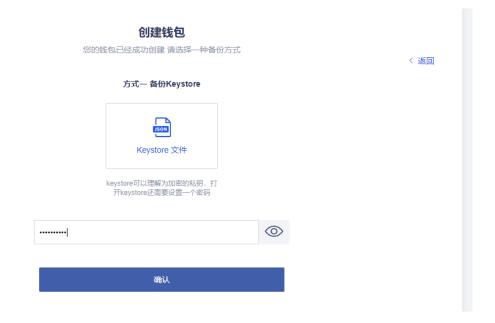


#### 创建钱包

您的钱包已经成功创建 请选择一种备份方式



2. 第一种钱包创建方式: `Keystore 文件` (需要输入一个密码)



3. 下载并保存 keystore 文件,然后点击"已下载,下一步"



创建钱包	
您的钱包已经成功创建 请选择一种备份方式	〈 返回
方式— 备份Keystore	
USON	
Keystore 文件	
keystore可以理解为加密的私钥,打 开keystore还需要设置一个密码	
下载keystore文件	
已下载,下一步	

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!

- 4. 设置问候语: 您可以根据自己的需要设置属于您的温馨问候语
- 5. 第二种钱包创建方式: 私钥, 复制并妥善保管自己的私钥



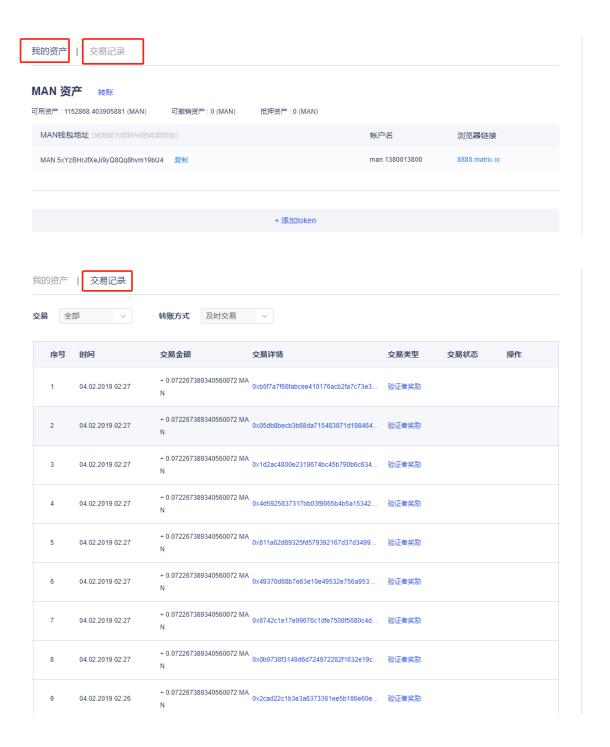


- 6. 点击"我已保管好私钥"进入下一步
- 7. 这里同样可以设置一个问候语
- 8. 第三种钱包创建方式: 助记词, 复制并妥善保管助记词



9. 解锁钱包后,可以进入资产页面,查看资产信息和过往交易记录

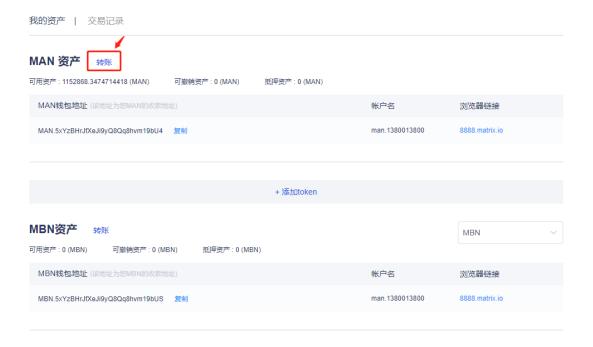






### 4 交易

打开钱包后,点击"转账"进入转账(交易)页面:



### 4.1 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

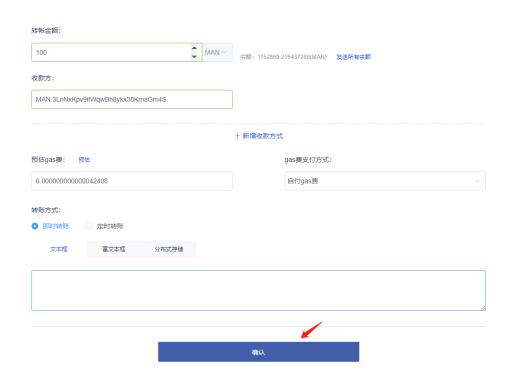
#### 4.1.1 一对一即时交易

向单个账户地址进行转账交易:

- 输入收款方地址
- 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"预估"可以估算要支付的 gas 费用



- 选中 `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 `确认`



#### 依次确认交易信息后:





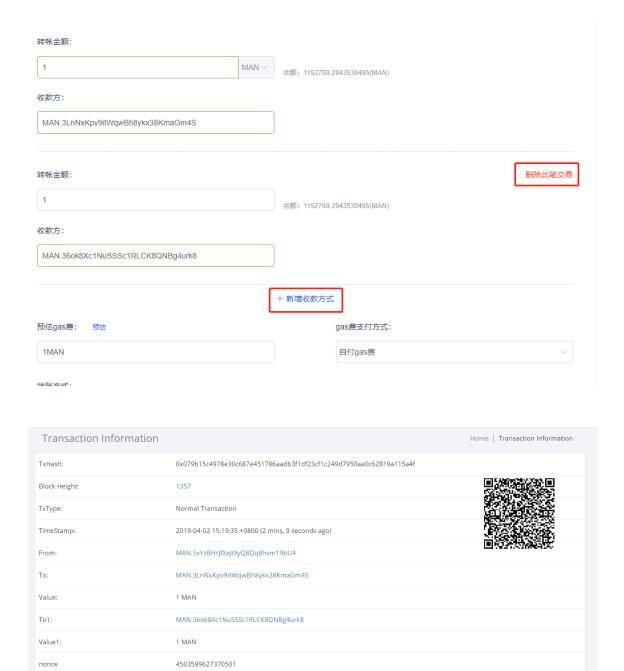
#### 交易信息可以在账户的交易记录里或通过账户地址在浏览器中查看



#### 4.1.2 一对多即时交易

MATRIX 网页钱包支持一对多交易(点击 '+新增收款方式'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):





其他操作同一对一交易,不再赘述。



#### 4.2 定时交易

定时交易是指,在指定时间(高度)真正完成转账

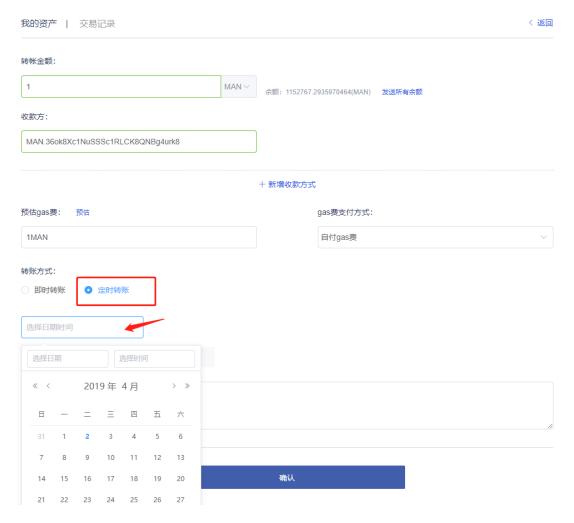
请注意:交易会在当时上链,而交易双方账户的余额变动会在指定时间完成。定时交易在 24 小时内都可以撤销

定时交易发送后,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



#### 4.2.1 一对一定时交易

钱包解锁及交易发起步骤同'4.1.1 一对一即时交易',转账方式需要选择'定时交易'



在交易记录里通过转账方式"定时交易"查询这笔交易

#### 4.2.2 一对多定时交易

钱包解锁及交易发起步骤同'4.1.2一对多即时交易',交易类型需要选择'定时交易'

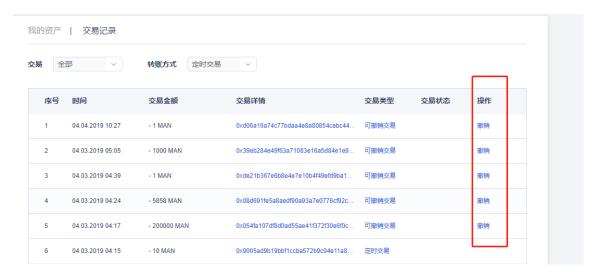
### 4.3撤销交易

所有定时交易在 24 小时内皆可撤销,撤销后,可撤销账户的余额会返回主账户。

注意:撤销交易只可以撤销自己发送的定时交易

进入交易记录界面,选择"定时交易"



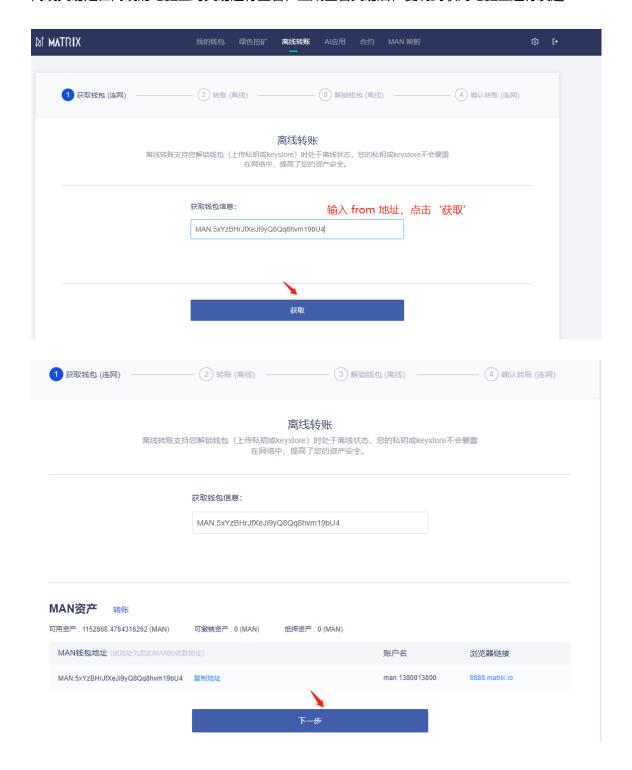


找到想撤销的交易,在对应的操作一栏中选择"撤销"即可



## 5 离线转账

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



点击 "下一步" 进入转账界面。此时请断开网络连接,并根据需要填写交易信息





#### 保持断网状态下,解锁钱包



联网状态下确认转账交易



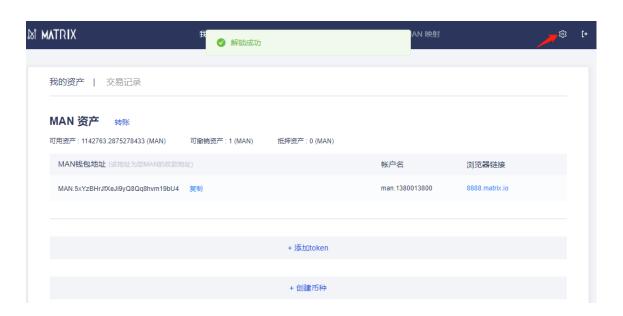


等待交易上链即可



## 6 设置

设置需要在解锁钱包后才可进行操作



### 6.1 关联钱包

关联钱包是一种委托行为,即,被关联的钱包在指定条件下发起的交易由关联方支付 gas 费

注意: 当被关联钱包发起转账交易时, 需要选择 "代付 gas"





#### 填入要关联的钱包地址

#### 选择一种关联方式:

● 块高:在指定的块高范围内,关联有效

● 时间:在指定的时间范围内,关联有效

● 次数:指定授权的次数

添加关联之后,可以在取消关联里查看

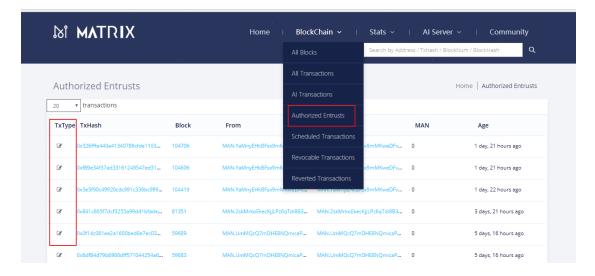




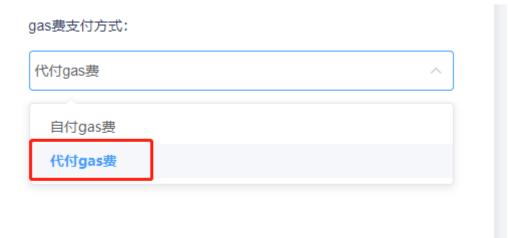
选中一条记录,可以取消关联



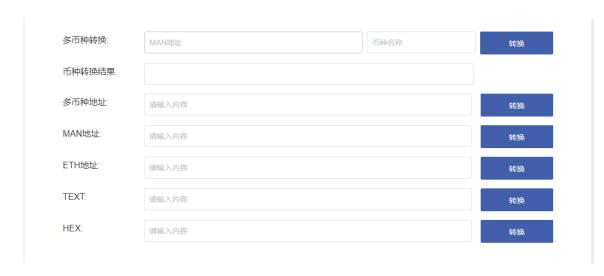
#### 交易上链以后,可以通过区块链浏览器 Authorized Entrusts 来查询



#### 完成委托后,即可在转账交易中选择"代付 gas 费"



### 6.2 地址转换





## 6.3 私钥备份

#### 私钥备份

私钥是一份随机生成的 256 位二进制数字

0x3ec3678077a79400081e525f516d722bce7d19f80b7288d09 **复制** 我已保管好私钥

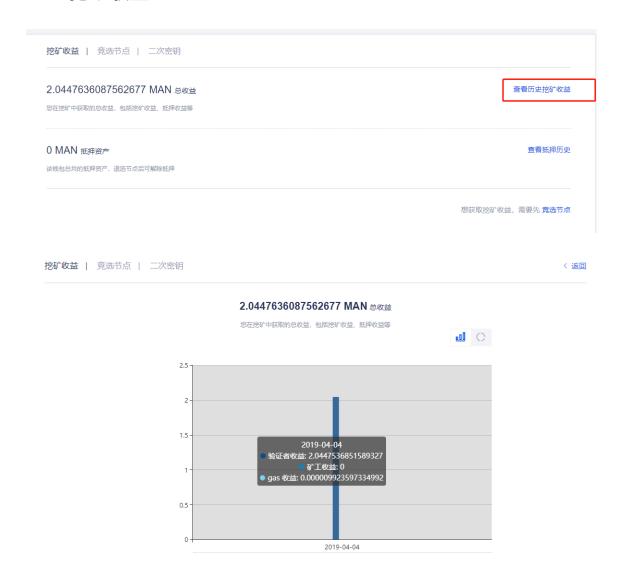
# 6.4 Keystore 备份





## 7 绿色挖矿

### 7.1 挖矿收益



### 7.2 竞选节点

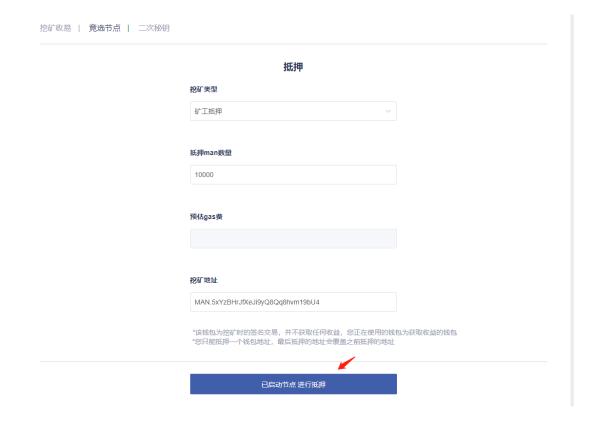
申请成为 MATRIX 区块链的矿工或验证者,需要抵押一定的 MAN 币。

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。

#### 抵押



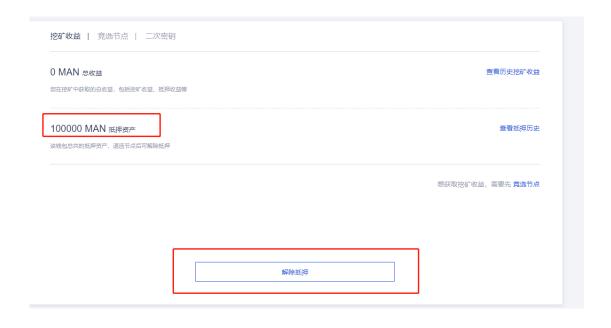
#### 解锁钱包后进入绿色挖矿界面:选择矿工抵押或验证者抵押



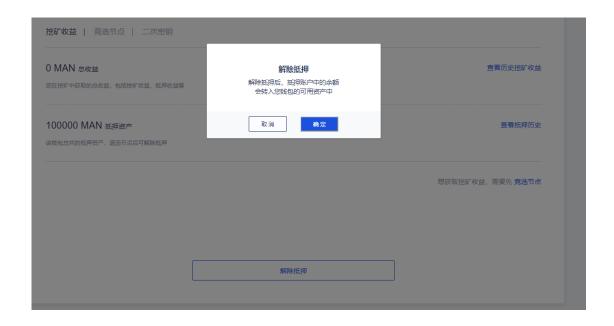
完成抵押后,可以在挖矿收益界面查看相关的记录,包括抵押状态、解除抵押、金额、抵押历史

#### 退选

在挖矿收益界面,可以通过点击"解除抵押"来退选





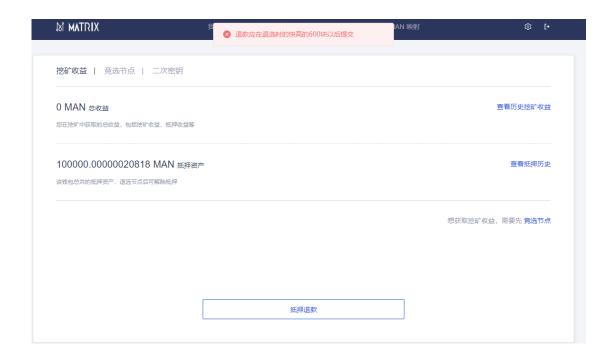


#### 退款

退选后 600 块才能发起退款, 如果未到 600 块, 会有错误提示







### 7.3 二次秘钥

挖矿打包区块时,可授权其他钱包代替挖矿钱包签名,保障获得收益钱包的安全





### 8 AI 应用

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



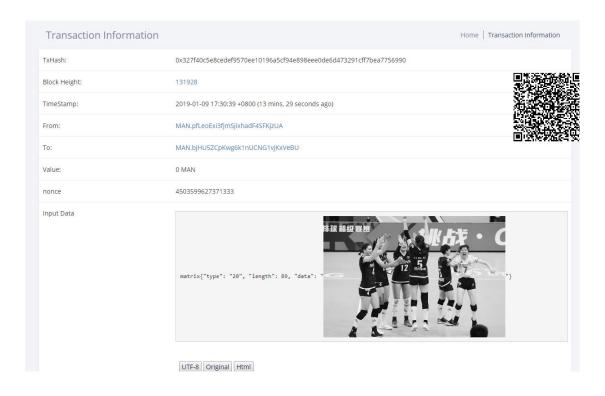
> AI 姿态识别: 人体姿态智能检测, 对图片中人体的不同部位进行检测和标识





#### 选择图片文件上传

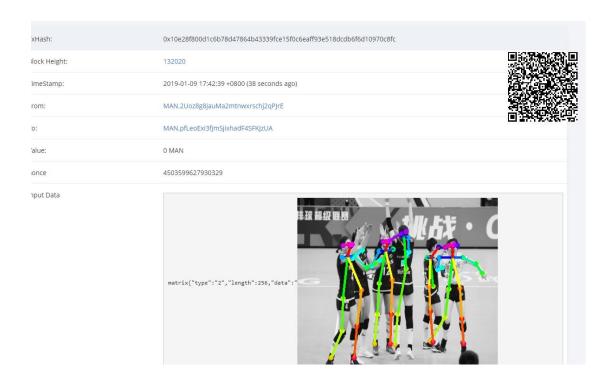
#### 生成并发送交易,记住交易 hash 在浏览器中查询



#### 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"

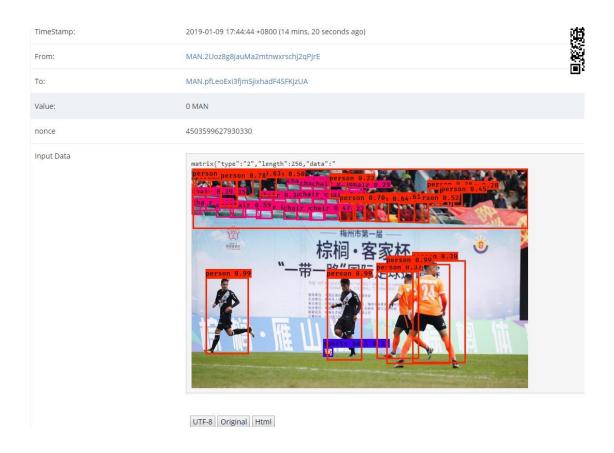


处理前的图片





#### 处理后的图片



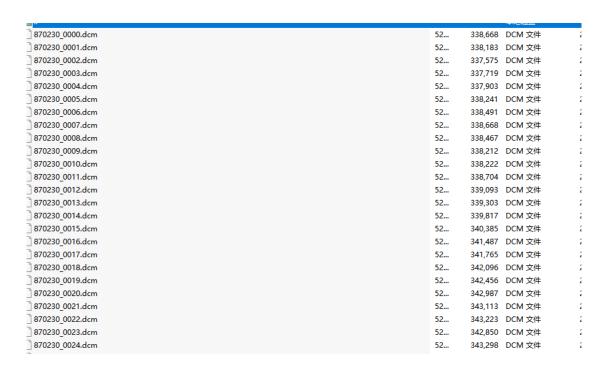
#### ➤ AI 医疗诊断



钱包解锁后进入交易界面后,选中"医疗诊断"



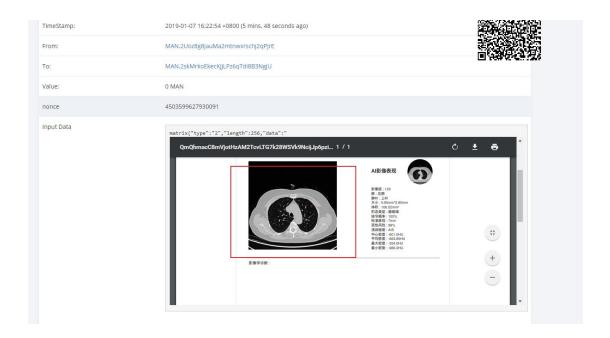
选取并上传指定格式的压缩文件 (文件要包含完整的一套医疗影像的 dcm 文件)



生成并发送交易,复制生成的 hash

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)



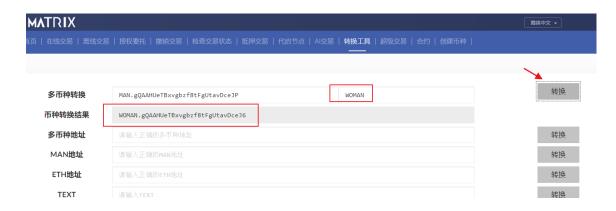


注:目前支持肺部诊疗影像的处理

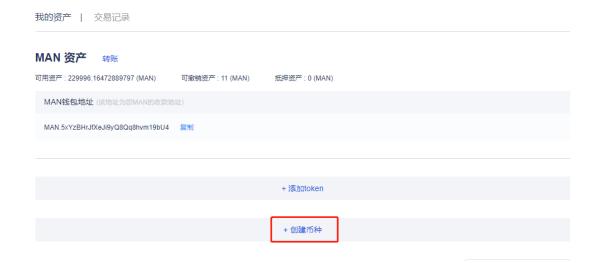


## 9 创建多币种

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



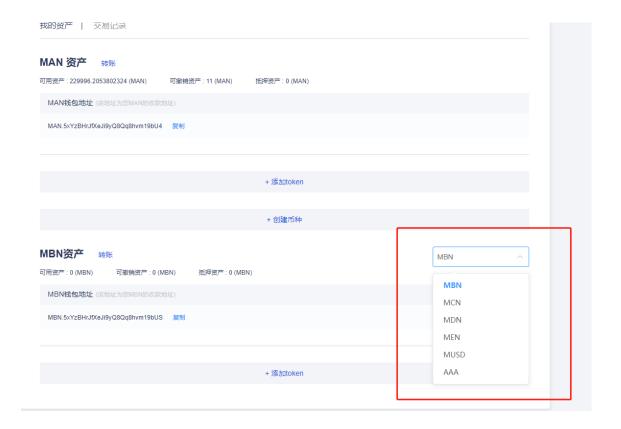




#### 点击确认创建

- 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
- 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



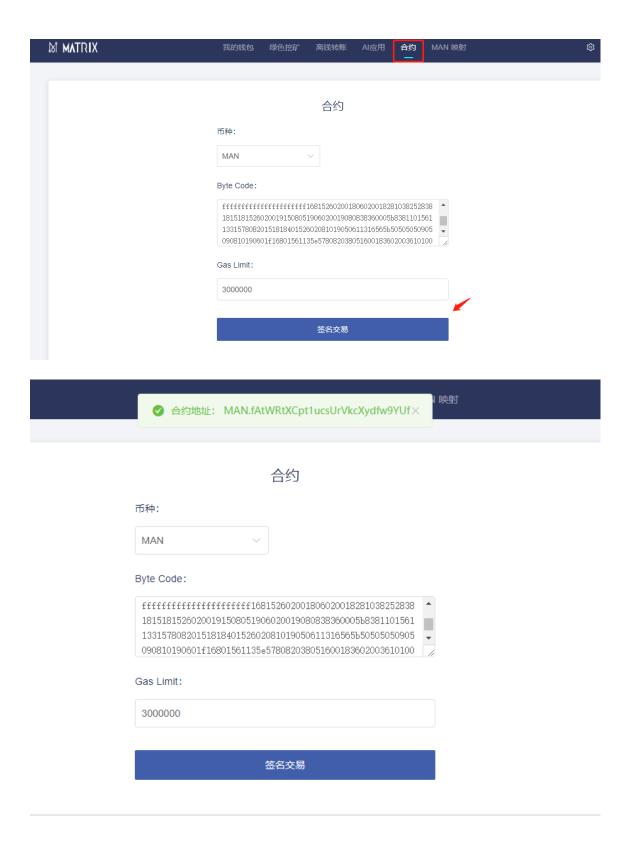


# 10合约

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):

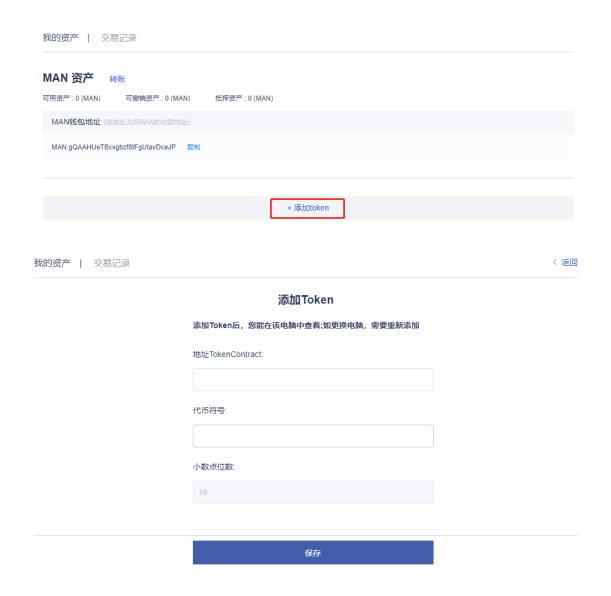




交易成功后会返回一个合约地址, 记录这个地址

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

