区块链隐私之忧

——隐私利器RAILGUN

谁适合看这篇教程？

- 墙内、体制内战友
- 关注隐私安全，想在区块链上隐藏交易记录的人
- 需要大额入金且不希望交易轨迹被发现的人
- 各行业的名人、大佬

何为隐私问题？

在之前的区块链概念中，我提到过，钱包地址是匿名的，正常转账时，其他人或政府机构无法直接知道你的身份。
只有掌握助记词的人才能访问钱包，而区块链系统只认助记词生成的密码，而不认具体个人。那么，为什么仍然需要隐私保护呢？

资金的流入都有来源。当我们用法币入金时，政府通常出于税收等考虑，要求交易所记录所有入金者的个人身份信息，即 KYC（了解你的客户）。

如今，几乎所有中心化交易所都要求完成 KYC 认证后才能入金。一旦你完成 KYC 并入金，你的资金流向就能被交易所追踪。当你将资产从交易所提取到个人数字钱包时，你的钱包地址实际上已在某种程度上与 KYC 信息绑定。

如果你使用的是某国的交易所，该国政府通常可以通过交易所查询你的交易情况，包括得知你的去中心化钱包地址，以及和该地址相关的所有交易记录。如果你的资金涉及商业机密，自然不希望泄露；如果你从事的是灭共事业，更不愿让个人信息外泄。

有需求就一定会有解决方案。这个世界出了个CCP，也就诞生了郭文贵先生，同样诞生了我们这群跟随灭共的人。面对区块链的透明性，有人提出了混币方案，以打破这种透明性，实现更好的财务隐私。

隐私匿名的基本原理

十分类似古代钱庄，不同人将大量的资金存到一个地方然后再各自取出。
首先你存入一笔银两，钱庄会给你相应额度的银票；这个银票只有你，之后你换个身份，拿着之前的银票去兑银两（钱庄只认银票不认人）
经过这么一存一取，外部观察者将无法直接关联某笔资金的真实拥有者

这就是实现区块链隐私的一个简单逻辑，下面我们讲讲具体如何来做。

区块链隐私匿名利器RAILGUN

不管你的链上资金来自中心化交易所，还是通过点对点入金，RAILGUN都能帮你实现真正的链上隐私。

RAILGUN是一个智能合约系统，可以把它理解成一个“虚拟保险箱”。它有两个关键操作Shield（存入）和Unshield（取出）

Shield（存入）：把资金存进去，就像用盾牌把它遮挡隐藏起来，一旦存入RAILGUN会给你提供一个“存款凭证”。外人可以看到你存入的钱包地址、时间和具体金额。一旦存入，外人就无法再追踪该笔资金的去向，包括这笔资金有没有取出，转到了哪个账号，甚至有没有人挪用了这笔资金，都无从知晓。

Unshield（取出）：你用“存款凭证”取出资金，RAILGUN会把钱转到指定地址。区块链上能看到出款时间和金额，但依然无法追踪资金来源。
RAILGUN 只认凭证不认人，只有拥有零知识证明的存款凭证，才能取出资金。

RAILGUN不像Tornado Cash被制裁，你可以证明你的资金合法性。另外你的资金始终是在你的账户上，并不会和他人自己混合，严格说它也不是混币，只是给你添加隐私匿名功能。
官网：http://railgun.org（据说区块链界大名鼎鼎的V神也在用）

RAILGUN 隐私化交易实战

下面我将一步步教你如何用RAILGUN进行匿名交易

准备工作

首先你的数字钱包里已经有数字货币，可以是交易所充值，也可以是线下对敲的。

安装一款RAILGUN钱包（下面以railway钱包为例）

如果railway失效了大家可以在RAILGUN官网找其它钱包，支持RAILGUN这个智能合约调用的钱包

iPhone用户

AppStore搜索railgun（不是Railway 非中国区）

或通过官网 railgun.org-> 点WALLETS菜单 -> 选择 Railway Wallet -> 点DOWNLOAD -> 点Railway Mobile iOS

Android 用户

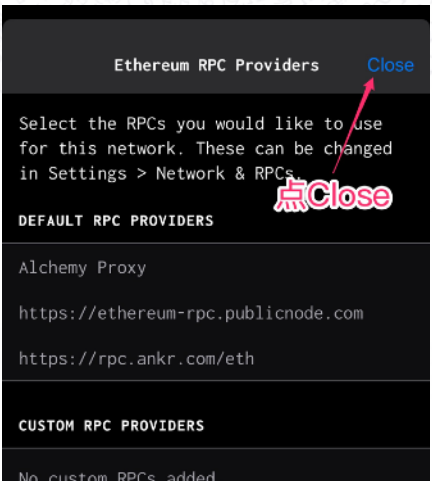
通过官网 http://railgun.org -> 点WALLETS菜单 -> 选择 Railway Wallet -> 点DOWNLOAD -> 点 Railway Mobile Android -> 选Android APK （直接能下APK这个非常友好）

创建隐私钱包

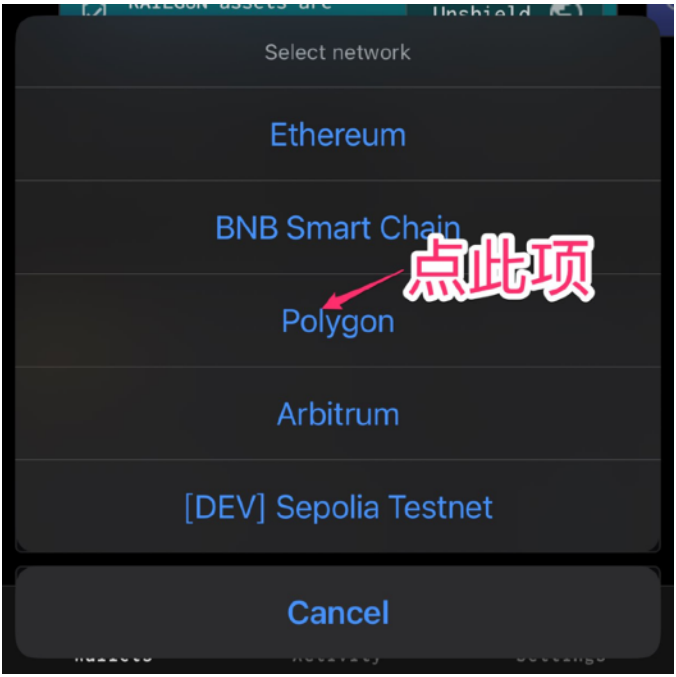
目前RAILGUN支持以太坊、Polygon、Arbitrum和币安链这几条链。我喜欢选Polygon和Arbitrum因为做隐私匿名需要不少费用，这两个链的手续费会比以太坊低不少。

下面以Polygon链POL币（之前叫MATIC）为例。（也支持其他代币比如USDT，USDC，你需要保证足够的Gas费，以Polygon为例，金额大可以考虑用USDT来做，资金流量大一些）

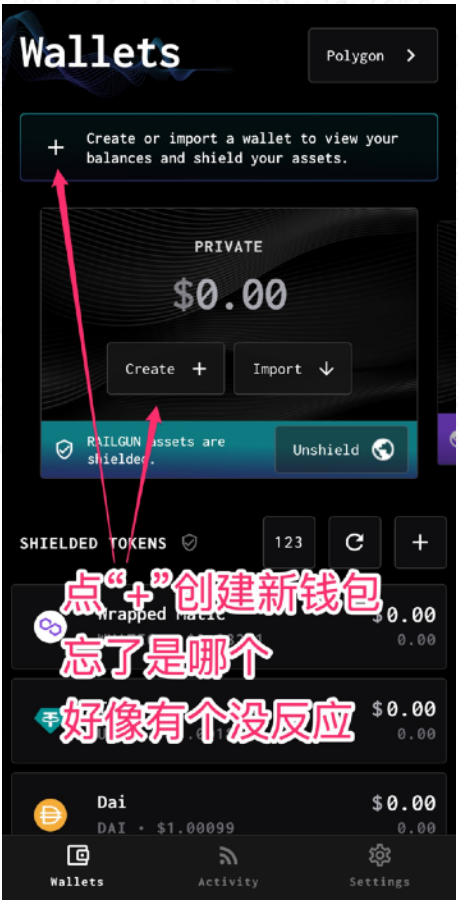
1、打开Railway APP，等待加载完成，点Close，默认区块链是以太坊（大额可以选以太坊，考虑手续费可以选Polygon和Arbitrum）



2、点右上角Ethereum -> 弹出对话框，选Polygon -> Polygon RPC Providers 选 Close即可 -> 右上角已变成Polygon



3、点“+”创建钱包（不建议导入已有钱包）
即使查到也可以说钱包被盗，直接用自己钱包做隐私，那就无法解释，要给别人枪口抬高一寸的机会
也可以通过Settings -> Wallets -> 点右上角”+“ 来创建



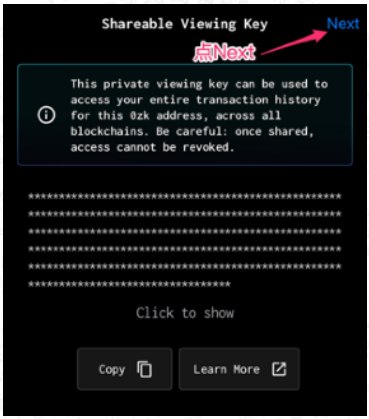
4、取个名字 -> 点击“Create”（根据用途取）

5、把助记词它抄下来（抄在本子里，不要抄在纸上）-> 点“Next”

这组助记词“**最好不要丢**”，未来可以用来是证明你资金合法合规

6、Shareable Viewing Key -> 这个暂时不用记，直接点”Next”

这个 Viewing Key 允许他人查看你的隐私钱包交易记录，不要随便给别人！一旦给出再也无法取消



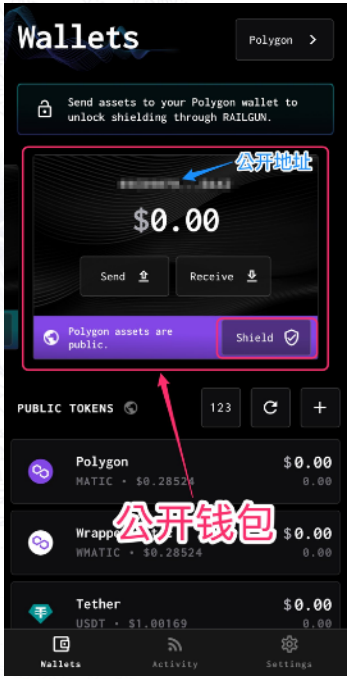
7、点“Finish” 进入Railway钱包主页

8、进入钱包主页

你会看到两个钱包地址卡片（左右滑动可以切换）

一个底部带unshield按钮，为隐私钱包账户，0zk开头的地址，只有你自己可见（任何第三方不可见）

一个底部带shield按钮，Polygon区块链上可见



隐私账户

- Send可以发送资产给其它隐私钱包地址
- Receive可以接收其他隐私钱包地址的资产，也可以接收公开钱包Shield到隐私钱包的资产
- Unshield可以将资产转给任何公开的钱包地址

公开账户

- Send是数字钱包正常的发送功能，可以发送给任何公开钱包地址
- Receive可以接收他人的公开转账，也可以接收隐私钱包Unshield的资产
- Shield可以将资产转到隐私钱包中

资金匿名化（Shielding）

创建好Railway钱包帐户后，我们就可以往里转入数字资产，进行隐私匿名化操作了

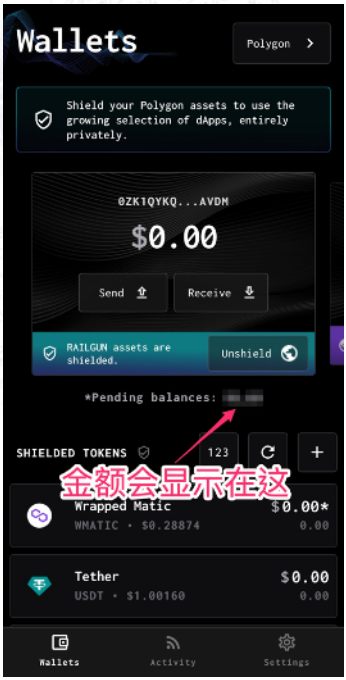
1、转账到Railway公开钱包：
切换到公开账户 -> 点击“Receive” -> 获得公开钱包地址（墙内一定要把钱转干净，伪造被盗现场）
用你其他的数字钱包转账到这个地址，我们教程仅以POL为例。
（注意看支持哪些币种，以Polygon为例支持USDC，USDT，MATIC（POL），Dai等，不在其罗列的币种里面最好不要转入，即使显示了如果你一个人在操作这个币，那没有任何隐私可言，我观察下来USDT来做的人比较多，如果在Polygon非POL请准备额外的Gas费）

2、切换到隐私钱包 -> 点击”Receive” -> Copy隐私钱包地址（地址是0zk打头）

3 、回到主界面 -> 切换到公开钱包 -> 点击Shield按钮 -> 点击左侧“MAX”按钮（也可以自己填具体数字） -> 再点右侧“SET” -> 再点“Next”

4、Review transaction界面 会显示需要匿名的金额，手续费，以及匿名后的金额，点击右上角“Shield” -> 会跳出关于Shielding的介绍（有时间可以仔细阅读一下）-> 点“Continue” -> 等待Shielding计算完成（此时并没有把你的资金匿名，只是帮你做了计算）

5、接下来会跳出对话框，让你等待1个多小时
（Railway会验证资金来源是否合规，同时帮你生成合规凭证）
此时金额并不会显示匿名钱包里，而是显示在匿名钱包底部，同时公开钱包里的资金已经扣除
你可以在Activity中查看相关记录状态
（如果你的资金来源有问题，那么你是无法完成这次Shielding）



6、等待1个多小时，资金会显示在匿名钱包里

资金公开化注意事项

接下来是要做资金公开化，在做资金公开之前我必须给大家普及一些注意事项：

1、存取必须使用不同的钱包地址，否则就是自欺欺人
2、杜绝“整存整取”，100%会被发现两个钱包的关联关系
3、避免“现存现取”，刚做的隐私匿名化，如果立即全部取出，即使换了地址也容易被人发现是同一个人
4、取钱不要取干净，一定要保留一部分余额，根据余额和手续费，以及转出金额，可以分析出绝对的关联关系

最佳实践：存入后分批次取，分不同日期间隔取，每次只取一部分，不要相同金额，保留部分余额，留作他用。

你甚至可以打开Polygonscan 搜索你的钱包地址，找到存入RAILGUN合约地址。
上看RAILGUN账户的出入金状况，来决定你提取的金额数量，你可以和别人提一样的金额，这样更有迷惑性。

未来区块链的审计一定是AI做的，我们即使做了隐私匿名化处理也很有可能被AI分析出来，所以不要做任何违法违规的事情。如果你隐私做的出色，AI只能分

析出两个账户的关联概率，并不能以此作为证据，证明另一个公开账户就是你本人的。

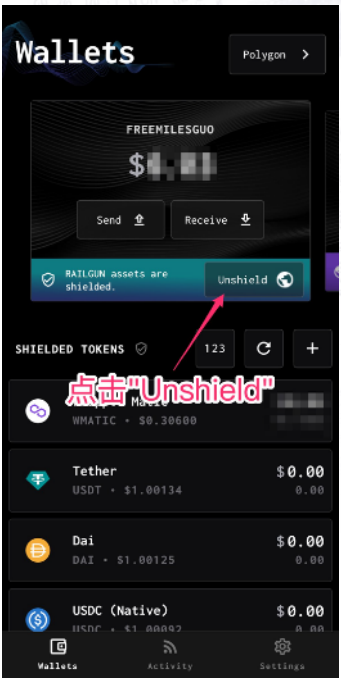
如果你什么都不做，那就是铁证如山的事情，区块链没有人能改变已经在链上的数据（CCP靠撒谎洗脑起家，区块链的时代就是灭共的时代🙏）

资金公开化（Unshielding）

前提：你已经完成资金匿名化

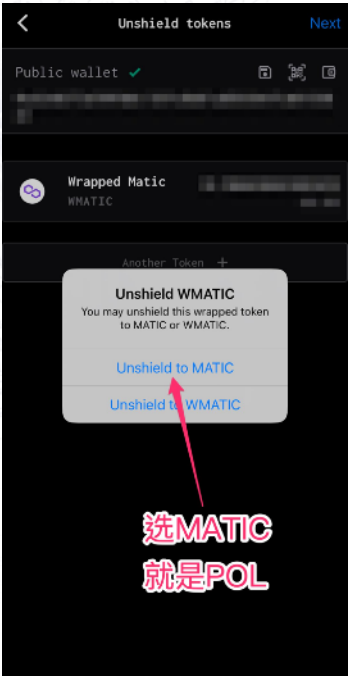
接下来我们要从隐私钱包里提取资金到公开的区块链钱包地址上

1、切换到隐私钱包 -> 点击“Unshield” -> 弹出Unshield tokens界面
在Public wallet下面输入框里粘贴公开提钱的钱包地址(不是存入的钱包地址)
在MAX右边的输入框中输入要提取的金额

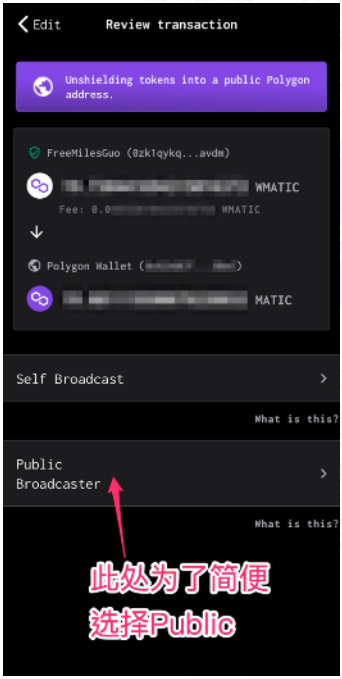


此处一定不能点MAX一次提完，至少要分两次以上提，否则前功尽弃
（提取金额数量最佳实践，请看资金公开化注意事项）

2、输入金额后点右侧的SET，再点右上角”Next” -> 弹出对话框选”Unshield to MATIC” -> 点右上角“Next”

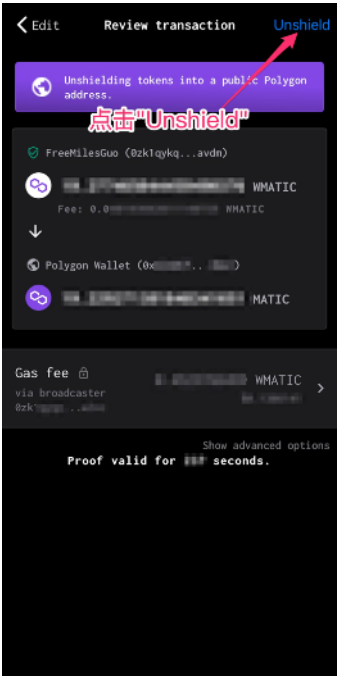


3、进入”Review transaction“，检查提取金额和交易费用 -> 点击“Public Broadcaster”，选择合适的节点，系统会计算Gas费用 -> 再点”Generate Proof”生成合规凭证后（凭证生成过程中不要关闭Railway）



此处选Self Broadcast是要从你自己的钱包里出gas费的（⚠️不能用存入的钱包地址来出gas费，那就是此地无银三百两了）
如果你的新钱包里有一部分匿名的钱，那么我更推荐Self Broadcast。Public其实是做了一次代理。

4、点右上角的“Unshield”，不要关闭Railway直到交易成功



这样就算大功告成，接下来想怎么浪就怎么浪，是买$TDCCP还是买灭共NFT，还是炒石头随你。

自由 我踏马来辣！
我们灭共，也要爱惜自己🙏
不要鲁莽，爱你们兄弟姐妹们💙