



初识以太坊

——钱包、测试网络和简单交易

2018.10



以太坊单位

- 以太坊的货币单位称为以太，也称为ETH或符号Ξ
- ether被细分为更小的单位，直到可能的最小单位，称为wei;
 $1 \text{ ether} = 10^{18} \text{ wei}$
- 以太的值总是在以太坊内部表示为以wei表示的无符号整数值。
- 以太的各种单位都有一个使用国际单位制（SI）的科学名称，和一个口语名称。



以太坊各单位名称

值 (wei)	指数	通用名称	SI 名称
1	1	wei	wei
1,000	10^3	babbage	kilowei or femtoether
1,000,000	10^6	lovelace	megawei or picoether
1,000,000,000	10^9	shannon	gigawei or nanoether
1,000,000,000,000	10^{12}	szabo	microether or micro
1,000,000,000,000,000	10^{15}	finney	milliether or milli
1,000,000,000,000,000,000	10^{18}	ether	ether
1,000,000,000,000,000,000,000	10^{21}	grand	kiloether
1,000,000,000,000,000,000,000,000	10^{24}		megaether



以太坊钱包

以太坊钱包是我们进入以太坊系统的门户。它包含了私钥，可以代表我们创建和广播交易。

- MetaMask：一个浏览器扩展钱包，可在浏览器中运行。
- Jaxx：一款多平台、多币种的钱包，可在各种操作系统上运行，包括 Android, iOS, Windows, Mac和Linux。
- MyEtherWallet (MEW)：一个基于web的钱包，可以在任何浏览器中运行。
- Emerald Wallet：旨在与 ETC 配合使用，但与其他基于以太坊的区块链兼容。



私钥、公钥和地址

- 私钥 (Private Key)

以太坊私钥事实上只是一个256位的随机数，用于发送以太的交易中创建签名来证明自己对资金的所有权。

- 公钥 (Public Key)

公钥是由私钥通过椭圆曲线加密secp256k1算法单向生成的512位 (64字节) 数。

- 地址 (Address)

地址是由公钥的 Keccak-256 单向哈希，取最后20个字节 (160位) 派生出来的标识符。



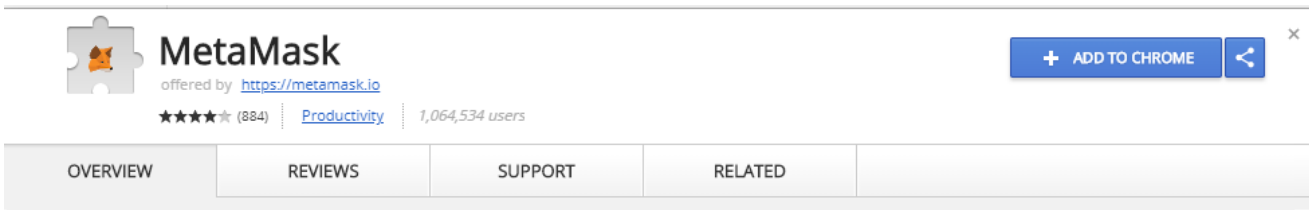
安全须知

- keystore文件就是加密存储的私钥。所以当系统提示你选择密码时：将其设置为强密码，备份并不要共享。如果你没有密码管理器，请将其写下来并将其存放在带锁的抽屉或保险箱中。要访问账户，你必须同时有keystore文件和密码。
- 助记词可以导出私钥，所以可以认为助记词就是私钥。请使用笔和纸进行物理备份。不要把这个任务留给“以后”，你会忘记。
- 切勿以简单形式存储私钥，尤其是以电子方式存储。
- 不要将私钥资料存储在电子文档、数码照片、屏幕截图、在线驱动器、加密PDF等中。使用密码管理器或笔和纸。
- 在转移任何大额金额之前，首先要做一个小的测试交易（例如，小于1美元）。收到测试交易后，再尝试从该钱包发送。



安装MetaMask

- 打开Google Chrome浏览器并导航至：
- <https://chrome.google.com/webstore/category/extensions>
- 搜索 “MetaMask” 并单击狐狸的徽标。您应该看到扩展程序的详细信息页面如下：

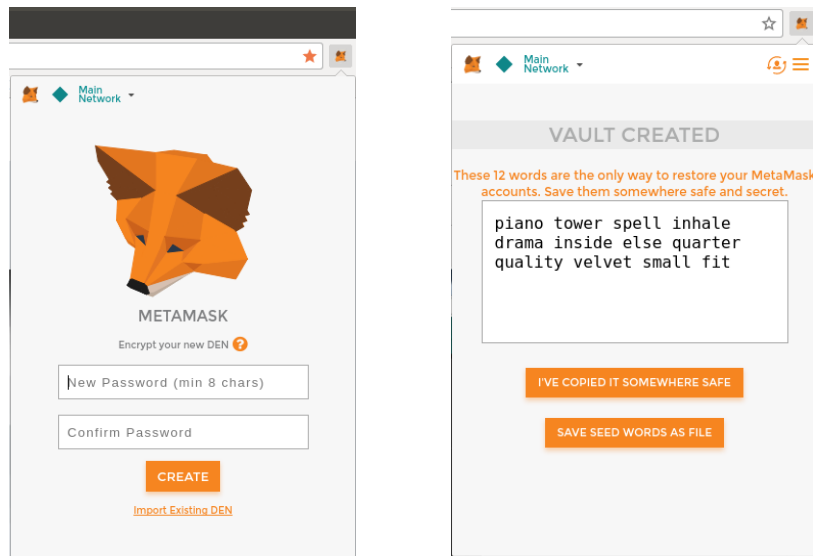


- 验证您是否正在下载真正的MetaMask扩展程序非常重要，因为有时候人们可以通过谷歌的过滤器隐藏恶意扩展。确认您正在查看正确的扩展程序后，请点击 “添加到Chrome”进行安装。



第一次使用MetaMask

- 安装MetaMask后，应该在浏览器的工具栏中看到一个新图标（狐狸头）。点击它开始。系统会要求接受条款和条件，然后输入密码来创建新的以太坊钱包：



- 设置密码后，MetaMask将生成一个钱包，并显示由12个英文单词组成的助记符备份。如果MetaMask或计算机出现问题，导致无法打开钱包，我们可以在任何兼容的钱包中使用这些单词来恢复对资金的访问。



怎样安全存储助记词

- 将助记词（12个单词）备份在纸上，两次。
- 将两个纸张备份存放在两个单独的安全位置，例如防火保险箱，锁定抽屉或保险箱。
- 要将纸质备份视为自己在以太坊钱包中存储的等值现金。任何能够访问这些单词的人都可以访问并窃取你的资金。



显示账户信息

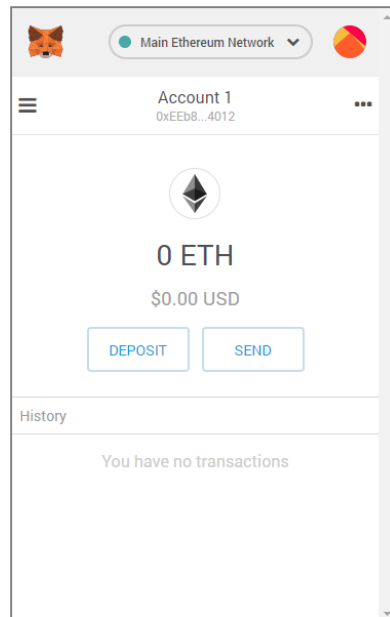
- 一旦确认已安全存储助记符，MetaMask将显示您的以太

坊帐户详细信息：

——账户名称：Account1

——以太坊地址

——账户余额：0 ETH





助记词

- 助记词是明文私钥的另一种表现形式，最早由BIP-39提出，目的是帮助用户记忆复杂的私钥（256位）。
- 技术上该提议可以在任意区块链中实现，比如使用完全相同的助记词在比特币和区块链上生成的地址可以是不同的，用户只需要记住满足一定规则的词组（就是上面说的助记词），钱包软件就可以基于该词组创建一些列的账户，并且保障不论是在什么硬件、什么时间创建出来的账户、公钥、私钥都完全相同，这样既解决了账号识记的问题，也把账户恢复的门槛降低了很多。
- 支持 BIP39 提议的钱包也可以归类为 HD 钱包（Hierarchical Deterministic Wallet），Metamask 当属此类。



切换网络

- **Main Network (Network ID: 1)**
 - 主要的、公共的，以太坊区块链。真正的ETH，真正的价值，真正的结果。
- **Ropsten Test Network (Network ID: 3)**
 - 以太坊公共测试区块链和网络，使用工作量证明共识（挖矿）。该网络上的 ETH 没有任何价值。
- **Kovan Test Network (Network ID: 42)**
 - 以太坊公共测试区块链和网络，使用 “Aura”协议进行权威证明 POA 共识（联合签名）。该网络上的 ETH 没有任何价值。此测试网络仅由 Parity 支持。
- **Rinkeby Test Network (Network ID: 4)**
 - 以太坊公共测试区块链和网络，使用 “Clique”协议进行权威证明 POA 共识（联合签名）。该网络上的 ETH 没有任何价值。
- **Localhost 8545**
 - 连接到与浏览器在同一台计算机上运行的节点。该节点可以是任何公共区块链（main 或 testnet）的一部分，也可以是私有 testnet。
- **Custom RPC**



获取测试以太

- 钱包有了，地址有了，接下来需要做的就是为我们的钱包充值。

我们不会在主网络上这样做，因为真正的以太坊需要花钱。

- 以太坊测试网络给了我们免费获取测试以太的途径：水龙头

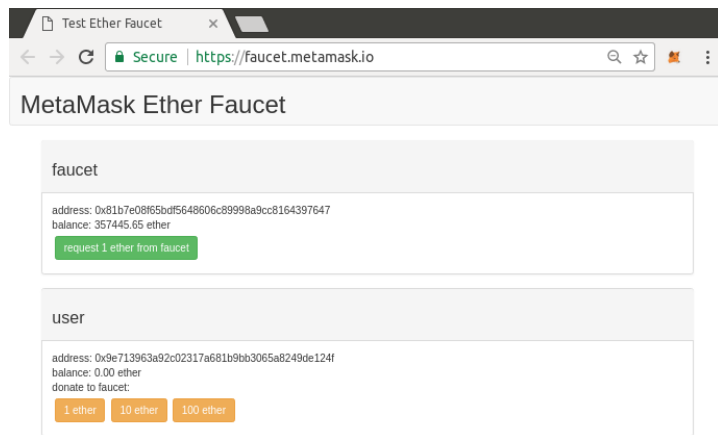
(faucet)

- 现在，我们将尝试把一些测试以太充入我们的钱包。



获取测试以太

- 将 MetaMask 切换到 Ropsten 测试网络。单击 “Deposit” ；然后单击 “Ropsten Test Faucet” 。 MetaMask 将打开一个新的网页：



- 按绿色 “request 1 ether from faucet”按钮。您将在页面的下半部分看到一个交易ID。水龙头应用程序创建了一个交易 - 付款给您。交易ID如下所示：

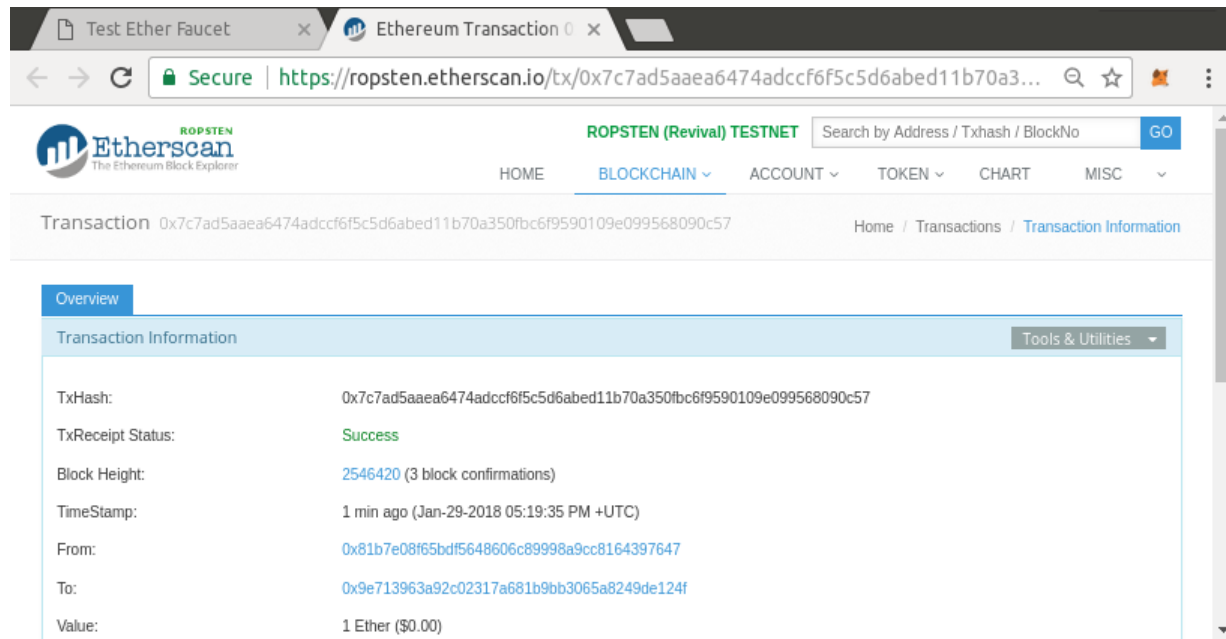
transactions

0xb53dcf15af8d86842c08e53474ed25beba17b122cccb7da77f559d3527c1b2f5



在区块浏览器中查看

- <https://ropsten.etherscan.io/>



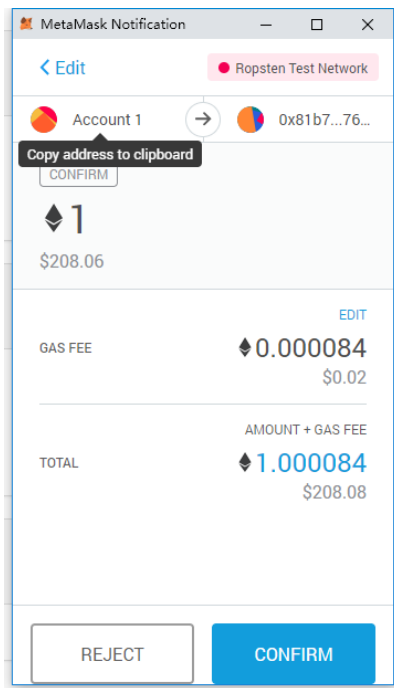
The screenshot shows a web browser window with two tabs: 'Test Ether Faucet' and 'Ethereum Transaction'. The address bar shows the URL <https://ropsten.etherscan.io/tx/0x7c7ad5aaea6474adccf6f5c5d6abed11b70a350fbc6f9590109e099568090c57>. The page header includes the Etherscan logo, the text 'ROPSTEN (Revival) TESTNET', a search bar, and navigation links: HOME, BLOCKCHAIN, ACCOUNT, TOKEN, CHART, and MISC. The main content area displays transaction details for the specified hash. The transaction is confirmed as 'Success' and includes details such as block height, timestamp, sender, receiver, and value.

Transaction Information	
TxHash:	0x7c7ad5aaea6474adccf6f5c5d6abed11b70a350fbc6f9590109e099568090c57
TxReceipt Status:	Success
Block Height:	2546420 (3 block confirmations)
TimeStamp:	1 min ago (Jan-29-2018 05:19:35 PM +UTC)
From:	0x81b7e08f65bdf5648606c89998a9cc8164397647
To:	0x9e713963a92c02317a681b9bb3065a8249de124f
Value:	1 Ether (\$0.00)



从MetaMask发送Ether

- 单击橙色 “1 ether”按钮告诉MetaMask创建支付水龙头1 ether的交易。
MetaMask将准备一个交易并弹出一个确认窗口：





Gas编辑选项

- Metamask 计算了最近成功交易的平均 gas 价格为4 GWEI
- 发送基本交易的 gas 成本是21000个 gas单位
- 花费的最大 ETH 量是 $4 * 21000$
GWEI = 84000 GWEI = 0.000084ETH
- 做 1 ETH 交易成本为 1.000084 ETH
- 从水龙头请求多一些的以太，如果有2个ETH的余额，我们就可以再试一次

Customize Gas



Gas Price (GWEI)

We calculate the suggested gas prices based on network success rates.



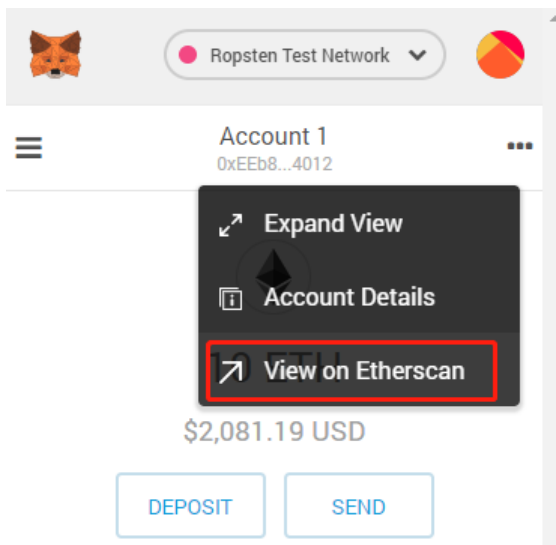
Gas Limit

We calculate the suggested gas limit based on network success rates.





搜索地址的交易记录



Address: 0xEEb8E564689Ddc6138263078bE00dec5E6AC4012

Overview

Balance: 9.999958 Ether

Transactions: 14 txns

Transactions

Latest 14 txns

TxHash	Block	Age	From		To	Value	[Tx Fee]
0xb53dcf15a08068...	426598	1 hr 27 mins ago	0xeeb0e564689ddc...	OUT	0xb1b7e08f5bd56...	1 Ether	0.000021
0x6a3b0524ec66fe...	4260513	1 day 35 mins ago	0xb1b7e08f5bd56...	IN	0xeeb0e564689ddc...	1 Ether	0.000021
0xb3e475bb5fc68ac...	4260356	1 day 1 hr ago	0xeeb0e564689ddc...	OUT	0xb1b7e08f5bd56...	1 Ether	0.000021
0x2d1d4242639cda...	4260319	1 day 1 hr ago	0xb1b7e08f5bd56...	IN	0xeeb0e564689ddc...	1 Ether	0.000021
0x23a7208effdc814...	4260315	1 day 1 hr ago	0xb1b7e08f5bd56...	IN	0xeeb0e564689ddc...	1 Ether	0.000021



Q&A



尚硅谷

