区块链生存训练

最易懂实用的区块链共创书籍

申龙斌

苏江 金炜 黄黎 苏耀勇 杨卫祥等　著

版本修改记录：

2018 年 2 月 28 日，发布 V2.0 版。

2017 年 10 月 12 日，发布 V1.0 版。

献给学习区块链技术、活在未来的朋友们。

目　录

2.0 版修订说明

2017 年 10 月 12 日，《区块链生存训练》1.0 版正式发布，一转眼四个多月过去了，币圈里流行一句话“币圈一天，人间一年”，在 1.0 发布之后的四个多月里，发生了许许多多的事情，国内交易所关闭、分叉泛滥、代币空投、私募盛行，期间也涌现出了一些优秀的海外交易平台，小白们想买入几个币又增添了几分障碍，因此原书中的一些内容已经跟不上形势的变化，必须要进行修订了。

上次汇编书稿是在 2017 年的国庆八天长假，这次的 2018 年春节长假也不能闲着，修订工作量仍然不轻，书稿由以前的 200 多页扩充到了近 400 页，主要有如下变化：

（1）由以前的五篇增加为七篇，其中一篇为脑力挖矿的内容，在以前 Steemit 的基础上增补了币问、币乎等内容；另一篇为投资实操篇，由挖矿、搬砖构成，加入了最新的公信宝、IPFS 挖矿的内容。

（2）增加了冷钱包、谷歌验证器、OTC 场外交易的内容以及场外交易防骗指南。

（3）增加了苏江 2018 年 1 月的一次线上分享内容“区块链投资生存指南”，还有其他朋友的投资感悟。

（4）竞争币中增加了 BIG 平台币，EOS 的内容中补充了地址映射的操作步骤。

（5）去掉了普通用户难以理解的椭圆曲线加密的算法细节；去掉了以前饭团的二维码；不时插入一些醒目的大字来强调某些重点内容；修订了一些读者反馈过来的错误；还有其它修改不再一一列举。

由于时间仓促，书中仍有许多错误或不完善的地方，请读者朋友们见谅。

1.0 版前言

初识比特币

2017 年，比特币和区块链异常火爆，很多人估计都从各种新闻媒体上听说了各种各样的消息，对于不了解区块链和比特币的人们来说，能够听懂的就是关于洗钱、非法集资等方面的负面传闻，但对于这个技术背后的原理一无所知。

我在 2016 年 7 月底的时候，无意间订阅了李笑来的《通往财富自由之路》专栏，也第一次听说了比特币，我以前学过的“绿灯思维”发挥了作用，当遇到一件新生事物时，不要根据自己的常识立刻下结论，先听别人说完，如果没有听懂，下来自己还可以搜索调查，再做出结论不迟。一念之差，可能就会错过很多精彩。

我随后买了《争议比特币》，并从知笔墨(zhibimo)下载了《精通比特币》，用几天时间快速翻完了这两本书，看得我那个热血沸腾啊。因为我大学本科读的是数学专业，以前看过密码学原理，并且有多年的编程经验，能够在较短的时间内理解其中的概念和原理。通货紧缩、去中心化、不可篡改性、可分割性、非对称加密等特性，让我后悔没有早一些发现它。

我用了三天时间，花了 100 元在 OKcoin 上跑通了安装钱包、开户、存入法币、交易、提币的全部流程，然后又买入 1 个比特币，当时感觉 4000 元/枚的价格真是高啊，现在回头望过去，可能这辈子它都无法再回到这个价格了。

区块链生存训练

我买来区块链、比特币相关的 10 本书，开始更加系统地研究其中的每一个概念，随着研究的深入，又逐步购买了一些其它币种，并且参与了李笑来的 BigOne 和 PressOne 的众筹（2017 年 9 月 4 日之后，根据国家政策已经退币），在剧烈震荡的行情中，我一直能够坚定地握住自认为有价值的数字货币。

我加入了多个微信群、小密圈（现在已经改名为知识星球），经常会看到一些新手贴，由于忘记密码、泄漏私钥、填错地址等初级错误，让自己的资产归零。在区块链的世界里折腾了 1 年多，此时回头望过去，感觉区块链真的很难在短时间给普通人讲清楚，比特币地址、区块、区块高度、去中心化、算力、确认数、难度调整、挖矿、矿工、矿池、哈希、分叉、工作量证明、双重支付、私钥、公钥、交易、交易手续费、钱包等等，这一大堆的新概念，把许多伸手

党拦在了门外。有些小白连最最基础的私钥、钱包等概念都不理解，就冲入了交易所，不仅握不住资产，还可能由于自己的误操作将资产清零。

我在 2017 年 5 月底开办了“区块链生存训练”饭团，尝试用简单的语言、形象的类比让团友逐个击破一个又一个的新概念，让大家理解未来的“价值互联网”的前景。心中认可一些观点，通过不断学习并达到笃信的程度，再按照自己的想法大胆地预测，预测之后，采取相应的行动，这才是活在未来。

2017 年 9 月数字货币市场风云变幻，国家对 ICO（初始代币发行）实行一刀切，交易所全面关停，事后我清点了一下持有的数字资产，币种控制在 BTC、ETH、EOS、SC、GXS、ZEC 等范围内，本来就认可这些币的价值，做好了长线持有的打算。我的成本单靠比特币就基本持平，其它币种虽然市值缩水严重，但仍是净赚的。

对于我们这些明白科学上网、OTC 场外交易的老司机来说，反正准备长线持有，不过是操作流程稍微麻烦了一点，但对于大量的没掌握好基本技能的炒币人士来说，国内的各种监管措施对他们则是致命的。大多数“韭菜”在这个期间交出了筹码，许多投机者损失惨重。

学习的好时机

现在的币圈比以前冷清了许多，巴菲特说过，别人疯狂的时候我恐惧，别人恐惧的时候我疯狂。此时正好可以专心地研究一番技术了，买入比特币虽然比以前麻烦了一些，但仍有多种途径。李笑来说过，区块链的世界里，没有穿过一次牛熊，都不算入行。与比特币相识一年多，穿越了 2017 年 9 月的熊市，我才算是有点入行了。

我在饭团里陆续发表了许多有关区块链的内容，第 66 篇文章之后我邀请了几位朋友一起创作，在 2017 年 10 月初已经积累了 90 多篇内容，但并不系统，对于刚加入群的朋友来说，面对一堆内容仍感觉无从下手。2017 年国庆期间，我们尝试着把以前的内容重新组织一番，有些内容已经不适应当前的现状，直接删除；现在国内交易所正在全面关停，我们增加了一些场外交易的内容；为照顾一些刚刚接触比特币和区块链的用户，仍是以实际的操作讲解为主，再逐步引入一个一个的新概念，从而快速进入区块链的世界，活在未来，所以才有了这本书的问世。

适合的读者

本书的主要目标用户是刚刚踏入数字货币领域的初学者,但许多原理和投资理念对于混迹币圈的老司机同样适用。尽管书中给出了比较详尽的配图，但读者最好有一些 Windows 操作系统的基础知识，如果有编程或密码学知识，将会更容易理解一些高级概念。

章节安排

2.0 版共分为七篇。

第一篇介绍比特币与区块链的基础概念，从钱包的安装使用入手，慢慢引入区块链中的一些相对基础的概念，介绍了多种场外交易平台。比特币是区块链中的第一个成功应用，它是数字资产领域的带头大哥，也是所有数字货币价格涨跌的风向标，深入了解比特币才能更容易理解其它的数字货币是否有其存在的价值。

第二篇是区块链的进阶内容，分叉、重放攻击、51%攻击、椭圆曲线算法等是区块链中的安全基础，学习起来有一定难度，但值得理解。不求看懂所有的技术细节，但得明白基本的运作原理，这样才有助于理解其它数字货币。

第三篇介绍智能合约、以太坊有关的内容，有人称比特币是区块链 1.0，以太坊则是区块链 2.0，智能合约的引入让区块链应用长出了翅膀，ICO（初始代币发行）容易成为非法集资的工具，已被国家禁止，但仍需了解这些技术的先进性。

第四篇介绍低成本参与区块链的方式，用户可以在区块链激励平台上发表原创文章，通过创造有价值的内容而获得代币奖励，我们把这种参与方式简单叫做“脑力挖矿”。

第五篇介绍一些有代表的竞争币，EOS、Siacoin、Zcash 等其它数字货币弥补了比特币的哪些不足？

第六篇是投资实操篇，介绍区块链世界里的挖矿、搬砖等套利手段，在一个尚未成熟的领域内，总是存在大量的套利机会，需要大家共同去发现。

第七篇是币圈混迹多年的老司机的投资原则或感悟,投资是一件需要自己独立深入思考并长期切身实践的事，希望这些经验可以让你少走一段弯路。

致谢

在饭团的开办期间，得到了许多的团友的大力支持，许多人二话不说，直接包年订阅。在本书的写作过程中，得到了金炜、黄黎、苏江等几位共创者的积极响应，大家都牺牲宝贵的国庆和春节假期来帮我一起修订书稿，才能让本书如期与大家见面。在这些文章的写作中，还得到了孩子的配图支持。另外，感谢媳妇忍受了几个月来没日没夜的键盘敲击声。

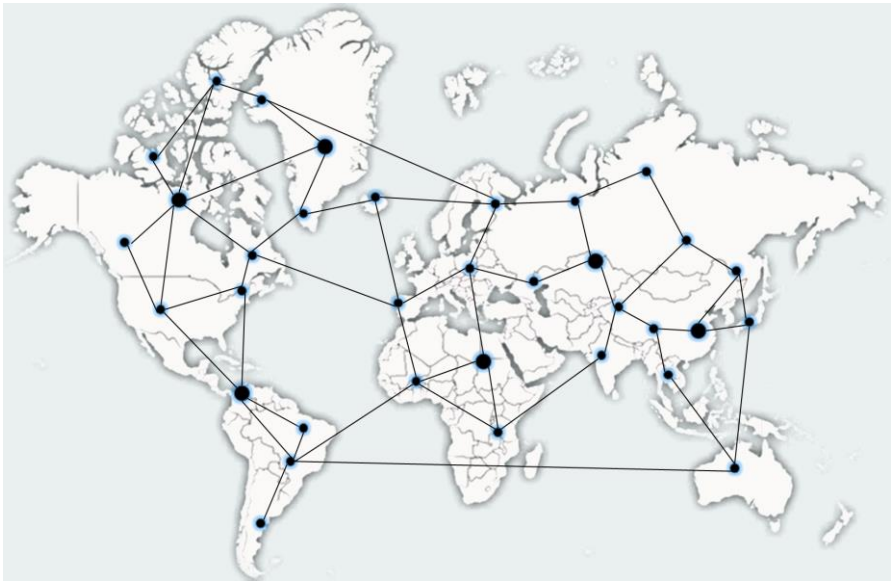
全书中，黄黎编写了脑力挖矿相关的内容，金炜编写了 OTC 场外交易及挖矿的内容，杨卫祥编写了谷歌验证器、搬砖、场外交易防骗相关的内容，苏江编写了交易原则、SPV 及非对称加密的内容，苏耀勇编写了 Siacoin、Zcash 和 EOS 相关的内容，申龙斌负责设计全书框架，编写了区块链基础、区块链进阶、以太坊基础等内容，并且整理汇总了全部书稿。

感谢林旷野、许明亮协助排版 DOC 书稿，感谢零月浅浅为本书制作封面。

如果您感觉本书对您有很大帮助，也欢迎捐赠，以太坊捐赠地址：

0xB4fd52AA5DB2820dC183aCa9ea8ff030a5F92D5E

第一篇 比特币与区块链基础



1 安装钱包软件 Bitcoin Core

欢迎来到区块链的世界。

新人在学习比特币的过程中，会遇到大量的计算机术语，如果缺乏一些必备的基础知识，理解起来非常困难。我受《穷爸爸富爸爸》中现金流游戏的启发，曾经想着设计一款多人互动游戏，让大家在游戏的过程中掌握这些基本概念，然而游戏的设计过程并不轻松，有一天我突然发现最好的学习来自于实际操作，最像创业的最佳思路就是**低成本快速试错**，在学习区块链知识上仍然适用。1 个比特币现价约为 50000 元（2018 年 2 月的价格），但它可以分得非常细，比如你可以先买 0.01 个比特币练练手，还不到 500 元就可以跑通整个比特币交易的主要环节。在真刀真枪的实践中学习您会更加用心，学习的速度也超乎想像。

我在践行 GTD(Getting Things Done)的过程中明白了做任何事的时候一定要找到**下一步行动（Next Action）**，完成了这个 Next Action，很多事情就能够顺利地向前推进，而且事情并没有像一开始想像的那样困难。在学习比特币这件事上，它的 Next Action 就是**安装 Bitcoin Core 钱包软件**。先别管钱包的准确定义，安装起来再说，以后会在第 4.2 节详细介绍钱包软件。

推进一个项目，请找到 Next Action，并开始行动。

多说一句，有些人已经接触过比特币，并且在手机上安装过**轻钱包**软件，但我仍然强烈建议你在首次学习钱包软件时，一定要安装 Bitcoin Core 这样的**全节点钱包**（全节点这个概念以后介绍），因为这款软件是中本聪（比特币的发明人）最早实现的，从这里可以了解到许多基本概念，虽然下载和同步的时间可能会长达一周，但这些时间的投入是非常值得的。

很遗憾的是，大量的人还没搞明白**私钥**、**公钥**、**密码**、**助记词**等基本概念，冲入交易所一番操作之后，自己亲手把自己的资产归零，这样的事情在多个微信群和小密圈里不断地发生。

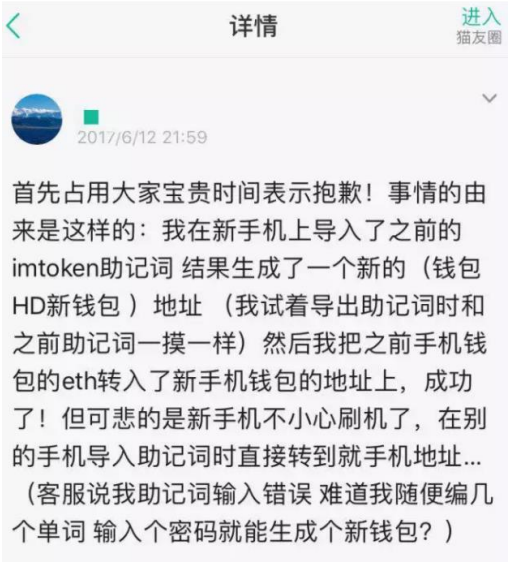


图1-1 钱包使用错误造成比特币的永久丢失

所以我仍然强烈建议一定要先安装并体验一下 Bitcoin Core 这样的全节点钱包，后来出现的上千种数字货币（1523 种，来源 2018 年 2 月的 coinmarketcap.com），它们的钱包软件大多是在 Bitcoin Core 的基础上修改而成的，所以当你学会了 Bitcoin Core，其它的钱包也就全明白了。

1.1 安装前的准备

1）电脑一台，台式机或笔记本电脑都行，Macbook 或 Windows 不限，由于 Windows 用户居多，本书介绍的软件主要都在 Windows 平台上运行。首选的操作系统是 Windows 7(64 位)，Windows 10 也行。从 0.15.0.1 版本之后，已经不再支持 Windows XP。

2）硬盘剩余空间 200GB 以上，因为全世界的公开大账本（所有的比特币交易记录）都将保存在你的这台电脑里，想想都兴奋。我写这段文字的时候（2018 年 2 月 9 日），全部账本的数据量大概为 160GB，所以预留足够的硬盘空间是必须的。如果你有快速的 SSD 硬盘，体验会更好一些。

3）宽带网络连接，这个不需要强调了吧？网络速度越快越好。

1.2 安装步骤

1）下载：在台式机电脑上打开浏览器，打开比特币的官方网站：https://bitcoin.org，英文不好也没有关系，已经有中文版了：https://bitcoin.org/zh_CN/。在顶部的“资源”菜单

里找到“Bitcoin Core”，找到您的机器的操作系统版本，下载相应的软件，这个就是官方的比特币钱包软件，我们这里以 Windows 64 位版本为例进行说明。写这段文字时，最新版本为 0.15.0.1。

图1-2 从 bitcoin.org 网站下载软件

2）安装：大部分都用默认设置，一路点击”下一步“就行，在设置区块链数据存放文件夹时，放在剩余空间超过 200GB 的硬盘中，否则区块数据会默认安装在 C 盘，以后还要进行区块数据搬家的操作。

3）启动

图1-3 Bitcoin Core 的启动界面

4）同步：因为要把全世界的大账本全部下载到本机，根据网络情况，这个过程可能需要几天到 10 多天，有进度提示，在它漫长的同步过程中，你正好可以静下心来认真学习后面的内容了。

进度窗口也可以隐藏，不必完成 100%的同步进度也可以接收比特币，只不过你的钱包软件中可能查不到相应的交易记录。

图1-4 下载公开大账本的进度提示

5）当下载到 100%，就可以看到钱包的余额和最近交易记录，当然，如果您是第一次安装，钱包里的数字都是 0。

图1-5 钱包的概况

Bitcoin Core 是第一款比特币钱包，值得掌握。

1.3 区块数据搬家指南

有些朋友可能早就安装过 Bitcoin Core 软件，但是在安装的时候没有留意，把软件默认安装在 C 盘，而 C 盘是系统盘，Bitcoin Core 要同步高达 160GB 的区块链数据，运行了没几天，C 盘就快满了。

此时如果重新安装 Bitcoin Core，又得花几天时间重新同步，实际上稍微处理一下，是

不需要重新安装的，这里介绍两种办法。

操作办法一：

1）关闭钱包软件；

2）假设你的区块文件夹在 C:\Users\Shenlb\AppData\Roaming\bitcoin 里，需要移到 F:\bitcoin-data 文件夹下，先把 C 盘的文件夹剪切、粘贴到 F 盘；

3）用管理员权限启动 cmd 命令行程序。在开始菜单里找到 command 黑窗口程序，右键菜单，以管理员身份运行；

4）在黑窗口里需要运行命令

```
mklink  /D  "C:\Users\shenlb\AppData\Roaming\bitcoin"  "F:\bitcoin-data"
```

这个命令的意思是，在原来的地方建立一个文件夹符号链接，实际文件的物理位置在 F 盘，注意空格不能省；

5）重新启动钱包软件，完成。

操作办法二：

1）先退出 Bitcoin Core 软件；

2）找到 Bitcoin Core 的 blocks 所在的文件夹，这个 blocks 保存着比特币网络的区块链数据（公开大账本），里面有近百个文件，文件名类似 blk?????.dat，每个文件约 130M 左右，默认安装的位置是 C:\users\[你的用户名]\appdata\roaming\bitcoin

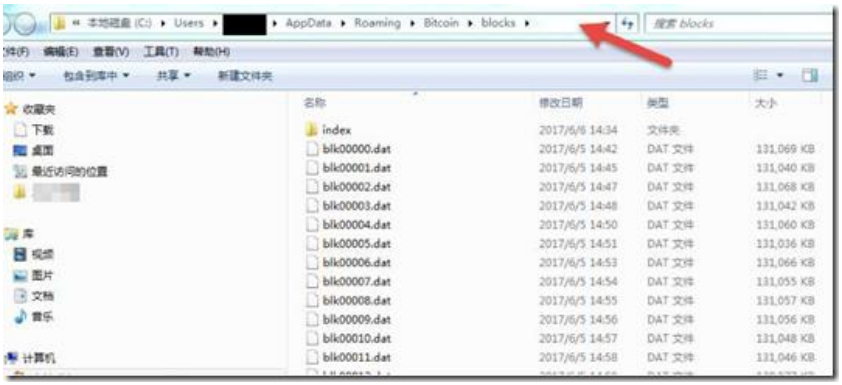


图1-6 找到 Bitcoin Core 区块数据的文件夹

3）找一个剩余空间最大的盘符，假设为 F 盘，在 F 盘建立一个文件夹 F:\bitcoin-data

4）将刚才在 C 盘的那个文件夹移动到 F 盘，并把文件夹改名为 F:\bitcoin-data

5）存储区块链的文件夹信息是保存在 Windows 的注册表中的，需要更改注册表项。新建一个 bitcoin.reg 文件，内容：

```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Software\Bitcoin\Bitcoin-Qt]

"strDataDir"="F:\\bitcoin-data"
```

双击运行这个 bitcoin.reg 文件，确认将注册表项添加进去。

6）再启动 Bitcoin Core，以后的同步数据都放在 F 盘了，完成！

操作办法三：

1）关闭 Bitcoin Core 软件

2）找一个剩余空间最大的盘符，假设为 E 盘，在 E 盘建立一个文件夹 E:\core-data

3）将刚才在 C 盘的那个文件夹移动到 E:\bitcoin-data

4）在桌面上建立一个快捷方式，指向 C:\bitcoin 安装文件夹\bin 中的 bitcoin-qt.exe 文件。具体的操作步骤：按住鼠标右键拖动 bitcoin-qt.exe 到桌面，在弹出的菜单中，选择“在当前位置创建快捷方式”。

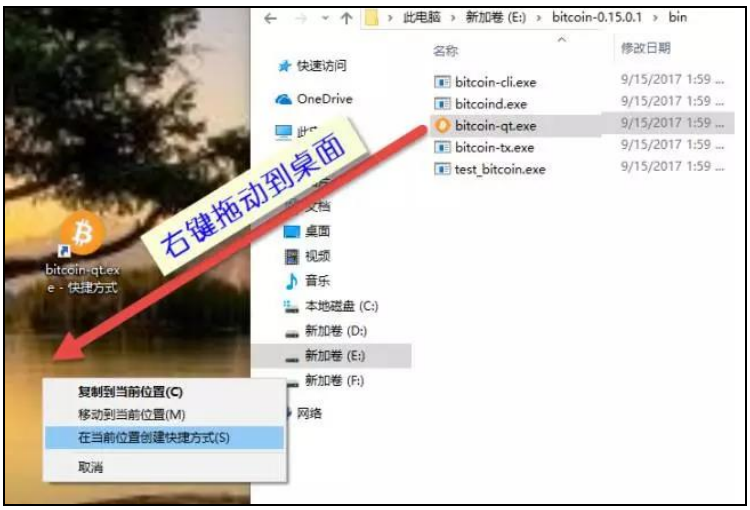


图1-7 创建 bitcoin-qt.exe 快捷方式

5）在桌面上的“bitcoin-qt.exe - 快捷方式”上按鼠标右键，找到“属性”菜单项，在目标的命令行里加上-datadir=e:/core-data，注意-datadir 前面有一个空格。完整的命令行是：

C:\bitcoin-0.15.0.1\bin\bitcoin-qt.exe -datadir=e:/core-data

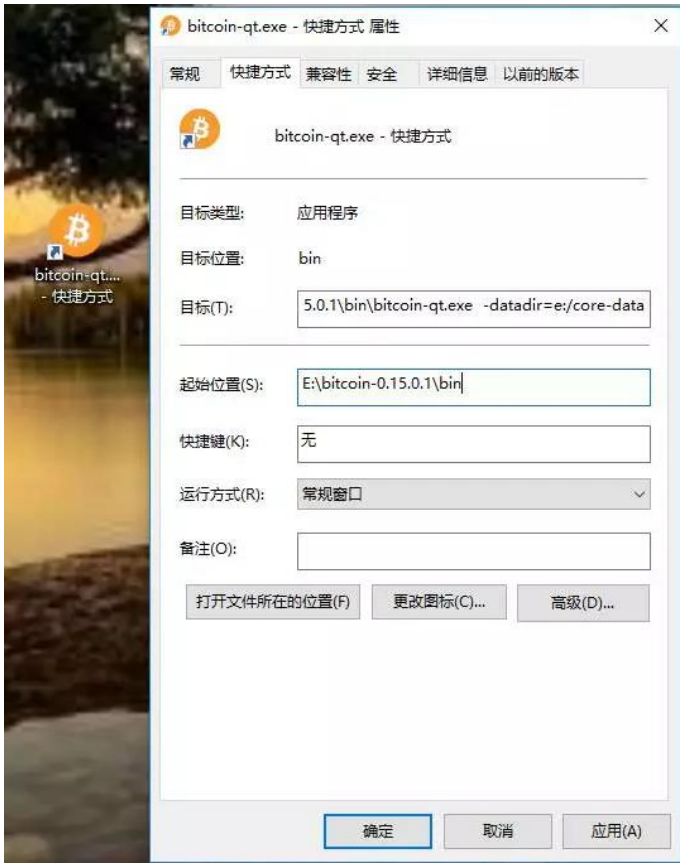


图1-8 修改 bitcoin-qt 的桌面快捷方式

6）以后只能用桌面上的那个快捷方式启动 Bitcoin Core，此时可以看见 core-data 中保存了钱包和区块等数据。

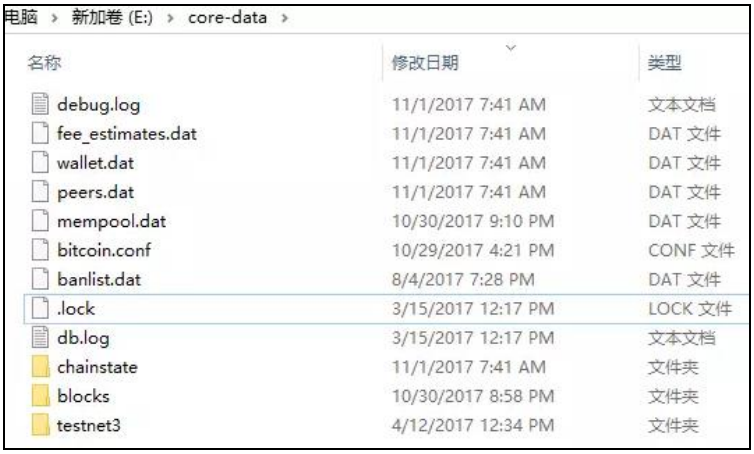


图1-9 区块数据文件夹中的内容

1.4 用 MD5 & SHA Checksum 工具确认钱包软件的正确来源

下载比特币钱包一定要认准 bitcoin.org 官网，即使非常慢也不能怕麻烦，不排除一些黑

客篡改源代码来生成其它安装包的可能性，那样你的私钥可能会泄漏。

还有一种办法来判断安装包的来源是否合法，可以用 MD5 & SHA Checksum 工具，官网在提供安装包的下载地址时，同时还会提供 checksum 的文本，用于检验文件是否被篡改。

1）下载 MD5 & SHA Checksum Utility

http://files.cnblogs.com/files/speeding/checksum.zip

2）下载 bitcoin 钱包软件，同时下载签名文本，SHA256SUMS.asc

图1-10 官网的下载页还会提供签名数据

3）运行 Checksum Utility，以 0.14.2 版本的安装文件为例，将下载的文件 bitcoin-0.14.2-win64-setup.exe 拖入文件选择区，则显示各种 checksum，核对一致的表示你的安装文件未经过篡改，可以放心使用。

图1-11 MD5 & SHA Checksum 工具

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

dd877bc247efa4c90a34ec9ce1a497a8ae1f7eac4c688aa8c8b25ffe30c20541  bitcoin-0.14.2-aarch64-linux-gnu.tar.gz
f273eb5e56694fe5baecdd5ee8cda9ac495541ccd9df5ca1c22a1b10dc6d89e8  bitcoin-0.14.2-arm-linux-gnueabihf.tar.gz
1a302092d9af75db93e2d87a9da6f1f2564a209fb8ee1d7f64ca1d2828f31c03  bitcoin-0.14.2-i686-pc-linux-gnu.tar.gz
a4e98906b4fa08727cbd81371a108ed7a19ea34bb421b078e64843560490a78d  bitcoin-0.14.2-osx64.tar.gz
463277b9139e890a713034b539583a0879bdcf0fc94c3c1fc08bb8aab81bb108  bitcoin-0.14.2-osx.dmg
1ac4e5ce51ac03c41df0ad1e759dbb55d91e1456b9a616e43344bf2258dbe8ca  bitcoin-0.14.2.tar.gz
522bf19ff2ac1a3f100194914071cf6d1a15076268c5c847b2f891277f427af6  bitcoin-0.14.2-win32-setup.exe
b3b0cc67a9a602fee4a270efc154f4422e1e49e2aefd9b0d44b0c601a326b05a  bitcoin-0.14.2-win32.zip
3a0057e4d6ca172566a93192234ef28916cbb052db9e15997569d9c08502c49a  bitcoin-0.14.2-win64-setup.exe
8a2a5657a8b3243ab4f549bb4b16c8c34b47acfb5c6bc07eb0b875ee71a3ad5b  bitcoin-0.14.2-win64.zip
20acc6d5d5e0c4140387bc3445b8b3244d74c1c509bd98f62b4ee63bec31a92b  bitcoin-0.14.2-x86_64-linux-gnu.tar.gz
```

图1-12 各个下载文件的校验码

1.5 安全提示

安装完 Bitcoin Core 钱包客户端后，在接收第一笔比特币之前，一定要加密钱包，从“设置”菜单中，找到“加密钱包...”，输入密码即可完成钱包加密的过程。请使用复杂的密码（8个以上大小写字母、数字和符号的组合），并务必**牢记密码、牢记密码、牢记密码**，重要的事情说三遍，因为没有找回密码的选项。

图1-13 Bitcoin Core 中加密钱包

务必牢记密码，遗忘密码将丢失所有的比特币。

背后原理：上述操作实际上是把你的 wallet.dat 钱包文件用 AES 算法（高级加密标准，Advanced Encryption Standard)进行了加密处理,这样即使别人拿走了你的 Wallet.dat 文件，没有密码也无法动用你的比特币。

关于 wallet.dat 文件：

（1）Bitcoin Core 中用 wallet.dat 文件保存你的**私钥**，请启用软件的加密选项，要用至少 8 位以上的**复杂密码**（建议 12 个以上的大小写字母、数字和特殊字符组合），并牢记密码。

（2）把加密的 wallet.dat 备份在 U 盘、移动硬盘等，多存放几份，牢记你的密码，如果更换电脑，则只需重装 Bitcoin Core，并更换 wallet.dat，就可以恢复你的比特币。

（3）还有一种导出私钥的方法，操作起来复杂一些，如果不明白自己正在做什么，就不要进行导出私钥的操作。详情参见第 8 章。

根据以上道理，比特币丢失有这样几种情况：

（1）私钥泄漏，被别人把币转移了。

（2）wallet.dat 找不到了，彻底没办法了，因为私钥没有了。

（3）wallet.dat 被偷。如果这个文件已经加密，则小偷还需知道密码才能真正偷走你的钱，所以务必要启用钱包加密功能。

（4）密码不记得了。你唯一的办法就是慢慢尝试吧，因为没有忘记密码的找回功能，只能把你以前用过的密码都试一遍。

（5）wallet.dat 被破坏了。用 Bitcoin Core 提供的备份功能，一般没问题，但如果这个文件被病毒感染（比如著名的比特币勒索软件，要支付 300 比特币），如果你的资金超过 300BTC，可以试试交赎金的办法。

总之，如果你用 Bitcoin Core，则加密 wallet，备份 wallet.dat、牢记密码！

1.6 升级到 0.15.1 版本

如果你以前安装过 Bitcoin Core 的早期版本，可以考虑更新到 0.15.1 版本，这个版本是在 2017 年 11 月发布，下载的地址：https://bitcoincore.org/bin/bitcoin-

core-0.15.1/

如何升级：

（1）先备份好你的钱包 wallet.dat，永远不要丢失你的私钥

（2）关闭正在运行的老版本的 Bitcoin Core

（3）运行安装包，或者直接运行新版本的 bitcoin-qt.exe 即可，升级过程可以要花点时间，请耐心等待

（4）升级完成后，最好别再使用旧版本了，否则会造成区块数据的混乱

0.15 版本更新的内容：

（1）支持隔离见证 SegWit。可以支持隔离见证的地址，如果你不知道是什么意思，也不影响使用。

（2）性能提升。内部链状态的数据库发生了变化，速度更快(30%-40%)，内存占用更少(10%-20%)，但磁盘占用会多一些(15%)。区块同步速度也有所提升，新块确认快了 40%-50%。

（3）交易费估算方法改进。有保守估算、省钱估算两种方式，号称估算得更准确。

（4）多钱包支持。命令行选项中可以支持多个钱包的切换，但在 GUI 用户界面中只能看到第一个钱包。

（5）在 GUI 中支持手续费更换(Replace-by-fee)。以前手续费填得太低，可能交易永远也得不到确认，虽然以前在命令行里有个高级选项，可以提高交易手续费来让矿工打包，但普通用户不会使用，现在的 GUI 界面中多了 RBF(Replace-by-fee)选项，可以在界面中操作这个功能了，你可以先试比较低的手续费，能省一点算一点，不行再追加手续费。

（6）移除了币龄优先级的概念，零手续费的交易可能永远也不会被矿工打包。还有许多零碎的改进，可以见这里：https://bitcoin.org/en/release/v0.15.0

2 区块、链、区块高度

钱包软件 Bitcoin Core 的数据同步过程要花好几天，现在我们先来了解区块链中最基础

的三个概念。

区块链是不可篡改的共享大账本。

区块链(blockchain) 可以理解为互联网上的共享大账本，要理解这个共享大账本的运作机制，则要面对更多的术语和原理，但也别担心，核心的概念并不太多，还是可以在较短的时间内入门的。

这里不准备给出每个概念的准确的、学术上的定义，而是用身边熟悉的事物进行类比，尽量用简单的语言去解释区块链的背后原理。为了不把事情弄得更复杂，在这一篇里全指比特币的区块链，其它币种的区块链会有所不同，放在后面再介绍。

区块链本身是一个复合词，可以分为两个简单的初中英文单词：**区块** block、**链** chain。

2.1 区块 Block

类比：账本盒。

区块可以想像为会计人员的账本盒，里面装着一页一页的账单，假设每个账单为一页 A4 纸，这个盒子大概能够装下 2000 页左右的这种账单。

图2-1 区块可类比为账本盒

每个区块都用一个唯一的、长长的字符串进行了编号（准确地讲叫**区块哈希**，在第 6.4 章会介绍 HASH 的概念），这个编号由里面的所有交易信息自动计算而成，里面的某笔交易发生细微的改变，这个编号就要发生显著的变化，来防止篡改交易数据。

2.2 链 Chain

看到“链”，我们会本能地联想到自行车上的链条，但这种类比不利于后面概念的理解。这里的链理解为**链接(Link)**更为准确，档案盒上要贴一张标签，上面记录着前一个区块的编号，这样可把这些盒子关联在一起。

这种方式就保证了前面盒子（压在了底下的盒子）里的内容不能再修改了（详见第 3.5 节的**不可篡改性**），因为里面的内容发生修改，编号就会变，链接关系就会被破坏。

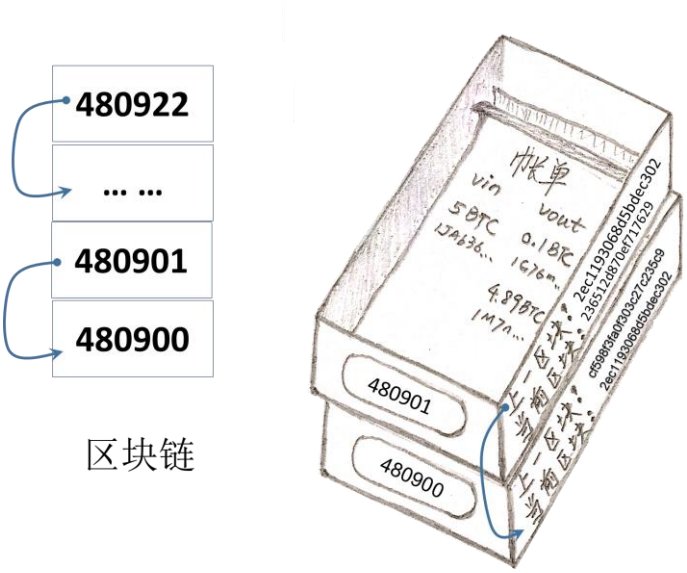


图2-2 区块链类比为堆叠且相连的账本盒

2.3 区块高度(Block Height)

类比：账本盒的堆叠高度

区块高度从 0 开始计数。

刚才说到把“链”想像成自行车链条不太合适，是因为链条有长度的属性，而区块链世界的准确术语是“**区块高度**”，你需要把区块链想像为堆叠在一起的账本盒，这样“**区块高度**”的概念就容易理解多了。

最底层的那个账本盒（区块）称为**创世区块(Genesis Block)**，计算机都是从 0 开始计数的，所以又叫做第 0 块，在第 2.4 章有更详细的解释。每叠加一块，高度增一，我写这段文字时的最新高度为 469629。

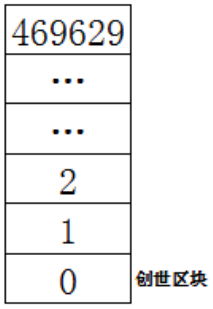


图2-3 区块高度与创世区块

访问 http://blockchain.info 网站，可以查到最近产生的几个区块的信息，如图 2-4 所示，最新区块高度为 487874，里面许多链接都可以点击查看详情，后面介绍。

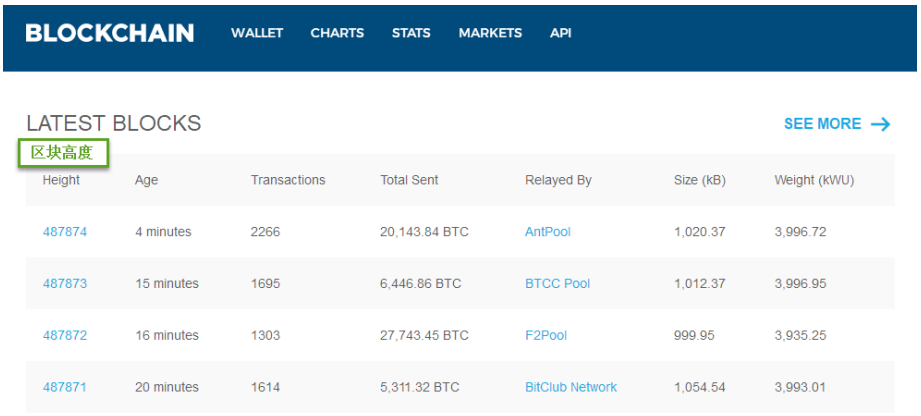


图2-4 查询最近产生的区块信息

2.4 创世区块(Genesis Block)

比特币的发明人是中本聪。

2009 年 1 月 3 日 18:15:05（UTC 时间，世界标准时间），比特币的创始人中本聪(Satoshi Nakamoto)挖出了比特币世界的首个区块——**创世区块(Genesis Block)**，区块序号为 0。让我们来看看这个区块中记录着什么关键信息。

打开这个网址：https://blockchain.info/tx/4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b

图2-5 创世区块的信息

从上向下解释一下这笔交易的主要信息，有些内容看不懂也不要紧，等学完比特币地址、交易等其它几个概念后再回来看这段内容：

1）4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b

这串长长的十六进制数值是交易的 HASH 值，见第 6.4 节。

2）没有输入

创世区块是凭空产生的，上帝创造的，所以没有输入。见第 4 章中有关交易输入 vin 的说明。

3）1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa

这是比特币地址，见第 4.3 章的介绍。

4）50 BTC

BTC 是比特币的基本计量单位，是 Bitcoin 的缩写，创世区块产生了 50 个 BTC。以后每个区块新产生 50BTC，大概每四年新币数量减半（准备地说是每 210000 个区块后，新币减半），在 2140 年达到极限值 2100 万个，参考第 3.2 节稀缺性的介绍。

5）大小：204 字节

整个区块占用 204 个字节。

6）接收时间：2009-01-03 18:15:05

这是格林威治时间 GMT 2009 年 1 月 3 日 18:15:05，换成北京时间为 2009 年 1 月 4 日 02:15:05。

7）显示交易脚本

点击“显示交易脚本”，可以看到这笔交易的详细描述，中本聪在这笔交易中永久地记录了这样一句话：“The Times 03/Jan/2009 Chancellor on brink of second bailout for banks”，中文意思为“泰晤士报 2009 年 1 月 3 日，财政大臣第二次对处于崩溃边缘的银行进行紧急救助”。

这句话正是泰晤士报(The Times)当天的头版文章标题。中本聪一方面留下了该区块是在 2009 年 1 月 3 日之后创建的证据，同时也是对中心化银行系统的讥讽。

图2-6 泰晤士报头版标题被中本聪永久地记录在区块链中

从这个区块之后，大约每 10 分钟会产生一个新区块，区块一经产生，不可修改，最近的区块数据可通过访问 https://blockchain.info 随时查到。

2.5 区块信息解读

区块链的信息是公开的，任何一个区块的信息都可以查到，比如我们来一起看看区块高度为 469629 的这个区块的详细信息，点击 https://blockchain.info/zh-cn/block-height/469629 这个链接打开一个网页。

区块序号469629 在比特币区块链中高度为469629的区块

概览	
高度	469629 (Main chain)
哈希值	00000000000000000142f3a65cb3e59cf0c5d8bda18af2011813f9db99e43e4d
上一区块	00000000000000000001ea1d02c698b994d49bf04c1e0fce4945f86d362a4e214
下一区块	
时间	2017-06-03 23:46:14
时间	2017-06-03 23:46:14
播报方	BTC.com
难度系数	595,921,917,085.42
Bits	402774100
交易次数	1060
输出总量	11,560.64407619 BTC
预计交易量	1,425.05427164 BTC
大小	998.11 KB
版本	0x20000000
二进制哈希树根	7498e3fe212f9cd25899a2d88d5628fecefc2f0374298923151e47e76a5eb216
随机数	3518278309
新区块奖励	12.5 BTC

图2-7 第469629个区块的主要信息

从下至上可以看懂这样几个数字，其它数字先不用管，还需要学习其它知识才能理解。

1）新区块奖励：12.5 BTC

创世区块的新区块奖励是 50 BTC，以后每挖出 210000 个区块（大约 4 年）后新币减半，2012 年 11 月 28 日第一次减半，为 25 BTC，2016 年 7 月 9 日 16:46:13，第二次减半，为 12.5 BTC，此时区块高度为 420000。下一次减半预计在 2020 年 5 月 8 日发生（来源于：https://coin.dance/stats），即只奖励 6.25 BTC。

2）大小：998.11KB

整个区块的大小控制在 1M 以内，比特币在刚产生时，交易非常少，一个区块才几 KB，当

时 1M 容量足够用。而现在比特币交易上升速度非常快，1MB 空间不够用，造成交易拥堵，所以**比特币扩容**势在必行，只是扩容的技术方案上存在着许多争论，2017 年 11 月 15 日原计划升级为 2MB，最后由于分歧太大而泡汤，比特币区块链的拥堵问题仍然未解决。

3）交易次数：1060

这个区块内一共打包了 1060 笔**交易**记录。

4）上一区块、下一区块

每个区块可以链接到上一区块（区块高度减一的那个区块），一直可以追溯到创世区块。

5）哈希值：00000000000000000142f3a65cb3e59cf0c5d8bda18af2011813f9db99e43e4d

这就是当前区块的哈希值，点击哈希值，可以看到这个区块内所有交易的详细信息，如图 2-8，这里可以看到每一笔交易的输入、输出、交易费等信息，以后再解释。

图2-8 区块中的所有交易信息

3 比特币及其特性

比特币(Bitcoin)是第一种成功地构建于**区块链**技术之上的数字货币，它是中本聪(Satoshi Nakamoto)发明的，这个名字听着是不是有点像日本人？据说日本大力推行比特币交易也与这个猜测有关。

3.1 可分割性

说起比特币，大脑的认知本能会让我们与已知的东西进行类比，比如马上会想到 **Q 币**，

但这种类比存在着极大的误导性。

普通的纸币因为分割性不好，所以有多种面额，分为 100 元、50 元、20 元、10 元、5 元、1 元……但比特币是数字货币，它的**可分割性**非常棒。你的比特币钱包中保存的只是一个数字（准确地说，钱包里保存的只是私钥和公钥，余额保存在区块链里），所以可以是任何值，比如你可以支付 0.402985 个比特币。

图3-1 纸币的可分割性很差，所以有多种面额

比特币这个概念的本身也是一个货币单位，符号：**BTC**，（取单词 BiTCoin 中的三个字母），我在写本书的 1.0 版本时（2017 年 10 月 2 日）的行情是 1BTC 换 28000 元人民币，修订 2.0 版本时（2018 年 2 月 13 日）比特币的价格为 58000 元。

比特币的最小单位是 10^{-8} BTC，即 0.00000001BTC，称为 1 **聪(Satoshi)**。为什么叫这个名字？因为比特币的发明人叫**中本聪**（Satoshi Nakamoto），日本人通过这个名字认定他是日本人。按 2017 年 10 月的行情，1 聪为 0.00028 元，即 0.028 分，比我们通常的纸币单位还精细得多。另一方面，假设未来上涨了 100 倍，最小单位才 2 分多，仍可满足市场交易的需求。

比特币最小可细分为 10 的-8 次方。

小结：

比特币可以分割得很细，最小单位是 1 聪。

- 1 比特币（Bitcoins，BTC）
- 1 比特分（Bitcent，cBTC）=0.01BTC

✧ 1 毫比特（Milli-Bitcoins，**mBTC**）=0.001BTC

✧ 1 微比特（Micro-Bitcoins，**μBTC** 或 uBTC,**Bits**）=10^{-6}BTC=100 聪

✧ 1 聪（Satoshi）（最小单位） = 0.00000001BTC

你此时可以打开 Bitcoin Core 钱包软件，从“设置”菜单中打开“选项”对话框，在“显示”栏里，可以看到 BTC、mBTC 和 μBTC 三个常用单位。

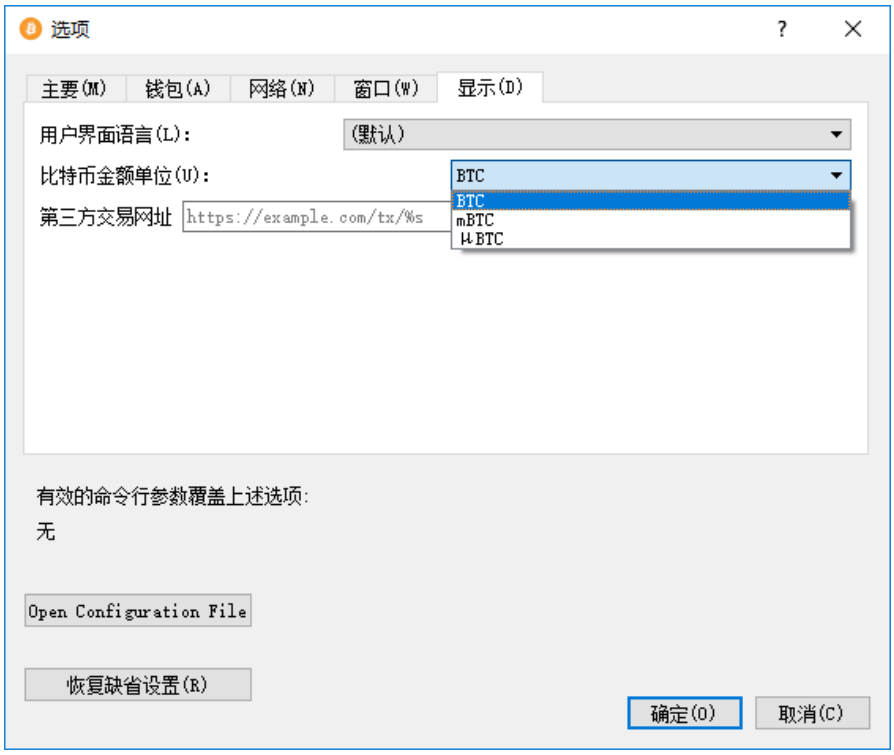


图3-2 可以设置比特币金额的显示单位

3.2 稀缺性

比特币的一个重要特性：总量有限，只有 2100 万个。

2100 万只是一个让人容易记住的数字，实际的准确数字应该是 20999999.9769 个，比 2100 万少一点点，图 3-3 的比特币发行量数据表来自于 https://en.bitcoin.it/wiki/Controlled_supply 。

Block	Reward Era	BTC/block	Start BTC	BTC Added	End BTC	BTC Increase	End BTC % of Limit
0	1	50.00000000	0.00000000	10500000.00000000	10500000.00000000*	infinite	50.00000006%
210000	2	25.00000000	10500000.00000000	5250000.00000000	15750000.00000000	50.00000000%	75.00000008%
420000	3	12.50000000	15750000.00000000	2625000.00000000	18375000.00000000	16.66666667%	87.50000010%
630000	4	6.25000000	18375000.00000000	1312500.00000000	19687500.00000000	7.14285714%	93.75000010%
840000	5	3.12500000	19687500.00000000	656250.00000000	20343750.00000000	3.33333333%	96.87500011%
1050000	6	1.56250000	20343750.00000000	328125.00000000	20671875.00000000	1.61290323%	98.43750011%
1260000	7	0.78125000	20671875.00000000	164062.50000000	20835937.50000000	0.79365079%	99.21875011%
1470000	8	0.39062500	20835937.50000000	82031.25000000	20917968.75000000	0.39370079%	99.60937511%
1680000	9	0.19531250	20917968.75000000	41015.62500000	20958984.37500000	0.19607843%	99.80468761%
1890000	10	0.09765625	20958984.37500000	20507.81250000	20979492.18750000	0.09784736%	99.90234386%
2100000	11	0.04882812	20979492.18750000	10253.90520000	20989746.09270000	0.04887585%	99.95117198%
2310000	12	0.02441406	20989746.09270000	5126.95260000	20994873.04530000	0.02442599%	99.97558604%
2520000	13	0.01220703	20994873.04530000	2563.47630000	20997436.52160000	0.01221001%	99.98779307%
2730000	14	0.00610351	20997436.52160000	1281.73710000	20998718.25870000	0.00610426%	99.99389658%
2940000	15	0.00305175	20998718.25870000	640.86750000	20999359.12620000	0.00305194%	99.99694833%
3150000	16	0.00152587	20999359.12620000	320.43270000	20999679.55890000	0.00152592%	99.99847420%
3360000	17	0.00076293	20999679.55890000	160.21530000	20999839.77420000	0.00076294%	99.99923713%
3570000	18	0.00038146	20999839.77420000	80.10660000	20999919.88080000	0.00038146%	99.99961859%
3780000	19	0.00019073	20999919.88080000	40.05330000	20999959.93410000	0.00019073%	99.99980932%
3990000	20	0.00009536	20999959.93410000	20.02560000	20999979.95970000	0.00009536%	99.99990468%
4200000	21	0.00004768	20999979.95970000	10.01280000	20999989.97250000	0.00004768%	99.99995236%
4410000	22	0.00002384	20999989.97250000	5.00640000	20999994.97890000	0.00002384%	99.99997620%
4620000	23	0.00001192	20999994.97890000	2.50320000	20999997.48210000	0.00001192%	99.99998812%
4830000	24	0.00000596	20999997.48210000	1.25160000	20999998.73370000	0.00000596%	99.99999408%
5040000	25	0.00000298	20999998.73370000	0.62580000	20999999.35950000	0.00000298%	99.99999706%
5250000	26	0.00000149	20999999.35950000	0.31290000	20999999.67240000	0.00000149%	99.99999855%
5460000	27	0.00000074	20999999.67240000	0.15540000	20999999.82780000	0.00000074%	99.99999929%
5670000	28	0.00000037	20999999.82780000	0.07770000	20999999.90550000	0.00000037%	99.99999966%
5880000	29	0.00000018	20999999.90550000	0.03780000	20999999.94330000	0.00000018%	99.99999984%
6090000	30	0.00000009	20999999.94330000	0.01890000	20999999.96220000	0.00000009%	99.99999993%
6300000	31	0.00000004	20999999.96220000	0.00840000	20999999.97060000	0.00000004%	99.99999997%
6510000	32	0.00000002	20999999.97060000	0.00420000	20999999.97480000	0.00000002%	99.99999999%
6720000	33	0.00000001	20999999.97480000	0.00210000	20999999.97690000	0.00000001%	100.00000000%
6930000	34	0.00000000	20999999.97690000	0.00000000	20999999.97690000	0.00000000%	100.00000000%

图3-3 比特币的发行量

具体的数字不细说了，记住大概每四年新币减半的规则，预计在 2140 年，比特币会达到极限值 2100 万个，不再增长了。由于有些人技术不过关、粗心或者保管不善，购买的一些比特币可能永远沉睡在浩瀚的区块链海洋中，有人估计丢失的数量可能有 400 万个，所以实际流通的比特币最多只有大概 1700 万个。

图 3-4 更可以清楚地看出发行量与时间的变化关系。

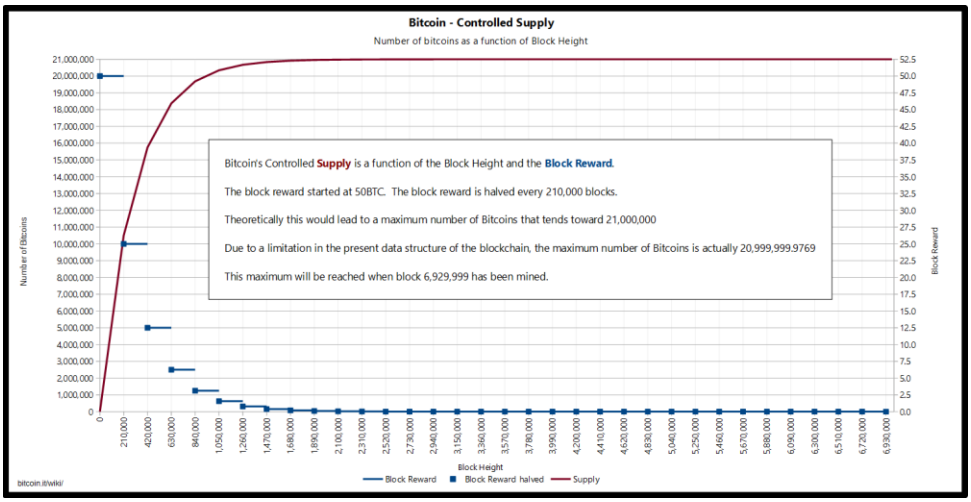


图3-4 比特币发行量与减半示意图

这种特性让它区别于市面上流通的纸币，通常把那些在政府控制下发行的货币称为**法币**，别把法币当成法国货币，也不是民国时期的那个法币，是指**法定货币**，下面一段话摘自百度百科：

> **法定货币**（legal tender/fiat money），是指不代表实质商品或货物，发行者亦没有将货币兑现为实物义务；只依靠政府的法令使其成为合法通货的货币。法定货币的价值来自拥有者相信货币将来能维持其购买力。货币本身并无内在价值（Intrinsic value），也就是说，当纸币产生之后，法定货币实质上就是法律规定的可以流通的纸币。
>
> 中华人民共和国的法定货币是**人民币**，中国人民银行是国家管理人民币的主管机关，负责人民币的设计、印制和发行。

20 世纪 70 年代，美元与黄金脱钩，通货膨胀就不可避免，因为政府会有各种理由滥用货币发行权。相对于各国政府发行的这些信用货币，比特币的内部算法机制严格确定了最终的数量为 2100 万个，任何人都无法修改，包括发明人本人。

这种数量有限的特性有点像黄金，所以有人把比特币比喻成数字黄金，但比特币的可分割性比黄金强得多，像我之前说过的比特币的最小单位为 1 聪，即 0.00000001 个 BTC，黄金可分不了这么细，每分一次还要有损耗，而比特币完全没有这方面的问题。

2100 万个带来了稀缺性，而这种稀缺会造成什么？请自行判断。

3.3 公开性

区块链是一个全世界的公开大账本，里面的每一笔交易都可以公开查询，你可以准确地知道什么时间、哪个地址给哪个地址发送了多少 BTC，有多个网站可以查询这些信息，比如：

- http://blockchain.info
- http://qukuai.com/search/
- https://btc.com/
- http://block.okcoin.cn/
- https://blockexplorer.com

请点击几个网站看看区块信息，内容看不懂暂时也不要紧，以后会详细介绍。有些网站可能需要科学上网。

3.4 去中心化（Decenteralization）

类比：中心化-->腾讯，去中心化-->BT 下载

说到**去中心化**，得先理解**中心化**。中心化的东西我们见得太多了，中心化的巨无霸公司现在有很多，比如 GAFATA（谷歌、苹果、Facebook、阿里巴巴、腾讯、亚马逊 6 个公司的首字母）。这些公司掌握着大量用户的数据，有着巨大的数据中心、服务器来支撑整个体系的运转，万一有个异常情况发生，可能就会影响上亿人。

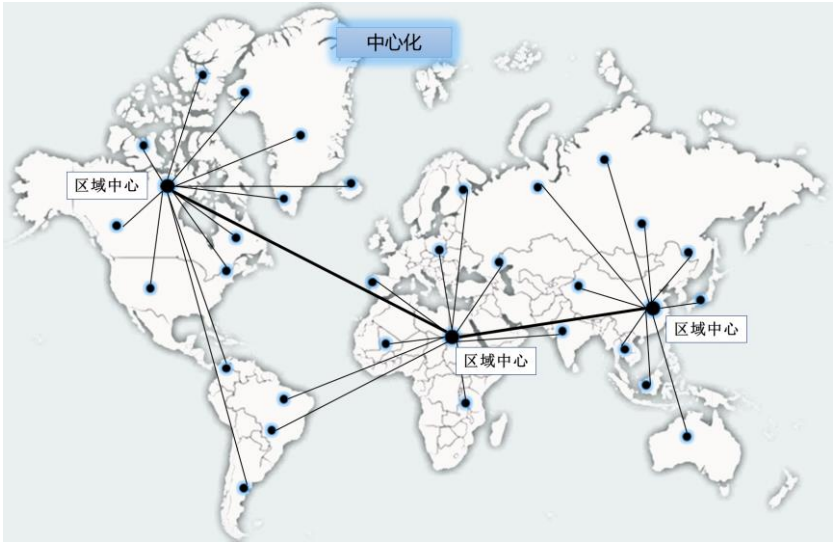


图3-5 中心化示意图

看上图，比如腾讯公司，它会在全国部署多个区域中心，以支撑庞大的用户及应用，假设微信在某个区域中心的服务器出现故障，可能会影响附近几千万的用户，这类中心化应用的优点是它的中心机房提供了超大规模数据的吞吐量，能够同时满足几千万人的使用，但其缺点也

非常明显，这类中心机房也是它们的薄弱地方，犹如蛇的七寸，要害部位的单点故障能够引发致命问题。当然，各大公司都做好了灾难备份、冗余备份等机制，无故障率都高达 99.999%，所以发生大范围故障的情况并不多见。

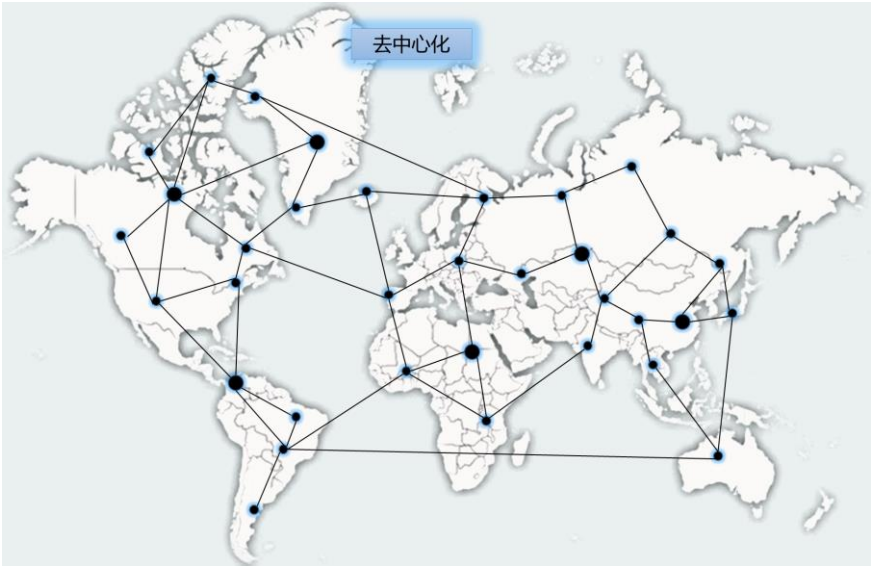


图3-6 去中心化示意图

再来看去中心化，去中心化类似于“BT 下载”、“电驴下载”，大家的连接方式是 P2P（Peer to Peer），即个人对个人，比如下载一部电影，大家互通有无，我从别人那里下载数据，同时我也为他人提供数据，当整个网络中充满着大量这样的节点时，你找不到中心，任何一部分节点的损坏并不影响整个系统的运行。

比特币网络中的交易信息就是在这样的去中心化的网络中快速传播的，如果你安装了一个 Bitcoin Core 钱包软件，你就接入了这个网络，注意，你的邻居可能并不是地理位置上与你最近的机器，很可能是远在地球另一端的某台机器。你下载最新的区块数据，同时你也在为他人提供区块和交易数据。当使用比特币网络的节点非常非常多时，你想摧毁比特币几乎是不可能的，除非你摧毁了整个互联网。

很难说，中心化与去中心化孰优孰劣，谁会是未来的发展趋势，未来的网络很可能是中心化网络与去中心化网络交织在一起的复杂体。现在已经诞生了巨无霸式的中心化应用程序，比如：苹果应用商店、微信等，将来肯定会出现去中心化的微信应用。

小练习：

我们再打开钱包软件 Bitcoin Core，在“帮助”菜单中打开“调试窗口”，在“同伴”

选项卡中，你可以看到与你正在进行数据交换的同伴，注意这里的同伴可能并不是在物理位置上与你接近，而是网络连接意义上的相邻。

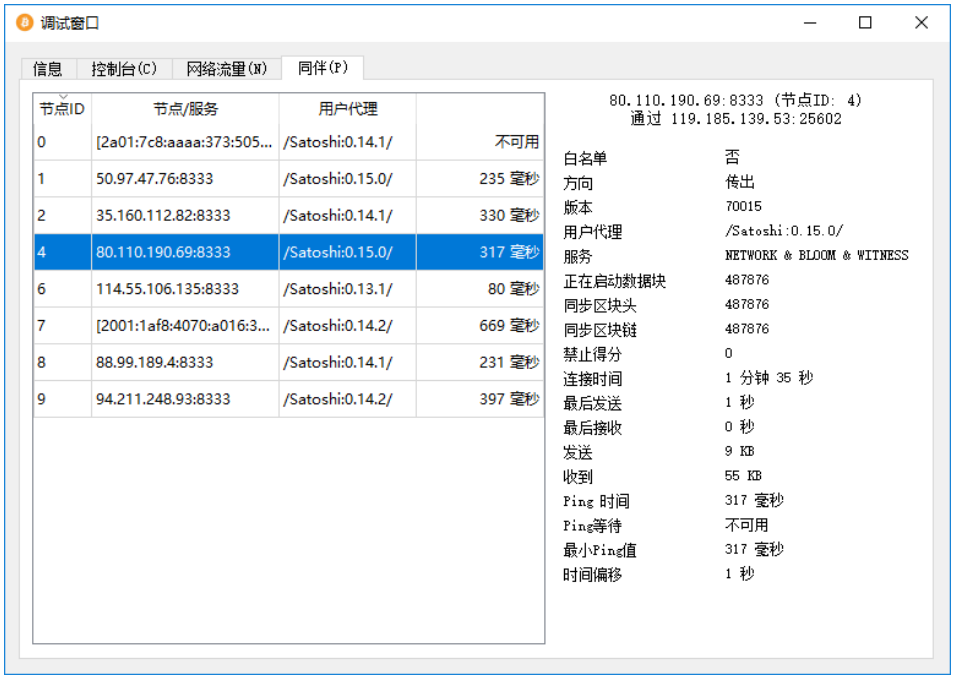


图3-7 Bitcoin Core 里查看同伴节点

3.5 不可篡改性

区块链里的信息具有不可篡改性，比如中本聪在**创世区块**中写的一段话：“The Times 03/Jan/2009 Chancellor on brink of second bailout for banks”，用来讽刺中心化银行的困境。这种不可篡改性是把双刃剑，好处是写入的内容有时间戳，可以作为证据，坏处是如果写入了不合伦理的内容，也无法删除。

我挺喜欢这种不可修改性的，就像微信公众号的文章推送出去后无法修改一样（2018 年初，微信公众号可以允许修改 5 个字了），这种特性可以让作者认真仔细地检查许多遍文章，直到自己实在看不出毛病的时候，再点击那个神圣的推送按钮。而“简书”没有这种限制，一篇文章逻辑是否清晰、是否有错字、内容是否完整等，我不太在意，因为将来还可以修改嘛。微信后来补充上了“删除”功能，可以把推送出去的文章链接强行失效，这点比区块链强。

虽然在区块链里可记录的字数非常有限，而且还要交手续费，但黑客们是不会放过这块区域的。在这笔交易中就隐藏着一封情书：https://blockchain.info/block/0000000000000000016f615859ca5cb88bb3983777df6f9f5ecbd57261cad454

图3-8 区块链上的一封情书

世界上每个人都可以点开链接，信的内容是这样的：

> “Dayah Dover, your personality is unmatched. Your intelligence just shines. You can do things few people can. And you’re always just gorgeous. You are really my entire world, giving my life meaning and fun. Dayah, I love you.”

写这封信的人用一堆收款地址拼出了这封信，还花了 0.00314159 BTC 的手续费，看来不仅是黑客，还是个数学迷。

2014 年 10 月，有一对新人 David Mondrus 和 Joyce 把结婚誓言写在了区块链上，据说这段话是：“For better or worse, ‘til death do us part, because the blockchain is forever”。

你也想发个毒誓吗？可以试着写到区块链上，真是公布给全世界的，没有撤消按钮的。

区块链刻字技术

本书作者之一申龙斌也研究过区块链刻字技术，我们没有矿池那么大的实力，可以在 coinbase 记录中写字符，但我们可以在挖矿发币的数值上搞点事情。我们在比特币现金(BCC)的区块链上写了一行字，网址：https://www.blocktrail.com/BCC/tx/b7971d23d28515a85cbb34cc0d30676d83d10805e4f14b23247639a28ce30569

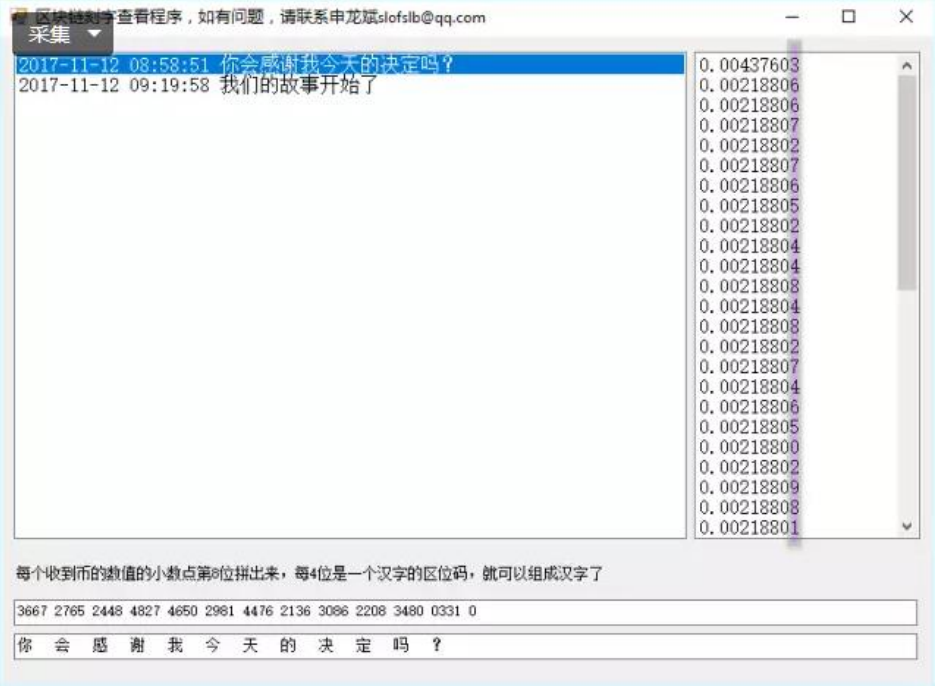


图3-9 区块链刻字技术

每个收币数量的最后一位数字可以拼成一串汉字的区位码，"3667 2765 2448 4827 4650 2981 4476 2136 3086 2208 3480 0331"代表着我们在区块链世界里写下的第一行汉字：**你会感谢我今天的决定吗？** 想了解详情，可访问：https://mp.weixin.qq.com/s/vxbc-Uc4xIxT35p527_fcw。

4 获得人生中的第一笔比特币

在购买第一笔比特币之前，还得先学习几个重要概念。

4.1 交易(Transaction)

类比：账单

前面把**区块**(Block)类比为账单盒，这个盒子里放的就是账单，对应的概念就是**交易**(Transaction)。我们每天都在进行各种各样的交易，比如今天我花了 5 元钱买了一份凉皮，可能会这样记录：

付款方	收款方	金额（元）
申龙斌	凉皮店老板	5

然而，在区块链里的记录格式与我们通常的记录方式稍有不同，是按资金的来源(vin)和

去向(vout)来记录的，大概是这样的（注意这里进行了极度简化）：

输入 vin	输出 vout
以前的某笔交易的某个输出	支付的币数 m，比特币地址 A 找零币数 n，比特币地址 B

先看输入 vin，你的币不是凭空来的，总是来源于以前某个交易的某个输出，这样一层一层地追查下去，总能找到创造货币的源头，这就涉及到了“**挖矿**”的概念了，稍后介绍。输出 vout 的币则作为下一次交易的输入，这样不断传递下去。

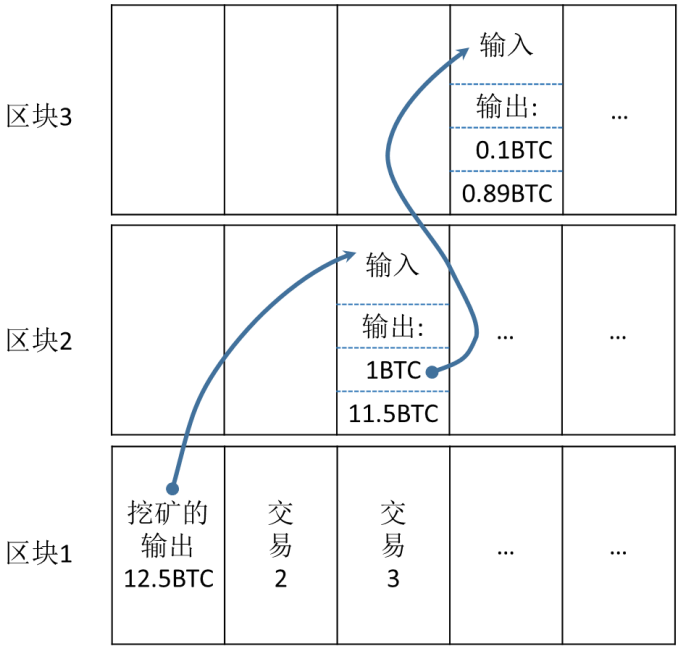


图4-1 价值传递示意图

假设我从**矿工**（矿工的概念在第 6 章介绍）那里买了 1 个 BTC，记录在区块链里可能是上图的样子。看区块 2 中的一笔交易，它的输入来源于区块 1 中的首笔交易，有 12.5BTC，也就是说 vin 为 12.5 BTC；而输出 vout 有两个，分别是 1BTC 和 11.5BTC，1 BTC 归我，另外的 11.5 BTC 是找零，仍归矿工所有，归属权是由加密原理来保证的，在后面的非对称加密原理中再介绍。

现在我有了 1BTC，我也可以消费了，假设我买东西花了 0.1BTC，我建立的交易会记录在区块 3 中，注意这里的输出为 0.1 + 0.89 = 0.99 BTC，还有 0.01BTC 哪去了？这个概念在第 4.5 章的交易手续费中再详细介绍。

我们知道区块是用链的方式串接起来的，内部的交易数据也是关联起来的，区块一层一层叠加起来，这样就形成了一个复杂的价值传递的链条，“**价值互联网**”在区块链内的表示方式就

是这样。

4.2 钱包软件(Wallet)

前面介绍过了一笔简单的**交易**，实际的交易会更加复杂，内部的记录格式是手工难以实现的，所以软件开发人员编写了一套软件，将用户从这些复杂的细节中解放出来，我们只管发币、收币、查询余额等常用的操作，复杂的处理过程全交给软件来处理，这种软件就叫**钱包软件**。本书一开始让大家安装的 Bitcoin Core 软件就是一款非常经典的钱包软件。

有些钱包软件的功能并不局限于处理交易数据，前面介绍过“去中心化”的概念，我们把参与到去中心化的比特币网络中的计算机软件称为**节点(Nodes)**，这些钱包软件也是节点，它们要与其它钱包软件互换区块数据和交易数据。

保存了全部大账本的钱包软件称为**全节点钱包**（2018 年 2 月的区块数据已经超过了 160GB），如 Bitcoin Core；而只保存了部分账本数据的钱包软件称为**轻钱包**(可能只需 160MB)，比如 Breadwallet 钱包等。

在下面这个网址有官方推荐的钱包可供选择，钱包软件一定要从官网下载，其它来源不明的钱包软件最好不要安装。

https://bitcoin.org/en/choose-your-wallet

图4-2 Bitcoin.org 官网推荐的钱包软件

不要下载来历不明的钱包软件。

4.3 比特币地址(Bitcoin Address)

类比：银行卡的卡号

钱包软件已经安装好了，可是里面的余额仍是 0，别人如何把比特币发送给我呢？类似银行卡的卡号，**比特币地址**(Bitcoin Address)就是用来接收比特币的。**比特币地址**的样子是一串长度为 30 左右的字母和数字组成的字符串，以“1”开头的地址最为常见，例如本书的捐赠地址是：

```
17CZJCqnTXoEkXgE19XeY1mSE1t8aLnShu
```

比特币地址这个术语是刚刚接触比特币的朋友最困惑的一个问题，这是由人的认知本能决定的，因为在看到**地址**这个词语时，他会与他以前熟悉的一个概念进行类比，通常能够马上想到电子邮箱地址或者是家庭地址。

这种类比本身并没有错，这些地址都是一种唯一的标识，用于收取别人发来的东西。电子邮箱地址用于收信，家庭地址用于收快递，比特币地址用于接收 BTC。只不过各种地址的表示方式差别非常大。

比特币地址在学术上是指**公钥的哈希 HASH 结果**。没学过密码学和计算机知识的人可能感觉这是外星人语言。这里先简单解释一下：

1）**公钥**是公开的钥匙，或公开的密码，好像有点自相矛盾，既然公开了，还叫密码？这是密码学中的**非对称加密原理**（在第 13.1 章再详细介绍）决定的，别人拿着你提供的公钥对信息进行加密处理，而只有你能用**私钥**进行解密。比特币的公钥是非常长的一串数字，用当前的电脑算上几万年，也猜不出私钥。

2）**哈希**是指 Hash，把一个长长的字符串进行一番数学变换，得到另一种字符串。在计算机中通常为了提高算法的效率，在比特币系统里是为了让字符串更短、更无规律、肉眼容易辨认，刚才说的那一串字符串中永远不会有数字 0，大写字母 O，大写字母 I 和小写字母 l 这些容易认错的字符。

比特币地址本质上就是公钥，所以可公开给别人，用于接收比特币。

比特币地址是公钥，可以公开给别人。

生成自己的比特币地址

打开 Bitcoin Core 软件，如果软件正在同步区块数据，可以点击“隐藏”按钮，显示出系统的主窗口。

图4-3 Bitcoin Core 正在同步区块数据

点击 接收(R) 按钮，再点击“请求付款”，则会弹出一个二维码窗口，里面有一串以“1”开头的字符串就是您的比特币地址。每次用过一个比特币地址之后，可以生成一个全新的比特币地址，这是出于安全的考虑，别担心，以前的旧地址仍然有效，仍可以接收别人发来的比特币。

图4-4 生成一个新的比特币地址

为了安全，Bitcoin Core 每接收一次 BTC 之后，会生成一个新地址。

4.4 私钥(Private Key)

类比：银行卡的密码

比特币里的私钥实际上是 256 位（32 个字节）的随机数字，如果你认为机器产生的数还不够随机，可以自己扔上 256 次硬币，正面为 0，反面为 1，生成的私钥记为 k 。

我们把私钥比做银行卡的密码，密码是自己掌握的，打死也不告诉别人。

把私钥看得比自己的命还重要，绝不泄露。

与银行卡的密码进行类比是不太准确的，比特币中的私钥代表了你的全部资产，因为区块链是公开的，别人拿到了私钥，就可以把你在区块链上的 BTC 全转走。而别人拿到你的银行卡的密码后，仍要知道银行卡的卡号，有时还要二次验证，需要手机验证码或 U 盾等才能把钱转走。

因为私钥非常重要，并且非常难记，所以私钥一般都隐藏在钱包软件中，你在支付比特币时，需要输入密码，钱包软件会自动把私钥取出，进行数字签名等操作，你得运用一些高级命令，才能看见私钥的本来面目。

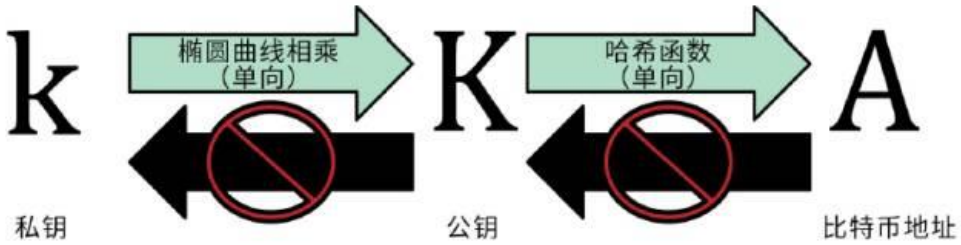


图4-5 私钥生成比特币地址的过程，摘自《精通比特币》

用上面这张图小结一下**私钥**、**公钥**、HASH、**比特币地址**这几个概念的关系：私钥经过非对称加密处理，产生公钥 K，因为是非对称加密，所以无法从 K 反算出 k。因为 K 还是太长、不容易辩认、可能还不够安全，就又经过一次 HASH 处理，才变成了我们公布给别人的比特币地址 A。同样，从 A 不能反算出公钥 K，就更不能算出你的私钥 k 了。整个比特币的安全体系就是建立这套加密算法的基础上的。

我们日常生活中用的钱包里夹着纸钞，这让我们许多初学者产生了一种错误认识"**比特币是保存在钱包里的**"，比特币系统中的所有 BTC 实际上都是保存在区块链上的，我们的比特币钱包里实际上保存的是一些私钥，我们拿着这些私钥去到区块链上验证各个交易，通过验证的才是我们的比特币。

钱包里其实并没有保存币，保存的是私钥。

4.5 交易手续费(Transaction Fees)

在当前的银行体系下，外币汇款不仅结算时间长，手续费还相当高，比如工商银行汇 2 万美元需要花 25 美元+110 元的手续费，大额汇款会更贵。而用比特币支付，手续费非常低，不管多大金额，0.0002 BTC 的手续费就可以快速完成支付，以当前 28000 元的行情折算还不到 6 元，不过 2017 年 11 月时比特币区块链没有扩容，拥堵情况严重，想快速到账，就要支付更高的手续费。

在介绍交易这个概念的图 4-1 中，区块 3 里有一笔交易，输入为 1 BTC，输出为 0.1 和 0.89，还有 0.01 BTC 不见了。这个 0.01BTC 正是交易手续费，这笔钱将被**挖矿**的矿工获得（在第 6 章介绍），比特币系统中关于手续费的设计还有重大的经济激励作用，以后再谈。

比特币转账的手续费不是按转账金额的大小来计算的，而是按照这笔交易在网络上传输时占用的空间大小来计算的。这些交易费最后是奖励给矿工的，因为矿工要耗费特别巨大的算力

来确认你的交易，他们的行为需要经济刺激，从而来保证整个比特币系统的安全。

也有不收手续费的交易，比特币系统根据币的新旧（币龄）、金额、输入、输出数量等来决定是否可以免手续费。在 Bitcoin Core 0.15.0 版本之后，不再支持零手续费。

在 Bitcoin Core 钱包客户端里可以自行选择支付多少的手续费，通常系统会给你一个推荐值，会让交易在较短的时间内得到确认。如果你想省点钱，则可以调低交易费，按每 kB 多少 BTC 设定。

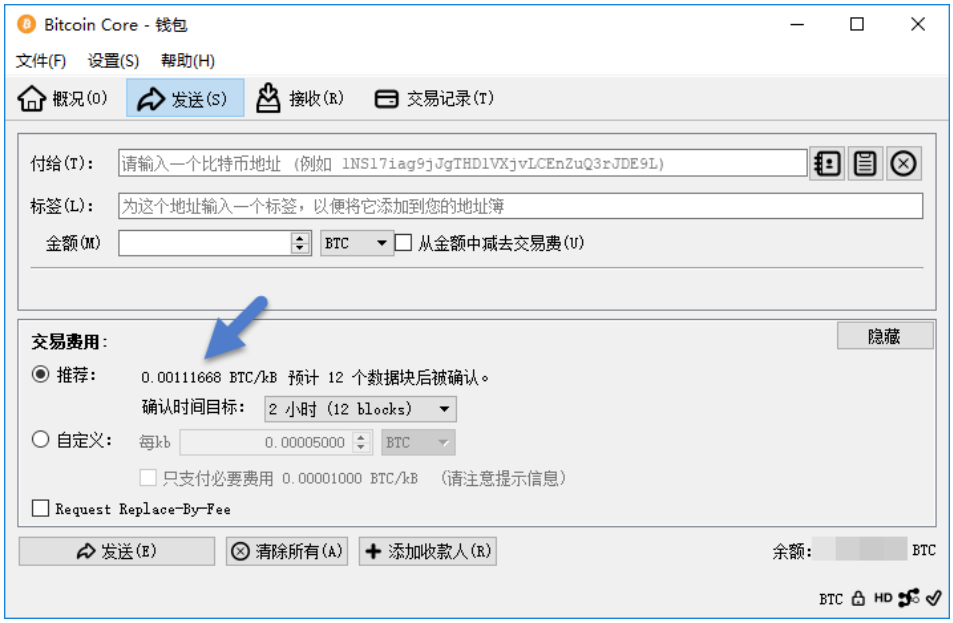


图4-6 Bitcoin Core 中可以自行设置交易手续费

如图 4-6 所示，在 Bitcoin Core 的发送界面中你可以自行设置手续费的大小，假如你想在 2 小时左右到账，系统根据当前区块链的拥堵情况给出推荐的参数，这里为 0.00111668 BTC/kB，一笔普通交易有 1 项输入，产生 2 个输出，则占用字节数为：148 * 输入个数(1) + 34 * 输出个数(2) + 10 = 226，最后的交易手续费为 0.00111668 * 0.226 = 0.00025237 BTC。以前我在饭团里搞活动时，给三位朋友分别转帐 0.001 BTC，手续费都是这个数。曾有一笔手续费设置得太低，曾经成为了一个孤魂野鬼在比特币网络中转了十多天，最后才得到确认。

详细的解读可以参考这一篇百度经验：http://jingyan.baidu.com/article/5552ef473c2bf4518ffbc914.html

几种交易费的实验结果：

我在饭团里举办过一次活动，有几位支付了 25 元获得了我发出的 0.001BTC，在这个过程

中，我试验了几种交易费，到帐情况果然差异很大。

5 月 27 日手续费低至 0.00000226 BTC 的交易，一直在内存池中徘徊，曾认为会成为孤魂野鬼在比特币网络中乱转，没想到在 6 月底竟然被确认。在 0.15.0.1 版本中增加了新功能，可以给未确认的交易增加手续费，这样就不会出现永远得不到确认的交易了。

交易费设为 0.000113 BTC，用了 1 周左右才被确认。

交易费设为 0.000226 BTC 时，在当前的网络拥堵状态下，比较安全，通常 1、2 天内可以被确认超过 5 次。

根据 Bitcoin Core 系统当时的推荐设置，当交易费设为 0.0007 BTC，一般 1 天内就被确认。10 月 2 日，1 个 BTC 报价 28000 元，现在看来 25 元真是赔钱的活动，还不包括给 jie 付了 2 次 0.001BTC 的情况。

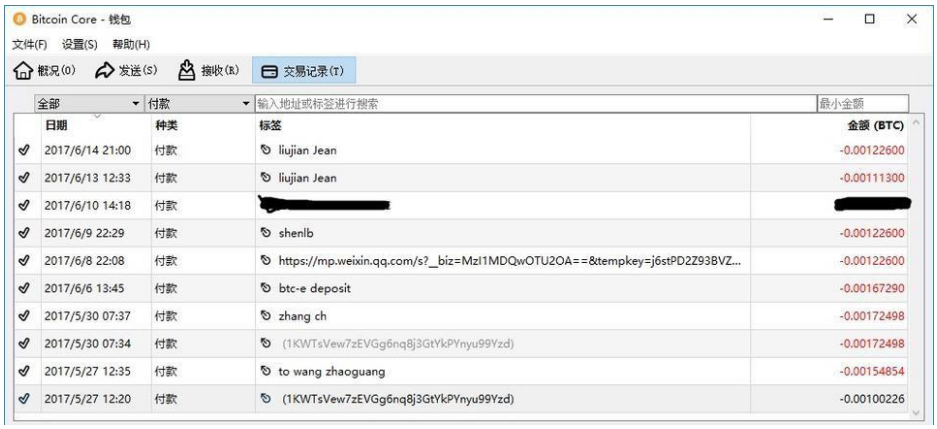


图4-7 付款记录

练习：

下面这个链接里有两笔交易，请说出每一笔交易的手续费是多少？是如何计算出来的？

http://blockchain.info/address/1KWTsVew7zEVGg6nq8j3GtYkPYnyu99Yzd

答案：

第一笔交易的手续费是：0.00072498 BTC（如果按现在的行情 2.9 万计算，相当于 21 元钱）

输入：0.98595146 BTC

输出：0.98422648 BTC + 0.001BTC

而第二笔交易的手续费则非常低，不过需要更长的时间才能确认。

图4-8 两笔交易的手续费

4.6 几种买币办法

有了钱包软件、比特币地址，明白了私钥等概念，就可以开始买币了。在 2017 年 9 月 30 日之前，国内买入比特币还是一件相当容易的事，当时可以在云币、OKCoin 等平台上注册账号，存入人民币，购买比特币，提币到你的比特币地址即可，但在 9 月 4 日国家下发了关停数字货币交易所的一纸公文后，买入比特币变得有点技术难度了。

（1）从朋友手中购买

如果你有一位值得信任的朋友，他手里有比特币，还愿意卖出，则双方协商后，你给他人民币，他转给你比特币，这应该是最方便的办法。

（2）从场外交易平台购买

这种办法对于初学者来说有一定难度和风险，场外交易称为 OTC，不信任的双方发起担保交易，一方把 BTC 锁定在交易平台中，另一方支付人民币，经过确认后，才把 BTC 转出。在 2017 年 10 月之后，国家关停交易所之后，这是国内用法币买入比特币的最常用的办法，详细操作步骤请继续阅读第 5 章。

（3）从国外交易平台购买

国内的交易所都不允许用人民币直接买卖 BTC，国外更不会接收人民币充值，将人民币兑换成美元等其它外币，然后再充值到国外平台中，再购买比特币，不仅要学会科学上网，还有外汇管制的问题，也是非常麻烦。

（4）挖矿

当前比特币这类主流数字货币的竞争非常白热化，你用家里的电脑挖上 100 万年，也挖不到一个 BTC，但其它的小币种还有点机会。自己可以找一台性能还不错的电脑，安装上挖矿软件，像 ZEC、XMR 等数字货币还能挖到一点点，再兑换成 BTC。这种办法，对于初学者就更难了。

4.7 取现(Withdraw)

老猫在 2017 年 4 月发表的《一切才刚刚开始》文章中，把区块链资产当做未来的现金，而把一切法币称为白条,话语虽有点偏激,但纸币货币正在向数字货币方向发展是不争的事实。

刚刚接触比特币的朋友对于买入 BTC（准确地讲，应该叫兑换）的过程感觉有点神秘，实际上就是没有把 **BTC** 与货币划上等号，如果把 BTC、ETH、EOS 等各种数字资产当做另外的一种货币，你在各种交易平台上完成的都是一种兑换操作。

在国内交易所还能用法币购买数字资产的时候，买入 BTC 的过程就是这样简单：存入人民币 → 买入 BTC → 取现。

但问题出在**取现**这一步，人民币取现需要提供卡号，BTC 取现需要提供**钱包地址**，这个地址不是你的居住地址，不是你的邮件地址，不是你的 IP 地址，也没有银行给你类似的卡号地址，而是前面介绍过钱包软件生成的比特币地址，取现完成后才有了第一笔数字资产，才有了活在未来的资本。

走过了这一步，其它各种竞争币的存入、取现就全明白了，你就进入了另外一个世界。以 BTC-e 网站（注：该网站涉嫌洗钱，已于 2017 年 7 月 26 日被查封）为例，各种币的买卖就是点击几次按钮这样的简单，USD（美元）不是数字资产，只是一种打通现在与未来的通道。

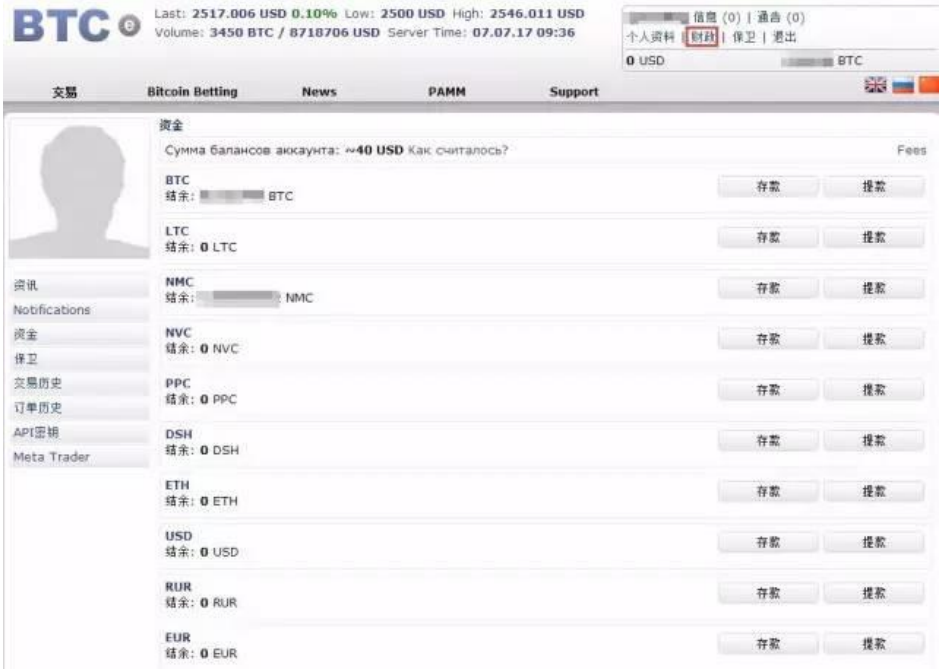


图4-9 btc-e 网站的账户资金页面

云币网(yunbi.com)上的买卖操作也是这样，不过云币网上把人民币 CNY 放在一栏，区块链资产另成一栏，充值和提现也彻底分开。根据国家政策，云币网已经在 2017 年 9 月停止了交易。

图4-10 云币网的账户页面

4.8 查询交易记录

刚才你已经一手交钱，一手发币，那么如何确认别人已经给你的比特币地址发送了 BTC 呢？以前说过区块链是公开的大账本，所有的交易信息都是全世界公开的，所以你可以有多种办法来确认对方是否已经发送了 BTC。

4.8.1 在钱包软件中查询

如果你的 Bitcoin Core 的数据同步进度是 100%，则可以点击“交易记录”工具栏看交易的情况。因为全世界所有的交易都要送到内存池里排队处理，根据比特币交易的火爆程度和手续费的多少，你的交易可能要等上几小时到几天才能得到确认。如果某一条交易的前面有一个问号，表示该交易尚未确认。双击该交易，还可以看到更详细的信息。

图4-11 查询交易记录

4.8.2 网站查询

如果你的 Bitcoin Core 没完成同步，还可以在互联网上查询，因为比特币的所有交易都会放到全球的共享大账本（区块链）中，谁都可以查，在 3.3 节中介绍了几个查询网站。我们这里以 blockchain.info 网站来介绍查询的过程。

登录网站 https://blockchain.info ，在搜索框中输入比特币地址，例如：1KWTsVew7zEVGg6nq8j3GtYkPYnyu99Yzd，这是以前我在饭团里搞个发送 0.001 BTC 小活动时 jie 的地址。

可以看到该地址的余额和交易记录，这里显示的是美元价，可以点击那个 $2.11 按钮，切换为 BTC 货币单位。

图4-12 用网站查询交易记录

注意那个“交易未确认！”信息，我为了试验不同交易费的效果，这笔转账只用 0.00000226 BTC，即 226 聪，这么低的交易费，24 小时过去了仍未确认，后来经过了十多天才得到了确认。如果是小额交易，1 个确认数就足够可信，如果是大额交易，则要有 6 个以上的确认数。

点击交易记录下方的那个长长的字符串 0353d...20dcd，可查询这笔交易的详细信息：

图4-13 交易详细信息 （美元为单位）

输入总额($53.41)是指付款方(左侧)比特币地址的余额，右侧上方有两个地址，$2.11 对应着**收款方地址**，$51.29 是找零的地址。**交易费**（矿工费）换算成美元显示为 0.00，可以换成 BTC 单位，这样可以看见 0.00000226 BTC 的交易费。

图4-14 交易详细信息（BTC 为单位）

点击可视化后的“浏览树状图”，可以看到一个简单的图示，比特币是从左边的地址发出来，右上的地址是收款地址，右下的是找零地址。

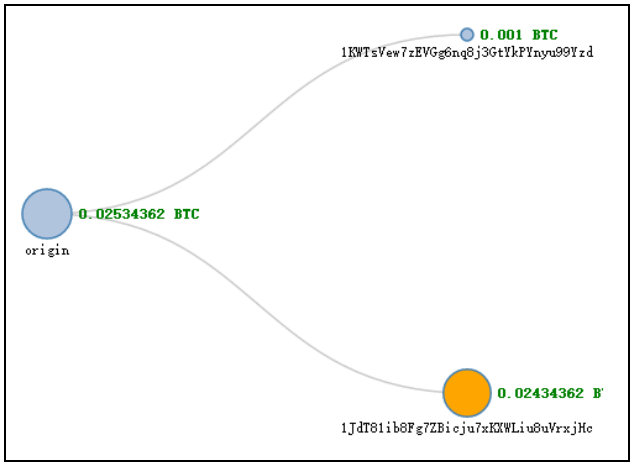


图4-15 交易信息的图形化显示

如果你已经用小额资金跑完了购买比特币并且保存到自己的钱包中的全过程,这时一定要再核查一遍钱包的安全，**你是否已经加密了钱包？将 wallet.dat 备份好？牢记住了密码？如果将来保存了大额资金，还要将密码告诉最亲近的人，以防自己发生意外时可以将遗产转移给亲属。**

5 场外交易(OTC)

2017 年 10 月，国内交易所关停，购入比特币需要使用场外交易方式，即 OTC 交易，Over The Counter。这种翻译不太好记，去药店的时候留心的朋友会看到 OTC 药，通常翻译为非处方药。从英文上直译，实际上是一种意思，over the counter 在柜台上就直接可以购买的药。而 OTC 交易，就是在桌子上就可以直接交易，面对面就可以交易的意思。

5.1 场外交易前的几点准备

5.1.1 科学上网

现在许多交易所网站都需要科学上网来解决，请自行搜索 VPN，即**虚拟专用网**(Virtual Private Network)，本来是通过互联网链路来访问自己公司内部的网站的一种办法，但现在 VPN 已经是科学上网的同义词。网上的 VPN 产品和服务非常多，但免费版的大多有流量限制或访问质量不佳。

一款常用的产品是 Lantern，可以从这个网站下载：http://lantern.findmysoft.com/download 。

图5-1 下载 Lantern

下载并安装后，会弹出一个网页页面，就代表已经完成连接 VPN 了，桌面上也会出现一个小图标，注意免费版本只有 500M 的免费流量使用。另外可以一试的 VPN 是一枝红杏，以前 200 元能用一年，现在越来越贵了。

5.1.2 实名认证 KYC

所有的正规的从事与资金交易有关的平台或网站都要经过这类审查，通常是扫描身份证，有些还要求通过人脸扫描识别。过程很简单，提交相关材料后，耐心等待结果即可。有些国外平台可以不经过 KYC 认证，但交易额度非常低。

这里引用百度百科对 KYC 的定义：

> Know Your Customer
>
> KYC 政策（即充分了解你的客户）对账户持有人的强化审查，是反洗钱用于预防腐败的制度基础。KYC 政策不仅要求金融机构实行账户实名制，了解账户的实际控制人和交易的实际收益人，还要求对客户的身份、常住地址或企业所从事的业务进行充分的了解，并采取相应的措施。了解资金来源合法性。

图 5-2 是 Otcbtc.com 网站上的实名认证步骤。

图5-2 Otcbtc.com 网站的 KYC 认证

5.1.3 海外苹果 ID

如果你要在手机上使用数字资产相关的软件，Android 手机上安装比较方便，但在苹果手机上会有点麻烦。许多软件在国内的 AppStore 无法上架，你需要使用海外或香港 ID 登录 App Store，才能安装相关的 App。比较方便的获取海外 ID 的办法是从“某宝”上用 10 元钱购买一个，记得购买之后马上修改密码。

5.2 谷歌身份验证器

5.2.1 什么是谷歌身份验证器

不少网站在登录或者操作时都需要谷歌身份验证器（Google Authenticator），就是说在输入用户名和密码之后还需要输入一个动态密码，而这个动态密码由手机 APP 谷歌身份验证器生成，不但不依赖于网络，还在每 30 秒自动更新，是不是很强大？当初办过农行的动态密码，是给一个小卡片，由横坐标和纵坐标组成，每次使用时根据坐标点来确认密码是多少，用着用着会出现重复，卡片还得随身携带，太不方便。再到后来的 U 盾，单独给个小 U 盘的东西，也方便不到哪里去。现在谷歌直接做一个应用就搞定了！

目前接触到比特币相关网站基本上都采用它，尤其是提现等与钱直接相关的操作时。

5.2.2 如何安装使用

（1）根据您使用的手机系统类型，下载并打开谷歌身份验证器 APP 到手机上。

✧ iPhone 手机：在您的手机上安装双重验证程序：Google Authenticator

✧ Android 手机：在应用市场中搜索“谷歌身份验证器”，或搜索 Google Authenticator。若搜索不到，可去官方或 Google play 上下载，不过需要科学上网

（2）网站会给出一张二维码和一行密文，在扫描之前一定要注意一点，先把密钥（或叫密文）记录备份下来再扫描，如果误删，或者手机丢失，可通过手动输入密钥来恢复你的账户，否则容易人财两空。密文和二维码不要泄漏给他人。

图5-3 谷歌验证器的密文及二维码

备份好谷歌验证器的密文，并且不要泄漏给他人

备份好之后在“Google Authenticator（身份验证器）”应用程序中，点击“添加新账户（iOS 下是 + 号）”，然后选择“扫描条形码”。 将手机上的相机镜头对准二维码扫描该条形码。

不少手机在这步会提示条码扫描器不可用，那就需要下载一个应用，可在应用市场搜索：条码扫描器。

（3）填入手机显示的动态密码就可以在网站激活两步验证了。

5.2.3 验证码失效原因分析

最近中国关闭比特币交易所之后大量人员需要注册海外交易网站，而这些网站基本上把使用谷歌身份验证当成必选。但因为各种各样原因不少人却卡在验证码上，收到“Invalid code”或者”Incorrect Code”或者”has expired”等验证码无效的消息，到底是什么原因呢？

原因一：30 秒时间已过

这个验证码是 30 秒自动更新的，如果输入之后恰好赶在它更换验证码，那原来这个已经失效，所以输入的时候看好时间，如果时间不够，就等它更新之后再输入。

原因二：时间不同步

有些人遇到过注册的 B 网、P 网、BFX 无效，一种可能的原因是 APP 没有正确同步，也就是说你手机的数据和谷歌服务器的数据不同步，可以试试如下步骤：

1）安卓手机

（1）打开科学上网。

（2）进入谷歌验证的主界面，点击右上角三个点，选择设置。

图5-4 身份验证器的设置

（3）选择“校正用来生成验证码的时间”，选择立即同步，完成之后，APP 就会提示已经同步，就可以正常使用了。

图5-5 校正用来生成验证码的时间

2）苹果用户

（1）打开科学上网

（2）进入苹果设置（注意，不是谷歌身份验证的设置）

（3）选择通用

（4）选择时间&日期

（5）激活自动同步设置

（6）如果已经激活，禁用下，过几秒之后再重新激活下就行了

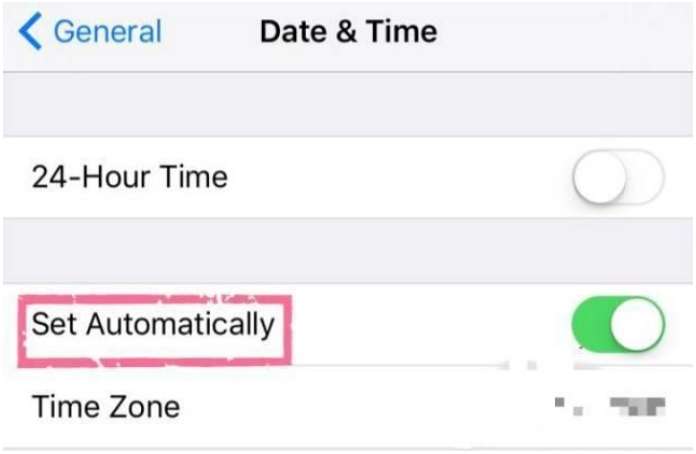


图5-6 苹果手机中的时间设置

5.2.4 不能扫码原因分析

在给一个手机装好这个软件之后竟然发现不能扫码，其它扫描正常的，只有这个应用不行，费尽九牛二虎之力终于在网上找到解决办法：

这个扫码器打开时，如果二维码恰好在红框里，则瞬间成功扫描；否则，即使后来手段将二维码移动到红框里面，也没反应。这肯定是个 BUG，软件的逻辑没写好。

解决方法：第一次打开扫描界面，如果二维码不在框中，则手动移动至合适位置，然后回到上一个界面（手机按下返回键），重新选择扫描二维码，整个过程中尽量保持手机镜头静止，不要有大的位移，那么第二次进入扫码界面时，由于上次的定位，这次二维码已经在框中了，于是立刻扫描成功。

有了这个利器，接下来你就可以到交易所愉快地玩耍了。

5.3 从 localbitcoin 上场外交易买币

localbitcoin 是全球交易量最大的场外交易所之一，可以方便的通过支付宝，微信，银行卡购买比特币。

1）注册 localbitcoin

注册地址：https://localbitcoins.com/zh-cn/，注册时按照提示步骤操作一般不会出问题，注意需要科学上网才可以完成验证码的输入。

图5-7 注册 localbitcoins

注册成功后一定要及时完成相关的安全设置，google 二次验证是必须的，其他安全措施按照账户安全的操作设置即可。

图5-8 开启 google 二次验证

2）发起交易

选择购买一个比特币，在快速购买选项选择币种 CNY，国家 China，点击搜索后就会看到国内的卖家，可以选择国内银行卡，支付宝等。

图5-9 快速购买

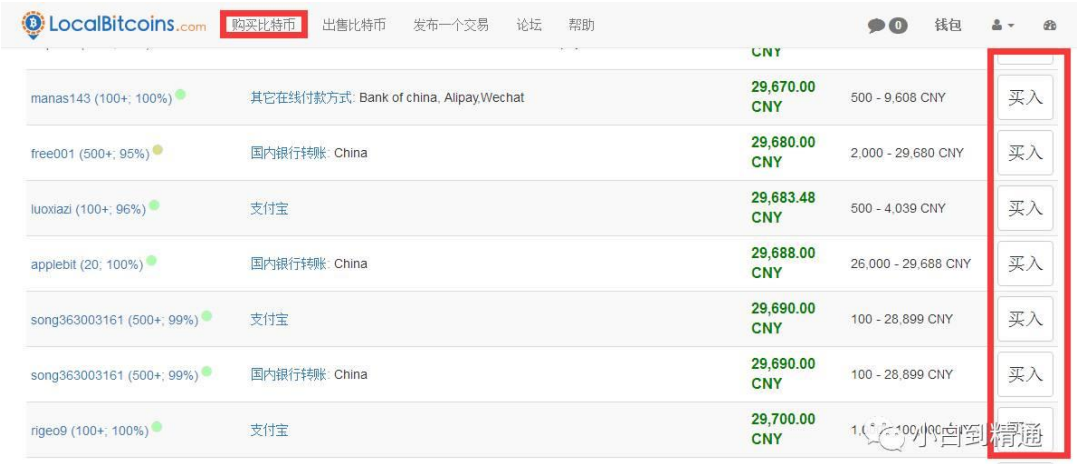


图5-10 挑选卖家

我们选择一个可以小额交易的卖家体验，购买价值 100 元人民币的比特币，发送交易请求。

图5-11 发起交易请求

卖家回复消息后，按照卖家给出的支付宝账号转账 100 元。

图5-12 转账

留言页面，localbitcoins 很贴心的在右侧有交易步骤的提醒。

图5-13 交易提示

确认我已付款后，卖家释放比特币交易结束。网站右上角的余额处发现比特币已经到账，是不是很方便呢。

图5-14 交易完成

3）交易体验

- ✧ 需要科学上网，略显麻烦些
- ✧ 网站有中文版，操作方便
- ✧ 交易量非常大，可选择的卖家非常多，支持小额交易
- ✧ 付款后卖家秒释放，体验非常快
- ✧ 没有找到靠谱的 app，如果有 app 的话会更方便的

✧ 交易完成后会有邮件提醒

5.4 在 OTCBTC 上场外交易（推荐）

OTCBTC 是专门的场外 OTC 法币交易平台，定位很精准。公司注册在台湾，技术团队是曾经与李笑来合作的郑伊廷带领，郑伊廷开班的全栈营专门培养技术人才，所以技术背景很强，在短时间内搭建交易平台，获得大家的认可。

1）注册 OTCBTC

打开连接：https://otcbtc.com，用邮箱开始注册（好像不能用 qq 邮箱注册）

图5-15 注册 otcbtc

到注册的邮箱进行验证通过

图5-16 otcbtc 的邮箱验证

点击验证邮箱

图5-17 收邮件，验证通过

点击实名验证，与通常的 KYC 流程一样。

图5-18 otcbtc 实名认证

2）发起交易

开始用法币购买你要的数字货币了，以 OTB 为例

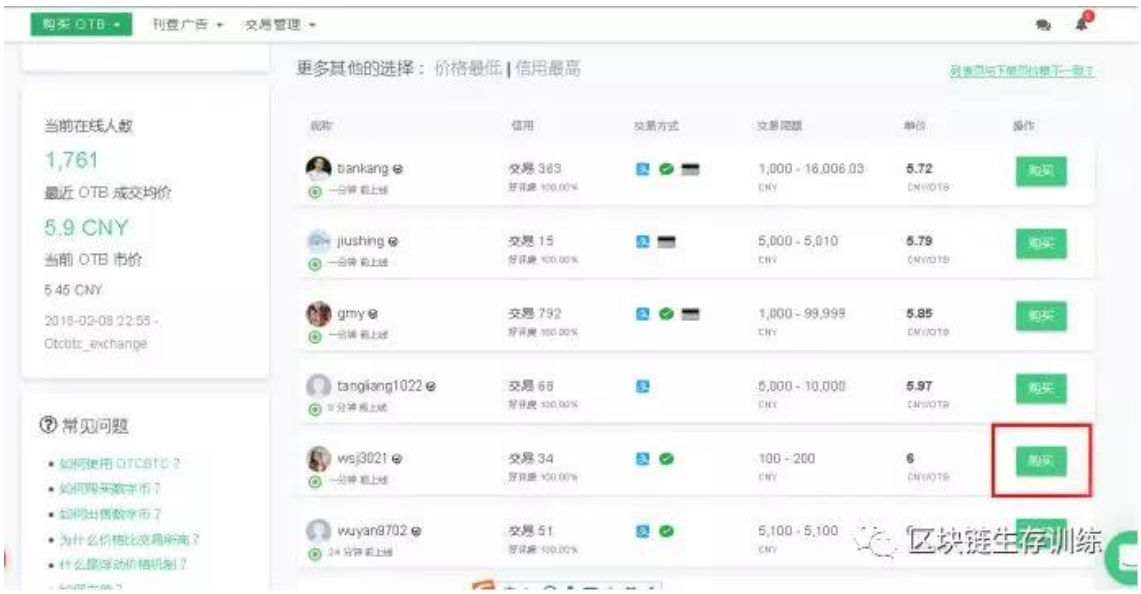


图5-19 发起交易

输入你要买的金额数

图5-20 购买的金额

付完款后，点击“标记付款完成”

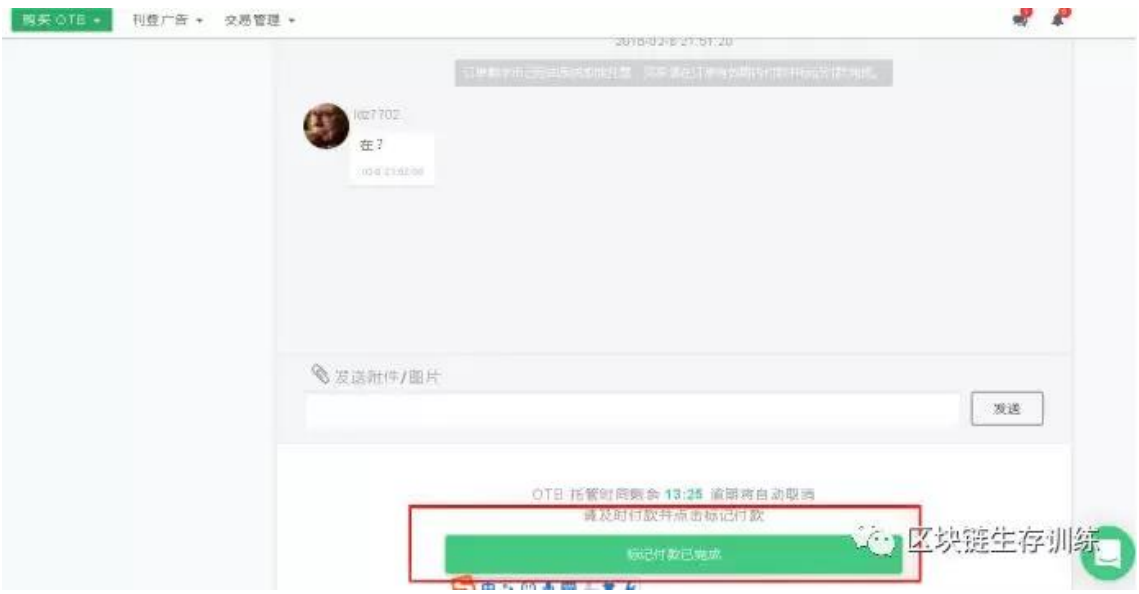


图5-21 标记付款完成

付款完成后，点击资产管理“我的钱包”查看买到的数字币

图5-22 付款完成后，到钱包中核实

3）交易体验

✧ 交易币种多是最大的优势

✧ 平台溢价比 localbitcoin 要多不少，价格偏高

✧ 大户严重垄断，除了 BTC，EOS 等几个活跃币种之外，其他币种交易量少。

5.5 币信场外交易 OTC 实战

币信场外交易软件是相当有历史的 App，操作流程：

1）安装币信，认准官方地址 https://bixin.com，也可从苹果商店安装。

2）启动币信，用手机号及短信验收码，马上就可以完成注册和登录操作，非常便捷。

3）通过 KYC 认证，实名认证，身份证扫描和脸部识别之类的。

4）扫码加入李荣强推荐的交易群，里面几百人在里面交易。

图5-23 OTC 交易群

5）如果对某人的出价感兴趣，点击该人头像，私聊，确认该人是否通过实名认证。

6）商量好价格，卖方发起一个担保交易(即由币信平台先锁定资金，待完成交易后释放)，同时告诉你付款的办法（银行卡、支付宝）。

图5-24 私聊发起担保交易

8）根据商量好的价格，完成支付操作，我此次用的是支付宝。

9）卖方发币，买方在币信中马上就可以收到通知，也可以到钱包中查询。

图5-25 在币信的钱包中确认 BTC

5.6 从 bitcoinworld 上场外交易买币

图5-26 bitcoinworld 网站

bitcoinworld 看起来是针对中国人操作的场外交易网站,方便的地方在于可以直接通过 app 来操作，放款速度也不错。

1）注册 bitcoinworld

注册地址：https://bitcoinworld.com，按照步骤操作，几分钟就可完成，很方便。注册完成后的 kyc 认证也很快。

图5-27 注册 bitcoinworld

平台关于安全方面的考虑也很全面，按顺序完成账户安全设置即可。

图5-28 安全设置

2）发起交易

打开 bitcoinworld APP，进入广告页面，可以看到很多买家

图5-29 找卖家

选择进行交易的卖家，进入在线购买的页面，输入自己要购买的金额，和卖家在线沟通即可。

图5-30 与卖家在线沟通

由于 kinki 的卖家没有及时回复，之后换了 lishikai 这个卖家沟通。

图5-31 再找一个卖家

和第二位卖家沟通确认后，转款支付宝

图5-32 支付宝转账

支付完成标记已付款，卖家回复已经放款成功。

图5-33 沟通交易结果

查看钱包余额发现 btc 已经到账。

图5-34 交易确认

3）交易体验

✧ 注册方便，认证简单

✧ app 操作上手容易，方便随时随地的买卖

✧ 支持小额交易，最低的见过 100 起的

✧ btcworld 也有自己的币币交易平台，可以方便兑换 eth

5.7 从 coincola 上场外交易买币

图5-35 coincola 网站

可盈可乐是国内平台关闭之后出现的位于香港的场外交易平台，也支持 APP 交易，界面操作和 bitcoinworld 类似，非常方便。

1）注册 coincola

注册地址 https://www.coincola.com，按照提示注册完成即可。平台安全验证也是必须的，和以上网站类似，此处略过。

图5-36 注册 coincola

2）发起交易

coincola 可以使用 APP 交易，下载登录 app 后，点击交易，进入交易市场

图5-37 找卖家

在交易市场中选择想要发起交易的卖家，输入购买额度，我测试的卖家是支持 100 元的小额交易的。

图5-38 发起请求

根据卖家给的支付宝账号，进入支付宝完成 100 元的支付宝转账

图5-39 支付宝转账

返回 coincola，在购买订单中标记付款。

图5-40 付款确认

卖家收到付款后，会释放 btc 给购买人的 coincola 的钱包，注意在付款前一定要和卖家联系沟通下，这样放款会快些，本次测试操作在 1 分钟内就收到卖家放款了。查看钱包，看到钱包总资产已经有 0.0034163，按照购买的汇率计算合人民币 100 元。

图5-41 确认收币

3）交易体验

- ✧ 注册方便，认证简单
- ✧ app 和 bitcoinworld 类似操作，上手容易
- ✧ 支持小额交易，最低的见过 20 起的
- ✧ 国内买卖交易多

5.8 在 bitpie 上场外交易买币

1）注册 bitpie

app 下载注册即可，注册过程略。

2）发起交易

bitpie 上的购买 btc 是通过 app 的多重签名服务来完成的，发起交易前需要首先完成 kyc 的认证，认证过程略。（其实是因为认证的太早，忘记截图了）

选择**多重签名服务**，选择卖家进行交易。

图5-42 选择多重签名交易

进入多重签名服务之后，选择卖家进行交易

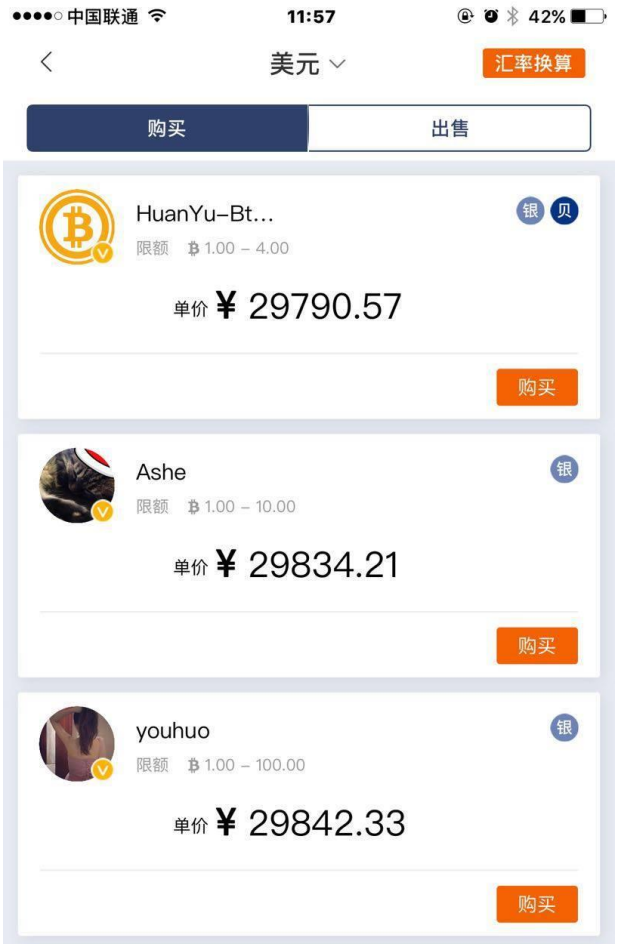


图5-43 选择卖家进行交易

选择卖家交易后，会发现交易之前需要完善个人信息，其实最重要的是完成押金支付。

图5-44 完善用户信息

押金充值的流程如下，按照提示完成支付宝转账之后就开通了多重签名服务，也就是我们要进行的 btc 的买卖交易功能。

图5-45 支付宝支付押金

发起交易后，等待卖家确认后，就可以完成支付，收到币了。由于支付金额较大，之后的支付流程未进行体验。

图5-46 未完成支付流程

3）交易体验

✧ 交易量小，交易金额大，卖家少是最大的劣势。

✧ 进行交易需要支付押金，从安全角度来说也并没有多少提升，反倒让用户交易变得麻烦了。

✧ 由于未完成最后的支付，付款后的释放部分未体验。

几种场外交易平台的小结：

本次体验完成了几种 btc 场外交易的尝试，几个场外交易网站的步骤都是按照如下流程操作：

（1）寻找卖家，创建订单，发起交易

（2）买卖双方线上沟通确认卖家收款账号

（3）买家通过第三方支付平台直接付款给卖家

（4）卖家收到付款后，释放比特币到买家交易网站钱包，至此交易结束

从场外交易的流程来看，已经非常方便了。除了 bitpie 钱包的交易略显麻烦之外，剩下几个场外交易平台都是非常方便的，otcbtc.com 的体验应该是最好的，如果小额的话，通过 bitcoinworld 和 coincola 两个平台的 app 来交易会更便捷一些。

最后，需要注意的重点是交易前一定要查验卖家的交易信用，如果以后有一个区块链的场外交易所，该是件多好的事情啊，未来的世界，信用真的是第一位的！

5.9 数字货币场外交易骗术汇总及防骗指南

现在禁止人民币直接在交易所购买数字货币，只能通过场外交易方式与个人交易。

场外交易有两种：场外交易群和场外交易网站，前者是通过熟人担保，后者是通过平台担保。

不管是买币还是卖币，操作流程是相通的：只要开始下单，币就会被担保人或平台锁住。等钱到账户后，才能释放货币，如下图的 OTCBTC 释放货币界面。

图5-47 释放数字货币

其实，骗子通常比我们想象的要精明，为了保障好自己的币和钱的安全，以下用部分人血和泪的经历，总结出以下的经验，希望能帮大家识别他们的欺骗手段：

5.9.1 骗术 1：利用支付宝、微信、银行的延时转账

骗子利用**延迟到账功能**，截图给交易方，要求放币，这时一定要查看各种账户界面的金额提示。因为支付宝、微信、银行都有延迟到账功能，骗子可以利用这段延长的时段，找理由去阿里、腾讯或银行进行撤回，结果钱被返给了骗子，且币也转给了骗子！

延时转账设置如下：

支付宝 App：转账→右上角三点图标→延时转账服务→可选择实时到账、2 小时到账或者 24 小时后到账。

支付宝还有一项功能“请你代付”，买家如果发来截图，这不一定代表付款完成，请先查看帐户钱已到账，才能放币。

图5-48 注意是否延期到账

微信钱包：右上角支付中心→支付管理→转账到账时间→可选择实时到账、2 小时到账或者 24 小时后到账。微信钱包只要设置过一次延迟到账，后面所有的转账都会延迟，要取消的话只能再重新设置一遍。

银行：除了实时转账外，“普通汇款”和“次日汇款”也有延迟功能，里面有提示：2 小时后可撤回，所以也要特别小心。

图5-49 银行汇款也有延期到账的情况

比如，对方给你发如下的截图说已经转账成功，但实际情况呢？

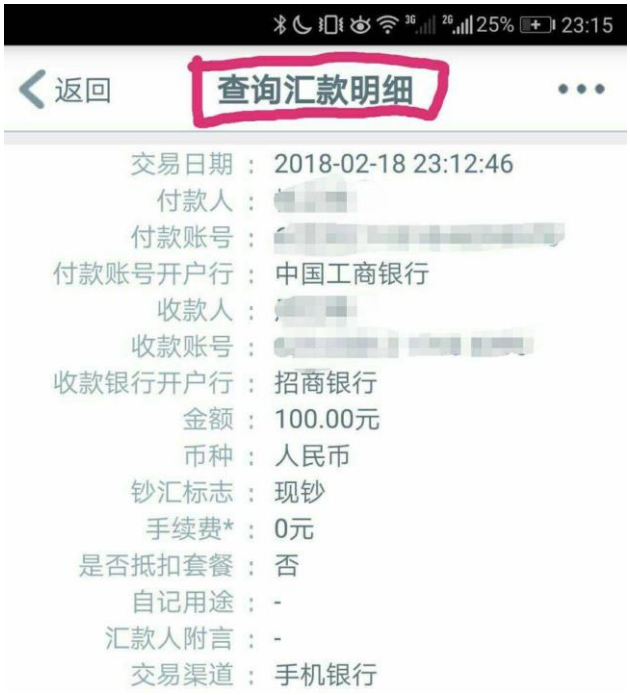


图5-50 转账明细并不一定实际到账

我们来看看这张截图的下半部分：开通了普通汇款，2 小时内可以自己撤销，若你不去银行账户查询，仅凭这个截图就相信，那就是钱去币飞。

图5-51 普通汇款可在2小时内撤消

鉴别方法：只要款未到账，绝不放币。怎么算到账？余额已经显示，甚至转账下，比如余额转到余额宝，微信提现，或银行再转账。

5.9.2 骗术 2：利用银行短信

（1）伪银行平台发出短信，截图告之已经付款，如下图。这时一定要查看这笔钱是否真

的到银行账户了。

图5-52 银行短信通知

（2）确实是银行短信，通知已经付款，

比如工行号码 95588 发来消息 ，是不是可信？ 答案是：**不！一！定！**

这一招极具迷惑性，骗子是这样操作的：

骗子事先通过各种方式，问你要手机号，然后用自己的两张银行卡左手倒右手，转账的时候勾上短信通知，并写上你的手机号上。所以骗子互倒之后，银行往你的手机上发了转账成功的短信，实际上钱还是到了他自己的账户上。

鉴别方法：这时请务必打开银行账户核查这笔款确定已经到帐，否则不能放币。

若发生银行账户被锁的情况，一定要极度小心。有时，情况太巧，是有原因的。账户被锁，无法查看余额，就不能放币。

有时候交易方会一直催着放币，并多次强调查收付款短信，但账户没收到就可以不理。

5.9.3 骗术 3：绕开平台，私下交易

（1）单笔订单 5 万元以上，银行需要一定的时间进行审核，平台需要进阶验证

因此理由，买家极力难说你要走私下交易，这一定是骗子，请务必当心。私自交易没有平台锁币功能，一旦付款后，卖家不放币也是没办法的，只能自己承担后果。

（2）为了省手续费等各种理由，而劝你走私下交易

有时候先和你交易下，获得你的信任之后，会说省交易费之类的话，再让你走私下交易，这个时候一样是骗子。下图就是一个朋友的朋友先和对方在平台交易 1000 元，取得信任后，绕开平台，不小心被骗了 4.9 万。

图5-53 勿走私下交易

所以：**不管是什么理由，让你不走平台交易，都不要同意！**

否则你的币流到哪里去，都无法查出，更别说去追回了。

5.9.4 骗术 4：其它

（1）混淆数字：比如应该付款 20000 元，对方直接付 2000 元，这时一不小心就会点击“释放货币”。

（2）直接在平台的聊天对话框输入已付款信息造成误导：

有时候人是容易麻痹大意的，在和你聊天的过程中，然后把付款信息发到对话框，告诉你已经付款了，一不小心就容易释放货币。

（3）大量下单，甚至是同样的单（适用广告主）：

比如你发了一个广告，销售 BTC，若多人同时购买你的 BTC，比如一下子几十单，在你忙不过来时个别订单不付款却点击已付款。

如果套路再深点，有几笔单子金额一模一样，然后有一两个不付款，这样迷惑性更大。

人在急的时候就容易出错，需要一个个仔细核对账户的钱，也可以限定同时处理单子的数

量。

最后，我们用换币网的防诈骗提醒来总结：

（1）记住，若没有核实确认已经收到钱，绝对不要放币、提币 !!!

（2）为避免因收到诈骗短信错误释放数字币，请您在收到银行到账短信时

务必登录手机银行核对银行卡的入账记录 !!!

（3）请勿相信买家的大额订单骗局，例如（打款 10 万元给你），让你把数字币直接提币到对方钱包

请不要直接把数字币提币到买家钱包 !!!

但大家也不用被骗子给吓倒，掌握核心的原则：到支付宝、微信或银行卡账户里仔细核对入账明细，保证通过平台交易，就比较安全了。

6 挖矿(Mining)

类比：挖掘黄金

对于刚刚接触比特币的用户来说，感觉最不可思议的术语就是“挖矿”了，一个运行在网络上的数字大账本，还需要动用挖掘机吗？实际上“**挖矿**”只是一种类比，与黄金的挖掘方式相类比，黄金的开采费时费力，而且黄金资源有限。比特币的挖取也是费时（需要大量的计算）、费电（一台专业矿机每天要消耗 50 多度电），而且 BTC 资源也有限，总量 2100 万个，每四年新币数量减半。

在第 4 章介绍“交易”的概念时提到，BTC 是通过交易链一层一层传递的，而最初的币是从哪里来的？就是通过 “挖矿”来的，而且所有的币没有其它来源，全部都是通过“挖矿”得来，没有任何一家机构可以无缘无故增发比特币。

6.1 矿工(Miner)与矿池(Pool)

挖矿任务的实施者叫“**矿工(Miner)**”，不像挖黄金里的矿工，这里的矿工是一台冰冷的计算机（通常配有专业的挖矿芯片，还有挖矿软件），它们靠电力支撑其复杂的计算，单个矿工的力量毕竟有限，它们则采用集团作战的方式，组成“**矿池(Pool)**”，每个矿工按贡献率分成。

挖矿的结果是产生一个新区块，也就是在共享大账本上增加一个账本，想获得这种记账权并不容易，需要完成复杂的计算（专业术语叫**工作量证明 PoW**，随后介绍），第一个完成计算的才有资格在区块链上增加一个新块，新区块中含有新币奖励（最早为 50BTC，每四年减半，2017 年新块奖励 12.5 BTC，2020 年 5 月将为 6.25 BTC）；新区块中还包含了网络上广播的数笔交易，这些交易中的手续费也全由矿工拿走。在 2009 年比特币刚诞生的时候，用一台电脑就可以完成这些计算，当时的 Bitcoin Core 中还内置了一个挖矿模块。

从这里我们可以知道挖矿有两个意义：一是验证交易的合法性，写入大账本；二是发行新币。由于这个行业的巨大经济诱惑，随着时间推移，大量的计算机投入到这种计算中，通常的 CPU 被高性能的 GPU 显卡取代，再后来，专用的挖矿芯片 ASIC 问世，运算效率是 CPU 计算的上万倍。如果你现在想用自己的台式机挖矿，就相当于你用一双手挖黄金，而别人用专业团队+全副武装的挖掘设备来挖，你忙活几百年也别想挖到 1 个币。

打开这个网站（http://www.qukuai.com/pools）或者这个网站（https://coin.dance/blocks）可以看到最新的区块都是哪些矿池挖出来的。

挖矿的作用：发行新币、验证交易的有效性。

6.2 双重支付(Double-Spend)

区块链解决了数字货币支付中的一项关键难题，称为“双重支付”，即 double-spend。即一笔数字资产既支付给了 A，又支付给了 B。有些书或网络文章中也把 double-spend 直译为**“双花”**，让初学者难以理解，千万别理解为两朵花。

在去中心化交易技术之前，这类问题通过中心化的机构来解决，比如：银行。你用手机银行给别人付了一笔钱，银行把余额变动一下，想多花也不可能。当然信用卡账户允许你 0 余额还可以支付一定数量的资金，能否透支那都是银行说了算，比特币世界里不让透支。

比特币的创始人中本聪设计了一套完整的体系解决了这个问题，共享大账本（区块链）、去中心化的网络（比特币协议）、交易验证系统（交易脚本）和货币发行（挖矿）等。

大家可能会想，又是挖矿、又是工作量证明，为什么把新区块的产生搞得那么复杂？一个主要原因就是解决在没有任何信任关系的网络中的**双重支付**的问题，当然这种挖矿机制还能够解决虚假交易、垃圾交易等问题。

这种技术也可以解决"**拜占庭将军问题**"，即一支分散在多处的军队里混入少数叛徒，如何才能通过一致的行动来保证战争的胜利。关于这个问题的更详细解释，请见第 8 章。

假如你在两台安装有 Bitcoin Core 的电脑上分别发出了 2 笔交易（同一笔 BTC 输入，支付给 A 和 B），这些交易都会向全网广播，矿工在收到这些交易时，不会将两个交易都打包。如果有矿工故意作假，把 A 和 B 都打包，交易广播后还有许多其他节点要进行验证，仍会拒绝承认这个区块，也就是说这笔交易的确认数会一直为 0。小额交易等待 1 次确认就行，大额交易等待 6 次以上的确认就足够的安全。

在比特币世界里想透支，是不可能的。除了创世区块中的 50 个 BTC 是凭空出现的，以后的 BTC 都是挖矿获得的。你是否拥有 1 个 BTC？通过比特币地址可以查个底朝天，一直追踪到这笔资金的诞生记录。这笔钱是不是你的？通过加密和签名算法来保证，无法伪造。

传统互联网上我们可以把一首 mp3 音乐复制无数份，发给许多人，如何判定谁真正拥有这首音乐？在区块链中，你的 BTC 无法双重支付，可以明确每一笔 BTC 的归属权。不需要中心机构的参与，就可以准确地实现归属权的转移，**价值互联网**也就因此而来。

6.3 工作量证明 PoW

PoW 是 Proof of Work 的缩写，即工作量证明的意思。为了解决**拜占庭将军问题**，即在不信任的去中心化的网络中，如何确认一笔交易的有效性？比特币系统中引入了“工作量”的概念，有意降低了信息传递的效率，让矿工必须完成一定的工作量，才能够在全网广播消息。

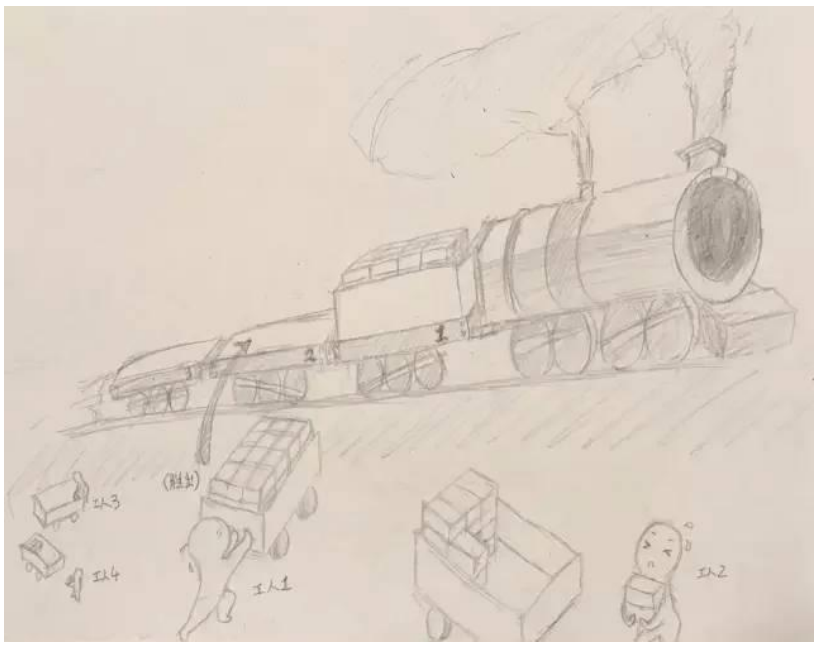


图6-1 工作量证明与搬砖

工作量证明可以与工地搬砖进行类比。一群工人们（**矿工**）向火车的车皮（**区块**）里搬砖，每个工人身边都有一个集装箱，这个集装箱与火车车皮一样大，正好能够装满 1000 块砖。

工人们只能往集装箱里搬砖，谁先装满集装箱，就把这个集装箱放到车皮里，领取 12.5 元的工钱（实际上并不是马上拿走，100 节车皮之后才能真正取走）。只有最快装满集装箱的工人能够获得奖励，在这个集装箱放入车皮的同时，其他工人的集装箱里也装了一些砖头了，竞争失败意味着全部作废，倒出来重新搬砖，继续投入到下一节车皮的竞争中。

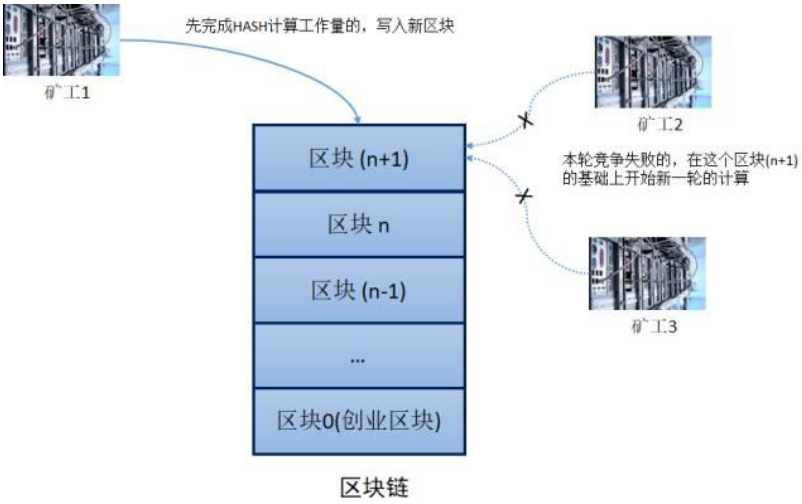


图6-2 完成工作量证明，写入新区块

比特币世界里的**矿工**（工人）也是这样辛苦，这里的矿工是一堆安装了专门芯片的电脑，它们的工作就是进行**哈希 HASH** 计算（准确讲是 SHA256，高级搬砖工作），谁先算完，写入一个新区块（**车皮**），得到奖励的 12.5 个 BTC（**发行新币，**前面讲过还有交易费的奖励），其它矿工则白忙活，继续进行下一轮的竞争。

因为电脑的计算速度太快，所以要安排上亿次的 HASH 计算，保证有矿工在 10 分钟左右能够完成任务。这种工作量，既是一种发行货币的过程，也是一种验证其他人交易的过程，从而保证了整个比特币系统的安全性。

6.4 HASH 哈希、散列

HASH 这个技术对于程序员们并不陌生，就是将一个值通过一系列的数学变换，转换成另外一个值。比如比特币系统中将私钥变为比特币地址、挖矿都用到了 SHA256 这种散列算法。

HASH 通常有这几种用途：

1）加密

HASH 算法通常与其它算法结合使用，来对信息进行加密，让密文更加复杂，不容易猜测。明文即使发生细微的改变，密文也会完全不同，只能通过穷举法来猜测明文，以当前的计算机速度测算，通常都要几千年。以比特币中常用的 SHA256 算法为例，明文中只是一个字符从 m 变为 n，最后的结果却完全不同。

SHA256(abcdefghijklm) = ff10304f1af23606ede1e2d8abcdc94c229047a61458d809d8bbd53ede1f6598

SHA256(abcdefghijkln) = a18201df18d4437cb18a4f97b4bd614955a6a21ec074ec5d3a11920b293994fc

2）冗余校验

在第 1.4 节介绍过 MD5&SHA checksum 工具软件，SHA256 算法也常用于生成数字摘要或数字指纹，用于验证下载文件是否被篡改。有些字符串中加入 checksum，是为了防止人为的输入错误，比特币地址里也加入了 checksum，输错一个字符将不会通过容错校验，可以防止录入失误把 BTC 打入其他人的账号中。

我们常见的 18 位身份证号码的最后一位就是容错校验码，算法是 ISO/IEC FCD 7064 MOD 11-2，有些人的身份证最后一位是 X，实际上是代表罗马数字 10。企业信用代码、书号、条码等许多地方都用到了冗余校验码，感兴趣的请自行搜索。

3）效率

编程时要操作的数据量越来越大，要在 0.1 秒内迅速查找一件东西是经常遇到的需求。假设有一个数据库里存放了 1 亿本书，并且书名都不重复，想根据书名快速查找书的其它详细信息，此时就用到了 HASH 算法，将 1 亿本书全部提前执行 HASH 运算，生成一个 64 位的数字（假设散列没有冲突，这种复杂的情形不再展开讨论），作为书的编号，将该书的详细信息存在这个编号所在的位置中。读者想找一本书，以后只需 HASH 计算一次，马上找到编号，取出书即可，效率非常非常高，而不用把 1 亿本书全查一遍。

练习：

可以登录下面的一个网站，随意输入一串字符，看看经过 SHA256 哈希运算后的结果，改

变其中的一个字符，看看运算的结果有何变化。

http://www.ttmd5.com/hash.php?type=9

http://www.yuangongju.com/encrypt?tab=hash

http://www.xorbin.com/tools/sha256-hash-calculator

6.5 工作量证明的 HASH 计算过程

这里举一个简单例子介绍一下比特币工作量证明的 HASH 计算过程。假设我有一个区块信息是“abcde”，要在其后面补一个随机数，使得 HASH 结果以 0 开头。由于 HASH 的加密特性使得原始数据即使发生极其微小的改变，得到的结果也有巨大不同。所以我只能一个数一个数地尝试，一直试到随机数 5 的时候，此时的字符串为“abcde5”，SHA256 的 HASH 结果为 051f2f...d7b9e1，以 0 开头，我找到了一个解，我就可以把“abcde5”加到新区块上，拿走 12.5 个 BTC 奖励。

```
SHA(abcde0) = 138ce038e5c818eb7ec43e85fa55cbda1d07816bc368e6870eb94a3eb7b9798e
SHA(abcde1) = 6d141e0503f9bec5560ac88f690b9a01ac975fcf6f83fd5e38088de08627eaa5
SHA(abcde2) = 7211218742567b1fd924f2748f8693a288b1d8d349d2291377985c9ea30515ce
SHA(abcde3) = 568b7211570894b16c69c3e899b14acb7a5569713de704ff5b0bad62409c2395
SHA(abcde4) = 1d726a4301379592a2a552a6e1d137cca5c219e4963a626da3e21de22373c782
SHA(abcde5) = 051f2f24ea5630784ab84d4a81d476835be9ae72cc7efc68b4987bb10dd7b9e1
```

图6-3 工作量证明就是 HASH 计算

区块链正如其名，是一个区块与另一个区块链接起来而成的，一个区块中用于参与工作量计算的主要有三部分数据（为了说明 HASH 计算的工作量，我对整个计算过程进行了极大地简化，更详细的细节请自行参考《精通比特币》一书）：

（1）父区块 HASH：用于指向父区块，当一个区块一个区块地链接起来后，想篡改一个区块，会影响子区块，再会影响孙区块，从而带来指数级的巨大计算量，从而使篡改几乎不可能。

（2）交易信息指纹：一个区块内通常有几百笔的交易信息，也用 HASH 算法产生一个指纹（准确地讲是 Merkle 树，以后再介绍），只占用 32 个字节。

（3）随机数 nonce：矿工所做的事就是找这个 nonce，通过不断地尝试变化这个 nonce，进行上亿次的 HASH 计算，得到满足要求的结果。刚才我们举的简单例子中，5 就是那个随机数 nonce。

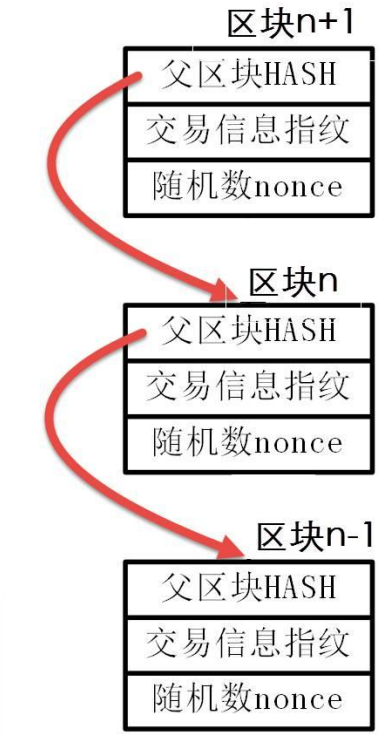


图6-4 区块中与工作量证明有关的几个属性

假设父区块 HASH 为“abc”，交易 HASH 值为“de”，不断变化 nonce，计算 HASH 值，假设 nonce=5 时，满足**工作量目标**（以一个 0 开头，这个术语以后再解释），获得到了全球共享大账本的记账权，然后将这个区块广播出去。

其它矿工收到这个区块后，首先要进行验证，验证别人是不是经过了大量计算并满足目标，而这个验证的计算量则非常非常小，一眨眼即可以完成。

就像前面说的搬砖一样，搬 1000 块砖的过程非常辛苦，但其它工人只需扫一眼就知道他是否完成了工作量（因为 1000 块砖正好装满一个集装箱），其它工人一看集装箱放到了车皮上（产生了新区块），则放弃当前的一箱砖，开始新一轮的工作（下一区块的竞争）。

关于工作量证明的小结：

- ✧ 工作量证明既用于发币，也是验证交易的有效性，保证比特币的安全
- ✧ 计算过程中不断调整 nonce，要进行数亿至万亿次的 HASH 运算
- ✧ 先完成计算的获得记账权，写入一个新区块，向外广播
- ✧ 其它矿工只用非常非常少的计算量就可以完成验证

✧ 竞争失败的矿工，获取最新区块信息，开始新一轮竞争

7 活在未来

7.1 区块链的自组织体系

介绍完区块链中的十多个概念，我用一张图把这些概念串一遍，大家可以看到区块链是一个多因素相互制衡的反馈系统，这也是我被其精妙的设计所迷住的一个主要原因。

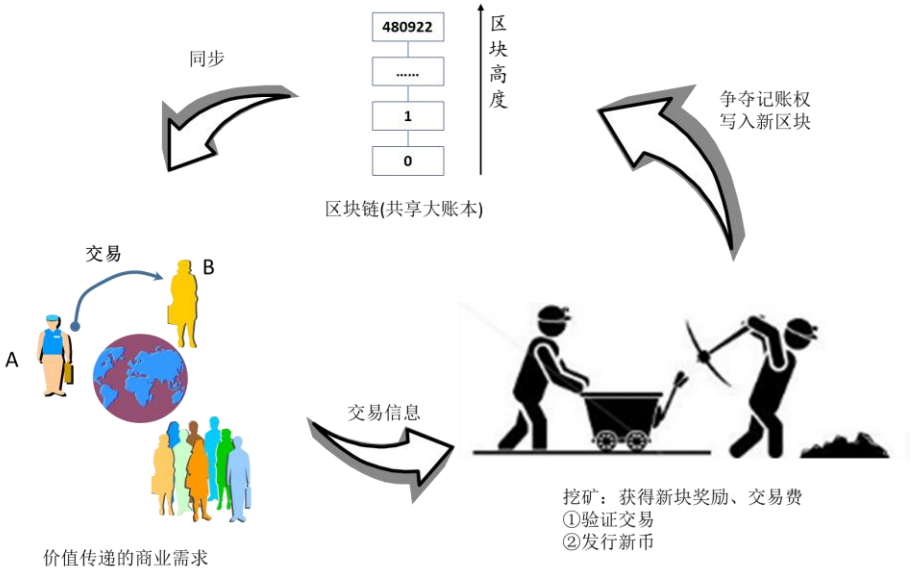


图7-1 区块链的自组织体系图

图的顶部是区块链，就是一个全世界共同维护的公开大账本，一个区块就是子账本，用**区块高度**来定位，我们生活在社会中，存在着大量商业往来，就有交易的需求，也就是价值转移的需求。但我们大量的个体之间互相并不认识，我给你发了货，你不给我钱怎么办？而区块链技术就实现了这种去中心化网络环境中的可信的价值传递，它实际上也有效地解决了拜占庭将军问题和双重支付问题。

我们安装钱包软件，同步下载超过 160GB 以上的大账本数据，我向你的比特币地址发送 1 个 BTC，运用公钥、私钥、非对称加密原理，建立一笔交易，发布到整个比特币网络上，这些交易数据通过合法性验证后，在整个网络中迅速传播。

矿工收到成百上千的交易数据后，会根据交易手续费从高到低排序，运用专业的显卡设备，开始了超大工作量的 HASH 计算，提交一份 PoW 工作量证明，第一个完成计算的矿工获得了记账权，在网络上广播一个新区块，拿走新区块奖励和这些交易的手续费。在经济利益的驱动下，

这些矿工验证了网络上交易的合法性，发行新币，从而保证了区块链的安全性。

当你用一张图把这些概念串在一起的时候，并且认真理解了其设计的原理，你就会明白价值互联网的威力，树立起活在未来的信心，从而不会轻易交出自己的筹码，祝大家活在未来。

7.2 价值互联网

当今的互联网已经构建了一个信息互联网，也就是说可以促进信息的传播，而且这种信息的复制和分发的成本几乎为 0。但对于把一个有价值、有归属权的东西（比如：货币），从一个人传递到另一个人，则是相当麻烦的事情，所以出现了支付平台。

为什么会出现支付平台？因为交易双方如果不是商业伙伴关系，谁也不认识谁，不可能建立信任，我付了钱，你不发货怎么办？我发了货你不给钱呢？而交易平台负责与每一个人建立信任关系，当平台越做越大时，大家都会越信任这个平台，感觉平台肯定不会因为我这点小钱无故跑路。看看微信、支付宝吧，大家都认为它们是大公司的，可以信任。

使用第三方平台还有一个原因，双重支付问题，数字货币本身就是一串二进制数字，是非常容易复制的，你如何辨别一个数字从 A 转到了 B，同时你又把 A 转给了 C？交易平台有这种支付和清算的功能，你保存在第三方平台（银行、微信、支付宝等等）的钱只是一串数字而已，在比特币之前，你别无选择，只能相信这些平台。

但这种第三方平台的介入就是风险，一方面会增加交易成本，另一方面，平台倒闭或跑路的事件屡有发生，当发生这样的事件时，我们只能是血本无归。

而比特币（严格说应该是区块链技术）解决了这个问题，它用一套优雅的系统（基于加密技术和程序算法）解决了这个难题。把钱从 A 付给 B，是你们两个人的事，信任关系不是交给第三方平台，而是由系统来保证，有全世界互联的计算机（矿机）为你验证。

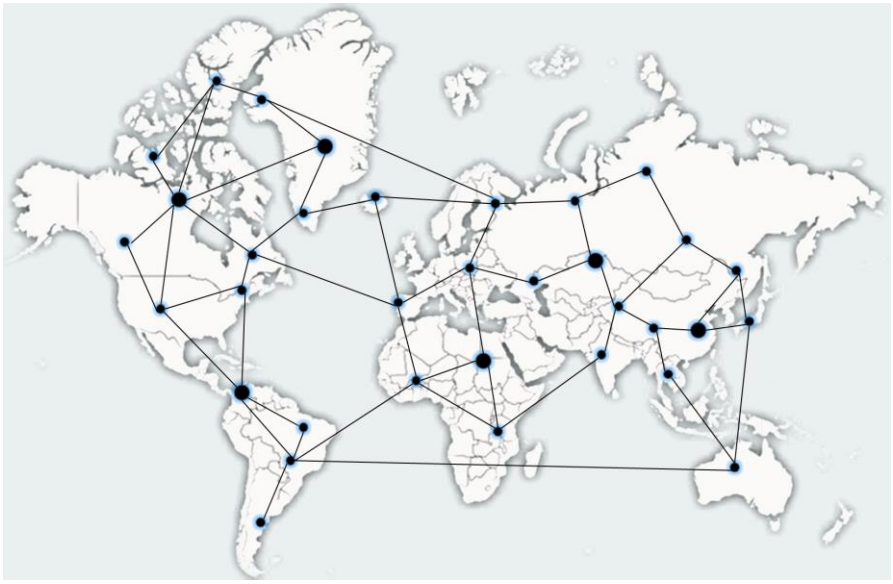
区块链技术实现了比特币的价值传输，可比特币只是一种数字货币而已，其它有价值的东西还很多（实体类的资产与这个价值互联网无关），这里说的是数字资产，即一堆可以用数字保存的有价值的东西，比如股票、债券、专利、域名、凭证等等。有人根据“互联网+”的名词创了个“区块链+”，指在区块链上传输这些数字资产，区块链的技术实现了在不信任的网络环境中的可靠的价值传递，必将给各个行业带来巨大变化。

有人这样比喻：HTTP 是互联网信息传输协议，Blockchain 区块链是价值传输协议。

未来已经来临，只是尚未流行。

---- 威廉•吉布森(William Gibson)

第二篇 区块链进阶



8 拜占庭将军问题(Byzantine Generals Problem)

每一本讲**区块链**技术的书籍，几乎都会讲到**拜占庭将军问题**，理解这个问题将有助于理解去中心化的网络中如何达成共识的机制。看到**拜占庭将军问题**这个词语时，我曾经一度认为有一位名叫拜占庭的将军带领着一支庞大的军队打仗时遇到了难题，但查阅了一些资料后，发现实际上并没有拜占庭将军，也没有这场战争，完全是计算机专家假想出的问题。

8.1 拜占庭帝国

拜占庭这个专有名词取自于**拜占庭帝国**，又叫东罗马帝国，其军事力量很强大，地处现今欧洲的土耳其国家。

图8-1 拜占庭帝国的地理位置，图片来源于百度百科

在《区块链----从数字货币到信用社会》中关于拜占庭将军问题的描述有点小错误，书中把问题描述成 10 个邻国去攻打拜占庭国家，但查到这个问题的提出者 Leslie Lamport 的论文原稿时，实际上这是一个假想的问题。

莱斯利·兰伯特（Leslie Lamport），是微软研究院的首席研究员，曾获得 2013 年图灵奖——计算机界的诺贝尔奖。这家伙觉得讲故事让问题变得更有吸引力，因此他在提出观点和问题时常用故事背景吸引眼球，拜占庭将军的故事就是兰伯特在研究分布式系统容错性的时候编出的一个故事。

外国研究人员引用欧洲历史来举例说明一个算法问题，中国人容易误解，拜占庭幅员辽阔、

军事力量强大，派出多支部队去攻打敌军，并不是挨打。

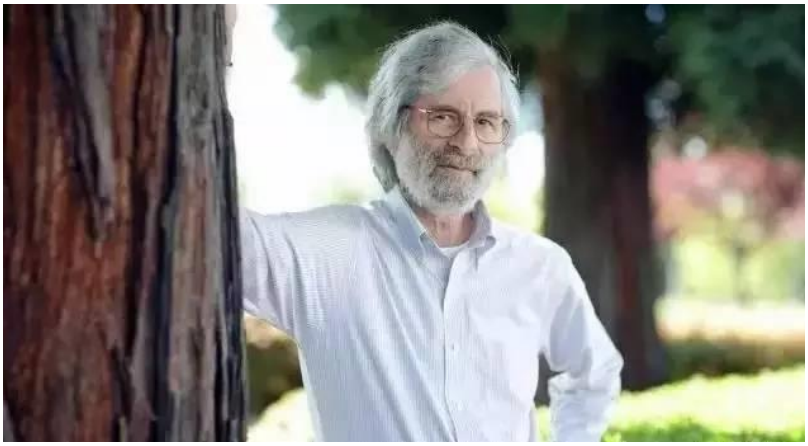


图8-2 莱斯利·兰伯特（Leslie Lamport），图来源于百度

8.2 问题描述

论文中的原文：

> We imagine that several divisions of the Byzantine army are camped outside an enemy city, each division commanded by its own general. The generals can communicate with one another only by messenger. After observing the enemy, they must decide upon a common plan of action. However, some of the generals may be traitors, trying to prevent the loyal generals from reaching agreement.

翻译：假设拜占庭帝国的几支军队在敌人的城池外扎营，每支军队听命于自己的将军，这些将军之间只能通过信使传递消息。在对敌军进行侦察后，将军们必须制订一份共同行动计划。但是，有些将军可能是叛徒，这些叛徒会阻碍那些忠诚的将军达成共识。

这个问题的简洁描述：在已知有间谍的分布式军队中，将军们如何达成共识，执行共同的作战计划，来取得战争的胜利。

8.3 问题的难点

这个问题困扰了程序员们很多年，出现了许多不同的算法，直到中本聪在比特币系统中引入了一种精妙的设计。拜占庭将军问题中的难点在于：

- ✧ 这些将军离得很远，不可能每遇到一个问题，就聚到一起开会商量对策
- ✧ 这些将军中可能有少量叛徒，叛徒会乱发消息

- ✧ 信使在传递消息时可能会把信弄丢
- ✧ 信息可能会被敌国截获
- ✧ 无法确认消息是否真的来自某位将军
- ✧ 将军们在商量过程中可能会浪费很多天时间，贻误战机

8.4 区块链的解决方案

把军队想像成计算机节点，把信使想像成计算机间的网络通讯，攻占敌军就是写入一个大家公认的区块记录。

区块链技术在发送信息中加入了成本，降低了信息传递的速率，并采用了**工作量证明**（PoW），即一个节点必须经过大量计算才能得出一个结果，而其它节点只需极少的时间就能证明其真伪，这样能够减少垃圾消息、假消息在节点间传播的状况。

挖矿节点把一段时间内的交易信息打包成一个区块，盖上时间戳，与上一个区块衔接在一起。每个区块都包含了上一个区块的索引（哈希值），然后再写入新的信息，从而形成新的区块，一个区块一个区块的连接在一起最终形成了区块链。

用工作量证明、公钥加密等技术，使比特币网络从一个去中心化的不可信网络变为可信网络，使所有参与者可以在某些事情上达成一致，从而使价值传递成为了可能。

其它可参考的文献：

- ✧ 《区块链----从数字货币到信用社会》，长铗、韩锋等
- ✧ https://www.microsoft.com/en-us/research/wp-content/uploads/2016/12/The-Byzantine-Generals-Problem.pdf
- ✧ 拜占庭将军问题深入探讨
- ✧ 区块链的工作原理之拜占庭将军问题
- ✧ 浅谈区块链技术翻过的大山——拜占庭将军问题
- ✧ 探寻区块链的源头——“重回拜占庭”

- 区块链与银行家（上篇：拜占庭将军问题）
- 区块链共识机制，拜占庭将军问题是什么

9 钱包进阶

9.1 导出私钥

私钥隐藏在钱包软件中，你在支付比特币时，需要输入密码，钱包软件会自动使用私钥进行数字签名等操作，你平常使用钱包软件时根本看不见私钥，如果很想看看私钥长什么样子，需要进行下面这样的操作。

> 私钥泄漏，则丢失你所有的比特币。

再提醒一句，如果你不知道自己正在做什么，不要进行下面的操作。

从“帮助”菜单里，打开调试窗口。

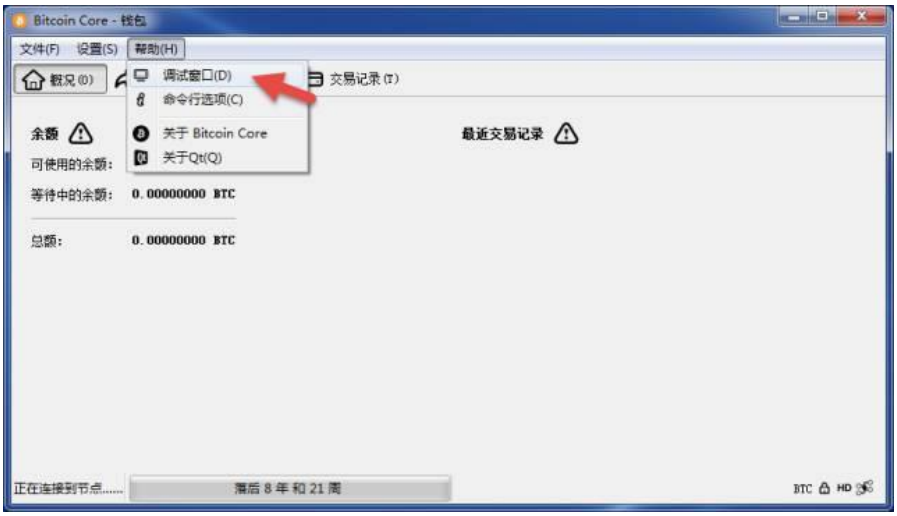


图9-1 从“帮助”菜单中打开调试窗口

在控制台窗口的底部的文本框中输入这两条命令，回车：

```
walletpassphrase "请换成你的钱包密码" 60
dumpwallet wallet-priv.txt
```

这条命令中的 60，表示密码的过期时间，在 60 秒之内不用重复输入密码。

图9-2 用密码解锁钱包

记住：在进行这些命令行操作时，千万不要让外人看到你的钱包密码。如果操作正确，每个命令之后会返回 null。再到 Bitcoin Core 的安装文件夹下，可以找到 wallet-priv.txt 文件，打开后，内容是这样的：

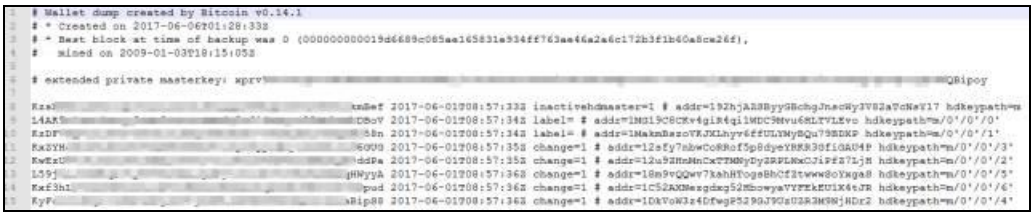


图9-3 Bitcoin Core 导出的私钥内容

从第 8 行开始，左侧的那一长串字符是**私钥**，在 addr=后面的是公开的比特币地址。

看完这个 wallet-priv.txt 文件之后，你可以保存在 KeePass 之类的密码管理软件中，然后将私钥文件彻底删除，以免落入外人之手。

小结：

- ✧ wallet.dat 钱包一定要加密
- ✧ 将加密的 wallet.dat 备份到其它地方
- ✧ 牢记密码
- ✧ dumpwallet 可以导出私钥为文本文件，如果你不知道正在干什么，就不要操作这条

命令了

9.2 HD 钱包

早期的 Bitcoin Core 钱包在第一次使用时会生成 100 个私钥，如果交易比较频繁，私钥可能会用光，然后再产生一批私钥，所以需要定期备份 wallet.dat 文件，否则有可能会丢失比特币。我查看了 0.15.0.1 版本里的私钥，有 1000 多个，如果不是非常频繁的交易，足够使用相当长的时间了。也就是说，如果在几年内你没有进行过几百次的比特币的交易，只备份一次 wallet.dat 就足够了。如果你使用了 HD 钱包，理论上只备份一次就足够了。

在 BIP032（在 10.1 节中介绍 BIP）中引入了 **HD 钱包**的概念，不是 Hard Disk 的缩写，而是指**分层确定性**（Hierarchical Deterministic）钱包。

所谓确定性，就是只需一个**主私钥**（根私钥），就可以生成所有其它私钥，这样备份起来更方便。当然如果这个主私钥泄漏，则所有子私钥也就泄漏了，所有的币也就都交给别人了。

所谓分层，就是一个大公司可以为每个子部门分别生成不同的私钥，子部门还可以再管理子子部门的私钥，每个部门可以看到所有子部门里的币，也可以花这里面的币。也可以只给会计人员某个层级的公钥，让他可以看见这个部门及子部门的收支记录，但不能花里面的钱，财务管理更方便了。

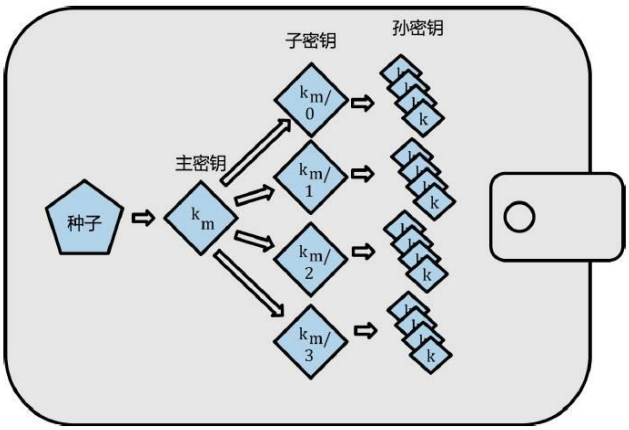


图9-4 HD 钱包示意图，摘自《精通比特币》

9.3 Bitcoin Core 里的 HD 钱包

Bitcoin Core 0.13.0 之后的钱包开始支持 HD 钱包，如果右下角的 HD 图标没有打叉，则说明你正在使用 HD 钱包。

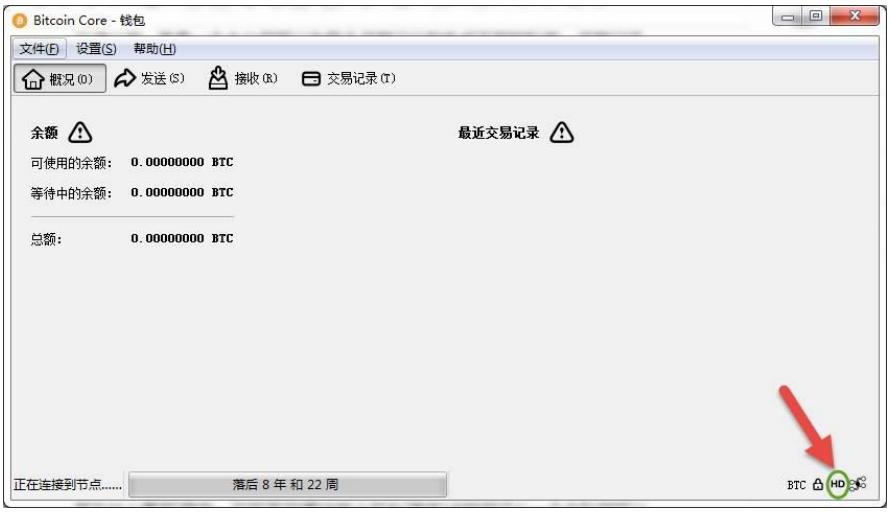


图9-5 Bitcoin Core 里的 HD 标识

对于 HD 钱包，导出私钥时，可以看到有一行标记着 **extended private masterkey**，这就是主私钥。实际上扩展型主私钥还包含着**链码(chain code)**，用于恢复所有子私钥，更多细节可以看本文之后的参考文献。

其后的每个私钥的末尾有 hdkeypath=m/0'/0'/1' 这样的标记，这就是它的分层路径，表示 m 节点（主节点）下的 0 节点的 0 节点的 1 节点。

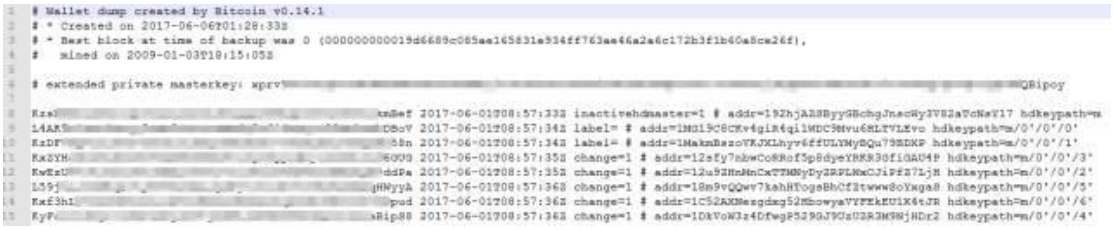


图9-6 Bitcoin Core 中导出的私钥

理论上说，这种 HD 钱包备份一次就可以了，以后总能恢复所有的私钥。但为了保险起见，养成定期备份的习惯总是好的，毕竟辛辛苦苦买的几个币别折腾没了。

为了万无一失，建好钱包后，先转入一点点 BTC，备份，再把软件卸载了重装，用密令或 wallet.dat 文件恢复钱包，看看 BTC 是否还在，最后再转入大额的 BTC，虽然麻烦一点，但绝对值得。当钱包里没有多少币的时候，把钱包的功能用熟，别在存入了许多币的时候再犯致命的低级错误。在写这篇文章的时候，群里的一位朋友，用 12 个单词的密令恢复钱包，钱包恢复了，可惜钱没了，正在寻求帮助呢。

小结：

- ✧ HD 钱包不是指硬钱包，而是分层确定性钱包
- ✧ 只备份主私钥就可以生成所有的子私钥
- ✧ 可以分层控制

参考资料：

http://www.8btc.com/hd-wallets

http://www.8btc.com/how-to-use-hd-wallets

https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki

https://github.com/bitcoin/bips/blob/master/bip-0044.mediawiki

9.4 简单支付验证(SPV)与轻钱包

我们前面介绍的 Bitcoin Core 是发明人中本聪最早开发的**全节点钱包**，根正苗红，是最值得依赖的去中心化客户端，但只能在 PC 上安装，需要 160GB 的磁盘空间保存区快链全节点文件和很长的时间进行同步。

还有一种钱包称为轻钱包，它只保留与你有关的账本记录，所需的磁盘空间比全节点钱包小 1000 倍，同步速度超快，几分钟就完成。在 https://bitcoin.org/zh_CN/choose-your-wallet 网站上还有许多其它轻钱包可供选择，分别支持不同的操作系统 Windows、Mac、Linux、Android、iOS.....现在市面上的轻客户端的安全性也很高，只要是官方提供的，基本上也是可以信任的。**仍要做好备份并保存好私钥**。

SPV（Simplified Payment Verification）不保存完整的区块信息，只保存区块头信息。大多数用户并不关心背后复杂的技术原理，只需知道它与其它钱包的区别、安全性风险就足够了。现在很多轻钱包已经实现了这种技术，这类钱包虽然安全性不如全节点钱包，但假如你不是腰缠万贯，这种钱包的安全性能满足使用要求。

关于 SPV 技术有一个类比，就是有两个人都从北京去罗马，一个人手里拿着全世界的所有地图册，大家都知道，一路上 99%的地图都派不上用场，带着徒占地方；另一人手里可能只拿着中国地图、欧洲地图、罗马地图，他到达一个地点后，问问附近的居民，更新一下地图，再到一个地方，再更新一点数据，最终也能到达目的地。前者说的是全节点钱包，后者就是实现

了 SPV 的钱包。

在 bitcoin.org 上挑选轻钱包软件时，你只需认准 Simplified Verfication 标志即可，你更需要注意它与 Centralized Validation 的区别，后者是指中心化验证，也就是说这款钱包软件是连接到一个中心服务器进行交易的验证，理论上是可以造假的。对于大额交易，还是亲自登录到 blockchain.info 等网站上输入交易 ID，查查是否有 6 次以上确认最靠谱。

以前许多用户使用过 Multibit HD 轻钱包，可惜 2017 年 7 月 26 日，Multibit 的开发团队已经不再维护此软件，请不要再使用 Multibit HD 这款轻钱包了。Breadwallet 是官网上推荐的一款轻钱包，苹果手机需要海外 apple id 才能下载安装，安卓手机需要科学上网安装 google play 再搜索安装，这款钱包的用户数量挺多的。国内用户很多是比特派(bitpie.com)钱包，虽然不在官网的推荐列表中，功能也不错。

如果资金比较多，可以使用**硬件钱包**，比如：Legder Nano S，它将关键信息写入类似 U 盘的硬件设备中，安全性挺高的，当然该设备也需要上千元的费用。

有些钱包软件提供打印**纸钱包**的功能，即把私钥（加密或不加密）等信息打印到一张纸上，你需要把这张纸放在安全可靠的保险箱里。

9.5 blockchain 钱包

Blockchain 网站(www.blockchain.info)上提供一种在线钱包，操作很方便，但不知道为什么 bitcoin.org 官网上并没有推荐它。这款钱包还配备手机 APP，并且支持比特币和以太坊的存储，由于是轻钱包，整个 app 及数据不超过 50M。

（1）下载后，初次登录需要**“创建一个钱包”**。

（2）输入邮箱和密码(至少 10 位/随机/大小写/数字/字符)。

（3）注册后系统会发送邮件到邮箱，点击确认，邮件内还有一个钱包的 ID，**一定要认真地抄下来**。

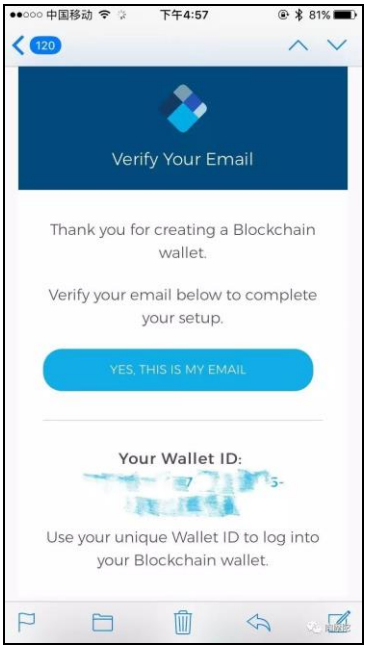


图9-7 邮件确认

（4）随后就可以进入 app 了，看到如下界面。

图9-8 进入 APP 的主界面

（5）在钱包中，点击“备份资金”，系统会生成一串 12 个单词组成的助记词，抄下来，保存在可靠的地方。这串助记词，可在你忘记登录密码的情况下恢复钱包，这串词就是用来生成私钥的。

（6）如果将来你要在其它手机上安装这款钱包，使用钱包 ID 和密码，或者使用 12 个单

词的助记词，就可以找回钱包。因为你要牢记住的一点是：这些钱包 ID、密码、助记词等等都是用来恢复你的私钥的，你的币实际上是保存在区块链上的，并不是保存在钱包里的，只是通过私钥来打开钱包，使用你的资金。

9.6 比特币冷钱包的制作和使用

9.6.1 比特币冷钱包

所谓的比特币冷钱包是相对于热钱包而言。热钱包是一直在线并能够随时发送交易的钱包，因此存在被黑客攻击而丢币的风险。而冷钱包让私钥永不触网，因此可以避免比特币被盗。目前大多数数字交易所都会将大部分比特币存储在冷钱包中，这样即使交易所被黑客攻破，也只会损失一部分比特币。

9.6.2 准备另外一台电脑和不同的操作系统

冷钱包需要两台计算机配合才能同时具备冷存储和热交易的功能。其中一台连接互联网，可以用于交易；另一台计算机保持断网离线状态，用于存储比特币。

用于存储比特币的计算机要和进行热交易的计算机安装不同的操作系统。这样，即便是出现了意外，因为木马和病毒通常不能兼顾两种不同的操作系统，也能提高钱包的安全性。因为钱包对计算机的硬件要求不高，使用比较旧的计算机也是可以的。

鉴于大家的使用习惯，用于交易比特币的计算机安装 windows 操作系统，存储比特币的计算机安装 linux 操作系统。安装前将硬盘重新格式化，消除原有硬盘可能存在的风险。

本文使用优麒麟 16.04 LTS(长期支持)中文版的 Linux 系统（Ubuntu）做演示，下载地址为 http://cn.ubuntu.com/download 。Ubuntu 是一个安全性好的开源操作系统，它由全球顶尖开源软件专家开发，适用于桌面电脑、笔记本电脑、服务器以及上网本等，并且它可以永久免费使用。

9.6.3 在 linux 系统中安装 electrum 钱包

electrum 钱包的官网地址：https://electrum.org/#download，目前钱包最新版本为 3.0.6。下载页面如下：

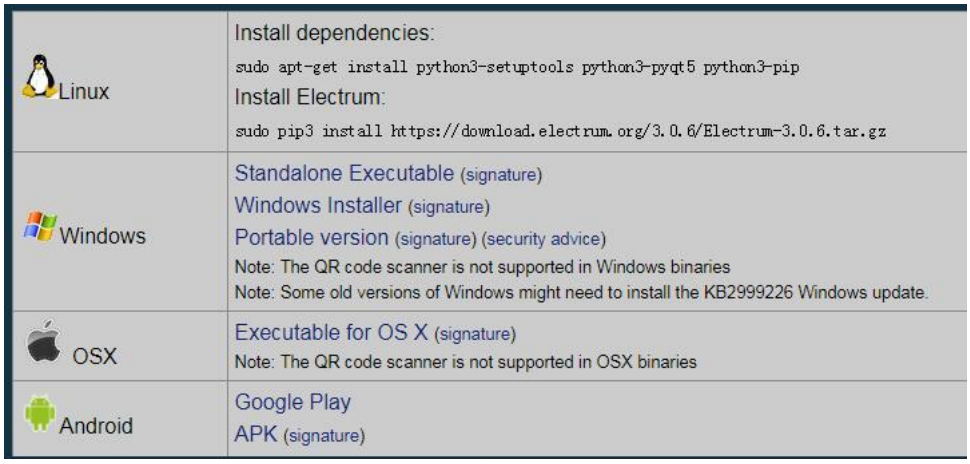


图9-9 下载 Electrum

基于 electrum 钱包一直在升级过程中，linux 系统在安装钱包软件过程连接上互联网比较方便和顺利，否则安装步骤会更加繁琐。

在获得 linux 系统的 root 权限后，按照网页的说明在 linux 控制台输入：

```
sudo apt-get install python3-setuptools python3-pyqt5 python3-pip
```

安装完相应的控件后，再同样在控制台用命令行方式安装钱包软件：

```
sudo pip3 install https://download.electrum.org/3.0.6/Electrum-3.0.6.tar.gz
```

安装结束后在 linux 桌面上会出现 electrum 钱包的图标。点击运行就可以了。这时就必须将网线拔掉，禁止无线连接，在设备管理中删除网络硬件，杜绝一切网络连接，成为一台不连接互联网的冷设备。

9.6.4 Electrum 冷钱包的设置

在另外一台计算机上下载并安装 windows 版本的 electrum 钱包，有安装版本，也有免安装绿色版本。推荐使用绿色免安装版本。

在钱包设置过程中，为了避免繁琐，只在关键的过程列出图形进行提示。如果没有特别说明，在两台计算机上的操作过程是相同的。

1.启动 electrum 钱包软件运行后，选择“auto connect”选项，显示如下：

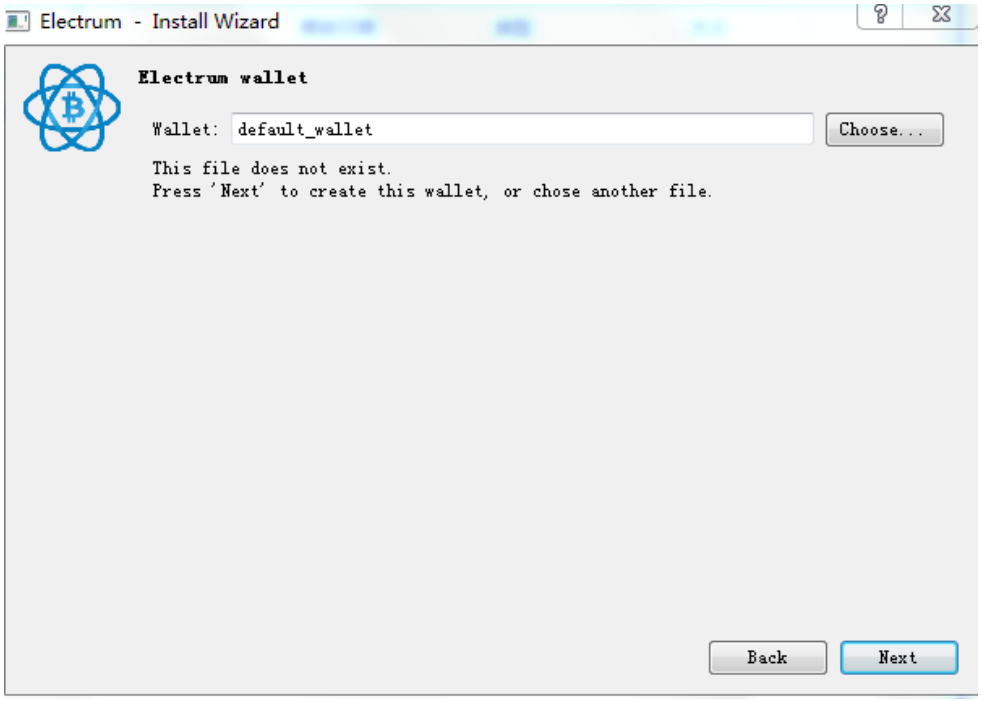


图9-10 建立新钱包的名称

这时可以在显示框内输入你要建立的新钱包名字,或者打开已经存在你计算机中的原有钱包。

2.给钱包命名后，点击“next”，进入下一步设置。

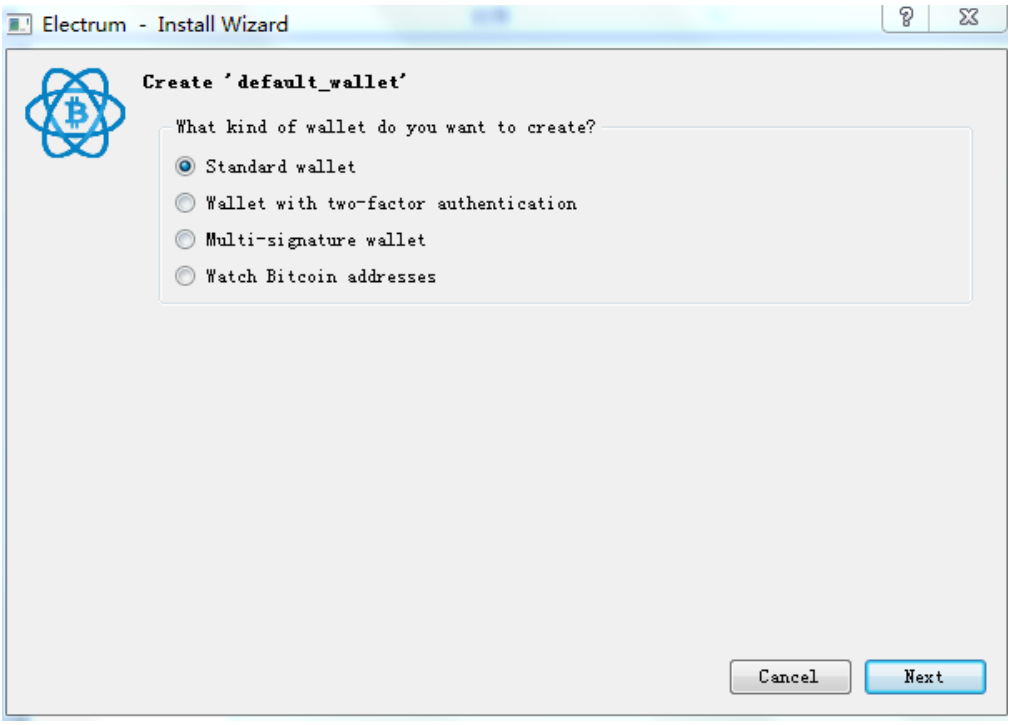


图9-11 创建标准钱包

3. 选择“standard wallet”（标准钱包），进入下一步。

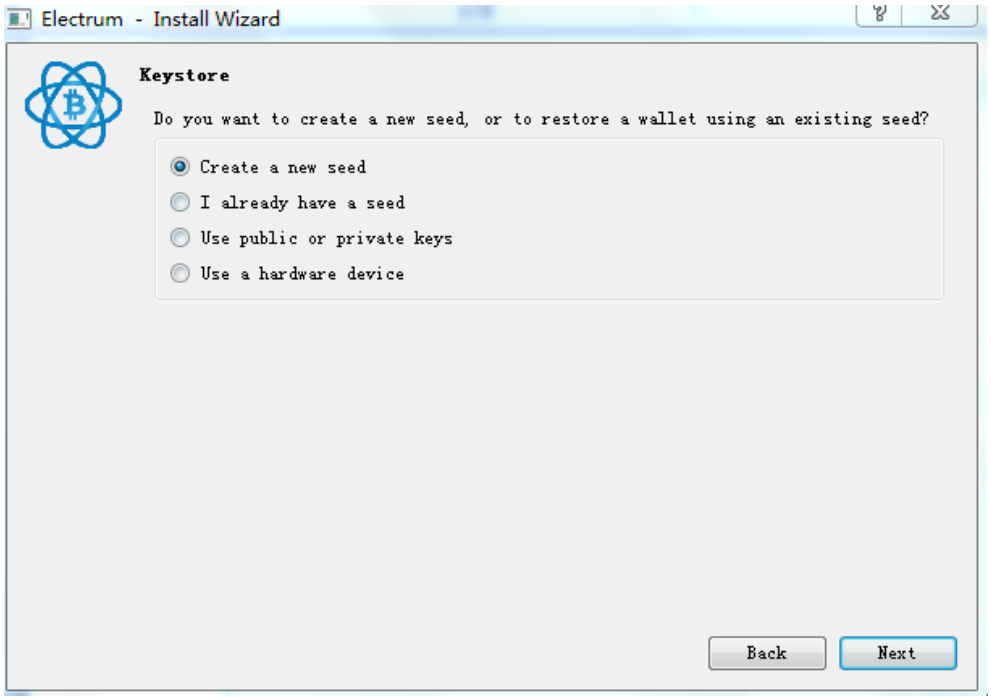


图9-12 生成新种子

4. 如果你要在 linux 系统的软件上建立新钱包，就选择第一项“Create a new seed”，再进入下一步。在 Windows 系统的计算机上不能选择这一项，必须通过导入公钥的方式建立“watch-only wallet”只读钱包。

图9-13 抄下种子单词

5. 这个时候，出现了 12 个随机的英文种子单词（seed），用笔和纸张记录下来，这是以

后钱包丢失用来恢复私钥的关键。不可以拍照，不可以通过微信和 QQ 等聊天方式传递，不可以存储在云盘和连接互联网的计算机中。失去了这些，就失去了对应钱包里的比特币。

随后，软件会要求你按照原有顺序重复输入一次刚才的种子单词，确定你已经记录好了种子单词。同时设定钱包的密码。密码要有足够的强度，减少被破解的可能性。

6.然后，软件就开始生成私钥（master private key ）、公钥（master public key ）和地址。

如果你已经有了比特币钱包，不准备更换。可以在第 4 步操作中选择“use public or private key”将私钥导入到软件中。操作界面如下图：

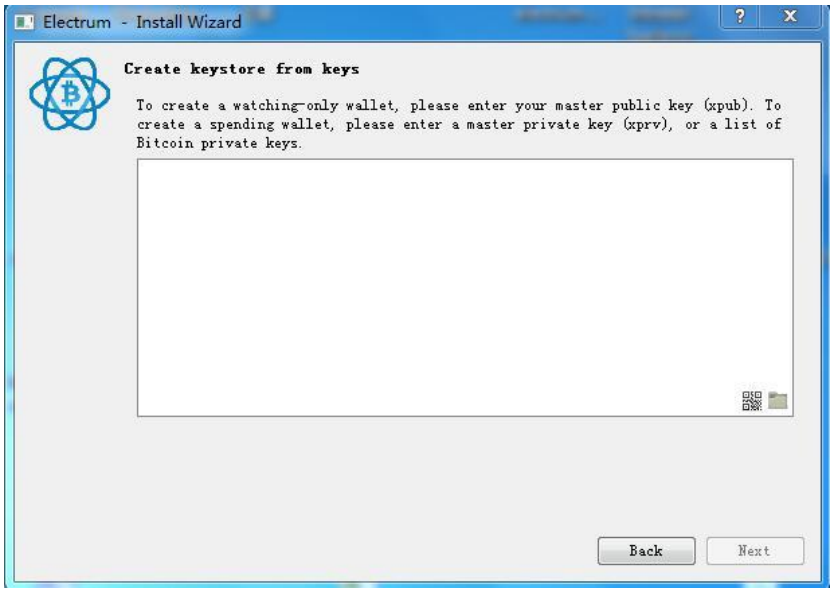


图9-14 用私钥恢复钱包

在空白框中输入你原有钱包的私钥，就会生成和以前钱包一样的公钥和地址了。

到这里，离线的冷钱包就制作完成了。你可以将你的收款地址告诉别人进行收款。

如果你想要随时能查询自己钱包的金额同时还具有交易功能，就在 windows 系统的计算机上同样使用 electrum 软件设置“watch-only wallet”钱包。

9.6.5 只读钱包的设置

在 linux 系统的钱包中，在菜单栏（钱包）导出公钥，用 U 盘拷贝出来。公钥的遗失并不会造成比特币丢失，所以可以公开。

前面的钱包设置的冷钱包设置过程基本一样，只是在第 4 步操作中选择“use public or private key”选项。然后在空白框中将你的比特币公钥拷贝进去。确认后软件会有提示，提示生成的钱包是“watch-only wallet”。也就是说这个钱包是只读钱包，只能查询你的比特币金额，单独使用不具备交易功能。

9.6.6 通过离线签名进行比特币交易

相比只是将私钥打印在纸上的离线保存方法,这里介绍的冷钱包搭配只读钱包是可以进行比特币交易的，即保证了比特币的安全，又具备交易的方便性。

使用方法如下：

使用联网计算机的“watch-only wallet”（只读钱包）发送比特币。按照钱包的要求填写好收款地址、说明、金额和矿工费。点击预览，检查一下各个内容是否填写正确，如果地址填写错误，你的比特币可能会被发到空虚中，无法撤回。确认无误后，点击保存，将交易保存为一个尾缀为 txn 的文件。

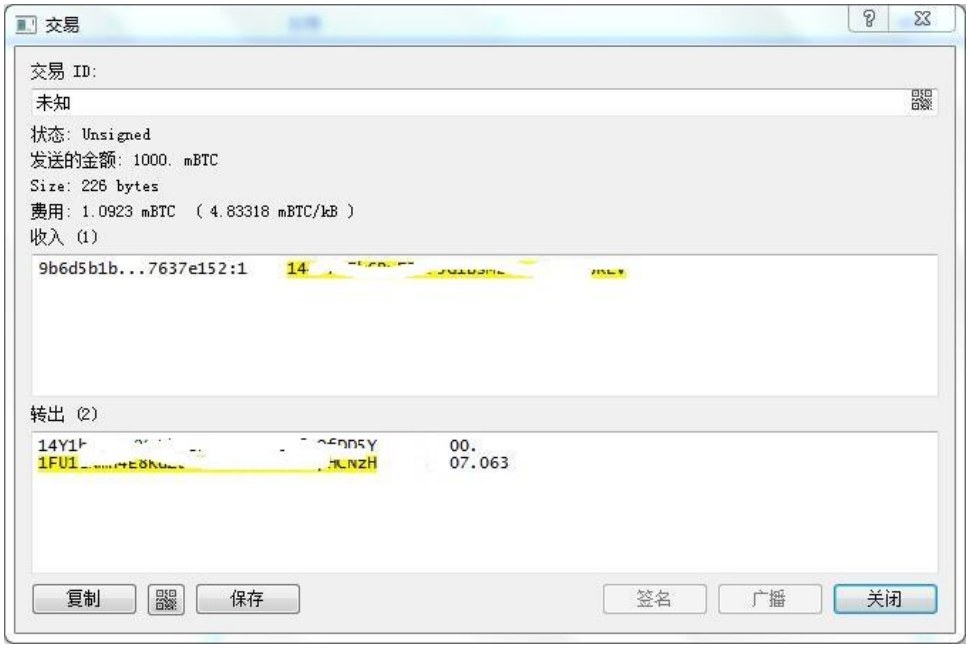


图9-15 用只读钱包发送比特币

将文件用 U 盘拷贝到安装了冷钱包的 linux 系统的计算机上。在这台计算机上打开钱包软件，从菜单的工具栏中选择钱包，再选择从文件加载交易。加载刚才拷贝过来的文件。这时会显示和刚才在另外一台计算机一样的交易内容。因为这台计算机的钱包有私钥，所以签名的按钮是可用的。点击签名对交易进行确认，再将这个交易另存为一个文件（可以覆盖原来的文件，

也可以另存为一个文件）。

再用 U 盘将签名过的交易文件拷贝到连接到互联网的的计算机上，同样选择从文件加载交易。加载刚才签过名的交易文件。这时候，广播按钮可用了。点击广播后，交易就向全网广播出去了。当交易被矿工打包和确认后，交易完成。

9.7 数字签名(Digital Signature)

比特币系统中的数字签名有三个作用：第一，证明你拥有某笔资金的私钥，第二，该证明是无可争辩的、不可抵赖的，第三，签名后的交易没有被其他人修改过。

数字签名使用椭圆曲线数字签名算法（ECDSA），算法非常复杂，普通用户不必掌握其算法的细节，但你需要掌握 Bitcoin Core 等钱包软件中如何用你的比特币地址对一段消息进行签名的用法和作用。

签名过程：

在 Bitcoin Core 软件的“文件”菜单下，点击“消息签名”菜单项，弹出一个对话框。

图9-16 消息签名

分别填写比特币地址，消息文本，点击“消息签名”按钮，则会在底部的签名区出现一行文本，这段文本可以证明你拥有那个比特币地址、那段消息是完整的、没有被修改过一个字，这个证明谁都可以验证、不可抵赖。

验证过程：

在 Bitcoin Core 软件的“文件”菜单下，点击“验证消息”菜单项，弹出一个对话框。

分别填写比特币地址、消息文本、签名文本，点击“验证消息签名”按钮，则会出现是否验证成功的提示。

图9-17 验证消息

很多网站都提供了这种验证工具，比如：https://tools.bitcoin.com/verify-message/

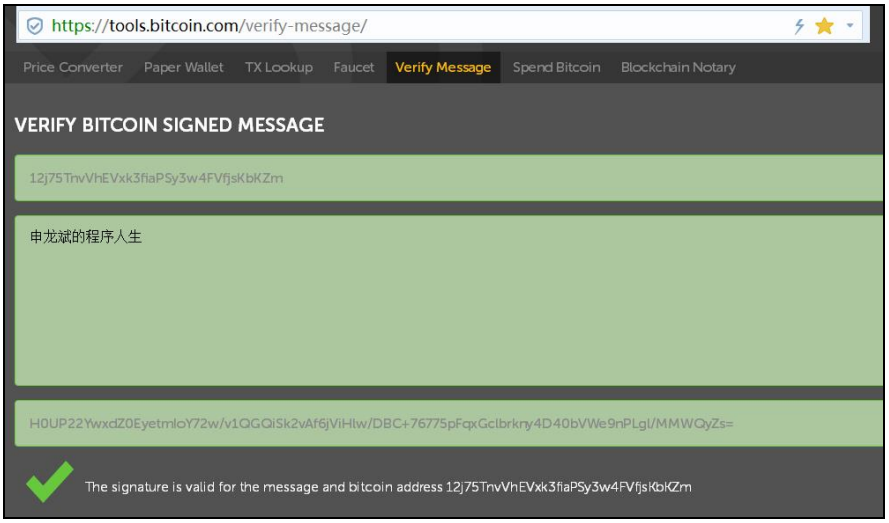


图 9-18 bitcoin.com 提供的在线验证签名的服务

再比如：https://reinproject.org/static/bitcoin-signature-tool/index.html#verify

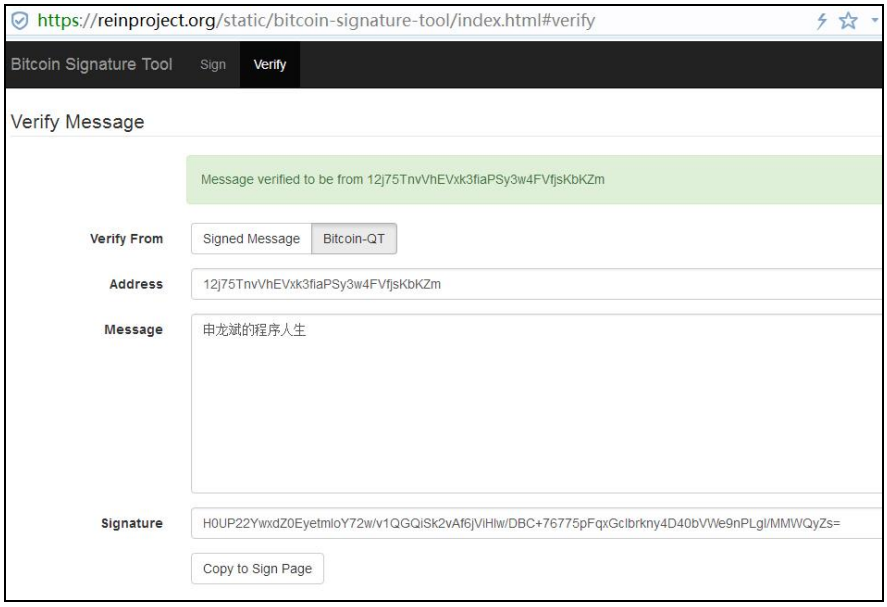


图9-19 reinproject.org 提供的在线验证签名的服务

练习：

大家可以在这些网站或在 Bitcoin Core 中验证如下的消息，比特币地址、消息文本、签名文本分别是下面三行：

```
12j75TnvVhEVxk3fiaPSy3w4FVfjsKbKZm

申龙斌的程序人生

H0UP22YwxdZ0EyetmIoY72w/v1QGQiSk2vAf6jViHlw/DBC+76775pFqxGclbrkny4D40bVWe9nPLgl/MMWQyZs=
```

9.8 别人如何偷走我的币？

本书的读者有个提问挺好，如果别人要偷走我钱包里的币该怎么操作呢？

我想到了这样几个办法，欢迎大家补充。

1）黑到你的电脑，把你的 wallet.dat 拿走，如果这个 wallet.dat 没有加密，那币就是我的了。

2）暴力破解这个 wallet.dat 的密码，如果密码设置得较为简单（比如 6 位以下，且只有字母和数字），那就是形同虚设。

3）如果你用手机截屏功能把私钥、密令拍过照，许多 app 都可以获得照片的读取权限，轻松把你的币转移，这是最常见的一种丢币情况。

4）如果你在手机钱包里的 app 保存了 keystore 文件，在 android 手机里，存储权限很开放，其它恶意 app 可以搜索这类文件，把文件拿走，很容易导入到其它钱包中。如果 ios 手机，稍微安全一些。

5）在一些交易所没有设置二级验证，你的登录密码与其它网站的密码又是一样的，那么黑客可以轻松登录并转移你的财产。

6）通常官方网站推荐的钱包是较安全的，但如果你使用来路不明的钱包软件，它可能会偷偷地保存你的私钥，那后果就太严重了。

7）使用来历不明的输入法软件，你输入的每个字符它都记得，甚至记录你的隐私数据。

8）你喜欢用纸钱包，如果小偷攻破了你家的密码箱，那就不安全了，不过小偷可能没学过区块链，可能把首饰、珠宝、现金都拿走了，没想到一张印着二维码的破纸会更值钱。

9）如果忘记了自己的私钥或者钱包密码，并且还没有备份，你的币是绝对安全了，黑客确实没办法偷走你的币，但区块链永久地锁住了你的币。

9.9 区块链资产保存在交易所还是钱包？

当我们购买了区块链资产 BTC、ETH 之后，就会面临一个问题，把这些资产放在哪呢？被盗事件频发，哪里更安全呢？

目前通过法币购买区块链资产有以下渠道：

- ✧ 通过场外交易网站，目前换币网（OTCBTC.com)有中文界面，体验很好，老牌的 Localbitecoins.com 无中文界面，体验一般，购买之后就可以放在场外交易网站。
- ✧ 老牌的几个交易所比如火币、OKEX 也陆续开通了 C2C（个人对个人）场外交易，账户地址其实和交易所地址一样的，购买之后相当于放在了交易所。
- ✧ 通过场外交易群购买，比如微信群等，有人做担保，并收取一定比例费用，在这买大多数放在了自己的钱包上。

现在不少交易所不但进行币币交易，也纷纷开发场外交易；场外交易网站是进行法币与区块链资产的对换，本质上来说也是交易所；因此我们可以把场外交易网站统一归成：交易所。这样，存储区块链资产的常用媒介归为两大类：交易所和钱包。

9.9.1 交易所和钱包各有什么特点？

表 9-1 交易所与钱包的对比

特点	复杂度	交易性	速度	专业性	支持币种	管理权
交易所	简单	方便	慢	强	多	低
钱包	复杂	繁琐	快	弱	少	高

根据表 9-1，我们可以从几个方面分析各自特点：

（1）复杂度

交易所的资产只要满足网站的安全设置（密码和二次验证等），不搞错自己的资产地址，其它不用操作太多，相对简单。

钱包则要学会保存密码、私钥、助记词、Keystore，操作过程相对复杂。

（2）交易性

交易所可以随时实现交易，流通性强。

钱包要想买卖则需要先转账到交易所，相对繁琐。

（3）速度

交易所转账速度相比钱包会慢不少，而且有的交易所提现金额大还要人工审核，甚至所有提现都要审核，还会经常出现提现繁忙或者钱包故障，甚至他们的热钱包没币了。

钱包则没有以上限制，速度也比交易所快很多。

（4）专业性

交易所通常会把大部分资产用冷钱包（离线钱包）管理，这点比个人钱包更专业些。

（5）支持币种数量

交易所一般支持多种币种，比如你可以充值 BTC、ETH、ZEC 等，而个人钱包一般按类别来分，不同的资产一般会有不同的钱包，比如要想存储 BTC、ETH、ZEC 可能需要三种钱包，但这个后期可能会有改进，同一个钱包支持的币种会越来越多。

（6）管理权

交易所拥有你资产更多的管理权，比如你提现他要审核，而你自己的钱包你就有完全的控制权。

（7）安全性

了解上述特点后，我们来比较下交易所和钱包的安全性：

资产放在交易所，若你的邮箱和短信被黑客截取，那账户的资产就有可能受损失。目前区块链交易所是黑客攻击的主要对象，懂的人知道那都是钱，那么交易所受到攻击及丢失币的可能性还是有的。

那放到个人钱包就一定安全了吗？也不一定，若密码丢失、私钥被黑客截取、助记词或 Keystore 丢失都有可能丢币。

所以没有绝对的安全，我们只能采取尽可能多的措施做到相对安全，并且要培养足够的安全意识。然后根据需要选择你存放的地点，若资金量不大，经常需要交易，持有多个币种，那只能放交易所。

而如果买币之后喜欢屯，不怎么交易，建议放在自己的轻钱包里，如果资金数额较大（比如超过 100 万），最好选择冷钱包存储。

9.9.2 如何更安全使用交易所和钱包

1）交易所使用时注意事项

一是**注册时选择更安全的邮箱**，经常在网上看到某某邮箱密码泄露，那么这些邮箱就不要用来注册这些有资产的交易所了，推荐大家使用谷歌邮箱。

二是**密码设置尽量复杂**，至少要选择数字、字母、特殊字符三者中的两者进行组合，并且每个网站密码千万不要设置成一个（自己想办法创建不同的密码），这点一定要记住，否则一旦一个网站密码泄露，所有网站都有危险了。

如果你嫌每个网站密码设置成不同太麻烦，推荐一个专业的密码管理工具 1password，是收费密码管理软件，每月 3 美元左右。

三是**使用谷歌二次验证**，这个比手机的二次验证更加安全好用，手机有时候信号不好接收不到，但这个会自动同步更新验证码，并且不需要连网，还免费。使用这个一定要注意，在

第一次用时一定要备份好密钥和二维码，否则丢这个可能就是丢币。

2）钱包使用注意事项

由于不同的币种会开发不同的钱包，所以钱包众多，但大致可以分为几大类别

- ✧ 比特币钱包
- ✧ 以太系钱包
- ✧ ZEC、ETC 等系列
- ✧ BTS、GXS 等系列

不管哪种钱包，要想足够安全，**钱包一定要保管好密码、私钥、助记词和 Keystore**（加密过后的私钥）。所以在注册时千万不要漏掉这些关键步骤，你有没有注意到上面加粗这句我已经写了三遍了，你说重要不重要？！

imToken 导出私钥和备份 Keystore 示例：

图9-20 Imtoken 导出私钥、备份 keystore

对于这些区别，以银行账户的类比非常形象：

- ✧ 地址 = 银行卡号
- ✧ 密码 = 银行卡密码
- ✧ 私钥 = 银行卡号 + 银行卡密码
- ✧ 助记词 = 银行卡号 + 银行卡密码
- ✧ Keystore + 密码 = 银行卡号 + 银行卡密码
- ✧ Keystore ≠ 银行卡号

所以你可以想像丢失密码、私钥、助记词和 Keystore 所带来的后果，直接就会丢币。

另外现在虽然这些东西存在电脑上非常方便，但也有可能被黑客截取，最安全的办法还是把密码、私钥、助记词手抄在纸上，并且多抄几份，放在不同的安全区域，并告诉家人，这样就足够安全。

只有培养了足够的安全意识，才能让我们的资产足够安全。

9.9.3 btc-e 网站的突然关闭说明了学会钱包软件的重要性

2017 年 7 月 26 日，著名的 btc-e 数字货币交易平台网站突然关闭，该交易所的创始人 Alexander Vinnik 面临多项罪名的指控，还可能与 MtGox 资金被盗案有关。我们不讨论这个事件的细节，而是说明在区块链世界生存的一项重要技能，学会使用钱包软件，把私钥放在自己的手里。

有一段时间，我对 NameCoin 这种币挺感兴趣，它是一种去中心化的域名币，币代码为 NMC，你花上一点点 NMC，就可以注册一个.bit 域名，大概 5 个月左右再花一点点 NMC 进行续费，再与一些网页绑定，就可以使用专门的浏览器看到一个永不消失的网站，想想都挺兴奋的。

为了试验这个技术，就想着买入几个 NMC，可是当时网内的交易平台上都不卖这种币，然

后发现 btc-e 平台上可以用 btc 兑换 nmc，才有了一次 btc-e 的亲密接触。

该网站不需要实名认证，开户、存入 btc（从云币买来的）、btc 兑换 nmc、提现 nmc 到钱包，一趟操作下来用不了多长时间，因为钱包软件没安装好，我兑换的 nmc 还在平台里放了 2-3 天，现在想想就有点后怕，万一那段时间里 btc-e 网站关闭，钱就永远消失了。图 4-9 是当时在 btc-e 网站取现的网页截图。

所以说，当你不信任一个平台时，一定要学会钱包软件，在尽量短的时间内完成充值、兑换、提现等操作，甚至不惜多花点手续费，分成几笔操作以减少风险，把币放在自己的钱包里才是自己的币。

我的 btc-e 里好像还有 0.002BTC，如果哪天 btc-e 恢复了，估计也提不出来了。

10 交易进阶

10.1 比特币改进提议(BIP)

BIP 是英文 Bitcoin Improvement Proposal 的缩写，可翻译为比特币改进提议，是指比特币社区成员所提交的一系列改进比特币的建议。所有的 BIP 可以在 https://github.com/bitcoin/bips/blob/master/README.mediawiki 找到，我写这篇文章时的最大编号为 199。

在《精通比特币》书里有些地方翻译为“比特币改进协议”是不对的，BIP 之所以被称为提议，说明它们可以不被批准，能够成为比特币标准的协议的少之又少。BIP 的状态一共可分为 9 种，它们分别是 Proposed （提出）、Draft（草案）、Active（激活）、Final（落地）、Replaced（被替代）、Withdrawn（撤掉）、Deferred（推迟）、BIP number allocated （BIP 编号被分配）、Rejected（拒绝）。只有处于 Active 和 Final 状态的 BIP，才成为大家公认的标准。

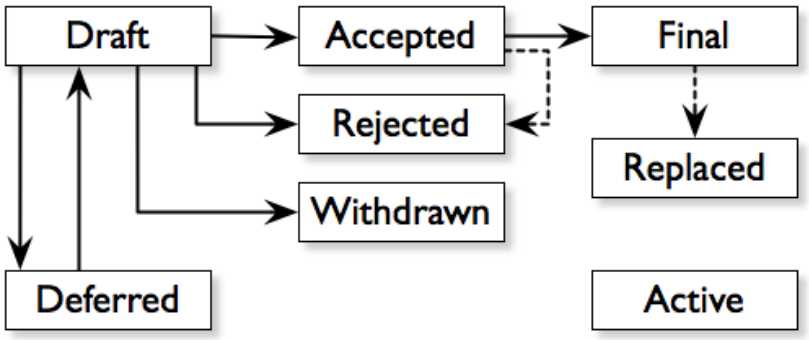


图10-1 BIP 的几种状态

第 9.2 节介绍过 HD 钱包（分层确定性钱包），它的编号是 BIP32，可以看到它的状态是 Final，已经成为一种正式的标准。很多钱包提供 12 个英文单词的助记码来生成私钥，这种方案是 BIP39，也处于草案阶段。以前让许多人担心的用户激活软分叉（UASF）属于 BIP148，还有在分叉时期被密切关注的是 BIP91，它让矿工在挖出的区块里投票，在 336 个区块周期里，如果有 269 个支持（80%），就锁定 BIP91，这时比特币的区块链不太可能分裂。

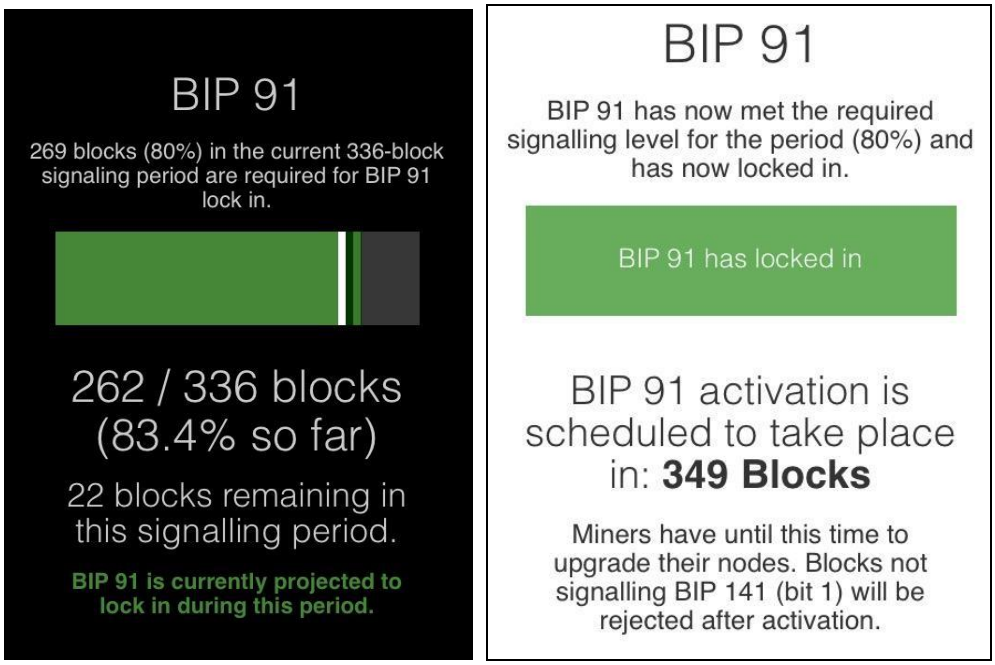


图10-2 正在投票 BIP91(左)，BIP91被锁定，分叉可能性不大(右)

10.2 交易数据查询 API

对于程序员来说，可以编程来访问一些网站提供的 API(Application Programming Interface)，即应用程序编程接口，例如：https://blockchain.info/unspent?active=1Dh1YpCoVCMjrFesquPrhzyHfXJWPLFogt

可以得到 Restful 的数据结果：

```
{
    "unspent_outputs":[
        {
            "tx_hash":"5ffae7ab8e3025266a80e834f680982ae38aa0afd91e6386ef5e5e184528072f",
            "tx_hash_big_endian":"2f072845185e5eef86631ed9afa08ae32a9880f634e8806a2625308eabe7fa5f",
```

```
            "tx_index":255103073,
            "tx_output_n": 0,
            "script":"76a9148b329b12b05ff4476961f2b7e1ebc329eaca918488ac",
            "value": 100000,
            "value_hex": "0186a0",
            "confirmations":150
        }
    ]
}
```


value 100000 表示 0.001BTC，即 10 万聪，我把这笔交易的交易费提高了一点，当时查询时，已经得到了 150 次确认，你的查询结果应该会有所不同。按照比特币的技术原理，达到 6 次以上的确认，该交易被伪造的概率极低。

10.3 交易频率

比特币系统的交易频率过低是被许多人所诟病的，每秒最多能够处理 6-7 笔交易，这个数据是如何计算出来的？

普通的交易都会有 1 个输入，2 个输出（1 付款+1 找零），占用 226 个字节(148*1 + 34*2 + 10)。中本聪在设计比特币系统时，单个区块容量最大为 1MB，这样一个区块最多可以包括 1024*1024/226=4639 笔交易，按平均 10 分钟产生出一个新区块计算，每秒能够处理 4639/(10*60)=7.7 笔交易。

图 10-3 是 2017 年单笔交易所占字节数的示意图（来源：https://charts.bitcoin.com/chart/transaction-size）。如果平均一笔交易按 600 字节计算，这样一个区块可以有 1024*1024/600=1748 笔交易，每秒能够处理 1748/(10*60)=2.9 笔交易。所以说，比特币的区块链每秒最多能够处理 3 到 7 笔左右的交易。

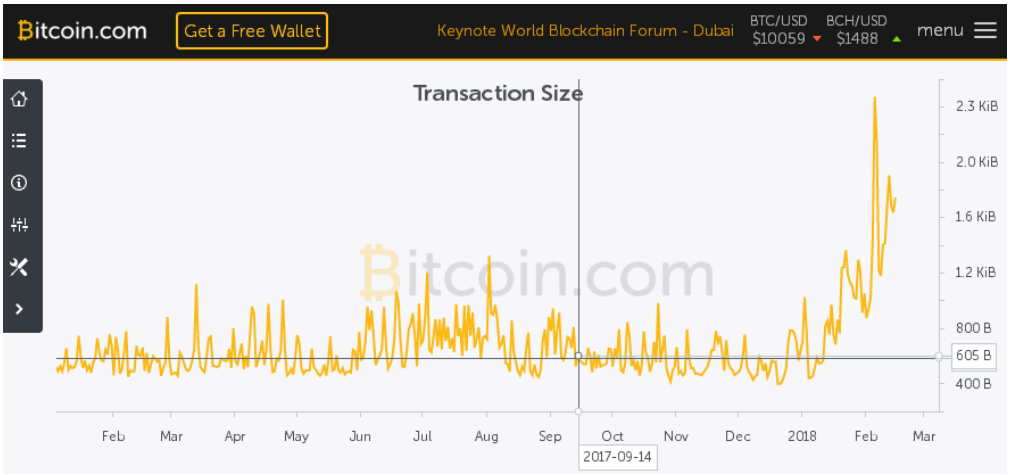


图10-3 单笔交易大小的统计图

可以看出，如果单纯地把区块容量限制从 1MB 升为 2MB，每秒也只能够处理 6-14 笔交易，这种方案只能暂时缓解区块链堵塞的现状，并不是一劳永逸的解决方案。所以又有了隔离见证（Segwit）等方案，把交易中与验证无关的数据搬到区块外边，从而大幅提升单个区块内的交易数量，提升交易频率。

10.4 交易确认数

在 2017 年 7 月 23 日 8 点（北京时间）的时候，比特币面临可能分叉的情况，在 bitcoin.org 网站上会出现提醒，比特币的确认数评估分可能变得比平常不太可靠。在这种时期，建议你在用 BTC 收款时，需要等待更多的确认次数才可信，在网络分裂期官方建议的确认数是 30。

表10-1 BTC 交易确认次数的推荐值

确认次数	轻钱包	Bitcoin Core
0	只在你信任那个人或商家的时候，才是安全的	
1	可靠	很可靠
3	很可靠	非常可靠
6	大额交易的最小确认数	
30	有人工干预的非常时期的建议值	

官网地址：https://bitcoin.org/en/alert/2017-07-12-potential-split

10.5 创币交易(Coinbase Transaction)

区块链是由一个一个的区块连接而成的，每个区块里记录着许多交易信息，而这里面的首

个交易一定是**创币交易**，称为 Coinbase Transaction。比如，我在写这篇文章时的最新区块高度是 478829，在浏览器输入：http://blockchain.info/zh-cn/block/000000000000000000007b14c2f63319afcd662bb01be5215a73e95fe5521c343c

图10-4 区块中第一条是创币交易

找到第一条交易记录，有一行提示文本“没有输入（新生成的比特币）”，意思是说这些比特币是凭空产生的，是矿工挖出来的，根据 4 年减半的规矩，当前的挖矿奖励为 12.5 BTC。

图10-5 创币交易中的详细内容

再往右侧看，总共的比特币为 13.77005022，比 12.5 要多出来 1.27005022，就是后面 2000 多笔交易的交易费之和，因为以前介绍过，矿工不仅得到新币奖励，还得到打包的这 2000 多笔交易的所有手续费。

点击第一笔交易 HASH 为 ebdc225bcd29603af483e1ea0ed8e7525b1b0fa12d89cb6cf03650a27709003d 的链接，可以看到这个创币交易的详情，在 CoinBase 和输出脚本里面有一些稀奇古怪的字符，这里面就是 BIP 投票或在 3.5 节里介绍不可篡改性时黑客喜欢写入的一些誓言或证明的内容了。

提醒大家注意，Coinbase 还是一个公司的名字，你从网站上搜索后找到的都是与这个公司有关的内容，本节介绍的内容与 Coinbase 公司没有半毛钱关系。

10.6 未花费交易输出(UTXO)

有人对交易中为什么会出现找零费用比较困惑，这里需要介绍一个重要概念 UTXO，Unspent Transaction Output，即未花费交易输出。再贴出第 4.1 节中介绍**交易**时用过一张图，这里只保留了区块 1 和区块 2 的内容，一笔交易分为输入 vin 和输出 vout，我们可以从一个 coinbase 的 12.5 BTC 的新块奖励出发，看一下它的资金流向，就可以明白 UTXO 的含义。

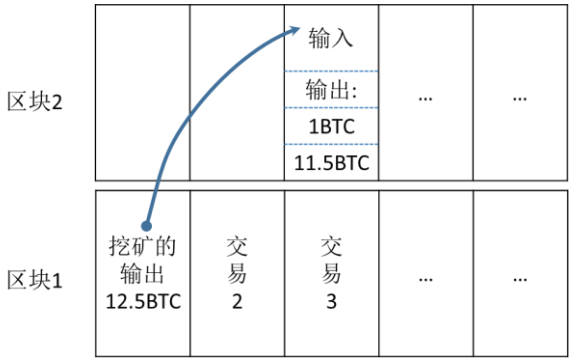


图10-6 交易中的 vin 和 vout

（1）矿工 A 挖矿产生了一个新区块，其中的第一笔交易是 coinbase，假设为 12.5BTC

（2）矿工 A 现在想买一台笔记本电脑，需要支付 1 BTC 给商家 B，他的币的来源只有这 12.5BTC，比特币系统中的 UTXO 有一项重要规则，**一笔 UTXO 必须一次性花完**，这里的 vin 是 12.5BTC，如果 vout 只有一笔 1 BTC 记录，那么剩下的 11.5 BTC 就会被当作交易费由其它矿工 C 得到，那这个矿工 C 可真发了一笔横财。

这肯定不是 A 的本意，A 只想支付 1 BTC，另外的 11.5 BTC 还要留给自己，所以在生成交易记录时，钱包软件会把 vin 设定为 12.5BTC，$vout_0$ 设定为 1BTC，锁定给商家 B，另外的 $vout_1$ 的金额是 11.5BTC，就是找零地址，锁定给自己。

当然这种情况下是零手续费，以现在的网络情况，将不会被确认。

这个 12.5 BTC 已经花了，这个时候就不是 UTXO 了。

（3）再向后推，商家 B 有了 1 个 BTC，这笔钱还没有花费，是 UTXO，表示将来可以动用。自己还剩的 11.5 BTC 也是 UTXO，以后自己还可以再花，价值就通过这种办法不断向下传递。

（4）钱包软件（如 Bitcoin Core）实际上就是扫描整个区块链中的所有 UTXO，并且与你的私钥进行匹配，如果解锁成功，则表明你拥有某个 UTXO 中的钱，这些 UTXO 中的钱加在一起，就是你的钱包里显示的余额了。所以你在 Bitcoin Core 的同步过程中，会看到一行提示信息：

> 近期交易可能尚未显示，因此当前余额可能不准确。以上信息将在与比特币网络完全同步后更正。

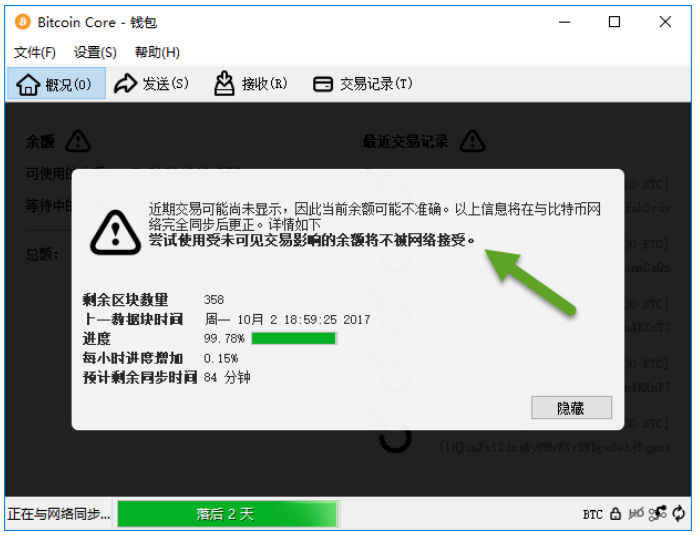


图10-7 未完成同步时给出的信息提示

因为比特币是数字货币，比纸质货币易分割（见第 3.1 节的可分割性），不用人为设置 100、50、20、10、5、2、1 这样的面额，一个 UTXO 是一个整体，必须一次性花完。除了付给别人的币之外，剩下的再付给自己，相当于找零。

10.7 一笔真实的交易例子

为了对交易细节有更直观的概念，我用一次在区块 468779 中的一笔真实交易作为例子来说明交易中的发币方、收币方、发币数量是如何得到的。

我以前教大家使用钱包发币、收币时，给地址 1KWTsVew7zEVGg6nq8j3GtYkPYnyu99Yzd 发送了 2 次 0.001 BTC。在浏览器中输入这个网址(图 10-8)：http://blockchain.info/address/1KWTsVew7zEVGg6nq8j3GtYkPYnyu99Yzd

图10-8 两笔收款记录

可以看到这个地址共有两笔 0.001 BTC 的收款交易，点击第一笔交易中那个 4b77...3818 那串长长的字符串（TXID，即交易 ID，占 32 个字节），可以看到这笔交易的详细信息（图 10-9）。

图10-9 交易的详细信息

浏览器中显示的许多内容都已经转换成了方便大家阅读的信息，在实际的记录中并不是这样存储的，而是分为两个部分：**输入 vin**、**输出 vout**。

可以使用 Bitcoin Core 软件带的命令 getrawtransaction 来查看这笔交易的内部细节，请先确保 Bitcoin Core 已经完成了全部数据的同步，在“帮助”菜单中点击“调试窗口”，然后再点击“控制台”，在底部输入命令：

```
getrawtransaction 4b77cb17105a61dc6ca0bfa535fd3df69bfd5b65d8123e067aa4953e169b3818 true
```

忽略其它信息，把目光注意到 vin 和 vout 两部分。

```
"vin":
[{
    "txid": "2f072845185e5eef86631ed9afa08ae32a9880f634e8806a2625308eabe7fa5f",
    "vout": 1,
    "scriptSig": {
        "asm": "3045022100c3d39df2a31f7a5df7b1a44144dfc73089cb628d888d53dc27a12
f2225810c0902204204e40bafd9a9db0e4e416f099ff3c05223c99b77abd2b5622ded4e4f72498
f[ALL] 0304ea538bb0aaace649751a98659d6ac7e55dae01707215164a578a408913cf91",
        "hex": "483045022100c3d39df2a31f7a5df7b1a44144dfc73089cb628d888d53dc27a
12f2225810c0902204204e40bafd9a9db0e4e416f099ff3c05223c99b77abd2b5622ded4e4f724
98f01210304ea538bb0aaace649751a98659d6ac7e55dae01707215164a578a408913cf91"
        },
    "sequence": 4294967294
}]
```



```
"vout":
[
    { "value": 0.98422648,
      "n": 0,
      "scriptPubKey": {
          "asm": "OP_DUP OP_HASH160 6a263f895ad9890653e8523d3bfb2823fa4ee96a OP
_EQUALVERIFY OP_CHECKSIG",
          "hex": "76a9146a263f895ad9890653e8523d3bfb2823fa4ee96a88ac",
          "reqSigs": 1,
          "type": "pubkeyhash",
          "addresses": ["1AgGSsAHVQEzaJq1GBDh54U55ECq6VWrLT"]
       }
    },
    { "value": 0.00100000,
      "n": 1,
      "scriptPubKey": {
          "asm": "OP_DUP OP_HASH160 cb04c1e7561fdb85f6360f9c3992ef41fd71d89f OP
_EQUALVERIFY OP_CHECKSIG",
          "hex": "76a914cb04c1e7561fdb85f6360f9c3992ef41fd71d89f88ac",
          "reqSigs": 1,
          "type": "pubkeyhash",
          "addresses": ["1KWTsVew7zEVGg6nq8j3GtYkPYnyu99Yzd"]
       }
    }
 ]
```


10.7.1 发送方地址和金额

先来看看图 10-9 左侧的这个比特币地址（1EXH329ttyGjoD5SS52hrbgTHWmkXAQGmT）是如何得到的。

比特币系统中规定：vin 一定是来自于以前的某笔交易的 vout，这样一笔一笔交易形成一个链条，一直追溯到**创币交易**(coinbase)。

看 vin 的内容，txid 是 2f072845185e5eef86631ed9afa08ae32a9880f634e8806a2625308eabe7fa5f，vout 是 1，表示这笔资金来源于交易 ID 为 2f07...e7fa 的第 1 项输出。

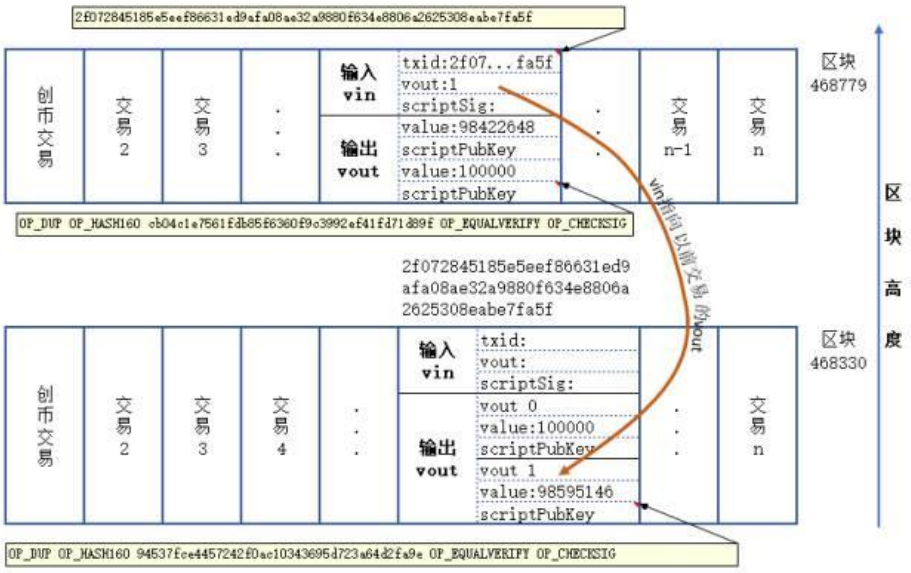


图10-10 交易的内部结构

在浏览器中输入 http://blockchain.info/zh-cn/tx/2f072845185e5eef86631ed9afa08ae32a9880f634e8806a2625308eabe7fa5f

图10-11 找到前面的某笔交易 vout

可以查到这条交易在区块 468330 中，vout 是从 0 开始编号的，找到 vout 1，可以看到比特币地址，正是"1EXH329ttyGjoD5SS52hrbgTHWmkXAQGmT"，金额是 98595146。

这里有个细节先不展开了，在交易记录中并不是记录以 1 开头的比特币地址，而是记录着下面这个内容：

```
OP_DUP OP_HASH160 94537fce4457242f0ac10343695d723a64d2fa9e OP_EQUALVERIFY OP_CHECKSIG
```

地址 1EXH329ttyGjoD5SS52hrbgTHWmkXAQGmT 实际上是**公钥** 94537fce4457242f0ac10343695d723a64d2fa9e 的 Base58check 表示法。

10.7.2 接收方地址和金额

图 10-9 中的发送方地址找到了，再来看接收方的信息，这时候看 vout 的内容。

```
"vout":
[
    { "value": 0.98422648,
      "n": 0,
      "scriptPubKey": {
           "addresses": ["1AgGSsAHVQEzaJq1GBDh54U55ECq6VWrLT"]
       }
    },
    { "value": 0.00100000,
      "n": 1,
      "scriptPubKey": {
           "addresses": ["1KWTsVew7zEVGg6nq8j3GtYkPYnyu99Yzd"]
       }
    }
 ]
```

这里面有两项，后面那项的 value 是金额：100000 聪，是收款金额，地址是“1KWTsVew7zEVGg6nq8j3GtYkPYnyu99Yzd”；前面那个 vout 0 的金额是 98422648，是找零金额，地址是"1AgGSsAHVQEzaJq1GBDh54U55ECq6VWrLT"。

10.7.3 交易费

交易费并没有直接记录在交易里，而是通过一个公式计算出来的：

```
    交易费 = sum(vin) - sum(vout)
```

上面的例子里 vin 的金额是 98595146，vout 里是 98422648 + 100000，所以

```
交易费 = 98595146 - (98422648 + 100000) = 72498
```

正好就是图 10-9 右侧的交易费的数字，注意这里用"聪"为单位，浏览器里显示的单位是 BTC。

10.7.4 脚本

再重复一遍，vin 要指向以前交易的 vout，那么我是不是能够把 vin 指向别人的 vout？去花别人的 BTC？当然不能，在 vout 里有一个 scriptPubKey，称为**锁定脚本**(Locking Script)或**见证脚本**(Witness Script)，表示要满足一定条件才可以花掉这些钱。（这里出现了**见证 Witness** 这个概念，以后理解"**隔离见证**"就会容易一些了）

而 vin 里面有一个 scriptSig，称为**解锁脚本**(Unlocking Script)，通常里面记录着所有人的签名。只有解锁脚本与锁定脚本匹配时，这笔交易才是有效的。

小结：

- ✧ 交易里主要记录着输入 vin 和输出 vout
- ✧ 输入 vin 来自于以前一笔交易的 vout
- ✧ vout 里通常有一个找零地址和找零金额
- ✧ 交易费 = sum(vin) - sum(vout)
- ✧ vout 里记录着锁定脚本
- ✧ vin 里记录着解锁脚本，通常是一个签名

10.8 交易加速的几种办法

2017 年 10 月，金炜搞了一个联合挖矿项目，一开始只有 50 人参加，后来规模不断扩大，如今每 10 天要给 200 多人发币，工作量可不轻。申龙斌写了一套 C#发币程序，根据每人参与的份额把所有的发币操作放在一笔交易中，这样发币效率高、错误少，还节省了大笔的手续费。

以这笔交易为例（txid 为 7ae1fd5dc58bbeb7680d2d31931a15408cfb1e2898fca4b6eaf348e5d830a8b2），同时给 100 多人发币，手续费只用了 0.0003 BTC，平均每人手续费为 0.000003 BTC，还不到 1 元钱。

不过这种幸福的日子没过多久，2017 年 12 月初的时候，比特币价格爆涨，比特币的区块链严重拥堵。

2017 年 12 月 16 日发出的这笔交易（txid 为 d7028391bbb41415ed1c837a1eb8e03b3583cbd22486529dc2d1890327bb903f）仍按往常一样将手续费设为 0.0003 BTC，结果所有的矿池都拒绝受理，10 多天之后仍为零确认。

寻找交易加速的解决办法当然不能用 X 度了，直接用 google，关键词用“transaction stuck”，最权威的一篇贴子在 bitcointalk.org 上，请科学上网访问这个网址：

https://bitcointalk.org/index.php?topic=1802212.0

交易被堵住的最主要原因就是手续费设置得太低，矿池是逐利的，优先挑选高额手续费的交易打包，而行情火爆，你的交易可能永远排在队伍的最末尾，也就是永远无法被打包。

1）等待

如果你不会一些高级操作，就只能等待了，如果运气特别好，几天后可能会被确认。或者，过了很久，让整个比特币网络忘记了你的这笔交易，你可以重新发起一笔新的交易。不过，我的那笔交易等了 10 多天，没看到任何被确认的迹象，也没看到被清除的可能性。

2）找矿池加速

有些矿池提供交易加速的服务，比如 https://pool.viabtc.com/tools/txaccelerator/ 。但免费加速的名额非常有限，它还提供收费服务，支付少量 BCH 之后，交易很快会被确认。

3）Replace-By-Fee (RBF)

这种办法实际上是一种双重支付（Double-Spend），后面发起的交易可以提高手续费，在 Bitcoin Core 0.15 版本中提供了界面可以进行这种操作，但前提是发起交易时要加上 Replace-By-Fee 选项。

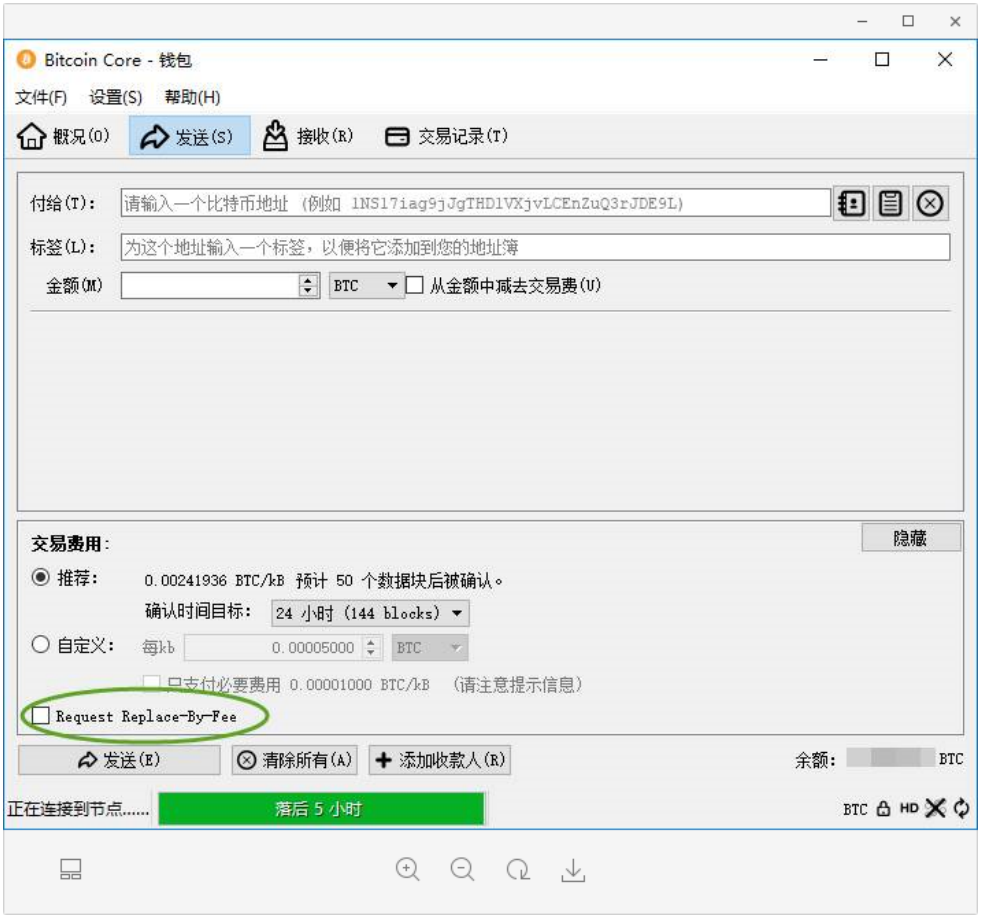


图10-12 Bitcoin Core 中的 RBF 选项

我转币到冷钱包的那笔交易就是用的这种办法，但在调用 RPC 接口的程序中并没有用这个选项，这种办法也不成。

4）发起 Child-Pays-For-Parent 交易

这种交易的意思是，被堵的交易作为**父交易**，里面的输出项是 0 确认的，但你有私钥可以控制，这样你可以发起一个子**交易**，用父交易中的一个未确认的输出当作新交易的输入，而交易费必须给足，让矿池愿意打包，打包**子交易**时会一起把**父交易**打包。

我最后采用的就是这个办法，父交易为 5400 字节（txid 为 7b02b4066ab66fc965a897a5f72414f886a8fd150245f8acf0ab1cafcb414ca4），我又发起了一个子交易为 8000 字节（txid 为 756d5afa45c5ef9a9ce2725de54f8538f4993e8156576ddeb9be34e6c45f2819），总共约 13 KB，按当时交易费行情大概为 0.004 BTC/KB，我应该设置手续费为 0.052 才是安全的。我最后采用了 0.056 的手续费，再加上父交易的 0.0015，总共为 0.0575 BTC，看来找矿池加速也就这个价。

10.9 比特币的隐私性

比特币的所有交易公开可查，那为什么现在中本聪或者李笑来拥有的真实币量都没人知道呢？

新币是从挖矿得来的，这个新区块首先向全网广播，这个区块里记录着一项重要信息，就是比特币地址，不可能不被人知道，但是仅凭这个比特币地址，能够获取的信息非常有限，你可能能够知道的就是这个地址与某个矿池有关，但矿池会根据每个矿工的贡献率把币分发下去，你能知道的信息只有一个比特币地址和币数量而已。

币的数量永远都是可以查到的，你只要不对外公布你的比特币收款地址，别人很难把那个地址与你对应起来。也就是说比特币地址是公开的，但与人是没有直接的对应关系的，在区块链里只记录地址，不记录用户信息。

中本聪从 2011 年就不知道了去向，一开始挖的币可能都是他的，很多币都没有花过，根本就不知道是谁的，后面参与挖矿的人渐渐多起来，就更不知道哪些币是他的了。

李笑来买的币也比较早，好像主要是从 OTC 场外交易直接购买的，当时的交易所可能也不需要实名认证，你就更无从查起了。理论上根据这些场外交易的发币人、交易时间也能查到一

些线索，但这个工作量可就相当可观了。

2017 年 9 月 4 日之前，我们从云币网等国内交易所买币，都要经过 KYC 实名认证，每一笔 BTC 取现记录，云币网都记录在案，只要想查，根据这个地址就能把你的家底清清楚楚地查出来。比如我以前做活动时，给几个人发过 0.001BTC，通过几个地址，你可以一路追查下去，发现我的钱包里共有几个币，还有几个未花过的，所以说在国内，比特币基本上是没有隐私可言的。

2010 年 5 月 22 日，某个人花了 10000 BTC 买了 2 块披萨，因为时间、币量、还有收款方（披萨店）的地址都清楚，所以很容易查出来。现在行情约 7 万元/BTC，这 2 块披萨已经值 7 个亿了，这个网址（https://blockchain.info/tx/a1075db55d416d3ca199f55b6084e2115b9345e16c5cf302fc80e9d5fbf5d48d）记录了这笔让人悔断肠的交易。

图10-13 用10000个 BTC 买披萨的交易记录

11 挖矿进阶

11.1 矿池(Mining Pool)

矿工（矿机）本来是指那些配备了专门显卡的用于挖矿的计算机，但这些计算机都是矿场老板投资的，有些人把这些矿场的老板也叫做矿工。这些老板只是出资方，技术人员和管理人员都是雇来的，购买了场地、设备等固定投资之后，日常最大的费用就是电费，收益则是挖出来的新块奖励（包括新币和手续费）。

随着 BTC 价格和交易费的高涨，加入挖矿大军的老板们也越来越多，算力竞争也越来越激烈，但比特币系统自动设定了平均 10 分钟的出块速度，10 分钟内只会有一个矿工拿到新区块奖励，这种挖矿竞赛既比拼算力，也要靠点运气。

如果你是独立矿工（Solo Miner），即自己搞了几块显卡独自挖矿，在当前的算力竞争环境中，有可能一辈子也挖不到 1 个新块，偶尔挖到新块需要有中彩票的好运。为了让收益稳定一些，一群矿工把算力联合在一起形成矿池(Mining Pool)，把那道难题拆分成许多子问题，大家分别去算，如果挖到新块，大家根据贡献率进行利益分配，这样收益比独立挖矿相对稳定有保障。

大型矿池里通常有成百上千的矿工,有专门的矿池服务器来负责协调各矿工完成工作量证明 PoW，矿池与矿工也有专门的 Stratum 通讯协议。如何做到比较公平呢？也利用了 PoW 工作量证明的原理，假设当前比特币网络上的难度要算出 70 个零，矿池可以把难度调低一些，设定为 67 个零，虽然矿工没有完成最终的工作量，但它没有功劳也有苦劳，而且这种证明是大家都公认的，所以利益的分配也是容易量化的。

矿池的存在也让矿工们轻松了许多，矿工甚至不用下载几百个 GB 的区块数据，只需完成矿池分过来的任务即可，它只需配备足够的内存和大量的 ASIC 芯片，拼命地进行 HASH 计算就够了，矿池会按规定好的协议给大家发放 BTC。当然，上面说的矿池是中心化的，这种矿池会有单点故障的危险，现在也有去中心化的矿池。

不过还有一个现象要值得关注，现在的大型矿池几乎都在中国，据称能够达到 70%-80%，如果中国人联合起来，来个 51%攻击也不是不可能，所以矿池太过集中也会毁了比特币。英文过关的朋友可以读读这篇文章：https://www.buybitcoinworldwide.com/mining/china/。

11.2 算力、哈希速率(Hash Rate)

Hash Rate 是用来评估矿机（或矿池）的计算能力的度量单位，直译为哈希速率，国内通常翻译为算力,用每秒完成 HASH 运算的次数来度量。挖矿计算机的最繁重任务就是 HASH 计算，计算得越快，越有可能得到新块奖励。

比特大陆的蚂蚁矿机(AntMiner)S9 是一款比特币矿机，广告上声称的算力为 13.5 TH/s，即 1 秒钟完成 13.5×10^{12} 次 HASH 运算。电源效率为 0.1J/GH，即完成 1GH 的计算只耗电 0.1J (1 J = 0.000000278 千瓦时）

据 http://www.qukuai.com/pools 在 2018 年 2 月 19 日的估计结果，现在比特币矿池的全球算力大概为 9211434 TH/s，即 9211 PH/s，或者 9.2 EH。这种巨大的能源消耗是被比特币反对者所抨击的，但正是这种巨大的运算量，才能保证比特币交易的安全性。

1 GH = 10^9 次 HASH

1 TH = 1000 GH = 10^{12} 次 HASH

1 PH = 1000 TH = 10^{15} 次 HASH

1 EH = 1000 PH = 10^{18} 次 HASH

11.3 计算目标与难度系数 difficulty

在介绍工作量证明 PoW 时，矿工们要完成一个繁重的计算任务，使 HASH 计算出来的结果满足一定的要求，即二进制值的前面有多少个 0，这个值称为**计算目标**，而且这个值是写入区块头的。

打开 blockchain.info 网站，找到最近的一个区块，点击进去，可以看到该区块的摘要信息（图 11-1），注意两行数字：难度系数、计算目标。

图11-1 难度系数与计算目标

计算目标是给程序员使用的，通过一个公式可以计算出难度系数，这个难度系数并没有保存在区块里，只是便于人类理解。例如图中的 804,525,194,568.13 的意思，表示要进行 8045 亿次 HASH 计算，能够产生出一个新区块。

当然计算过程有点运气的成份，有时可能几亿次 HASH 就可以算出一个区块。比特币系统设定平均每 10 分钟产生出一个新区块(也称为比特币的心跳)，但挖矿的速度是难以预测的，因为有时计算机的性能会成倍提升，有时参与挖矿的节点数量也不一样，中本聪就设计了一种工作量目标难度的自动调整机制，即每 2016 个区块后，对难度值进行一次调整，从而让它接近于 10 分钟产出一个新区块。

为什么是 2016 个区块？因为 10 分钟产出一个区块，1 小时产生 6 个区块，1 天产生 144(6*24)个区块，14 天产生 2016(14*6*24)个区块，也就是说大约 2 周会自动调整一次难度值，具体难度调整的公式就不介绍了，让挖矿的速度不快也不慢。

下面的内容涉及到二进制计算，程序员可以继续往下阅读：

计算目标：402742748，二进制为 0x18015ddc，这是一种压缩存储格式，分为两部分，0x18 是指数部分，0x015ddc 是系数部分。

target = 系数 * $2^{8*(指数-3)}$

= 0x015ddc * $2^{8*(0x18-3)}$

= 0x00000000000000015ddc0000000000000000000000000000000000000000

前面有 17 个十六进制的 0，即 68 位的二进制 0，再加上后面的 0x15ddc 的 3 个二进制 0，总共要有 71 个 0。

也就是说计算结果要使这个 256 位的二进制数的前面 71 位都是零。

难度系数是这样计算出来的：

0x00000000FFFF0000000000000000000000000000000000000000000000000000 / 0x00000000000000015ddc0000000000000000000000000000000000000000 = 804525194568.1318

12 分叉(Fork)

12.1 临时分叉

2017 年 8 月 1 日 20:20，Bitcoin Cash（前身是 Bitcoin ABC）给比特币的区块链来了个硬分叉。虽然一开始支持它的矿工的算力并不大，但最终还是整出了 BCH（以前叫 BCC）新币来，到 2018 年 2 月，BCH 的价格一度超过 4000 美元。

图12-1 BCH 价格走势图

如图 12-2，分叉这个概念看似并不难理解，与道路的分叉很像，一条主路是 BTC→BTC1，另一条路是 BCH，注意这里的 BTC1 只是我为了区分 8 月 1 日之前的 BTC 而起的新名字，并没有这个币。BCH 和 BTC 的观点不一致，谁也说服不了谁，最后分道扬镳，分别在各自的区块链上挖矿。

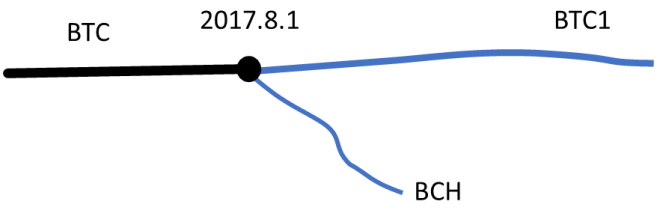


图12-2 分叉示意图

分叉也有叫分裂(Split)的，但比较专业的说法是 Fork，因为**软分叉**简称为 SF（Soft Fork），**硬分叉**简称 HF（Hard Fork）。至于什么是硬分叉，什么是软分叉暂时先不管，先来仔

细看看分叉是如何形成的。

比特币系统中**矿工**们想写入一个新区块，非常不容易，需要完成工作量证明 PoW，也就是要做一道计算量非常大的算术题。这道题说简单不简单、说难也不太难，平均 10 分钟就有矿工计算出来，然后发布一个新区块。

如图 12-3 所示，假设黑点是分布在世界各地的节点，大黑点代表**矿工**节点，小黑点代表普通的**钱包**节点，真实世界里的节点比这多得多，而且连接关系也不是按照地理位置相连的，这里为了形象化地说明分叉进行了大量简化（本图借鉴了《精通比特币》中的思路，这里进行了简化和改进）。

左下角为区块链，假设最新产生出来的**区块高度**为 478129，这个区块已经在整个世界的网络中进行了广播，并且全网都认可了这个区块。

图12-3 区块链世界的通常情况

世界这么大，有些事就是非常凑巧，假设两个矿工（矿工 A 和矿工 B）几乎同时完成了工作量证明 PoW，分别向比特币网络上广播他们的成果。由于大家所处的位置不同，网络连接不同，有些节点先收到 A 广播出来的区块，有些节点先收到 B 广播出来的区块，这时候就出现了临时分叉。

如图 12-4，节点 A 附近的收到了 478130 的蓝色区块，节点 B 附近收到编号也是 478130 的红色区块，其它的那些仍是黑色的节点尚未完成同步。

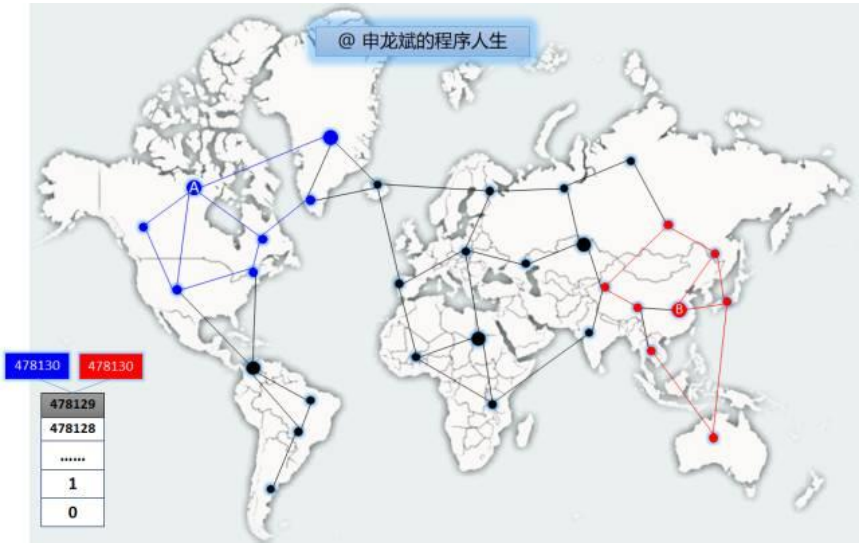


图12-4 两个矿工几乎同时都找到新块

随着时间的推移，它们很快就分化为蓝色阵营或者红色阵营（图 12-5），蓝色阵营承认蓝色的 478130 区块，红色阵营承认红色的 478130 区块。再强调一遍，实际情况并不与地理位置相关，这里只是让分裂或分叉看得更形象。

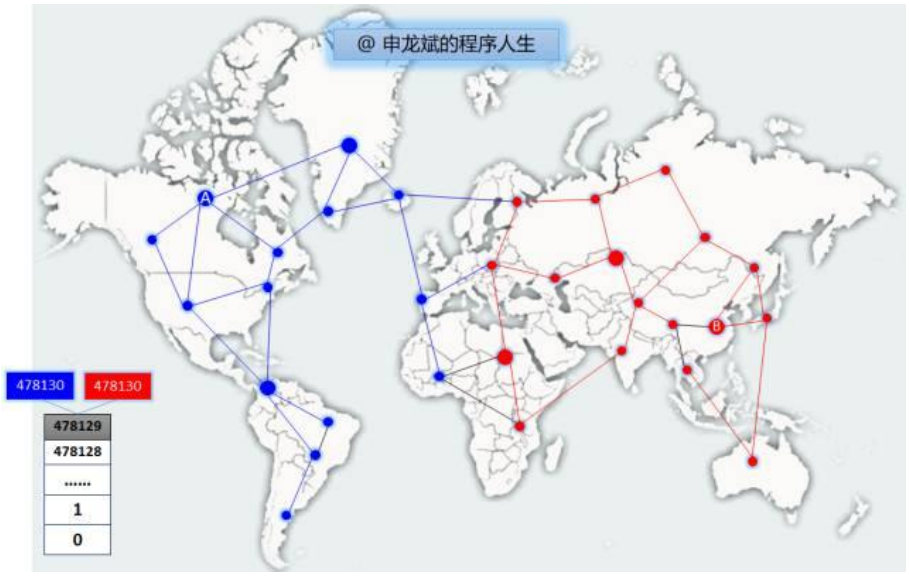


图12-5 区块链世界分为两个阵营

不管收到了蓝色区块还是红色区块，矿工们可没有闲着，因为矿场要交巨额的电费，挖不出比特币，矿场就要关门。此时，假设红色阵营的矿工 C，挖出了 478131 区块（用黑色标记），立刻通知全世界。它附近的节点并不傻，只认最长的链，马上变为黑色阵营（图 12-6）。

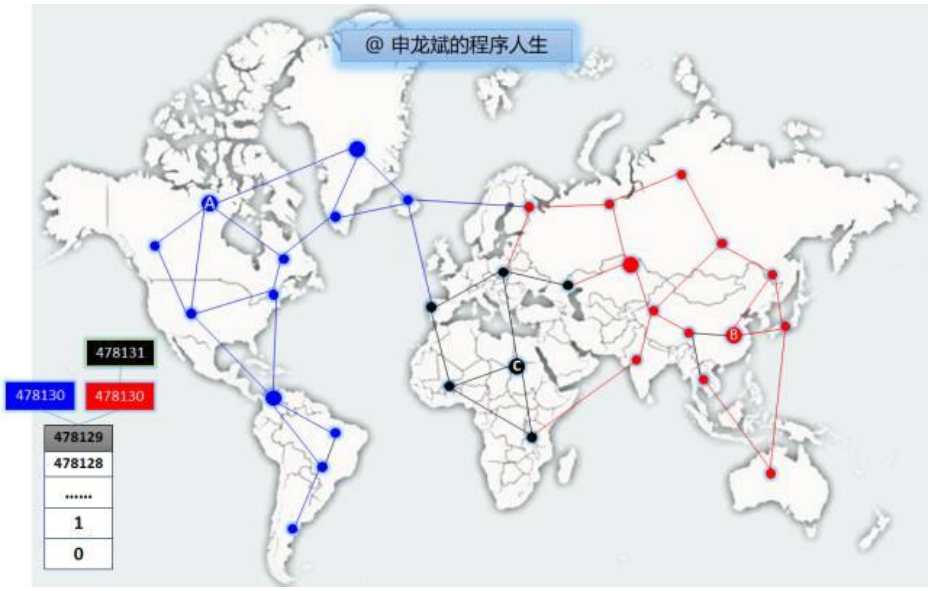


图12-6 在红色阵营里又有新块产生

随着时间的推移，如果这段时间内没有矿工计算出新答案，则全网很快就承认右侧的链为主链。这时候整个世界又和平了（图 12-7），最新的区块高度为 478131，蓝色的 478130 区块被孤立了，明智的矿工不会基于它再做工作，马上在最长的链上投入算力，开始下一轮的计算。

图12-7 区块链世界又回归和平，蓝块被孤立

区块链上的临时分叉很常见，但工作量证明 PoW 的计算量太大，在最长的链上进行计算是非常明智的，经过一段时间后大家就会达成共识，主链旁的小叉叉慢慢会被大家遗忘的。

小结：

- ✧ 区块链世界里的临时分叉很常见
- ✧ 两个矿工几乎同时挖到新块时，会产生临时分叉
- ✧ 由于挖新块要耗费巨大的计算量，明智的矿工会在最长链上挖矿，大家很快会找到一条共认的主链

12.2 重放攻击(Replay Attack)

在 2017 年 8 月之前，BIP91 被锁定，大家以为比特币不会分叉了，没想到分叉出来一个比特现金 Bitcoin Cash，以前买入 BTC 的朋友现在又遇到了一个新挑战：**重放攻击**。

12.2.1 什么是重放攻击？

重放攻击的英文是 Replay Attack，一句话来说，就是你在一条链上产生的交易，会被重放(replay)到另一条链上。本来你只是支付了一种币，结果却额外支付了另外一种币，感觉好像被攻击了。

先来个类比吧，假设你去欧洲旅游时带了一张双币信用卡（欧元 EUR 和人民币 CNY），买了一把瑞士军刀花了 10 EUR（欧元），刷卡时竟然被黑客把你的交易信息全部复制了一份。回国后，你发现竟然多了一笔 10 元人民币的消费记录，你只刷了 10EUR，却多支付了 10 CNY（人民币元），你被**重放攻击**了。

当然这个类比有许多不太恰当的地方，这种情况在现实世界中几乎不可能发生。一方面欧元的交易信息和人民币的交易信息根本就不同，另一方面有银行这个中心机构来结算，没有签字的刷卡交易还可能被追回，与去中心化的区块链世界差别很大，记住这只是一个类比而已。

现在来看比特币世界里的重放攻击，如图 12-2 所示，假设 8 月 1 日分叉前的币是 BTC，分叉之后，出来一种新币 BCH，原来的 BTC 旧链为了区分方便起个新名字叫 BTC1。

假设你总共有 5 个 BTC，8 月 1 日之后，你发起一笔交易，从钱包地址 A 向钱包地址 B 支付 1 个 BTC,这笔交易被确认的实际意思就是把这条交易打包进了区块链里，以前只有一条链，一切正常。

现在出来两条链了，你把交易信息写入了 BTC1 这条链上，但竟然有人把这条交易信息原封不动地发送到了 BCH 新链上，这条交易信息还是完全合法的，这样实际上你还支付了 1 个 B

CH!（不必担心，现实世界中的 BCH 交易不会被重放攻击，因为 BCH 的钱包中添加了防重放攻击的代码，你的 BTC 交易拿到 BCH 不会被承认，反之也不认）

12.2.2 攻击

攻击这个词有点夸大了，因为你本来只有 5 个 BTC，分叉后你仍持有这 5 个 BTC（或者换个新名字 BTC1），支付了 1 个 BTC，如果你不知道 BCH 的存在，本身啥也没损失，谈不上被攻击。

但现在问题不一样了，你学会了区块链基本原理，不再是一个小白，分叉之后，你竟然拥有了两种币，你的币被加倍(double)了。原来你只有 5 个 BTC，现在你有 5 个 BTC1 和 5 个 BCH。这里需要提醒一点，虽然你的币多了一倍，但交易所的行情可能会发生剧烈波动，这些币的市值可能并没有加倍，甚至还可能减少。

你现在明白了这 5 个 BTC1 和 5 个 BCH 原本都是自己的，现在**攻击**就成立了，我只想支付 1 个 BTC1，竟然有人偷偷地从我的钱包里还拿走了 1 个 BCH（重放 Replay），你的 BCH 币也减少了，你感觉被人**攻击**了，这才是**重放攻击**。

12.2.3 以太坊分叉回顾

历史上能够借鉴的真实案例就是**以太坊**（在第 3 篇里介绍以太坊）的分叉事件了。2016 年 7 月，众筹项目 TheDAO 的智能合约存在严重漏洞，被黑客攻击，偷走了大量以太币 ETH，以太坊区块链被迫进行硬分叉以挽回被盗者的损失。

以太坊核心开发者将被盗资金转移至新链（仍叫 ETH）地址中，原来的旧链暂时被人遗忘。没想到没过多久，当时最大的交易平台 Poloniex (简称 P 网)突然宣布，旧链的代币命名为 ETC（Ethereum Classic），开始上架交易。

这可把其它交易所弄了个措手不及，遭受了严重的重放攻击，比如云币网赔了 4 万枚 ETC，其它交易所分别是什么情况就需要自行搜索了，这个事件也从另外一个方面考验了交易平台的信誉。

2017 年 7 月，交易平台都有经验了，提前进行了 BCH 上线前的部署工作，分别发出了相应的声明。

12.3 如何应对分叉？

在 2017 年 7 月，bitcoin.org 网站上就发布了关于分叉事件的官方通知：https://bitcoin.org/en/alert/2017-07-12-potential-split

这件事情现在已经是过去式了，但将来仍有可能发生分叉，仍有借鉴意义。

在 8 月 1 日前 1、2 天内：

- ✧ 不要进行接收 BTC 的交易
- ✧ 如果发送 BTC 或者向交易所充值，可能在这段时间内会暂停服务
- ✧ 如果把币存在交易所，并且交易所不让你备份自己的私钥，则要警惕了，交易所可能会损失币，而损失全部由用户来承担。
- ✧ 此时价格会剧烈波动，如果你承受不住这种变化，请落袋为安。

（1）假如你的 BTC 放在交易平台

1a）如果平台承诺帮你自动申领一份 BCH，负责分叉期间的所有操作，并且你信任这个平台，则啥也不用管，静等着多出一种币。

1b）交易平台只给你一种币，则你要当心了，说明了这个平台的技术实力并不过关，是否卖出或取现就自己拿主意了。

（2）假如你的 BTC 放在自己的钱包中

这种情况下，你掌握了你的比特币私钥，也就是说你真正自己掌握了自己的钱。

2a）仍没看懂我上面写的文字，握住不动，什么也不做，等尘埃落定之后，再操作。

2b）不会自己操作，又非常信任某个交易平台，在 7 月 31 日之前充值进去。

2c）可以参考公众号“闪电 HSL”发过的一篇文章《安全地分离 BTC 和 BCC》，摘录如下：

- ✧ 分裂前，用钱包软件导出私钥
- ✧ 最好存一个只有 0.01BTC 的地址，用来测试
- ✧ 到 https://www.bitcoincash.org/ 下载 一个比特现金（BCH）钱包，将上述私钥导

入这个钱包。（这个步骤可以在分裂后做，也可以分裂前做。）

- ✧ 分裂后，到交易所买 0.011BTC 和 0.012BBC，都往你的地址上发
- ✧ 在两个钱包软件中同步区块，污染你的币
- ✧ 分别将你污染的币发到另一个你自己控制私钥的地址上
- ✧ 先用分裂前做好的 0.01BTC 的那个钱包来完成测试，然后再将你的大额钱包做分离

8 月 1 日分叉之后几天内，直到问题被解决，需要这样：

- ✧ 不要信任此时的 BTC 交易，不管有多少的确认次数，它可能都会从你的钱包中消失
- ✧ 不要进行发送 BTC 的交易
- ✧ 不要轻信一些人或机构能帮你把币一分为二，他们也能偷走你的币。

小结：

- ✧ 分叉并不可怕，还多了一种币
- ✧ 重放攻击就是一条链的交易数据重新广播到另一条链上
- ✧ 分叉期间，如果不会操作就握住不动，静等尘埃落定
- ✧ 自己掌握私钥的话，还能分离出一种币，随时可以领取，丢不了
- ✧ 分叉期间，有良心的交易所会配发给你另一种币

12.4 51%攻击（51% Attack）

任何事物没有绝对的安全，比特币的区块链也一样，最有名的一个安全性问题就是 51%攻击了。前面我们已经知道临时分叉很常见，也就是图 12-8 中左侧的情况。

图12-8 51%攻击示意图

假设某个超级矿工或矿池突然研发成功了一种超级芯片，可以快速完成 PoW 工作量证明，以前需要 10 分钟完成的工作量，它只需 2 分钟就可以搞定，当普通矿工正在长链 A 上进行计算时，它集中火力去延伸链 B，10 分钟之后，普通矿工可能在链 A 上延伸了一个块，然而超级矿工一口气挖出了 4 个块，如图 12-8 的右侧部分。

这个时候链 B 成为了全网中公认的最长链，如果超级矿工在链 B 中的区块中放入对自己有利的交易信息，则会对整个区块链形成攻击。而 51%是为了便于理解的数字，如果超级矿工拥有 51%的算力，也就是其它的所有矿工加在一起也比不过它，这时候超级矿工几乎就可以控制长链了，称为 51%攻击。实际上算力不到 50%，也会具有一定的威胁性。

我们来看一张矿池算力的实时分布图（图 12-9），在 11.2 节中介绍过算力的概念，当前世界上的总算力大概为 9211P，最大矿池 BTC.TOP 的算力占比为 19.6%，如果它能够联合另外两家大矿池（BTC.com 和 AntPool），就可以发起 51%攻击。

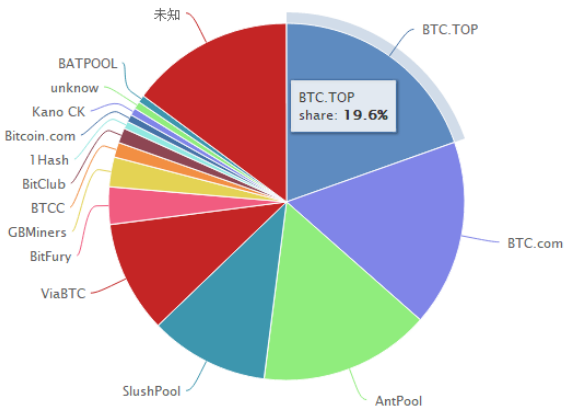


图12-9 全球矿池算力分布图(2018年2月20日)

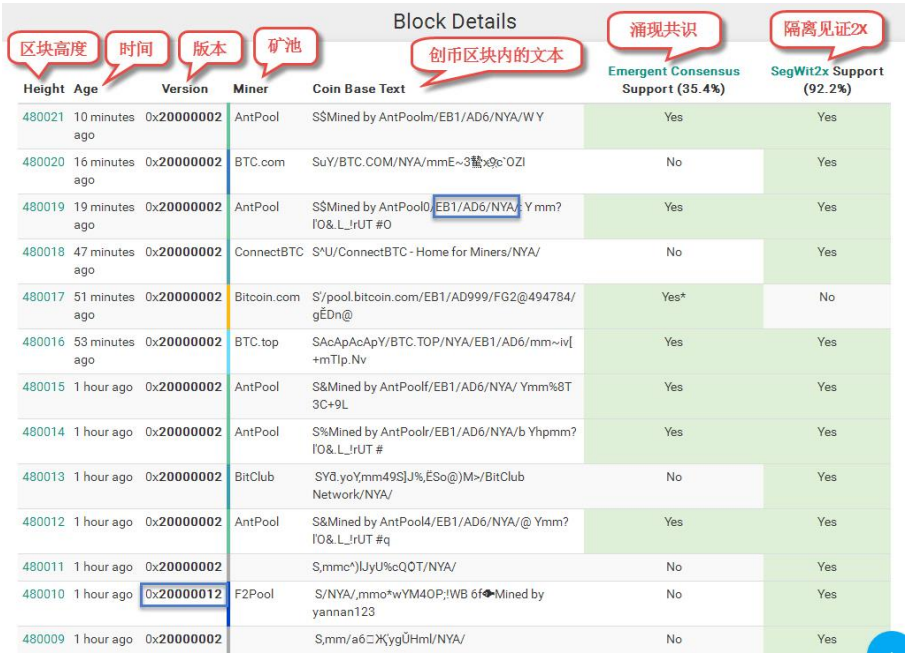
但这种攻击也是非常有限的，超级矿工不能篡改以前区块的数据（至多影响以前的几个块），也不能偷走别人的币，能做的就是双重支付或拒绝服务攻击，而这里又有一个经济学方面的考虑，矿池要消耗巨大的电量，电就是钱，费这么多钱去做损人不利己的事，还不如诚实地挖矿，收益也是相当可观的。历史上曾经有过矿池在算力太大时，主动降低算力来减轻大家对比特币安全性的担忧，来获得最大化的收益。

以比特币当前的算力分布来看，51%攻击的可能性非常小。你在评估其它币的安全性时，也要找到该币的算力分布图，如果算力分布太集中，就有一定的危险性，曾经 Namecoin（代币名 NMC）就有过算力集中的问题。

12.5 解密 Coin.Dance

在比特币分叉时期，关注区块链动向的网站有很多，CoinDance 网站(https://coin.dance)就是非常有名的一个，里面提供了包括市值、价格、节点、矿池、区块等多种指标的统计图表。但是这个网站中的各种数据太专业了，如果区块链中的基本概念不了解，普通人根本理解不了这些数据和曲线的含义。这里我们来一起去解读其中的一个区块信息表。

请在桌面浏览器里打开网址：https://coin.dance/blocks#blockDetails。请忽略页面上部的大量图表，以后再慢慢解释，直接翻到底部的这张“区块详细信息表”。



Height	Age	Version	Miner	Coin Base Text	Emergent Consensus Support (35.4%)	SegWit2x Support (92.2%)
480021	10 minutes ago	0x20000002	AntPool	S$Mined by AntPoolm/EB1/AD6/NYA/W Y	Yes	Yes
480020	16 minutes ago	0x20000002	BTC.com	SuY/BTC.COM/NYA/mmE~3鼙x9c`OZI	No	Yes
480019	19 minutes ago	0x20000002	AntPool	S$Mined by AntPool0/EB1/AD6/NYA/ Y mm? l'O&.L_!rUT #O	Yes	Yes
480018	47 minutes ago	0x20000002	ConnectBTC	S^U/ConnectBTC - Home for Miners/NYA/	No	Yes
480017	51 minutes ago	0x20000002	Bitcoin.com	S'/pool.bitcoin.com/EB1/AD999/FG2@494784/ gĚDn@	Yes*	No
480016	53 minutes ago	0x20000002	BTC.top	SAcApAcApY/BTC.TOP/NYA/EB1/AD6/mm~iv[+mTlp.Nv	Yes	Yes
480015	1 hour ago	0x20000002	AntPool	S&Mined by AntPoolf/EB1/AD6/NYA/ Ymm%8T 3C+9L	Yes	Yes
480014	1 hour ago	0x20000002	AntPool	S%Mined by AntPoolr/EB1/AD6/NYA/b Yhpmm? l'O&.L_!rUT #	Yes	Yes
480013	1 hour ago	0x20000002	BitClub	SYđ.yoY,mm49SJJ%,ESo@)M>/BitClub Network/NYA/	No	Yes
480012	1 hour ago	0x20000002	AntPool	S&Mined by AntPool4/EB1/AD6/NYA/@ Ymm? l'O&.L_!rUT #q	Yes	Yes
480011	1 hour ago	0x20000002		S,mmc^)IJyU%cQOT/NYA/	No	Yes
480010	1 hour ago	0x20000012	F2Pool	S/NYA/,mmo*wYM4OP;!WB 6f◆Mined by yannan123	No	Yes
480009	1 hour ago	0x20000002		S,mm/a6□Ж'ygŮHml/NYA/	No	Yes

图12-10 Coin.Dance 网站的区块详细信息表

第一列：区块高度

在第 2.3 节里介绍过**区块高度**，它是区块链里的一个最最基本的概念，代表着一页共享大账本的编号，我在写这篇文章时的最新区块高度为 480021。

第二列：产生时间

表示每个区块分别是在什么时间被挖出来的，比特币系统设定平均每 10 分钟会出来一个区块，从 2009 年的第一个创世区块开始，到现在已经产生了 48 万个区块了。

第三列：版本

这又是给程序员们看的一串数字，"0x"来源于 C 语言中的十六进制，0x20000002 代表 BIP141，0x20000010 代表 BIP91，而 0x20000012 则代表 BIP91 及 BIP141。程序员们需要理解其中的 bit1 和 bit4 的含义。

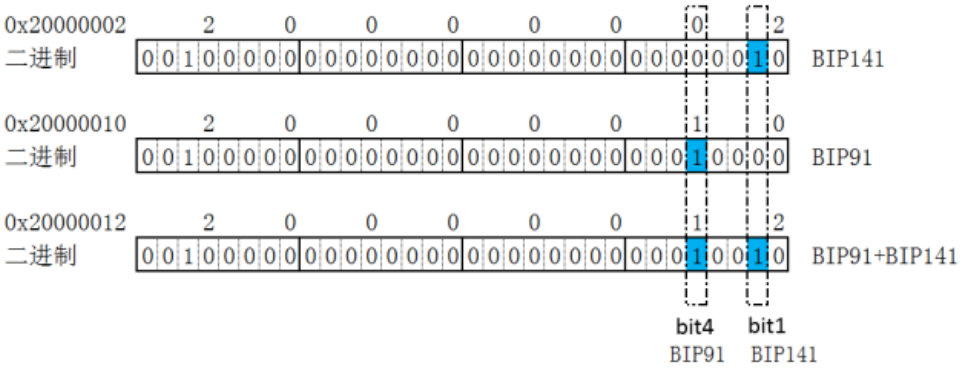


图12-11 新块中的版本信息

BIP 是在第 10.1 节里介绍过的**比特币改进提议**，BIP141 就是隔离见证 Segwit 方案，BIP91 就更复杂了，可以暂时理解为通往 Segwit2x 的一个积极信号吧。

第四列：Miner

矿工或矿池，在第 11.1 节里介绍过，从表中可以看出，大部分区块都被 AntPool、BitClub、Bitcoin.com、BitFury、Bixin 等这些大矿池挖走。

第五列：Coinbase Text

创币交易在第 10.5 节里介绍过，这里面可以写入一些不可篡改的文本。这里面还可以记录矿池的投票信息，需要注意的是“EB1/AD6/NYA”这些神奇的字符。

NYA 就是著名的**纽约共识**（New York Agreement）扩容方案，先实施隔离见证 Segwit，再扩容到 2MB。

EB 表示 Excessive Block Size，EB1 的意思是超过 1MB 的就算作大区块。

AD 表示 Excessive Accept Depth，与 EB 标识同时出现才有意义，AD6 的意思是：如果遇到大区块，一开始拒绝，但如果大量矿池都支持大区块，有 6 个大区块出现，那么我也认可该区块。图中的 480017 区块中的“EB1/AD999”就表示拒绝大于 1MB 的区块。

第六列：Emergent Consensus 涌现共识

最后两列最关键，是 CoinDance 给出的汇总信息。Emergent Consensus 这个名词在"闪电 XL"的文章里被翻译为“**涌现共识**”，是 Bitcoin Unlimited 提出的扩容方案，意思是让市场或矿池来决定区块的大小。

第七列：Segwit2x Support

支持先隔离见证(Segwit)，再扩容 2MB 的方案。

如果表中前面几列的信息看不懂，最重要的是能够看懂最后两列。从表中可以看出大多数矿池支持**纽约共识**(NYA)，有许多矿池脚踩两支船，大区块和隔离见证都支持。而 Bitcoin.com 在 480017 区块的态度最诡异，好像没准备扩容。

12.6 软分叉

《区块链生存训练》的系列文章最早分享于 2017 年 5 月 23 日的饭团中，三个多月共完成了 66 篇文章，我模仿区块链的区块高度的思路，给每篇文章也弄了一个编号，这样就有了块 0、块 1、……直到“块 66”。

写这些小块块文章通常要参考好几本权威书籍，消化到自己的肚子里，然后再搜索一堆网文，寻找恰当的类比，用自己的话表达出来，憋出一篇文章经常需要几个小时。然而最近要搞一件大事，写文章的精力慢慢有点不济，就寻找了几位区块链自媒体的朋友共同创作，当然内容仍要经过互相审核，绝对保证质量。

我啰嗦了这么多，与**软分叉**有什么关系？现在进入类比的正题。

假设“块 67”将由黄黎执笔完成，那么我的饭团将迎来一个软分叉的历史时刻。虽然呈现在大家面前的仍然是一篇一篇的小文章，但是作者将不是我一个人，而变成一个团队、一个集体。

图12-12 软分叉示意图

12.6.1 软分叉其实并没有分叉

上面类比的意思就是，虽然每个块的作者发生了变化，但整个创作团队仍是共同维护一系列的文章，实际上并没有分叉。

在比特币里也是这样，软分叉只是区块的版本或协议发生了变化，但所有的区块仍在一条区块链上，实际上并没有分叉。

12.6.2 新区块欺骗旧软件

文章的作者发生了一点变化对于系统可能影响并不大，但“饭团 APP”是有多个版本的。假设饭团 1.0 版本的程序员考虑不全，只允许阅读申龙斌团长的文章，其它嘉宾的文章虽然不报错，但却无法正常阅读。为此，饭团发布了 2.0 版本，修正了上述问题，所有文章都可以正常打开并阅读。

现在回到区块链的世界，用户进行比特币交易会安装不同版本的钱包软件，有人安装了 0.8.1 的旧版本软件，它知道有新区块 67 产生了，钱包软件不报错，但它并不理解区块 67 的内容，即使里面有几笔交易与他有关，他也一无所知，这时他的钱包软件中的余额信息很可能是错误的。

有人则安装了最新的 0.14.1 版本的钱包软件，所有区块（旧区块、新区块）的信息都可以正常解读，软件运行完美。

从这一点上来看，新区块实际上在欺骗旧版本的钱包软件，旧版本钱包软件不给用户任何警告或错误信息，看上去一切正常，但交易信息、余额信息可能是不完整，甚至是错误的。

12.6.3 协议升级的无奈之举

我的饭团引入更多的人共同创作，创作人有点变化，但“为大家带来价值”的共识是不变的。

比特币协议从 2009 年诞生，期间也发生了很多次变化，钱包软件要升级，但全世界的用户太多了，使用的钱包版本都不相同，不可能商量好一起升级。软件开发人员也不能让钱包软件崩溃，影响用户的使用。关键的是不能影响矿工的挖矿，那可是真金白银的苦力。

所以这些升级大多通过软分叉方案来渐进实施，区块链仍是一条，旧块与新块有所不同，而且一直共存，大家的共识是一样的：让比特币交易顺利进行。

现在我们再来看看**软分叉**的学术定义，你能看懂吗？请对应我给出的类比仔细理解这段定义。

> 软分叉是指比特币交易的数据结构（这就是被广泛流传的“共识”）发生改变时，未升级的节点可以验证已经升级的节点生产出的区块，而且已经升级的节点也可以验证未升级的节点生产出的区块。

小结：

- ✧ 软分叉其实并没有分叉，还是一条链
- ✧ 新区块欺骗旧钱包软件，让旧钱包软件承认新区块，但并不知道新块中的内容
- ✧ 软分叉是为了协议的升级，共识没有大的变化

12.7 分叉币 BCH

2017 年 8 月 1 日，比特币分叉出来了 Bitcoin Cash（现在简称 BCH，以前曾经叫 BCC），11 月 15 日，比特币为了扩容可能又要分叉，有些人感觉 Core 团队把事情搞得太复杂了，转而看好 BCH，结果 BCH 的价格飞涨，已经超过 3800 元，历史上曾高达 2 万元人民币。

图12-13 BCH 价格曲线图（2017年8月至2018年2月）

Bitcoin Cash 钱包冲突的解决办法

保管 Bitcoin Cash 的钱包软件叫 Bitcoin ABC，它是在 Bitcoin Core 的源代码基础上修改而成的，两个软件的界面完全一致。不仅模样相同，两个软件保存公开大账本（区块链数据）的文件夹也默认相同，有些朋友同时安装了 Bitcoin Core 和 Bitcoin ABC 两款软件，结果互相打架，造成了区块链同步功能的混乱。

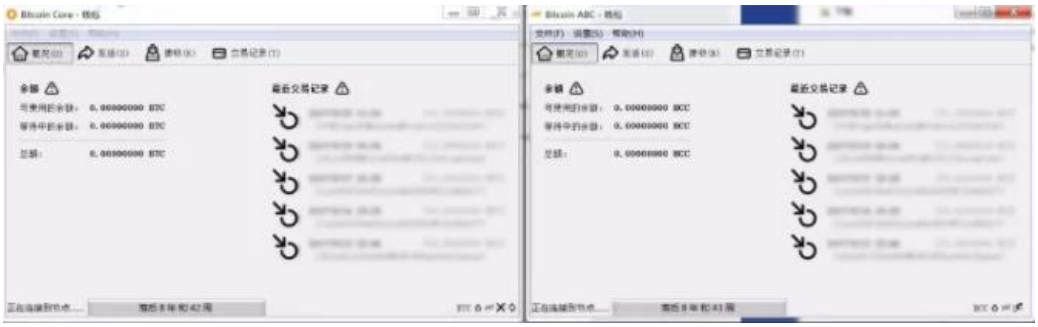


图12-14 Bitcoin Core 与 Bitcoin ABC 同步混乱

最简单的一种解决办法是安装一个VirtualBox虚拟机，将Bitcoin Cash安装在里面即可。想让 Bitcoin Core 与 Bitcoin ABC 在同一台机器里和平共处，需要如下操作：

（1）按 1.3 节中介绍的区块数据搬家的办法三，给 Core 钱包建立一个桌面快捷方式：

```
E:\bitcoin-0.15.0.1\bin\bitcoin-qt.exe  -datadir=e:/core-data
```

（2）对于 Bitcoin ABC 软件，重复类似的步骤，把区块数据放在 bcc-data 文件夹下，命令行是这样的：

```
E:\bitcoin-abc-0.15.1\bin\bitcoin-qt.exe  -datadir=e:/bcc-data
```

最后两个软件都有各自的程序目录和数据目录，以后启动程序时记着点击桌面上的两个快捷方式分别启动即可。

图12-15 两款钱包的不同文件夹设置

13 进阶概念

13.1 非对称加密(Asymmetric Cryptography)

很多人在看《精通比特币》中的加密原理那一部分时，内心可能是崩溃的，那些密码学的原理和内部细节，实在是太烧脑了。对于大多数不想成为密码学专家的朋友来说，能够了解“**非对称加密**”这个术语的基本原理和用途就够了，更多的细节可以忽略。

想理解“**非对称加密**”，就必须得了解“**对称加密**”，先来一个例子：我把饭团里的第二期内容汇总为一个 PDF（下载链接），并设置了一个密码：142857，这就是我们经常遇到的加密技术，所谓**对称加密**，就是加密和解密都是用一个密码（一套规则）。现在麻烦来了，我必须把这个密码告诉饭团会员们，否则大家无法打开 PDF，但是天下没有不透风的墙，密码可能会被泄漏给更多的人，用这套密码加密过的文件都没有秘密可言了。

再来一个例子：你的电脑中了比特币勒索病毒，有估值 1 亿元的一批文件被加密存储了，无法打开，需要支付 300 BTC 才能从黑客那里拿到密码，你估算了一下，600 多万的赎金比 1 亿还是便宜不少，看来赎金还是得交。这里用到的加密肯定也是**对称加密**，即黑客加密的密码与你解密的密码是一样的。

举一个比特币中的例子，在第 1.5 节里让大家把 Bitcoin Core 里的 wallet.dat 进行加密，这里用的是 AES(Advanced Encryption Standard)加密技术，这个 AES 就是一种对称加密算法，别人拿走你的 wallet.dat 文件，必须用你设置的密码才能解开。

非对称加密则是加密的密码与解密的密码不是一样的，这有什么用呢？其它方面的例子

不说了，主要就说比特币里面的例子。我们收款的比特币地址本质上是一个公开的密码，称为公钥(Public Key)，别人给你付款时，拿这个公钥就可以生成交易记录，而这笔钱只有你的私钥(Private Key)才能打开。

另外在 9.7 节里介绍数字签名时，你用私钥加密的消息，别人用公钥（比特币地址）就可以验证，从而可以证明你真正拥有那个比特币地址。

这里再简单谈一下**非对称加密**的原理，不感兴趣的可以自行忽略后面的内容，主要都是用到一些不可逆的、非常难的数学问题。在非对称加密算法中，主要有这两种典型的代表：

- ✧ RSA 算法
- ✧ 椭圆曲线算法

比如：RSA 算法用到大素数分解，比如给你一个**公钥**：769346501175973283，知道它可以分解为两个素数的乘积，解这种题没有好办法，只能一个一个地试，最后发现是 817508477 和 941086879 这两数，你可以拿其中的一个数当私钥。注意这里只是个简化的例子，内部的公钥、私钥生成规则还很复杂，当素数达到几百位时，计算机也难以分解这个大数。

比特币里使用了**椭圆曲线加密算法**，简单来讲，它是一个方程，在平面中呈现为曲线状，同样，它也是一个数学问题，单向计算很容易，逆向计算却极其困难，椭圆曲线算法太复杂，一时半会真心看不懂……你要知道的关键是它比 RSA 还难破解，无法用公钥（比特币地址）算出私钥，但用私钥得到公钥则不费吹灰之力。

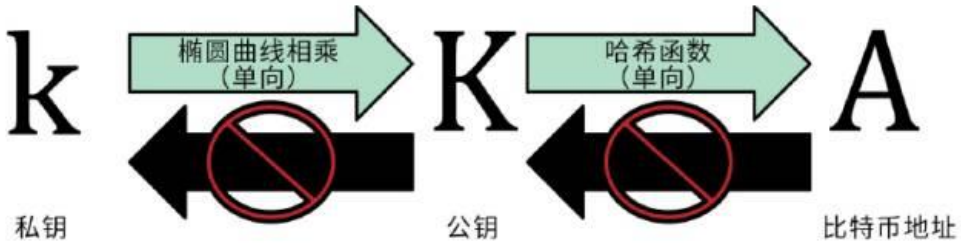


图13-1 私钥生成比特币地址非常容易，反之再不行，摘自《精通比特币》

13.2 Merkle Tree 与 SPV

Merkle tree（默克尔树）是一种数据结构，通常是一个二叉树（也有可能是多叉树），它以特定的方式逐层向上计算，直到顶部。Merkle tree 最为常见和最简单的形成是二叉默克

尔树。知道默克尔树的基本原理也有助于理解轻钱包的概念。

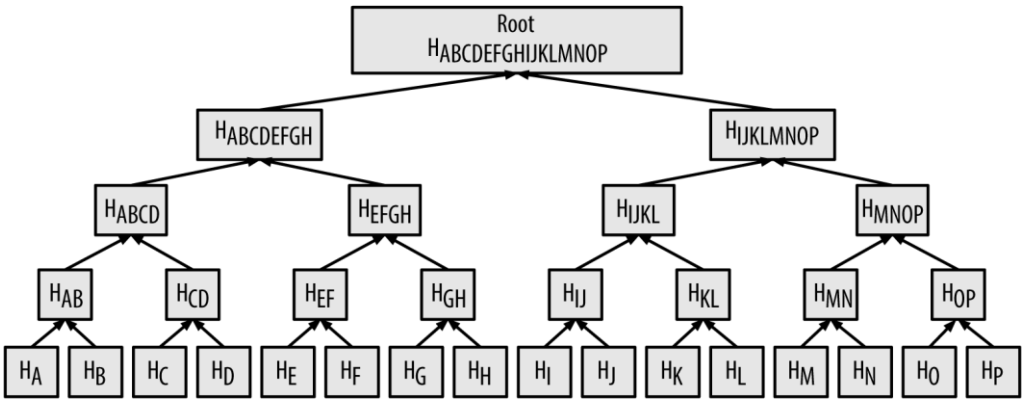


图13-2 默克尔树

在比特币的设计里，也使用了 Merkle tree 的数据结构，只不过里面存放的数据内容都是哈希值(HASH)。

哈希算法是一种摘要算法，你给它输入一个任意长的数据 A，经过 HASH 运算后，它返回给你固定长度的数据 B，也称 B 为“**数据指纹**”。这种哈希算法理论上是不可逆的，所以构成了加密数字货币设计的基础。

比特币的每一笔交易，都有一个交易 ID，是一串很长的数字，如 T1、T2、T3.....。

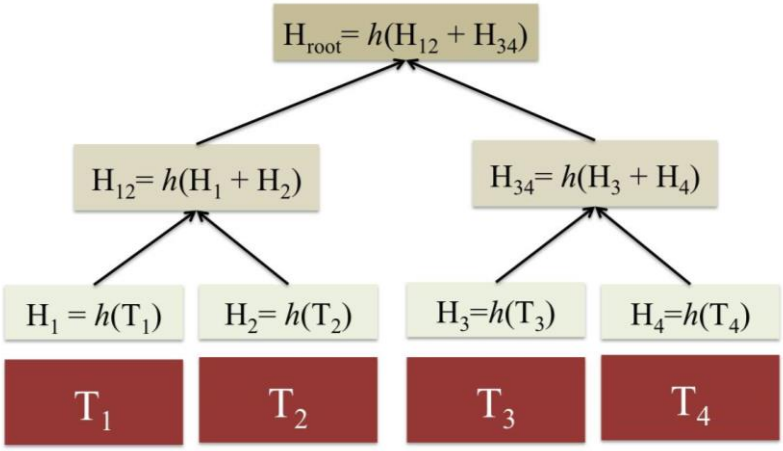


图13-3 对每一层交易 ID 进行哈希运算

每个 transaction ID 进行哈希运算，生成一个哈希值 H1，H2，H3 等。然后相邻的两个哈希值相加之后，再进行哈希计算，形成它的父节点，以次类推，一直到根节点，形成**默克尔树**。

根节点的哈希值就是比特币单独一个区块的哈希值。比特币的每一个区块都可以通过其区块头的“前一个区块的哈希值”字段引用前一区块，形成一个区块链条。Merkle tree 的根哈希值则可以确保区块中所有交易的真实性。

如果恰巧交易 ID 的总共数量为奇数个呢？那么排在最后的这个交易 ID 就 copy 自己一份，凑成偶数。

在比特币的设计里，有一点非常重要，一定要把所有的交易（transaction）按顺序排列下来，通过时间戳的功能就可以做到，如果顺序有误，那根哈希的结果就会大相径庭。

比特币的 Merkle tree 只存哈希值，没有任何实质的内容，实质的内容存在尾部的每笔交易里。

比特币为什么要用 Merkle tree 呢？

因为比特币有一个 SPV 功能，即：**Simple Payment Verification（简单支付验证）**。比特币的 Merkle tree 就是用来支持 SPV 功能。

SPV client 是个轻量级的客户端，SPV Client 只会下载所有的区块的头部信息，而不会下载交易部分，所以整个 client 下载比较快。

这里的头部信息仅包含 5 项内容，数据块大小为 80 字节：

- ✧ 上一区块头的哈希值
- ✧ 时间戳
- ✧ 挖矿难度值
- ✧ 工作量证明随机数（nonce）
- ✧ 包含该区块交易的梅克尔树的根哈希

SPV 的目标是为了验证某个支付是否真实存在，并得到多少个确认。比如我向你转了一笔比特币，我告诉你我已经转了，那你如何验证这笔支付的真实性呢？

支付验证的过程很简单，只是判断这笔支付交易是否得到了区块链节点共识验证，并得到了多少的确认数即可。

（1）首先计算待验证支付的交易哈希值。

（2）节点从区块链网络上获取并存储最长链的所有区块到本地。

（3）节点从区块链获取待验证支付对应的 Merkle tree 哈希认证路径。

（4）根据认证路径，计算 Merkle tree 的根哈希值，将计算结果与本地区块头中的 Merkle tree 的根哈希值相比较。

（5）如果一致则说明支付真实有效。

（6）根据区块头所处的位置，确定该支付已经得到的确认数量。

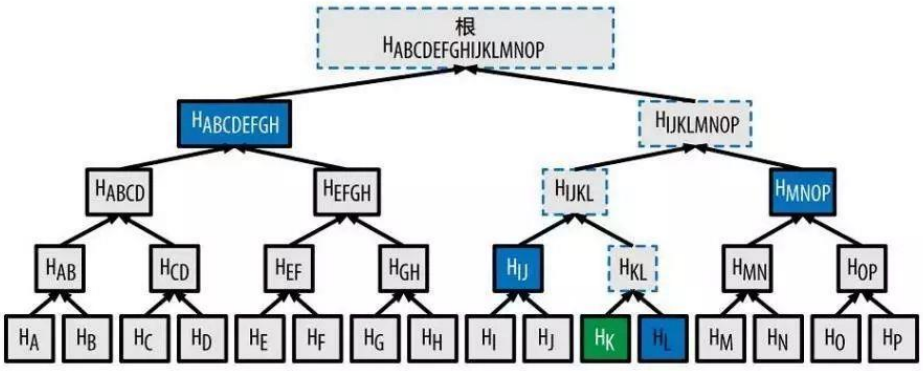


图13-4 默克尔树的验证过程

第 3 步中，假设你的交易是 HK，则计算根哈希值的办法是找到 HL、HIJ、HMNOP 和 HABCDEFGH，这里有一种专门的遍历算法可以得到。

总的来说，Merkle tree 在区块链的应用实现了**简单快速验证**的功能。

13.3 侧链（Sidechains）

现在已经出来了上千种币，在 http://coinmarketcap.com/all/views/all/ 可以查看各种币的行情，这还不包括无数已经死掉了没有留下名字的币。

All CryptoCurrencies

All ▾ Currencies ▾ Assets ▾ USD ▾ ← Back to Top 100

#	Name	Symbol	Market Cap	Price	Circulating Supply	Volume (24h)	% 1h	% 24h	% 7d
1	Bitcoin	BTC	$76,050,977,209	$4599.62	16,534,187	$1,914,620,000	0.23%	0.00%	10.66%
2	Ethereum	ETH	$35,630,747,306	$377.68	94,340,352	$1,305,200,000	-0.07%	1.32%	18.51%
3	Bitcoin Cash	BCH	$9,549,285,571	$576.88	16,553,188	$440,881,000	-0.64%	5.60%	-13.32%
4	Ripple	XRP	$8,715,363,541	$0.227295	38,343,841,883 *	$187,269,000	-0.52%	2.88%	-9.13%
5	Litecoin	LTC	$3,441,839,532	$65.30	52,711,257	$312,190,000	0.87%	3.66%	25.75%
6	Dash	DASH	$2,788,741,440	$370.64	7,524,023	$45,738,400	0.45%	2.86%	26.49%
7	NEM	XEM	$2,685,015,000	$0.298335	8,999,999,999 *	$9,632,320	0.34%	4.93%	18.05%
8	IOTA	MIOTA	$2,486,092,491	$0.894429	2,779,530,283 *	$17,413,300	1.56%	10.51%	5.59%
9	Monero	XMR	$1,995,731,193	$132.93	15,013,174	$111,350,000	-0.71%	0.58%	47.98%

图13-5 查看数字货币市值的网站

比特币核心开发组想通过**侧链**这种方案把链与链打通，难度之大可想而知。各种币现在自由竞争，确实解决了比特币当前问题的币才会留下来，比如以太坊。将来可能并不是侧链一统天下，可能是某一种链的出现，通过高层的智能合约来把所有的链全部打通。

也有可能世界上本来就该有大量的币种、大量的区块链，就像每个国家都有不同的货币一样，自由竞争是最公平的，市场会决定各种币之间的兑换率，从这个逻辑推断，交易所的营业额未来将会翻好几倍。

最近听说 drivechains 的技术方案比侧链方案更好一些，观望其发展。

13.4 闪电网络

扩容问题拖了好几年，2017 年终于开始实施**隔离见证** SegWit 方案，因为 2017 年初的区块已经到达 1MB 的限制了，扩容这件事真的是没办法再拖下去了。不过 2017 年 11 月，SegWit2X 失败，看来扩容这件事还得继续拖下去。

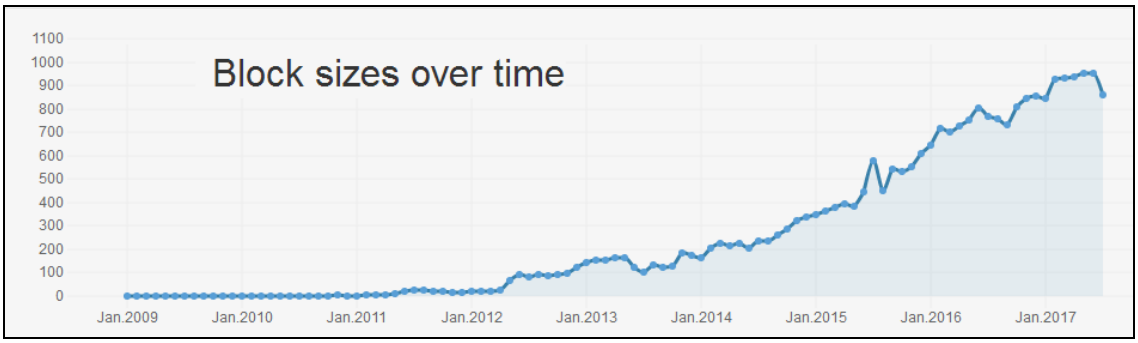


图13-6 区块链交易增多，逼近1MB的区块容量限制

在《区块链----从数字货币到信用社会》的 96 页出现了扩容之争的一堆**比特币改进提议**(BIP)，但该书中所列的那些 BIP 已经不是问题了，前一阵子让大家担心的用户激活软分叉（UASF，即 BIP148）没有搞成，杀出来一个 BCH，BIP91 在 2017 年 7 月成功锁定，BIP141 就是隔离见证方案也被锁定，曾经全网 94%的矿工支持 SegWit2x 方案，但 2017 年 11 月 SegWit2x 仍然流产，图 13-7 是当时 coin.dance 网站上的实时投票情况。

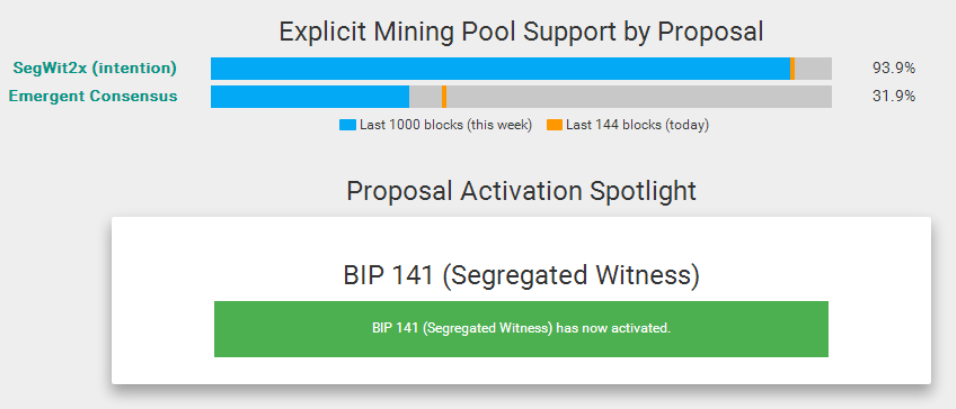
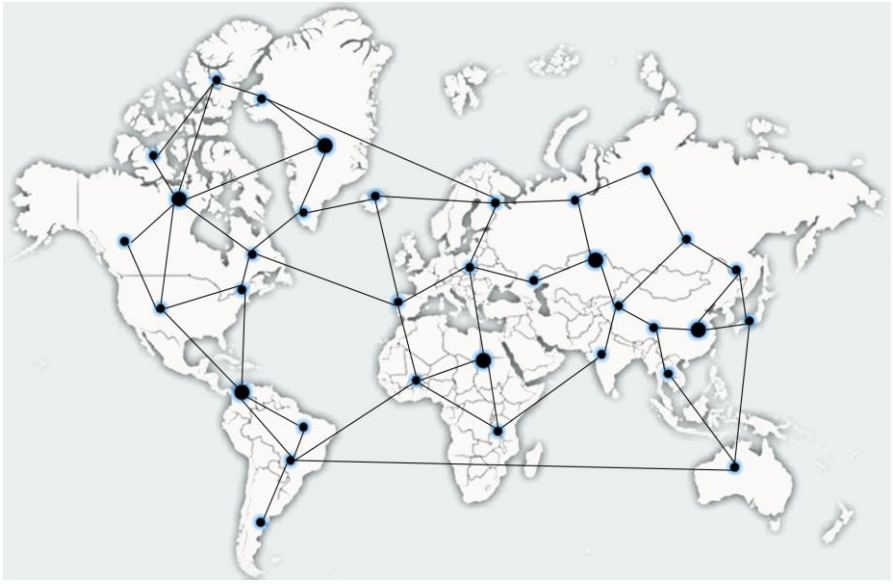


图13-7 BIP141投票进度

想实现每秒百万级交易数的量级，看来还得与中心化的方案相结合，所以**闪电网络**的具体技术细节可以暂时不用了解，对于普通用户来说，仍是等待与观望。BM 大神说他的 EOS 只使用 DPOS 共识机制就可以实现百万级交易量，以太坊的创始人也要推出一个方案，BTC、ETH、EOS 正在上演一场大戏，有胆量的投资人可以重仓这三种币，谁赢了都不怕。

第三篇 智能合约与以太坊



14 以太坊

比特币第一次实现了在不信任的网络中实现可信的价值传递,区块的内部是用一段数字签名的代码来实现的，为了安全起见，这段代码的功能非常有限，进行币的转移完全没有问题，但要实现一些复杂的逻辑就非常困难了，也就是说用比特币实现智能合约非常困难。

以太坊相当于一个造币的工厂，可以轻松地修改几个参数，就实现一种数字货币(token)，其内部的程序代码功能更为强大，让智能合约成为了可能。如果比特币是区块链 1.0 时代，以太坊的出现算是区块链 2.0 时代。

14.1 智能合约(Smart Contract)

智能合约这个概念早在 1993 年就提出来了，可惜由于那时的互联网和技术水平，无法落地。合约(Contract)这个词比较好理解，可以理解为合同，利益双方签订的协议。“智能”这个词就用得太滥了，智能电视、智能手机、智能油田等等，都没有统一的定义，好像是“先进”的代名词。把“智能”两个字用在“合约”上，可以简单地理解为让合同在约定条件下能够自动执行。

先举个例子：假设现在是 2017 年 7 月 1 日，1 BTC 价格大约为 2.8 万元，李笑来与罗振宇打赌，在 2017 年 8 月份的 BTC 价格一定会超过 3 万，如果没过 3 万，笑来给罗胖 100BTC；如果超过 3 万，罗胖给笑来 100BTC（据说罗胖在 2016 年买了 100 BTC 给女儿当嫁妆）。注意这是我编的一个小故事，仅为了加深对智能合约的理解。

这件事很简单，用传统的手段，双方需要签一份书面合同，一式两份，签字后各自收好。如果只是口头协议，则需要找个第三方当见证人，因为增加了中间环节，还需要修改合同，从赌注里拿出 1 个 BTC 给公证人。到了 8 月 31 日 24:00，大家聚在一起，查一下 BTC 的实时行情后立马见分晓，输家马上转帐，合同执行完毕。

现实世界里，这只是一个小合同，真正的合同涉及订立、履行、变更、终止等多个步骤，如果引入第三方，还有审查、监督等事务。假设币安网价格过 3 万，而 OKcoin 不到 3 万，又产生了新的分歧；假设一方拒不付钱呢？假设大家把钱都押在第三方，第三方跑路了呢？类似的细节非常非常多。

而把上面的例子放在区块链世界里，就好办了。把上面的合约写成一段程序代码，放在区

块链里，双方进行数字签名，各把 100BTC 锁定在区块链上，合约开始生效。8 月 31 日 24:00，程序自动抓取行情数据，超过 3 万，罗胖的 100BTC 立刻转到笑来的比特币地址中，反之亦然。整个过程不需要第三方，那段程序可以算做第三方。

从这个例子中，可以看出，智能合约相当于把合同编写成了程序代码，签订后由于区块链的数字签名、不可篡改性等特点，谁也不能抵赖，并且自动根据双方的履行情况强制执行。

人们普遍认为比特币算是区块链 1.0，智能合约则是区块链 2.0 时代。1.0 时代解决了不信任网络中的价值可信传递，2.0 则让双方（或多方）的价值转移完全程序化、自动化了。

区块链的出现让 1993 年提出的智能合约概念落地，比特币系统内部是用程序代码来锁定、解锁 BTC 的，只不过功能太弱。而**以太坊**则是第一个可以运行智能合约的区块链平台，你设立一堆规则（表现为一组 IF...THEN...的程序代码）就可以发行一种**代币**(Token)，发行 ICO 的门槛变得相当低。智能合约的签订、执行都要消耗数字货币(Coin)，想活在未来，是不是需要持有一些筹码？

14.2 代币(Token)

在区块链技术文档中，尤其是曾经火热的 ICO 中，大家经常看到 token 这个单词，有些地方 token 被翻译为“代币”，在有些钱包软件中被翻译为“令牌”，给大家造成了困惑。

中本聪发明的比特币系统中流通的数字货币是比特币（代码为 BTC），而**以太坊**进行了更高层的抽象，实现了智能合约，可以轻松地发行一种的新的数字货币，这种数字货币就叫 token，所以说翻译为“代币”应该是准确的。

为什么有翻译成“令牌”的？因为在 1970 年代，IBM 发明过一种环状网络 Token-ring network，中文名称叫令牌环网（图 14-1）。这种网络结构中的机器连成一个环形，网络中存在一个令牌 token，一个一个顺序向下传，持有令牌的主机才能向网络中发数据，该技术早已过时，几乎绝迹，被星型网络所取代。令牌给人一种独占性的感觉，带兵打仗的令牌只有将军才能持有，所以翻译成“令牌”很不准确。

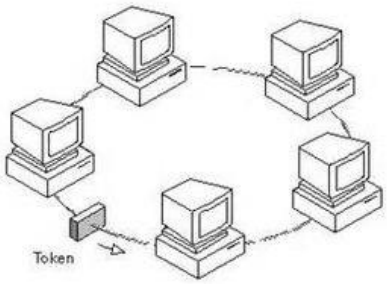


图14-1 令牌环网的示意图，来自于百度百科

Token 这个词在赌场或游戏厅里翻译为“筹码”，有不同的面额，实际上也是代币的意思。在各种 ICO 中，就是想要入手各种 token，期待它涨价。但 token 是否有长久的价值？还得看 token 能够用来做什么。比如：SC 可以使用存储服务，REP 可以参与预测服务，ZEC 可以实现匿名转账，Steem 可以实现社交应用，有真正应用场景的 token 才会体现它的价值。

14.3 ERC-20

在一些钱包或交易所中经常会出现 ERC-20 这样的术语，让一些初学者非常困惑。

你首先需要知道这个该死的ERC是什么东西的缩写？原来ERC是 Ethereum Request for Comments 的缩写，表示以太坊社区的成员对于一些规范或建议提出修改意见（比特币里叫 BIP），20 是建议的编号，ERC-20 就是这样来的，能看懂英文的可以直接到这里：https://github.com/ethereum/EIPs/issues/20。

代币(Token)在以太坊的区块链里是一种数字资产，这些代币可以使用以太坊里的智能合约。我们可以称 BTC 是比特币系统里的代币，没有以太坊的时候，你想发行一种新的代币，其复杂程度超乎想象，这种事情几乎是不可能的。但以太坊在 2015 年 11 月推出了 ERC-20 标准，使发行代币的门槛降低了许多。

虽然 ERC-20 只是规定了代币该如何运行，并不包含代码，但网上可以找到免费的、现成的源代码，稍有编程经验的人抄抄改改就可以创建出一种 ERC-20 标准的代币。现在的 ICO 乱局也就是这么来的。

ERC-20 定义了六种函数，包括如何传递一个代币(由所有者或代表所有者)以及如何访问代币的数据(名称、符号、供应、余额)，还提供了两种信号。这个规范给软件开发者和用户都提供了方便，只要以太坊钱包支持 ether，几乎就可以支持 ERC-20 规范的各种代币。

常用的与代币有关的函数：

* 获得代币总供应量

* 获得账户余额

* 转让代币

* 批准花费代币

本书的前言部分留的以太坊捐赠地址也符合 ERC20 规范,如果本书对您提供了非常大的帮助，欢迎捐助，我们将持续改善本书。

0xB4fd52AA5DB2820dC183aCa9ea8ff030a5F92D5E

15 权益证明(PoS)

首先注意这个 PoS 与您刷银联卡时见到的 POS 机没有半毛钱关系。如果您没看过工作量证明 PoW，建议您翻到第 6.3 节再复习一遍。这里把 PoW 的主要作用简要重复一遍，为了验证用户的交易数据，并防止大量节点在网络上乱发无用信息，让矿工们去解决一个非常非常麻烦的计算题，大概 10 分钟能够算出来，哪个矿工先完成，它就可以拥有记账权，在公开大账本上写入一个新块，并拿走新块奖励和这里面的交易手续费。

PoW 这种机制从 2009 年 1 月开始已经运行了 8 年多，经过了实践的检验，唯一被指责的一点是浪费巨大的电力。环保人士们不干了，说矿池耗费巨大的电力，就为了共同维护那 100 多 GB 的数据，因此就出现了许多替代方案。2011 年 Quantum Mechanic 提出了 PoS（Proof of Stake，权益证明）算法，2012 年首次应用于 Peercoin（点点币，币代码 PPC，2018 年 2 月的价格是 19.3 元人民币，说明 PoS 也可行）。

一句话来描述 PoS 的特点，就是有钱人说了算，你拥有的币越多，责任越大，就有更多的机会写入新块。Stake 在这里被翻译为权益，与股份 share 的意思相近，拥有某种币的人相当于拥有了这种币的股份，为了收益最大化，股份越多越想维护币的安全与稳定。

当前采用 PoS 的主要有：Peercoin、Nxt、BlackCoin、Lisk、ShadowCash、NuShares/NuBits、Qora,、NavCoin 等，以太坊也准备转换成 PoS（CASPER 协议），但还没有实施，这也是有争议的地方。

以元老 Peercoin 为例，它引入了币龄(coin age)的概念，等于币数×持币的天数（大于 30 天才算），币龄越大，越有可能获得写入新块的权利，写入之后，币龄重新从 0 开始计算。这只是最原始的算法，后来还有许多改进的算法，甚至还有 PoS 与 PoW 相结合的算法。

在 PoW 中，矿工可能一个币也没有，也可以参与挖矿。但在 PoS 机制下，造币者本身就拥有大量的币，所以他们会维护币的安全，没有币就没有游戏资格。

在 PoS 中，所有的币一开始就铸造好了，总币数不变（当然也有例外），原始版本的 PoS 是没有新块奖励的，只能拿交易费。因为没有可挖的，PoS 中的写入新块者通常不叫矿工 Miner，而叫 Forger(造币者/铸造者)。

PoS 因为不消耗能源，代价太低，所以理论上矿工可以随便分叉，因为什么也不损失。为了防止乱分叉，PoS 中又设计了一些惩罚措施，配合智能合约机制，可以提前交保证金，谁违约就扣保证金，并取消它的资格。

表 15-1 PoW 与 PoS 的特点对比表

	PoW 工作量证明	PoS 权益证明
共同点	用来决定谁能写入新区块的算法	
发明时间	比特币之前就有	2011 年提出，2012 年实现
币	BTC 等	Peercoin, Nxt, BlackCoin, Lisk，ShadowCash, NuShares/NuBits，Qora, NavCoin
写入新块	算力+运气	谁的币多，谁的概率大
能源	非常费电	可以忽略不计
新块奖励	50 开始，4 年减半	通常为 0
交易费	2140 年之后全是交易费	矿工主要靠交易费
挖矿者	矿工 Miner，可能没有 1 个币	铸币者 Forger，没币别玩
算法	HASH、SHA256	币龄
分叉	不容易，因为代价太大	经常，因为几乎没成本

	PoW 工作量证明	PoS 权益证明
惩罚	无	交保证金，不按规则，罚
攻击	51%攻击	币龄攻击(Save-up Attack) 权益粉碎攻击 （nothing-at-the-stake attack）

参考阅读：

https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/

16 去中心化应用(DApp)

DApp 是去中心化应用（Decentralized application）的缩写。在第 3.4 节中介绍了中心化和去中心化的概念，现在各种常见的网络程序的后台都有一台或多台的中心服务器，比如微信 App，在它的后台有腾讯公司的多台服务器提供数据和其它服务，当腾讯公司的机房发生严重故障时，微信 APP 肯定会受到影响。

而 DApp 程序运行于去中心化的点对点网络环境下，在比特币和区块链没出现的时候，这种 DApp 程序已经出现了，比如我们熟悉的 BT 下载程序（BitTorrent），你给它一个下载的种子文件，它会自动寻找网络上的其它节点，如果在线的 BitTorrent 程序越多，你的下载速度也就越快。那个时候的 DApp 与数字货币没有关系。

随着区块链和智能合约的出现，现在 DApp 与数字货币、交易发生了密切关联，产生了更广阔的应用前景，我们的全节点钱包软件实际上就是一款 DApp，它没有中心服务器，只要网络不断，谁也杀不死它。类似的软件还有 Popcorn Time，BitMessage，Tor 和 Maidsafe 等。

Popcorn Time 是款相当邪恶的软件，有了它，各种最新的电影、剧集可以边下载边观看。

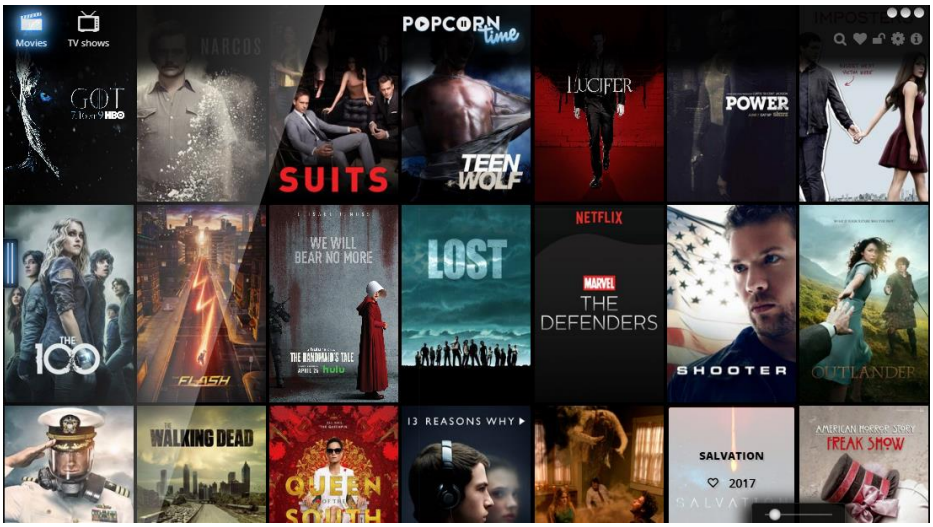


图16-1 去中心化应用 Popcorn Time

Bitmessage 是一个去中心化的通讯软件，他能允许你在匿名的情况下传输任何信息给接收者或者从一个发布者那里订阅信息。这一切都是建立在 P2P 网络上的，也就说没有一个中心服务器可以控制和窥探使用者的行为。

Maidsafe 更是一个庞大的工程，要实现一个去中心化的互联网，它有这些特性：第三方保存你的密码；数据加密存储，别人无法窥探你的数据；去中心化的网络中；数据存储的高可靠性等。Maidsafe 本身还是一个平台，可以开发其它的 DApp。它的代币叫 Safecoin，还有一种币叫 MaidSafeCoin，MaidSafecoin 是写在比特币块链上的媒介标注，将在 SAFE 网络里的一个 P2P 网络平台，按照 1：1 与原生货币 safecoin 进行兑换 。

参考阅读：

https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/

http://www.8btc.com/bitmessage

http://www.8btc.com/maidsafe-makes-data-safe

https://maidsafe.net/features.html

http://www.8btc.com/3005574

17 用 MyEtherWallet 钱包参与 ICO

如果用 ICO 平台没有抢到币的话，还可以用钱包自己参加 ICO，2017 年 9 月国内禁止了 ICO，你如果发现了好项目，只能用这种办法直投 ICO 了。

第一步：如果以前没有 ETH 钱包，登录 MyEtherWallet 网站，生成一个新钱包。设置一个密码，生成钱包。

图17-1 MyEtherWallet 生成钱包

第二步：保存 Keystore 文件，放在一个安全的地方，坚决不能让别人看到，也可放在 KePass 工具统一保管。

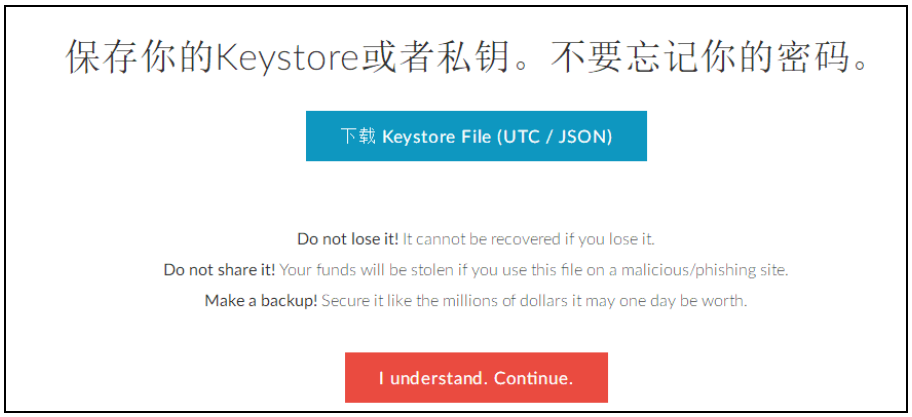


图17-2 下载 keystore

第三步：保存私钥。第二步、第三步选择其中一种方式就行，保存好，坚决不能让别人看到。还不放心？打印纸钱包，生成 PDF 文件，**同样保存好，别让人看见**。

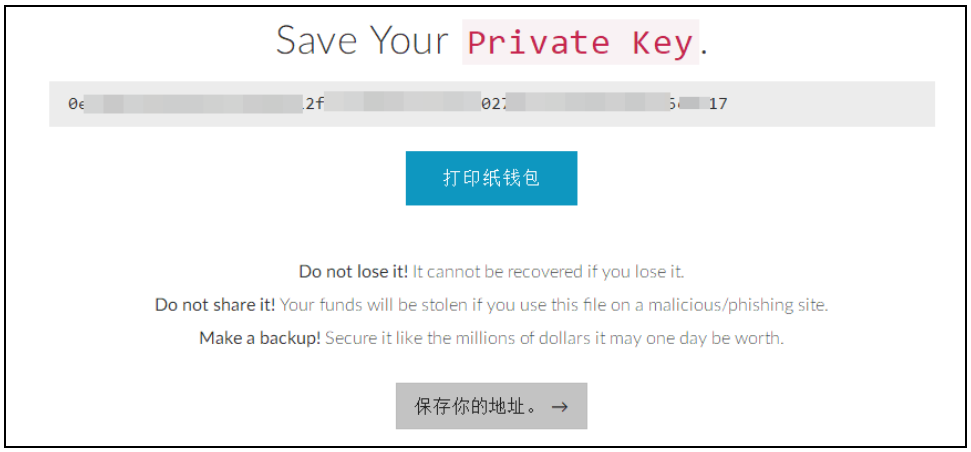


图17-3 保存私钥

第四步：用刚才的私钥解锁，进入你的钱包，余额肯定都是 0。记住收款地址，我的是：**0xB4fd52AA5DB2820dC183aCa9ea8ff030a5F92D5E**，写这个教程用去了 0.06ETH（取 0.05ETH，矿工费 0.01ETH），欢迎捐赠到这个地址。

图17-4 解锁钱包

图17-5 解锁后的钱包界面

第五步：到场外交易所买点 ETH，**提现**（需要 0.01ETH 的矿工费）到刚才的地址：0xB4fd52AA5DB2820dC183aCa9ea8ff030a5F92D5E

第六步：等待提现到帐，不同交易所的处理时间不一样。

第七步：再登录你的钱包，看看是否到帐，如果到帐，进入下一步。如果没到帐，可以登录这个网址查查进展，把你的收款地址敲进去，查一下即可。

https://etherscan.io

第八步：我曾经参加了 lampix 项目的 ICO，登录它的官网 https://lampix.co/，找到它的众筹地址：~~0x8eFFd494eB698cc399AF6231fCcd39E08fd20B15~~，该众筹已经截止，这里只是示例，请勿再向该地址转 ETH。

再次确认一遍这个地址，曾经有黑客入侵过 ICO 网页，把收款地址修改成了黑客的地址，然后就悲剧了……

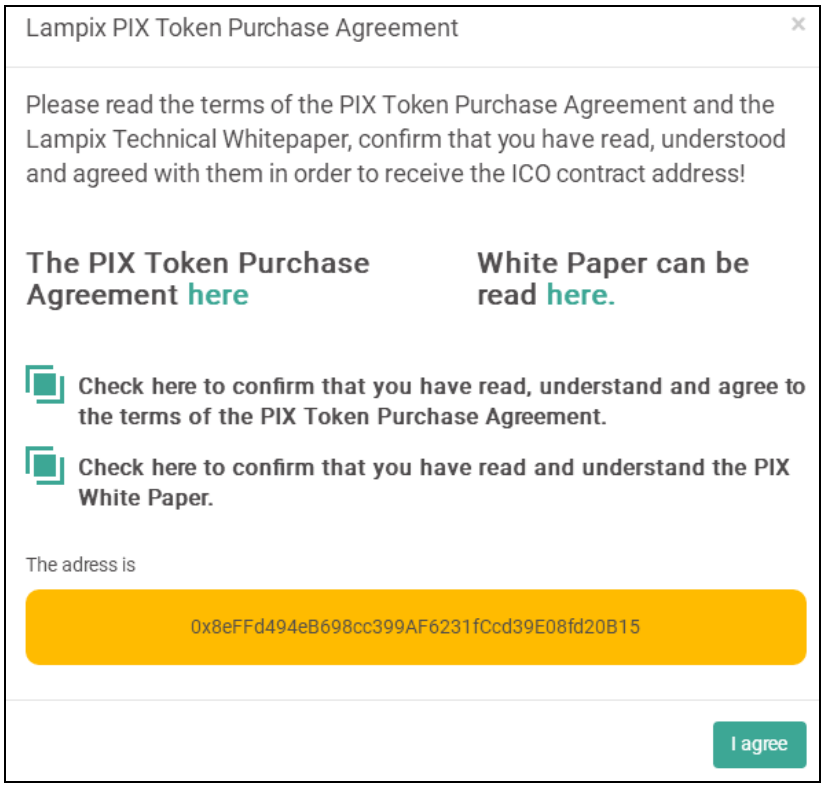


图17-6 参与 lampix 项目

第九步：登录 myetherwallet，发币到众筹地址，留出足够的 GAS 费用，生成交易，再发送交易。

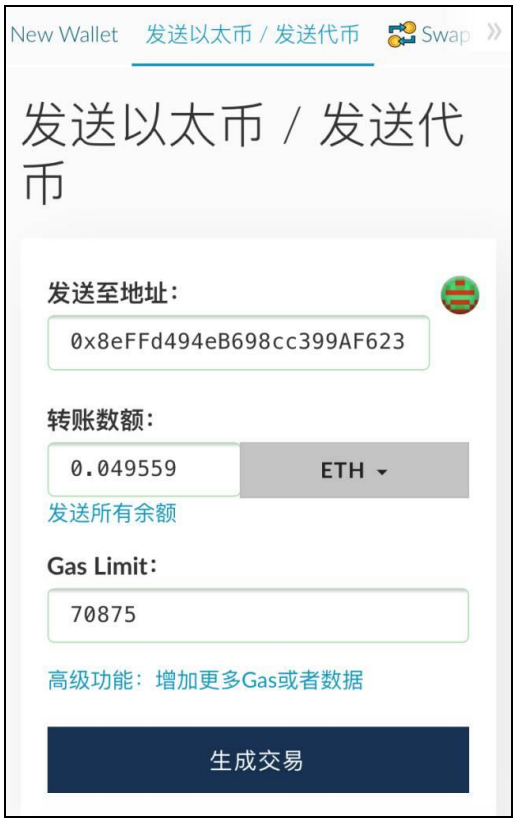


图17-7 发送代币

第十步：增加 token 代码。点“Add Custom Token”按钮，把 PIX 代币名称输入，完成。等众筹成功后，PIX 代币里就会有数字了。

图17-8 增加代币代码

18 Gas Limit 及 Gas Price

2017 年 8 月，国内币圈的 ICO 太火，有些项目在 ico.info 平台上几分钟就完成众筹，一些朋友纵然使出各种解数，还是抢不到（注意 9 月 4 日之后所有 ICO 项目都已退币），然后他们就开始使用以太坊钱包参投项目，安装钱包和参投的过程本来并不麻烦，但向众筹地址发送 ETH 时的 Gas Limit 和 Gas Price 两个参数最让人摸不清头脑。

图18-1 发送代币

最近唯链的 ICO 刚刚结束，我查了一下交易记录，由于 Gas Limit 填错的交易失败了不少，白白为矿工贡献了不少 ETH。

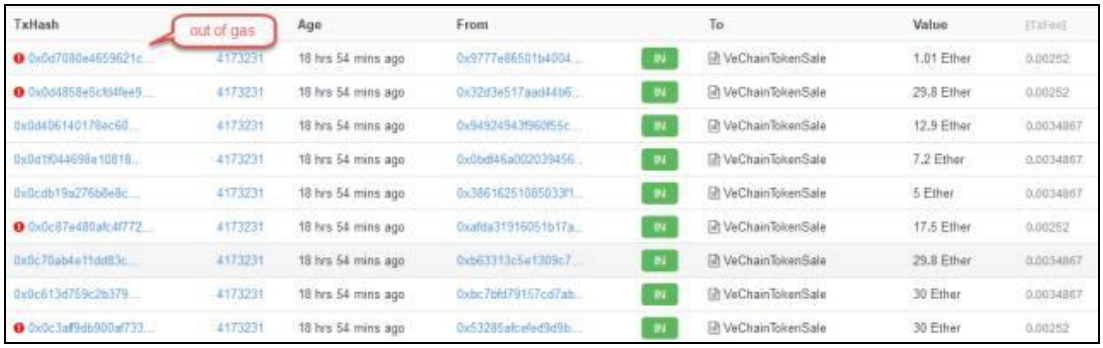


图18-2 失败的 ICO 记录

18.1 到底这个 Gas Limit 和 Gas Price 是个什么鬼？

以前学过比特币发币操作的朋友，对于交易手续费（Transaction Fee）的概念是不陌生的，大多数钱包软件会自动算出一个比较合适的手续费供你选择，比如 0.001BTC 一般没问题。

但以太坊里非把**交易手续费**搞得异常复杂，多整出一个 GAS 术语来，有点多此一举，最后仍要落实到 ETH 的消耗上。在这件事情的设计上，感觉以太坊的创始人 Vitalik Buterin 比中本聪逊色不少，大多数事情保持简单通常是最好的。

不多扯了，这两个参数反正就是要换算成 ETH，矿工们要进行 PoW 工作量证明，最后把

这点手续费拿走。

类比时刻（借鉴了 MyEtherWallet 网站上的思路）：

Gas 直译天然气，翻译为**燃料**，类比**汽油**

Gas Limit 相当你汽车上的**油箱总容量**，比如最多装 50 升

Gas Price 相当于**油价**，比如每升 6.18 元

18.2 先来看 Gas Limit

你参与 ICO，发送 ETH 到众筹的合约地址，在比特币里相当于发起了一笔交易，在以太坊里相当于发起一份**智能合约**，矿工负责把这份合约加到区块链上，交易手续费相当于激励措施，让矿工干活更卖力。

Gas Limit 就是你准备消耗的最大燃料数量，以太坊里的交易相当于程序代码，有不同类型，消耗的燃料数量也不一样，一开始无法准确估计，就设置了一个最大量，以免有些人操作失误钱包被掏空。

但麻烦来了，如果你提供了较少的燃料费，交易可能会失败，但燃料费不退。就像你加了 50 升的油非要跑到西藏去，结果半路汽油用光了，用了就用了，没人退给你油钱。油箱有个好处，可以加油继续跑，以太坊上的交易就没那么幸运了，合约代码已经执行了，执行过程需要许多步骤，刚走了 2 步，没油了，只能作废，想补 Gas 也来不及了，所以**提前设置好 Gas Limit 很重要**。

如果 ICO 交易成功，手续费是按实际花掉的燃料计算的，多余没花掉的燃料，会以 ETH 的方式自动退回到你的钱包中。

举例：

```
Gas Limit：90000

Gas Price：100 Gwei （即 0.0000001 Ether）

Gas Used：34867
```

先别管 100 Gwei 那个奇怪符号，你设置了高高的 90000 最大量限制，实际上只用了 34867，那么实际消耗的燃料费为

34867 * 0.0000001 Ether = 0.0034867 Ether

按 5258 元/ETH 的价格计算，你交了大概 18.3 元的手续费。

我看了网上那些失败的交易，大多是因为设置了 Gas Limit 为 25200（可能是看了哪篇参投权威教程吧？），这样白白浪费了 0.00252 ETH。

交易失败只损失手续费，参与 ICO 的大笔资金并不受影响。也就是说，你参投 50ETH，假设失败，只扣掉 0.00252ETH，50ETH 丢不了。

我简单查了查那些成功的交易，Limit 一般设置为 90000，还有最高设置 20 万的也没问题，但不能太高，有些钱包软件可能会报错。

18.3 再来看 Gas Price

意思是单位燃料的价格，我们熟悉的单位是 Ether，最小计量单位是 wei。这个计量单位(为了纪念一些名人)实在是太小了，官网上提供了一个很全的列表：

'wei':	**'1',**
'kwei':	'1000',
'ada':	'1000',
'femtoether':	'1000',
'mwei':	'1000000',
'babbage':	'1000000',
'picoether':	'1000000',
'gwei':	**'1000000000', // 9个零**
'shannon':	'1000000000',
'nanoether':	'1000000000',
'nano':	'1000000000',
'szabo':	'1000000000000',
'microether':	'1000000000000',
'micro':	'1000000000000',
'finney':	'1000000000000000',
'milliether':	'1000000000000000',
'milli':	'1000000000000000',
'ether':	**'1000000000000000000', // 18个零**
'kether':	'1000000000000000000000'

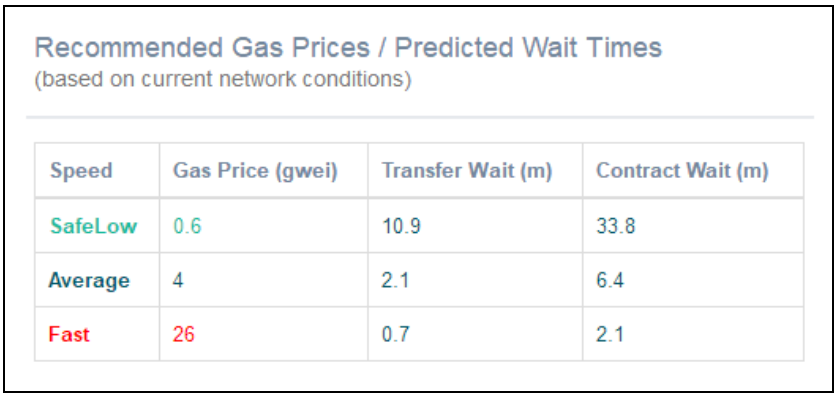
```
'grand':    '10000000000000000000',
'einstein': '10000000000000000000',
'mether':   '10000000000000000000000',
'gether':   '10000000000000000000000000',
'tether':   '10000000000000000000000000000'
```

刚才的 100 Gwei 现在知道意思了吧？1 Gwei 相当于 10^9 wei，那么

100 Gwei = 100 * 10^{-9} Ether = 10^{-7} Ether

这个 Gas Price 也很重要，你给的价格越高，你的交易就越优先被矿工取走，就越早地被确认。你可以登录这个网站看看设置什么价格比较合适：

http://ethgasstation.info



Recommended Gas Prices / Predicted Wait Times
(based on current network conditions)

Speed	Gas Price (gwei)	Transfer Wait (m)	Contract Wait (m)
SafeLow	0.6	10.9	33.8
Average	4	2.1	6.4
Fast	26	0.7	2.1

图18-3 参加 gas 价格

看出来了吧？网站上给出的最高价格为 26Gwei，而参加 ICO 的朋友给出的价格高达 100Gwei，为了抢上，真是够拼的。

18.4 以太坊货币单位中的名人

前面提到了一堆以太坊 Gas 的计量单位，有几个比较奇怪的：wei、ada、babbage、shannon、szabo、finney、einstein。这些都是一些计算机方面的名人，以太坊的创始人估计崇拜这些专家，把他们的名字都弄成了计量单位，不过太不好记，除了 wei、gwei、ether 常用以外，其它大部分单位都不常用。

wei：Wei Dai，他发明了 B-Money，中本聪在 2008 年写的比特币白皮书中引用了他的 B-Money 论文。

ada：Ada Augusta，阿达·奥古斯塔，被封为 Lovelace 女伯爵，所以经常称她为 Ada Lovelace。19 世纪诗人拜伦的女儿，数学家，被称为“第一个给计算机写程序的人”，建立了循环和子程序概念，为计算程序拟定“算法”。第一位程序员竟然是女士，为了纪念她，有一门编程语言就叫 ADA。

babbage：Charles Babbage，查尔斯·巴贝奇，英国发明家，用一堆机械发明了差分计算机，还用了一堆图纸设计了第二代差分计算机，可惜工艺太复杂，他在世时没造出来。N 年过后，有个大学按他的设计把机器造出来了，竟然真能运转。虽然没有用电，原理却与现代的计算机一样，详细的介绍请参考《信息简史》一书。

shannon：Claude Shannon，香农，美国数学家、信息论的创始人。首先提出了信息熵的概念，为信息论和数字通信奠定了基础。https://www.zhihu.com/question/27068465

szabo：Nick Szabo，尼克·萨博，计算机科学家、加密大师，1993 年最早提出了智能合约(smart contract)，1994 年写成了《智能合约》的开山之作，1998 年就设计出了“比特黄金”(bit gold)的去中心化的数字货币机制，有人怀疑尼克·萨博就是中本聪(Satoshi Nakamoto)。

finney：Hal Finney（哈尔芬尼）是一名密码朋克（cypherpunk），比特币的第一笔测试交易是中本聪向他转 10BTC， 2014 年 8 月死于渐冻人症，终年 58 岁。http://www.8btc.com/hal-finney-2

最后一个 einstein 爱因斯坦就不用介绍了。

18.5 小结

- ✧ 交易费按 Gas(燃料)来计算
- ✧ Gas Limit 是最大使用的燃料数量，参投 ICO 的数值都比较大，90000 是个参考值
- ✧ Gas Price 是愿意支付的燃料单价，价格越高，越早被矿工打包确认
- ✧ wei 是燃料的计量单位，太小，常用 Gwei
- ✧ 平常交易为 20-30Gwei，参投 ICO 的人们都拼到了 100Gwei
- ✧ Gas Limit 设置太小，交易可能会失败，此时交易费不退，但你参投的大额 ETH 不受

影响

- ✧ 实际交易费 = 实际使用燃料数量(Gas Used) * 燃料价格(Gas Price)

19 以太坊代币取出到 imtoken 钱包

2017 年 9 月币圈发生了许多事，“ICO”一刀切、交易所全关，真是币圈一天人间一年。还有一些坚定地活在未来的人们恶补区块链知识，开始忙着把一些 token 拼命地往钱包里导。

我这样的 IT 人士+区块链爱好者都被世面上五花八门的钱包软件、密令、密码、keystore 等折腾得不轻，小白们可真要小心操作啊，辛辛苦苦屯了几个币，别因钱包操作不慎而归零了。

今天开始取现以太坊中的代币，ETH 当然是这个世界的主要燃料了，另外像 qtum、ven、eos、snt、lun、pay、omg、1st、dgd 等都是以太坊系的资产，只要支持 ETH 的钱包，应该都支持这些代币的保存。

19.1 可供选择的 ETH 钱包

以太坊的钱包有很多种，MyEtherWallet 是非常经典的一款钱包，国内用户更喜欢 imtoken 钱包。

- ✧ Ledger Nano S，CoinPayments，MyEtherWallet
- ✧ MyEtherWallet，Mist，Parity，Metamask，imtoken
- ✧ Coinbase，Exodus，MyetherWallet，Jaxx，EthAddress 纸钱包
- ✧ Ledger Nano S，Trezor，Exodus，Jaxx，Mist，MetaMask，MyEtherWallet，Coinbase，EthAddress，Keepkey

前面介绍过 MyEtherWallet 钱包，虽然“ICO”被禁，但前面一部分建立钱包的过程还是一样可用的。

19.2 安装 imtoken

这一步竟然拦住了许多苹果手机的用户,因为这个 imtoken 软件在中国区的苹果商店里找不到，你需要用国外的 apple id 来下载、安装 imtoken 软件。

最简单的获得 apple id 的办法是使用“某宝网”，搜索 apple id，会有一堆结果的，我选了一个 10 元的，实在太好用，现在已经忘了切换回中国的 apple id 了。

Android 手机直接到官网 token.im 下载安装即可，imtoken 是下面这个样子：

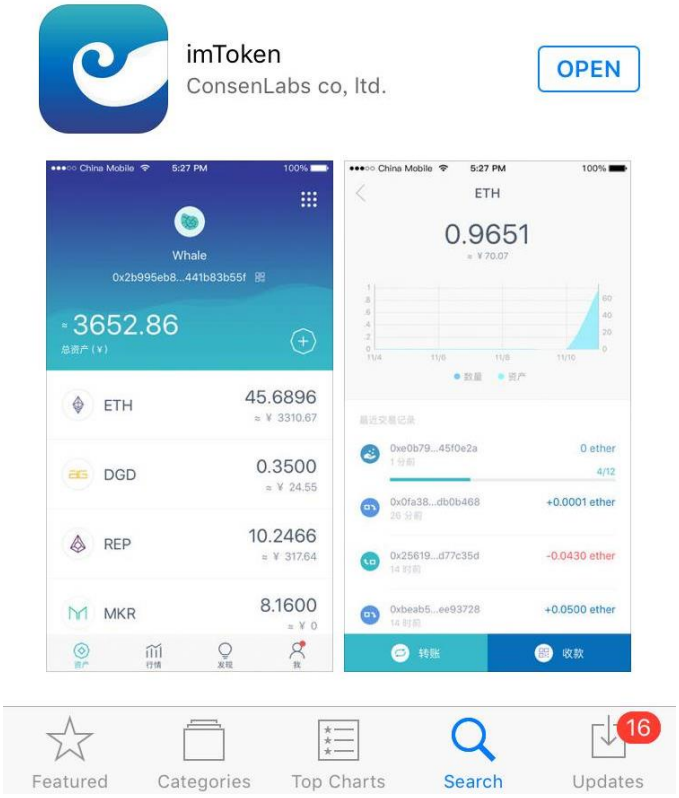


图19-1 Imtoken 手机应用

19.3 设置新钱包

创建钱包的过程中非常简单，输入钱包的名称和密码，1 秒钟就建好了。但备份钱包的过程尤为重要，在备份这一步里，可以备份私钥、助记词、keystore 这三种东西，实际上只备份一种就行，但为了保险起见，你可以备份两种。

当然，如果这些内容泄漏给其他人，你的 ETH 可能会被盗。我以前推荐过 KeePass 类的保管密码的软件，可以一试。

1）导出私钥

私钥是长长的字符串，区块链世界里，私钥是你的全部，不要拍照、不要发短信、邮件、微信，认真抄上三遍，锁在保险柜里。

请保管好你的私钥。

请保管好你的私钥。

请保管好你的私钥。

重要的事情说三遍。

2）备份助记词

这里会出现 12 个英文单词，认真抄好，放在安全的地方。

3）备份 Keystore

这个文件可以方便地导出到其它 ETH 钱包中，比如：MyEtherWallet。

19.4 找到收款地址

在钱包的“资产”的顶部有一排以“0x”打头的字母和数字，点进去，复制收款地址，记好了。

图19-2 收款地址

19.5 绑定取现地址

很多小白到现在也没搞懂“取现”这个概念，在知识星球（以前叫小密圈）里经常会遇到类似这样的问题：

我在云币网的 EOS 后面点击了“取现”，怎么没有收到人民币呢？

坚定的数字货币持有者们认为：数字货币才是未来的现金，我们所说的提现就是指把数字货币放到自己的口袋（钱包）中，当然你也可以把币直接搬到其它交易平台去。

登录云币网或 ico.info 中，在“我的账户”中找到区块链资产提现那一栏，先点击”绑定区块链资产提现地址“。

图19-3 绑定提现地址

还记的刚才说的一堆币代码吗？eth、qtum、ven、eos、snt、lun、pay、omg、lst、dgd，这些可以用 imtoken 存放，其它币就别绑定了。选好币种，标签任意填，把刚才复制好的以“0x”开头的收币地址填上，通过短信验证后，就绑定了提现地址。

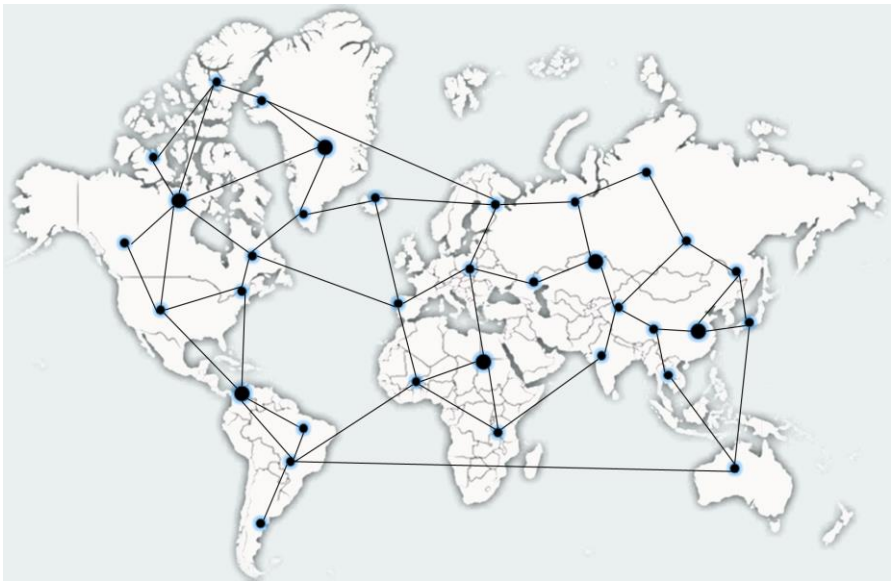
最后一步，取现。回到刚才的区块链资产提现页面，点击相应币种后面的“提现”，先小额试试，操作无误后，再全部提走。

在 ico.info 中会自动扣除矿工费，也就是说，如果你有 1 个 ETH，要全部提出，输入 1 就行，如果矿工费为 0.015，那么你实际转到钱包的币为 0.985ETH。

19.6 查看结果

当提币申请受理后，你可以在 imtoken 中看看余额是否变化，也可以到这个网站查询交易的确认情况：https://etherscan.io/ 。

第四篇 脑力挖矿



20 零资金成本参与区块链

参与区块链投资你可以投资挖矿，可以搬砖，可以做场外交易，可以在二级市场交易买入卖出……这些都需要资金成本，投资风险较大，其实还有另外一个零资金成本的参与方式，就是参与到 UGC（UGC 是“User Generated Content”的缩写，是指用户将自己原创的内容通过互联网平台进行展示或者提供给其他用户）的区块链激励平台，通过在这些平台创造有价值的内容而获得代币奖励。

我们把这种参与方式，简单叫做**“脑力挖矿”**。

20.1 传统 UGC 的问题

UGC 是指用户将自己原创的内容通过互联网平台进行展示或者提供给其他用户，相关的网站有社交网络的 Facebook、人人网；视频分享网站 youtube、优酷网；知识分享百度知道、百度百科；社区论坛知乎、天涯；微博类的 Twitter、微博等。

目前这类网站都是参与其中的用户作为优质内容的制造者和传播者，为 Facebook、Twitter、微博、知乎等社交网络和 UGC 平台带来了海量的流量和巨额的利润，但是参与其中真正为平台创造内容价值的用户却没有分享到平台的任何收益。

20.2 区块链应用在 UGC 可以解决什么

基于区块链的 steem 内容社交网络平台，在白皮书中写了这样一段话：

> 用户生成的内容为社交媒体公司如 Reddit、Facebook 和 Twitter 的股东创造了数十亿美元的价值。Reddit 曾在 2014 年提出这样的假设：如果每一位以帖子、留言或者投票的形式贡献于 Reddit.com 的用户，都能公允地获得 Reddit 公司的股份，则这个平台将变得更好。

而 steem 通过区块链技术，让 Reddit 公司 2014 年提出的假设成为现实。区块链应用到 UGC 平台，会有如下特点。

1）通过去中心化的方式实现信任网络

传统的平台，比如微信公众号、知识星球等用户间的付费、打赏等，都是通过中心化的方式实现信任交易。你的付费和打赏，都是先转移到平台，通过平台的中心化担保来达成交易。

区块链构建一个去中心化的信任网络，可以实现点对点的价值传输。用户间的付费、打赏、

点赞等都不需要任何中心化的担保来实现交易信任。

2）版权确认

在区块链出现前，互联网一直没解决一个问题，就是版权确认的问题，所以中心化的出版商有其存在的必要性。

区块链出现后，提供了一种历史不可篡改的数据库技术，应用在 UGC 上就意味着被录入区块链的内容信息具有不可篡改性，不可篡改意味着任何欺骗行为会在区块链里留下证据。你只需要最早录入原创内容信息，后来者的抄袭只会留下永远不可删除的证据。区块链真正通过互联网的方式实现了去中化方式下的版权确认。

3）代币的激励模式

传统的 UGC 行业，用户一般需要通过广告或者开发其它产品来解决变现问题，区块链应用在 UGC 行业中，提供了一种代币的激励模式。用户参与原创内容的创造和分发可以直接获得代币奖励，代币让优质原创内容变现更容易。

20.3 区块链应用在 UGC 是否是机会

以区块链的内容社交平台 Steemit 为例，成立 2 年市值约 100 亿人民币，在所有区块链项目中排名在 30 名左右，Steemit.com 网站排名也达到全球 1600 名左右。

用户可以在 Steemit 发表文章，分享自己的绘画、摄影等各种内容形式的作品为平台创造价值，其他用户可以为有价值的内容点赞，点赞直接以平台代币的形式获得收益。一篇文章的收益，作者获得 75%，点赞者获得 25%。所有的收益不是来自自己的打赏或者充值，而是来自平台。

作为整个 UGC 行业，区块链在 UGC 行业的应用也一定会有一个类似 Facebook 这样的伟大公司出现。作为个人可以零资金参与平台内容创造获得收益，你投资持有代币也意味着就是这个去中心化公司的股东，可以享受公司的发展红利。

20.4 “内容搬砖”时代来临

继 steem 之后，国内及国外相继出现了许多类似的内容激励平台的区块链项目，比如国外的 yours.org、view.ly、synereo.com 等，国内的 YOYOW、币乎、PressOne、Ulord 等。随着

更多项目在 2018 年应用落地，预测会出现一种现象，叫做“内容搬砖”。内容搬砖就是：把自己的原创内容，从一个平台复制到另外一个平台，获得 N 份收益。这对于很多作者来说，这将是一次机会，相比传统的平台不仅可以获得收益，现在还可以把同一份时间出售 N 次。

21 Steem 区块链

Steem 是一个基于区块链的奖励性公共内容平台，是一个利用数字货币奖励社区建设和社区互动的区块链数据库。Steem 将社交媒体的概念融入数字货币及其社区建设，设计了一个能够公平反映个人贡献的会计系统。

不同于其它的加密货币，Steem 以数字货币作为奖励，设计了一套激励系统和投票制度，把其价值的一大部分回馈给价值贡献者，这也使得 Steem 具有“智能”和“社交”的特性。

21.1 Steem 区块链 DPOS 共识机制

在 Steem 的蓝皮书里提到，相比于工作量证明 POW（比特币的共识机制），Steem 能提供更大规模和更快速度的算法，即委托权益证明（DPOS）。简单来说，这个共识机制就是在**解决到底谁来给各种信息**（区块链里的各种交易、转账，Steemit 里的点赞、转账、评论等等都是区块链里产生的信息）**安全记账的问题**。

在中心化的世界里，记账是由中心平台来解决，比如班上的考勤记录由学习委员来记录，如果学习委员哪天生病了没来上课，那么那天的考勤记录就没人管了。所以，区块链发明了一种去中心化的记账方式来应对中心化的系统风险。很多人共同来记录同一个账本，其中一个人记账出现问题都不会影响整个系统，参与记账有报酬鼓励更多人参与。

去中心化的记账又有很多种方式，最熟悉的就是比特币的工作量证明 POW，另外 steem、bitshares、EOS、公信宝都是委托权益证明股权 DPOS。那么这两个共识机制是怎么约定谁来记账的呢？

POW 共识算法的比特币就是找出一个最能算题的来记账，而这个最会算账的可以不拥有比特币或者也可以不了解比特币，反正只要他最会算题就可以了。

DPOS 共识算法的 Steem 要想记账，需要持有股份（Steem 代币）先来竞选，所有持有代币的人可以投票来决定谁来记账。所以，持有 DPOS 代币就是类似于持有这个公司的股份，你大量拥有 Steem 代币就拥有竞选的筹码。区别于 POW，Steem 的 DPOS 共识算法里记账人必须是股

东。

21.2 Steem 见证人

Steem 见证人是 Steem 区块链委托权益证明（DPOS）共识机制的产物。区块链就是一个公开的数据库账本，共识机制就是用来解决到底谁来给各种信息（交易、转账，Steemit 里的点赞、点踩、留言等等）安全记账的问题。

Steem 里记账的这个职业人，就叫做见证人，见证人被选出来负责创建与签核交易区块，一个见证人就是一个网络数据节点。

Steem 的白皮书是这样描述的：

> Steem 的区块链采用轮流制，每一轮，21 位见证人被选出来负责创建与签核交易区块。见证人当中的二十位用户投下的赞成票数选出，另一位则由所有票数未达到前二十名的见证人分时担当。21 位见证人每轮完一圈之后，都会重新排序，以避免任何一位见证人持续忽略某个顺位的见证人所生产的区块。见证人一旦错过某个区块且在过去 24 小时内未生成区块，就会丧失资格。

简单理解上面的一段话：

（1）负责创建与签核交易区块见证人由社区投票产生，共 21 位。

（2）21 位见证人由投票产生的前 20 名+1 位未达到前 20 名的见证人分时担当。

（3）21 位见证人创建和签核区块的排序是变化的。

（4）没有履行好见证人职责的会丧失资格。

因为负责创建与签核交易区块的见证人的数量有限，见证人实际上会互相竞争来获得记账的工作，获得记账工作的见证人每完成一次记账都可以获得系统的代币奖励。

21.3 如何给 Steem 见证人投票

Steem 采用的共识算法跟全世界大多数的股份制公司很类似，任何持有 Steem Power 的用户都可以理解为是 Steem 这一家去中化公司的股东，而 21 位见证人可以理解为由所有股东推选出来的董事会。所以，持有 Steem Power 的用户都可以参与到见证人的投票中。

在 Steem 里，你可以自己投票，你也可以把自己的票数代理给别人帮你行使投票权利。

https://steemit.com/~witnesses 可以看到所有的见证人名单,网页只显示了前 50 位见证人。每个人可以投票给 30 位见证人（witnesses），50 名以内见证人的投票可以直接点图上点赞标识。

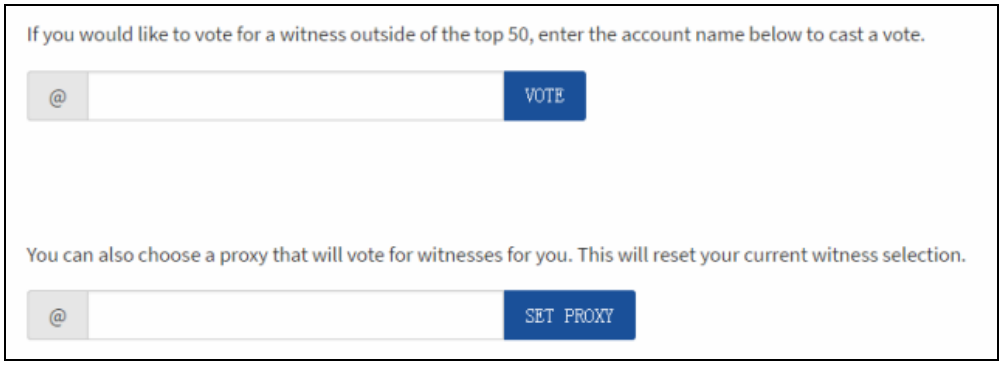


图21-1 直接投票或代理给见证人

如果你想投的见证人在 50 名外，可以通过输入账户名来进行投票，最下面一栏你可以把票数代理给别人帮你行使投票权利。

21.4 基于 Steem 区块链的 SMTs

SMTs 是基于 steem 区块链的一个类似于以太坊的智能合约系统。以太坊的最大作用就是让每个人可以发行自己的代币，并且发行自己的代币变得很简单，不需要自己创造或者管理一个区块链。我们知道的大部分代币都是基于以太坊发行的。

可以把以太坊理解为一个股票发行结算系统,每个公司都可以在以太坊上发行自己的股票（把代币可以简单理解为股票），而不需要去管理这些股票如何交易结算，以及不需要担忧这个交易系统的安全性。交易结算、安全性等都由以太坊区块链帮你解决。

现在 SMTs 也是一样，它要做以太坊可以做的事，每个公司都可以通过 SMTs 很容易的发行自己的股票（代币），而不需要自己做一个区块链，也不需要对区块链技术的管理。

1）基于 SMTs 的众筹

理解了什么是 SMTs，于是我们就可以来搞点事情了。比如申龙斌创建的“区块链生存训练”社群是一个提供区块链知识服务的内容社群，我们想搞一个公司发行自己的社群股票，代码 SLB。但是没有钱只有内容和技术，怎么办？

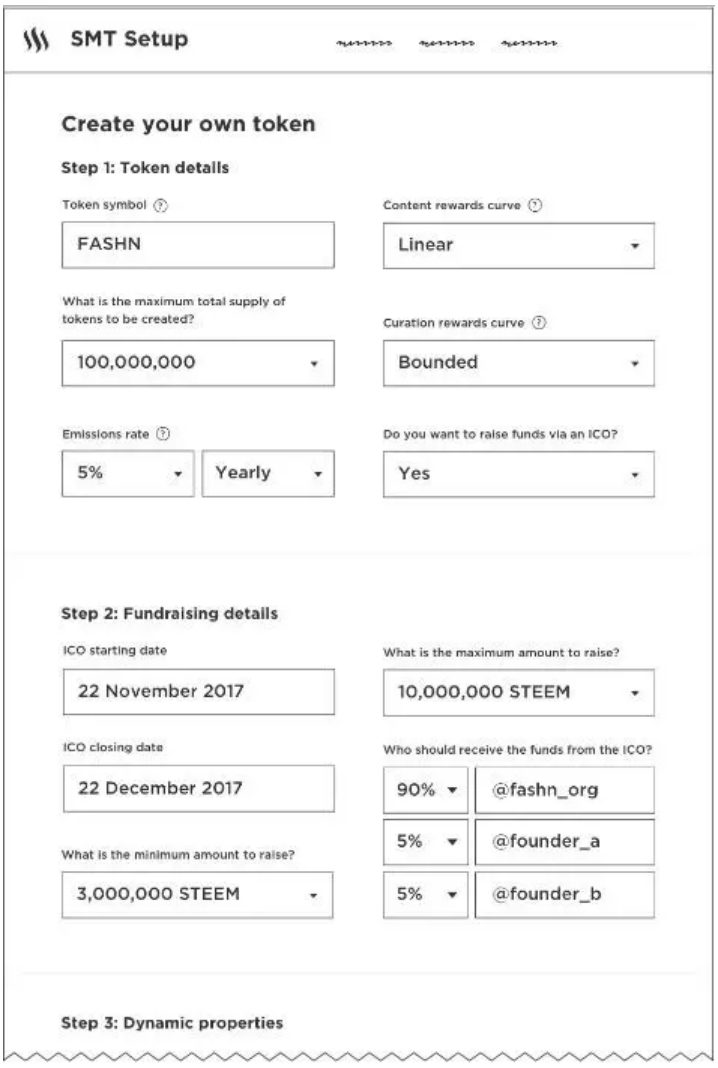


图21-2 SMTs 中 FASHN 代币发行操作

（1）在正规的证券交易所去发行股票筹集资金？想也不用想。

（2）自己创造一个区块链，通过众筹来筹集资金？技术要求太高，没戏。

（3）在 SMTs 上发行代币 SLB 筹集资金？这个可以有。

在 SMTs 上发行社群代币（股票）SLB，筹集 Steem 代币来解决资金问题，代币（股票）的流通交易结算都是运行在 Steem 区块链技术上，我们不需要管理它。我们发行的 SLB 可以自己定义“区块链生存训练”社群的股份分配方案、利润分配方案等等。

认可公司价值的个人和团队可以通过 Steem 来参与众筹，持有 SLB 成为社群股东，成为股东的你可以享受到社群的服务参与社区的发展。社群不断壮大，价值也就不断增大，SLB 代币的价值也就增大。

2）SMTs 生态

SMTs 的提出旨在构建内容生态，SMTs 不是重新创造一个区块链，是基于 steem 区块链，所以 SMTs 的众筹也必然会用 Steem，就像很多基于以太区块链的发行代币众筹都是以太坊一样。

Steem 代币是 Steem 区块链的燃料，通过 SMTs 在 Steem 区块链上构建新的内容公司（发行自己的股票）需要 Steem 来保证整个系统的运行。

所以 SMTs 发展出更多的内容生态，会增加 Steem 的流通性和价值。

3）SMTs 与 ETH 的智能合约的不同

如果都是筹集资金，发行自己的代币（股票），为什么不用以太坊的智能合约，要用 SMTs。要回答这个问题，你需要了解 Steem 区块链和 ETH 区块链背后的区块链技术的不同。

最大的不同点是，Steem 是基于石墨烯区块链技术，处理信息比以太坊更快，快到可以用在一些内容相关的应用上。我们在 Steemit 网站上的每一个操作（发文、点赞、评论等）都是产生信息，如果 Steemit 运行在以太坊上，速度肯定很慢，用户体验差，这样的内容网站是没有竞争力的。

如果纯粹用作发行公司股票（代币），以太坊还是有它存在的价值——每个公司发行自己的股票变得很容易。处理的信息也主要就是代币间交易，目前以太坊的处理速度还是可以接受的。况且，在以太坊上的这种代币发行机制，相比真正意义的股票，很好的解决流通性（全球流通）、发行难度（股票要求很高审查很严）、结算系统和安全性等问题。

综上，内容相关的公司鉴于本身需要更快信息处理速度，以满足良好的应用体验，通过 SMTs 来发行自己的代币是目前为数不多的选择（未来的 EOS 也是一个选择）。

22 Steem 区块链应用生态

Steem 是少数已经有落地应用的区块链项目，目前 Steem 上已经有非常丰富的应用生态。比如博客类的内容网站 Steemit.com 和 busy.org、音频内容 Dsound、视频分享网站 DTube、视频直播和分享网站 Dlive、手机端的 esteem（www.esteem.ws）、出售货物的网上商店 thesteemitshop.com（只接受 steem 或 SBD 付款）以及著名的乌托邦（utopian.io）等。乌托邦是

通过完善开源程序、给开源程序找 Bug 或者翻译一些开源程序的文档等方式来获得收益的一个项目。

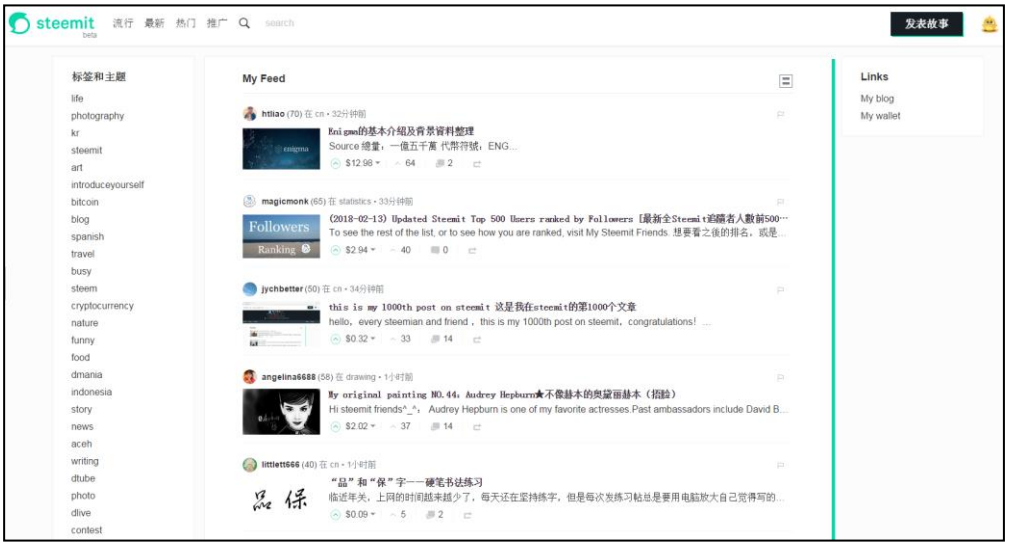


图22-1 steemit.com 网站

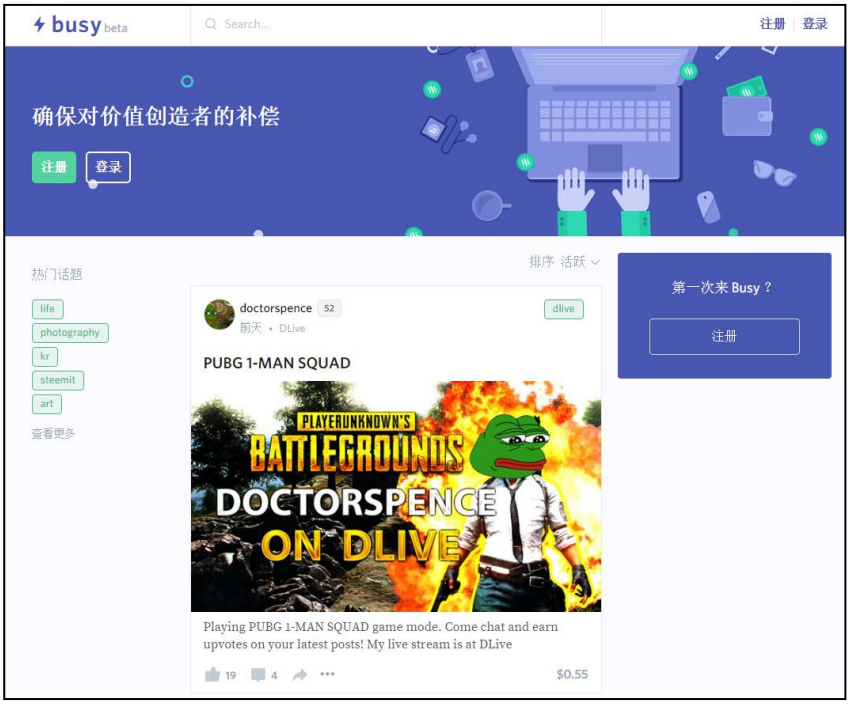


图22-2 busy.org 网站

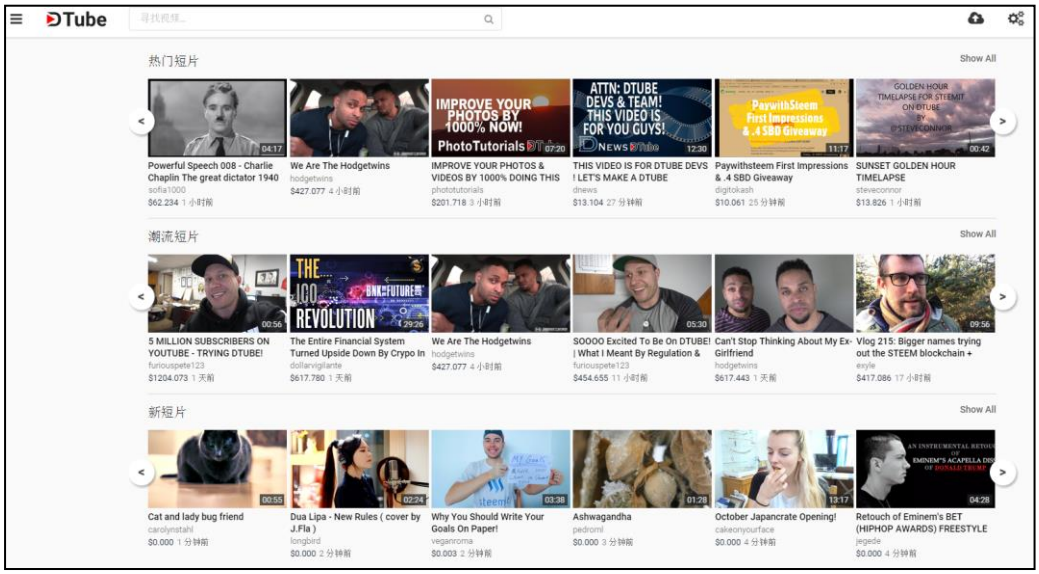


图22-3 d.tube 网站

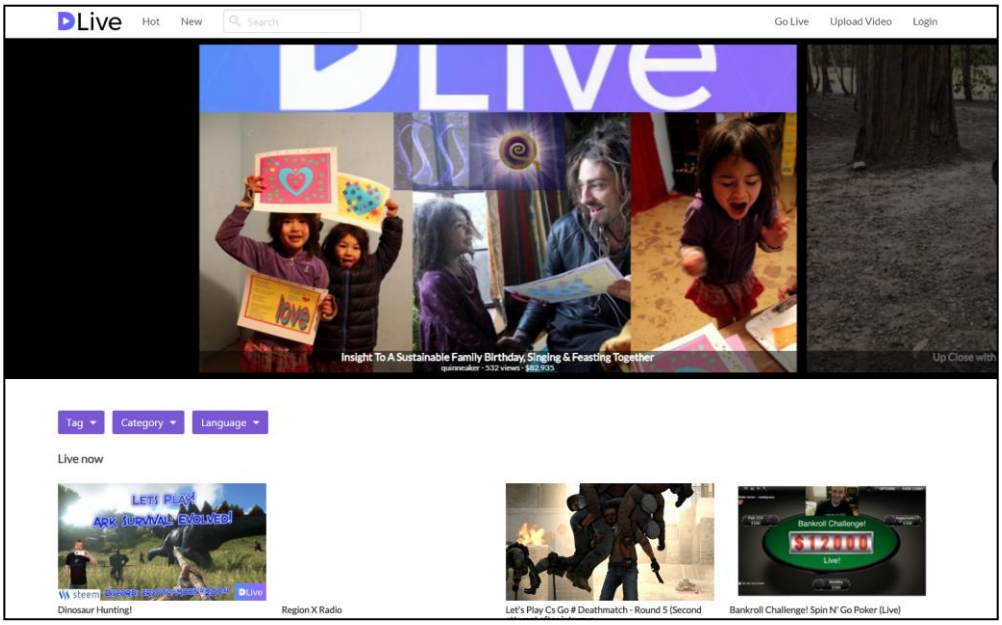


图22-4 dlive.io 网站

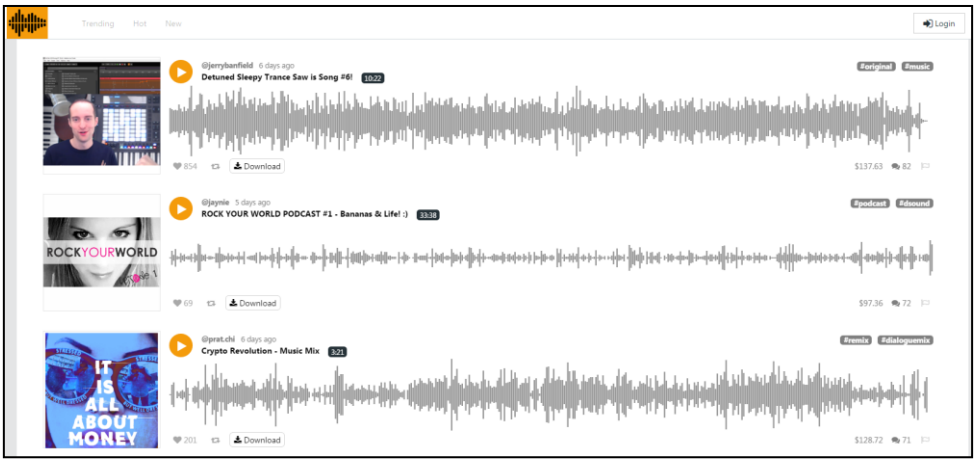


图22-5 dsound.audio 网站

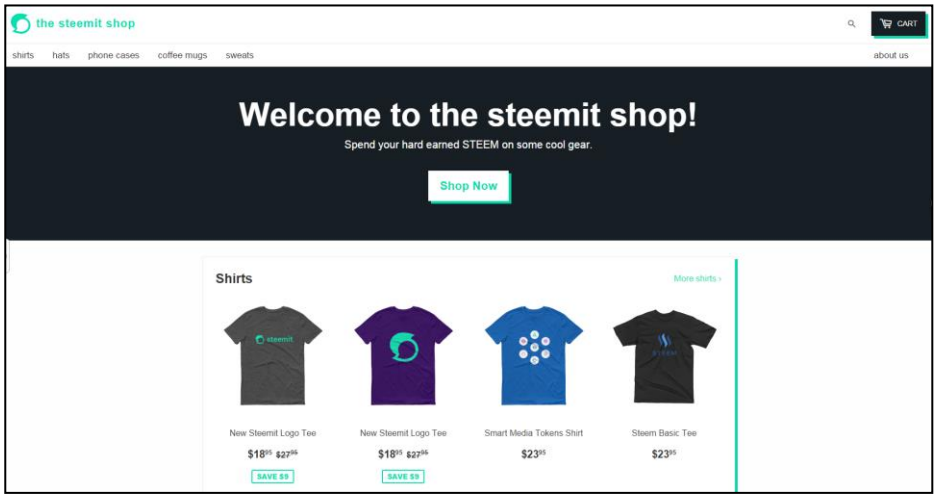


图22-6 thesteemitshop.com 网站

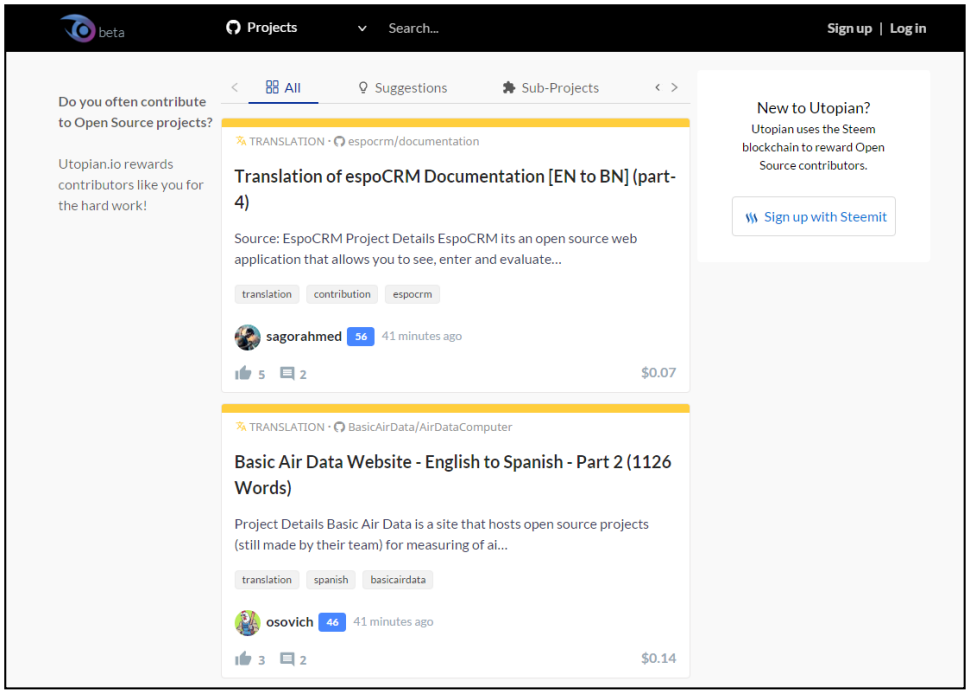


图22-7 utopian.io 网站

这些应用生态都是基于 steem 开发，用一个账户就可以登录使用这些应用。比如 Steemit 账号就可以登录 busy 并使用。基于 steem 的 SMTs 开发成功后，Steem 的应用生态也将会更加丰富。

22.1 busy.org 使用教程

Busy.org 是 Steem 区块链上的第三方应用前端，busy.org 与 Steemit 功能类似属于一个

网站平台，方便大家内容社交。Busy 与 Steemit 只是使用界面风格不太一样，它们背后的数据是一致的。也就是你在 busy 上发表一篇文章，在 Steemit 里是同步发表。

Busy 网址为 busy.org，点击右上角的 log in，进入 steemconnect 登录页面，登录账号。登录后进入个人主页面。

图22-8 Busy.org 个人主页面

网站有时会自动识别你的 IP，自动显示为简体中文版，如果显示的是英语，你可以自己通过设置里选择你的语言。

登录后的界面，如上图中间部分是我关注的好友最新动态。busy 的风格给人的感觉不错，QQ 空间、人人网等风格很类似。

图22-9 Busy.org 中的设置

点击右上角可以进入设置界面，设置界面的第一行及第二行是控制投票比例，在 Steemit 里只有持有的 Steem Power 大于 500 时，才能设置投票能量。在 busy 里 500SP 以下也可以设置。

第三行可以设置选择你的使用语言，第四行 NSFW Posts 是设置网站上不良帖子是否显示。

图22-10 Busy 中的个人首页

点击右上角的账号名，可以进入个人主页，主页左侧一列可以显示你的个人介绍，何时加入 Steemit，目前的投票能量是多少；中间一列显示你发表的文章，评论，关注者等等；最右侧是推送你的朋友。

在个人主页的最上面，可以看到自己的等级（等级代表威望，信誉），比如目前@yellow bird 是 59 级，小鱼的级别。

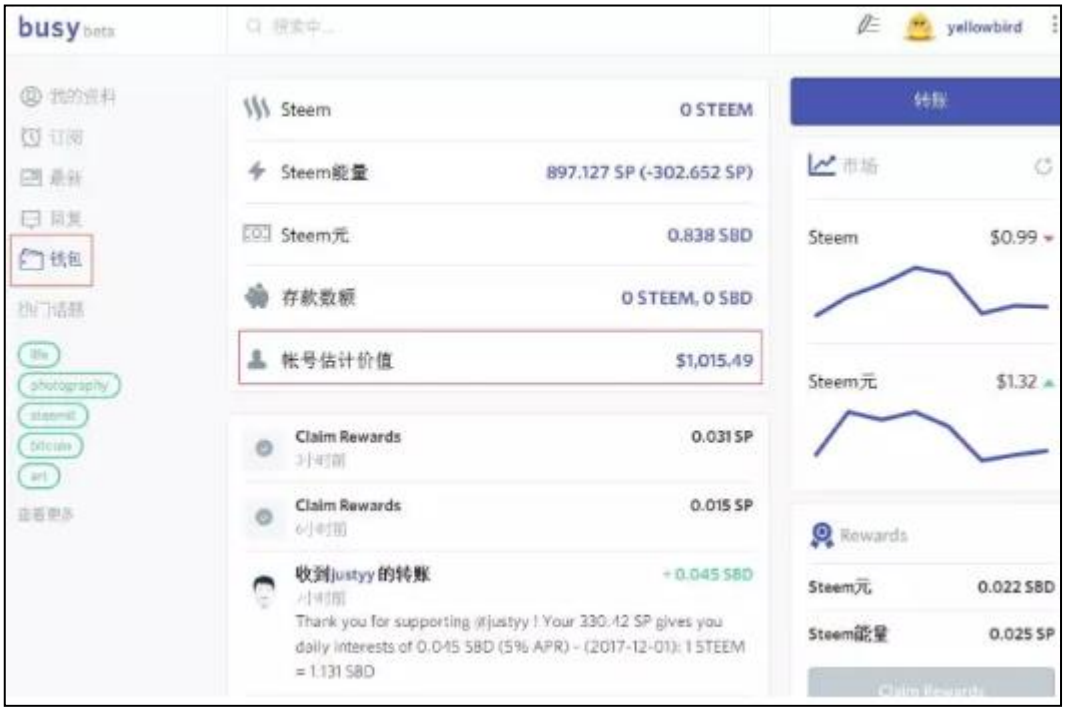


图22-11 Busy 中的钱包

点击钱包可以进入个人钱包页面，中间部分可以看到个人或者你想关注的钱包情况，右侧是 steem 目前的市场价格情况。

图22-12 Busy 中的点赞情况

Busy 里有个 Steemit 没有的功能，就是把鼠标移动到文章点赞手势右侧的数字上，可以显示谁给你点赞了多少钱。如果，发表文章后你想查看哪个大鲸鱼点赞了你多少钱，busy 是挺方便的。

使用 busy 除了页面风格更人性化外，登录 Busy.org 发帖子并添加标签 “busy” busy.org 的机器人会来赞你的帖子，机器人会根据每个账号情况来分配点赞权重。busy.org 机器人只在 12 小时内赞一个帖子，12 小时内发表 2 篇帖子只会得到一篇帖子的点赞。目前 busy 在推广阶段，也许 busy 点赞会取消。

22.2 DTube 使用教程

DTube 是基于 steem 区块链开发的一个去中心化的视频分享网站，跟 busy.org 和 Steemit.com 是类似的概念。在 DTube 上点赞留言分享，数据上传 steem 区块链后在 Steemit 上是同步更新的。

那么 DTube 具体是什么，如何使用，我们来初步体验下：

1.登录

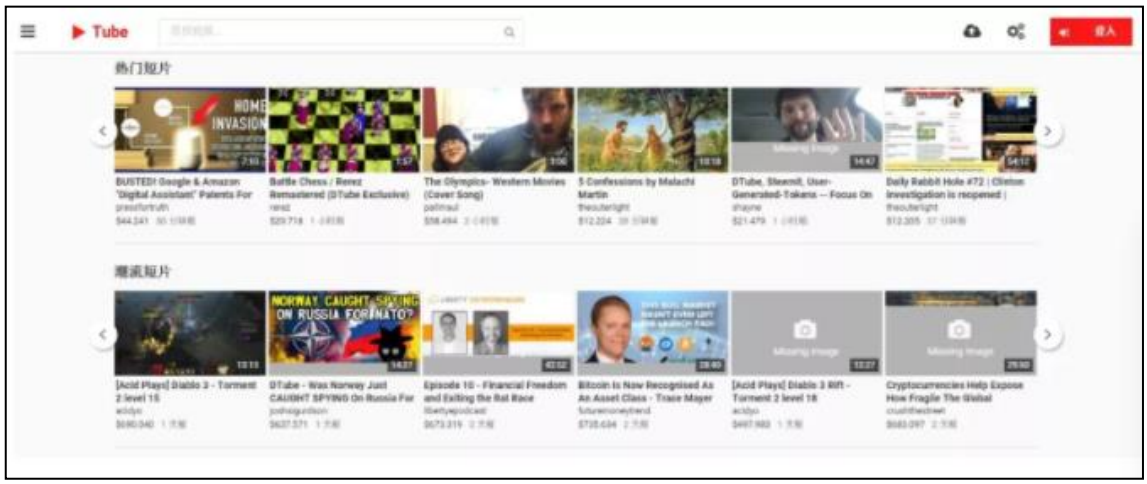


图22-13 d.tube 首页

登录网址：https://d.tube。

打开网站后，我们可以看到网站的首页已经有很多的视频分享，有热门短片，潮流短片等等。视频下面有个美元$的符号，跟 Steemit 一样是分享内容获得点赞的收益。

在页面的右上角登录，由于 DTube 是搭建在 steem 区块链上，使用 Steemit 账号+post 私钥登录，如果没有 Steemit 账号，那你需要注册一个。

输入 Steemit ID 账号，注意登录密码一栏是输入 private post key。需要登录 Steemit 获取 private post key。

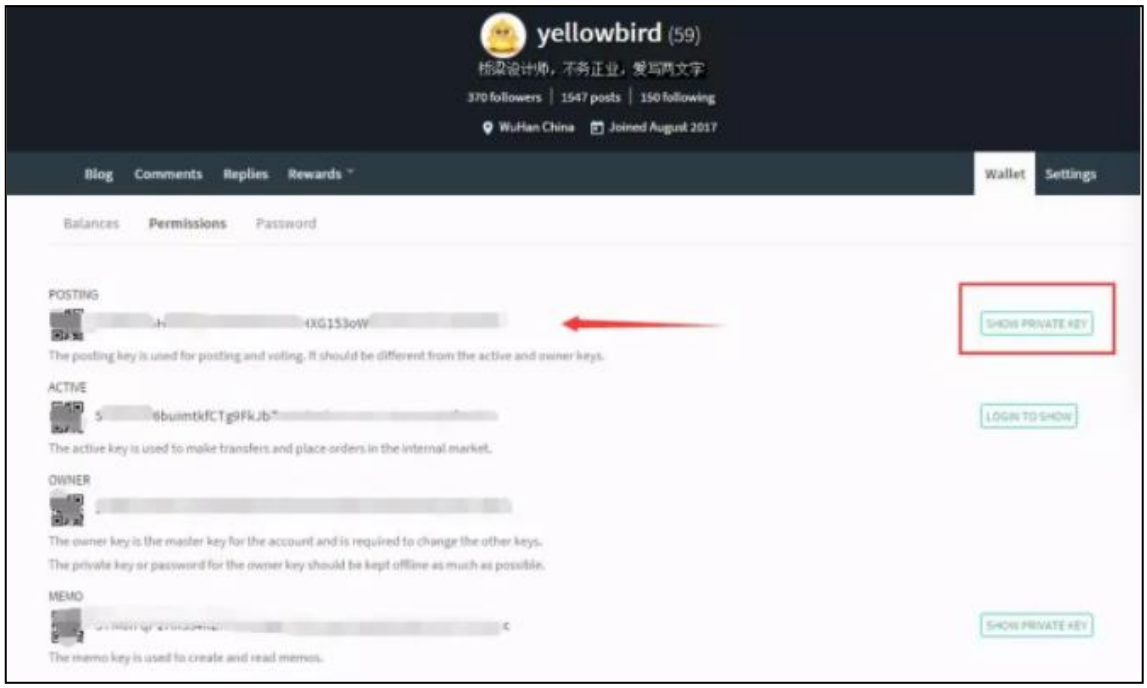


图22-14 需要 private post key 登录

进入在 Steemit 的钱包页面的 permissions，在第一行，点击右侧的 show private key，我们可以在左侧得到我们需要的 DTube 登录密码（密码千万不要泄露）。

2. 点赞留言

登录后，你就可以去访问大家分享的视频，可以给他们点赞和留言了。

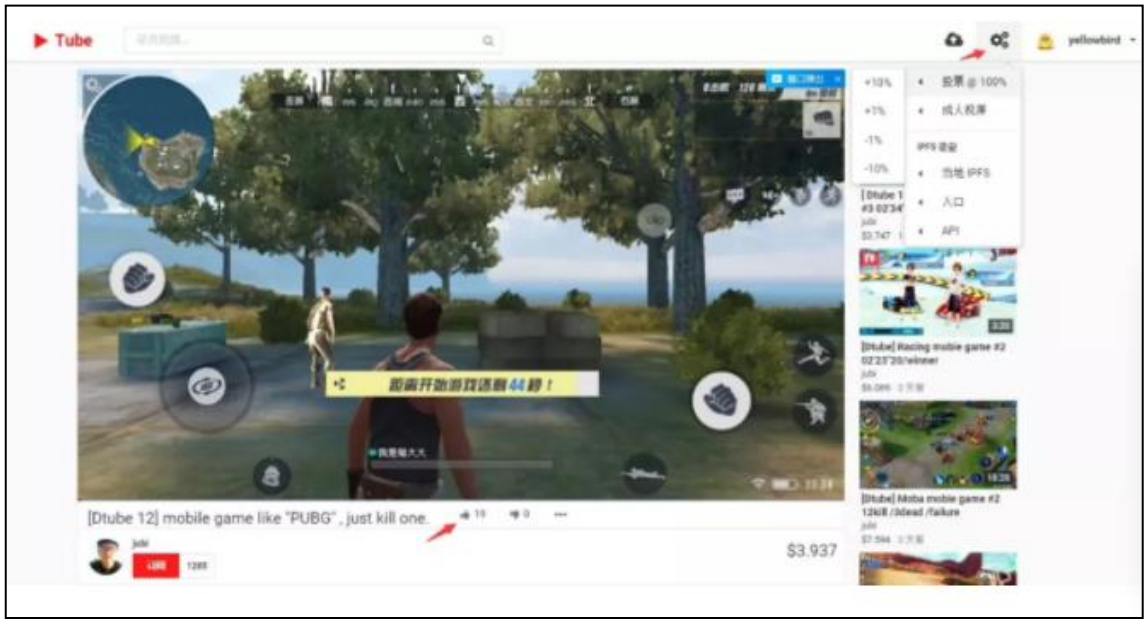


图22-15 Dtube 的点赞留言

如图，访问了一用户的游戏视频分享，在视频下面有一个大拇指的按钮，就是点赞。也可以留言，在这里的留言点赞是同步显示到 Steemit 上。

3. 分享自己的视频

在网站右上角有个向上镜头的云朵，点击进入上传视频的页面。按照步骤一步步操作。1、上传视频 2、上传封面图片 3、提交到区块链。添加标题，内容摘简要和标签（dtube 是默认标签，可自行再添加其它标签）。

图22-16 分享视频1

封面图片可以由 DTube 直接截屏视频获得。DTube 只支持用户自己上传视频，不支持其它视频链接。

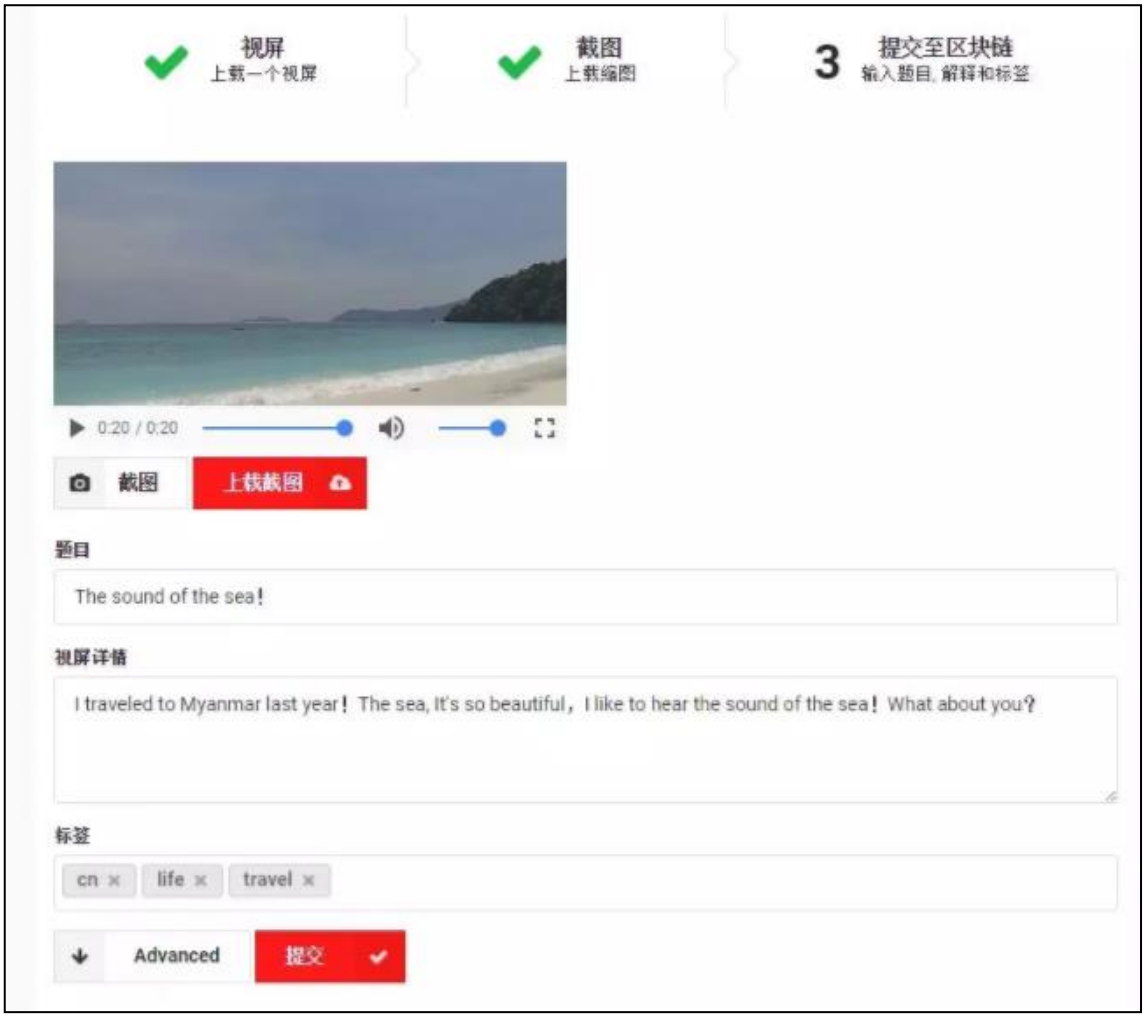


图22-17 分享视频2

跟 Steemit 上传图片一样，DTube 视频上传的速度很慢。在 Steemit 中发文上传图片，图片并不上传到 steem 区块链上。DTube 也是类似，不过 DTube 上传的视频接入了 IPFS 存储服务(一个去中心化的可能颠覆 http 网络协议的区块链项目)所有的视频将会上传到 IPFS 存储。

视频及截图上传完成后，填写标题，摘要及标签后就可以点击提交。提交完成后，弹出提交完成的信息，点击 WATCH YOUR VIDEO 你就可以查看你上传的视频了。同时 Steemit 上也自动分享了 DTube 上分享的视频。

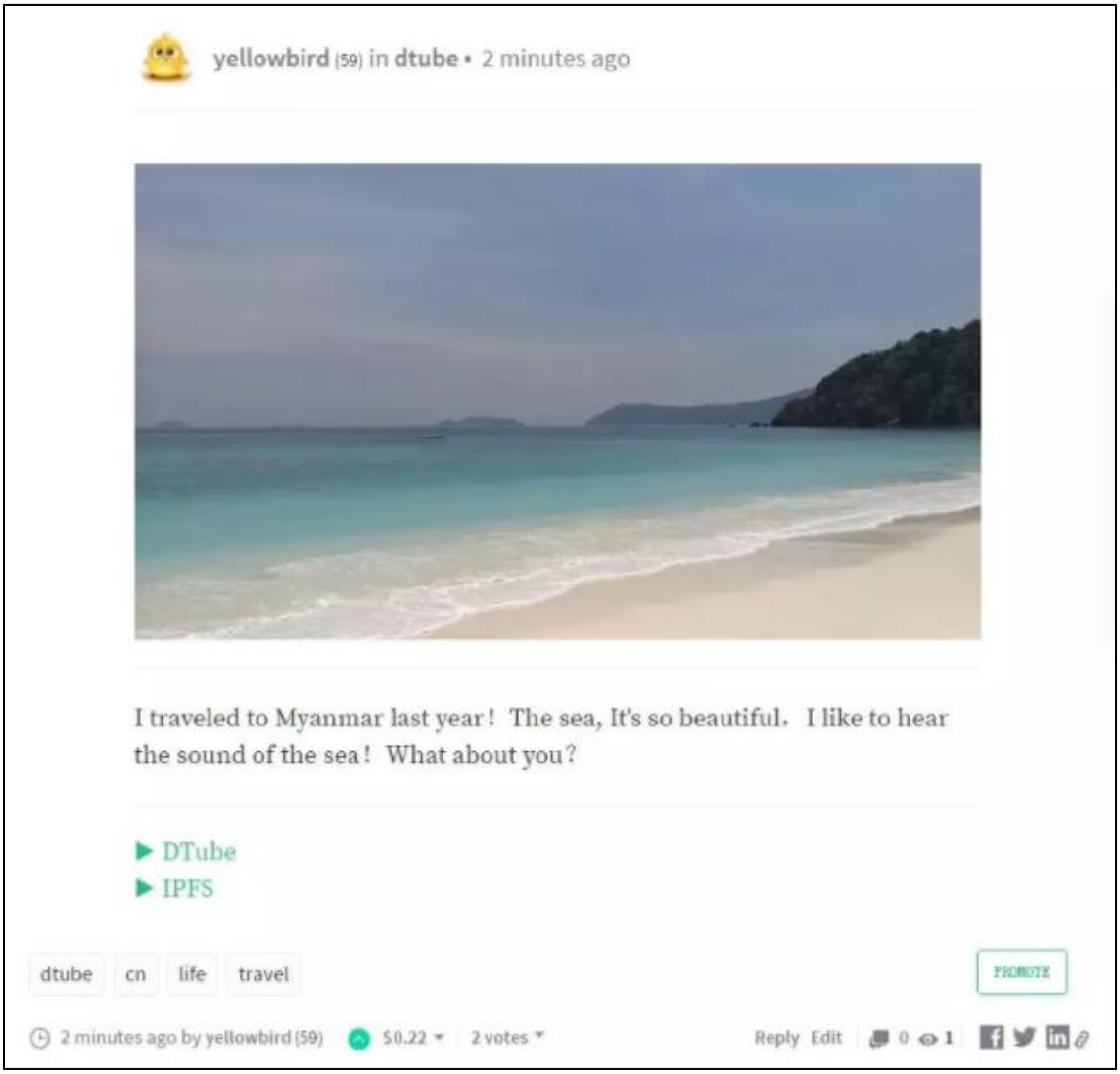


图22-18 steemit 里同步更新视频

在 Steemit 里同步更新的视频分享如上图，Steemit 里点赞在 DTube 里数据也是同步的。在 Steemit 里点击编辑，可以对 DTube 分享的视频摘要进行修改。

23 Steemit

23.1 Steemit 注册教程

23.1.1 Steemit 官网注册流程

1.点开 Steemit 官网的页面，点击 sign up 进入注册界面

2.输入账户名称

有以下几点需要注意：账户名称就是你的登录账户名称，这里面不同于国内很多网站除了账户名称还有个昵称，这里没有昵称，这里输入的账务名称就是你 Steemit 的名片以及登录账户。账户名称只能英语字母，没有大写。

个人建议取名尽量简单易记的英语单词(尽量不要汉语拼音或者一堆外人很难看懂的字母组合），这样有利于大家容易记住你，follow 你（关注你）。

3.填入手机号并验证

4.填入你的邮箱账号

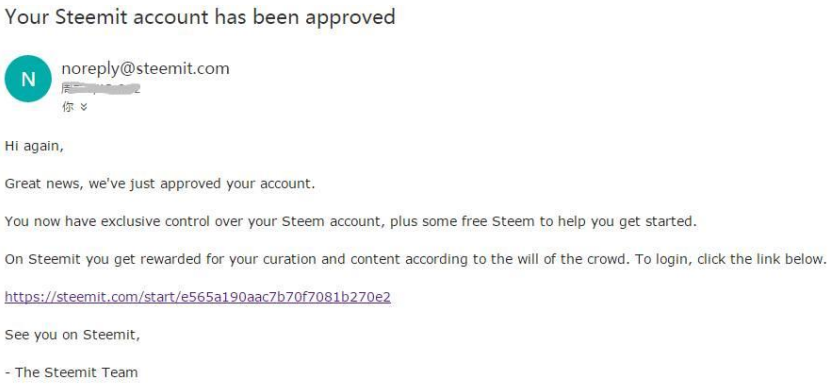
输入邮箱账号，点击提交后，如果提示验证失败，那么你可能需要科学上网。

5.科学上网完成邮箱验证

6.等待验证通过的邮件

大部分人的经验是一般需要 1-10 个工作日不等，当然也有其他情况发生，也可能一直没通过，如果长时间未收到邮件，注意在垃圾信箱检查一下，或者换台电脑（换个 IP）重新填写资料申请一次。

如果验证通过，你会收到这样的一封邮件：


Your Steemit account has been approved

N noreply@steemit.com

Hi again,

Great news, we've just approved your account.

You now have exclusive control over your Steem account, plus some free Steem to help you get started.

On Steemit you get rewarded for your curation and content according to the will of the crowd. To login, click the link below.

https://steemit.com/start/e565a190aac7b70f7081b270e2

See you on Steemit,

- The Steemit Team

图23-1 邮箱通过验证

注意，收到这封邮件，**远远还没结束**！

7. 保存私钥

点击收到的验证通过邮件链接，进入一下界面：

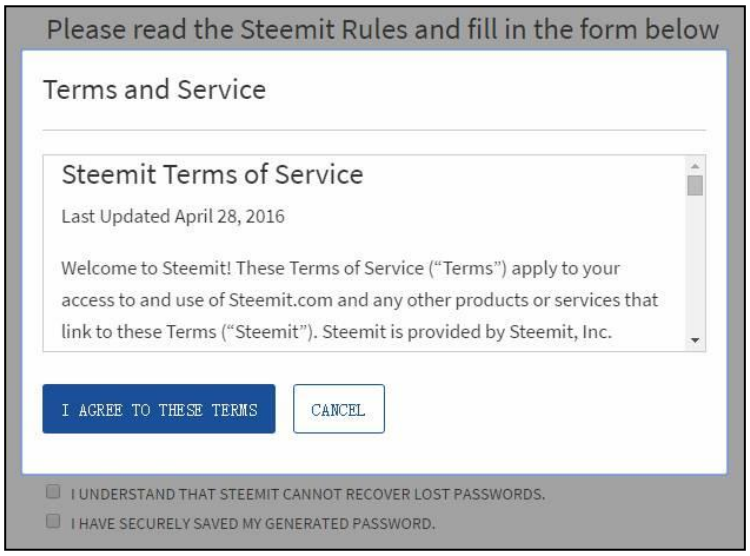


图23-2 同意许可条款

勾选下面两个复选框，点击同意后，就会看到下面的界面，红色部分一长串红色的字符串就是私钥，是你登录账户，操作账户（设置、转账等等）的唯一密码。

重要的事情说三遍：**务必保存！务必保存！务必保存！**如果遗失，任何人讲无法找回。

保存方法建议：直接用鼠标选中字符串，CtrL+C，然后新建一个 Word CtrL+V。把 word 加密备份到其他处，备份到其他电脑，备份到一个 U 盘（U 盘单独保存），或者 word 打印出来保存，推荐使用 KeePass 等工具保存。

不建议，手抄写下来。因为极有可能会抄错，有大小写之分。

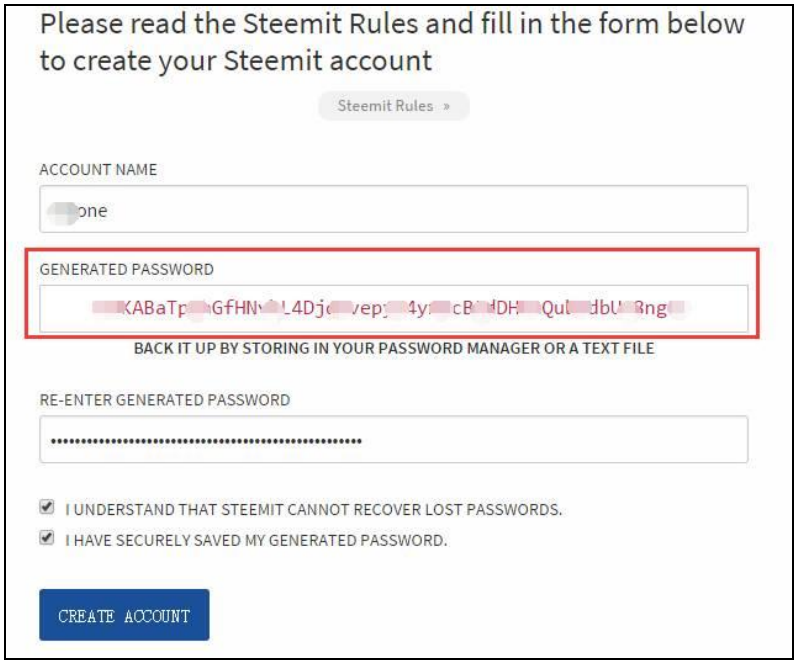


图23-3 私钥

通过 CtrL+C 和 CtrL+V 在下面的一行中输入密码确认。完成密码验证。进入下面的登录界面，CtrL+V 密码，完成注册。

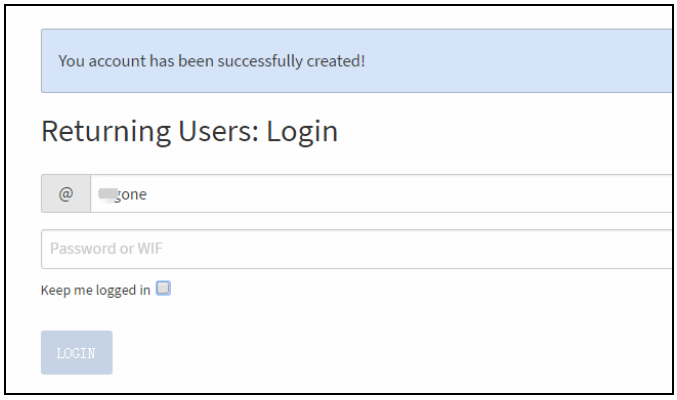


图23-4 登录 Steemit

完成注册后，你就可以开始探索 Steemit 的世界了。再次强调，务必正确保存好私钥，如果遗失任何人无法找回。

需要说明的是 Steemit 官网一直在更新，注册的流程和方法也随时可能在调整。按照提示一步步操作即可。

23.1.2 Steemit 快捷注册流程

官网注册审核时间较长，通过率无法保证，你可以尝试以下快捷方法注册。

方法一：利用已注册账号注册新账号，不需要科学上网，不需要手机号及邮箱，需要 6steem 代币，快捷迅速五分钟可注册成功。

（教程链接：https://steemit.com/cn/@lemooljiang/6hgzux）

方法二：利用已注册账号注册新账号，不需要科学上网，不需要手机号及邮箱，需要消耗已注册的账号 0.2steem 给新账号。快捷迅速五分钟可注册成功。

基于方法二，cnsteem 的创建者@skenan 开发了一个便捷的注册工具。注册详细流程如下：

1.注册详细流程

图23-5 steemit 注册

登录 cnsteem.com，在右上角点击注册进入 cnsteem.io，或者直接登录 cnsteem.io 填写资料完成注册。

输入你想要注册的用户名，邮箱地址，用户名如果被注册点击支付宝付款会有提示。

图23-6 填入注册用户信息

输入合适的信息，进入支付宝扫码付款。

图23-7 可以用支付宝付款

付款后很快会在邮箱里收到注册链接，点击进入。

图23-8 收到注册的密码

密码一览务必**先 Ctr+C 复制粘贴到 word 文档中，确保粘贴密码保存无误后，点击注册**。

图23-9 注册成功的提示

注册完成后，会提示注册成功。注意，还没有结束。由于账号密码是通过邮件直接发送过来，有泄露的风险，以及 cnsteem 平台发送邮件也可能有第三方保存账户密码的风险。所以，**你还需要登录账号，重置密码**，重置密码为了确保账号密码绝对安全。

图23-10 重置密码

登录账号，在“钱包—密码”一栏填写信息重置密码。

图23-11 备份好密码

输入当前密码，点击生成新密码，Ctr+C **把生成的密码复制粘贴保存备份（不建议手抄写，字母太多极易抄错），请务必保存备份好密码，遗失后任何人无法找回**。

保存好新密码后，Ctr+V 输入重新生成的密码，勾选，点击修改密码。

密码修改成功后，返回到登录界面，用新密码登录即可。

2.注册流程小结

1）填入用户名和邮箱；

2）通过支付宝支付价值 2 美元的人民币；

3）付款成功后，登录邮箱查看注册链接；

4）打开注册链接，牢记密码，点击注册；

5）注册成功，即可登录 Steemit；

6）登录官网 Steemit 重置密码。

3.注册中可能存在的问题

1）无法收到注册链接

请检查是否在垃圾邮件里，半小时后未收到，可以发邮件到 cnsteem@gmail.com 确认。

2）显示"注册失败,无法创建账号"

可能@skenan 账号里的 Steem Power 不够了，可以前往 https://steemd.com/@skenan 查看他的 SP 是否大于>30。如果不足了，可以发邮件提醒他，他可能需要一些时间进行充值。

3）创建成功了，但无法登录 Steemit

显示 incorrect password，你确定你记录了正确的密码吗？这种情况下，任何人没法帮你找回密码，只能换一个用户名重新注册。

4） 无法发帖提示 Voting Weight is too small

原因是刚注册的账户 steem power 太低了，需要增加自己的 steem power，如果是在 CNsteem.io 注册，可以到 https://cnsteem.io/delegate 免费申请 2 Steem Power（实际情况有时会提示领取失败）。

方法三：通过 BlockTrades 注册

访问 https://blocktrades.us,打开 buy steem account,按照账户注册步骤一步步操作。

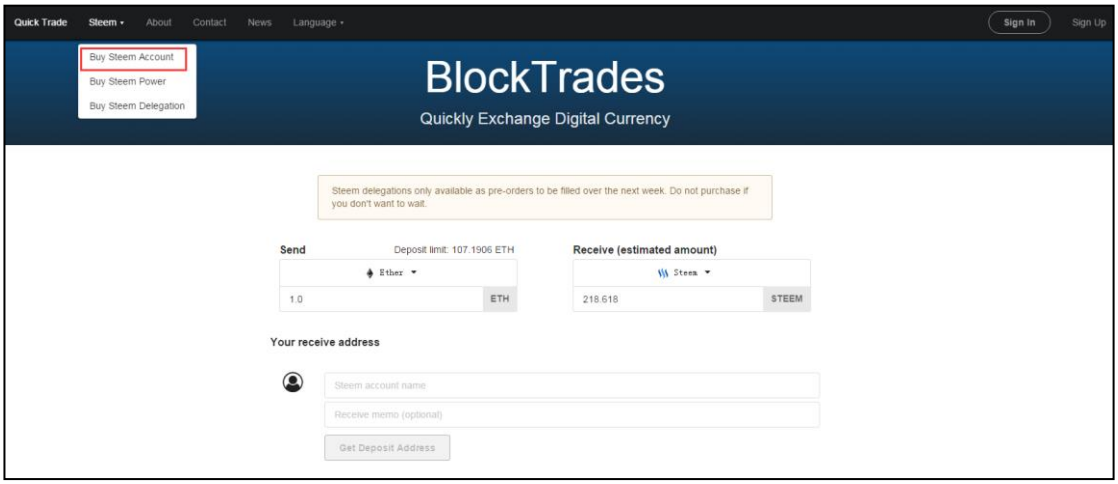


图23-12 登录 blocktrades

1. 填入你的账户名。

2. 把 BlockTrades 生成的密码复制到密码验证框。

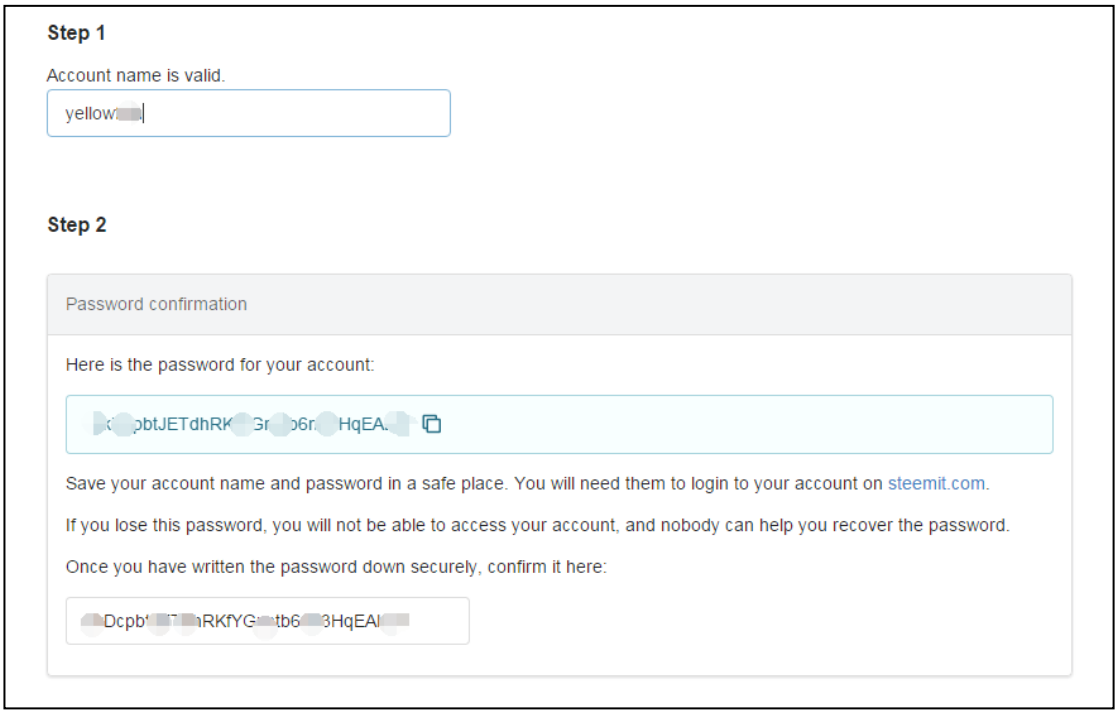


图23-13 保存好密码

3. 保存密码信息。点击下载密码信息，是一个 txt 的文件格式保存了账号的所有密码信息。

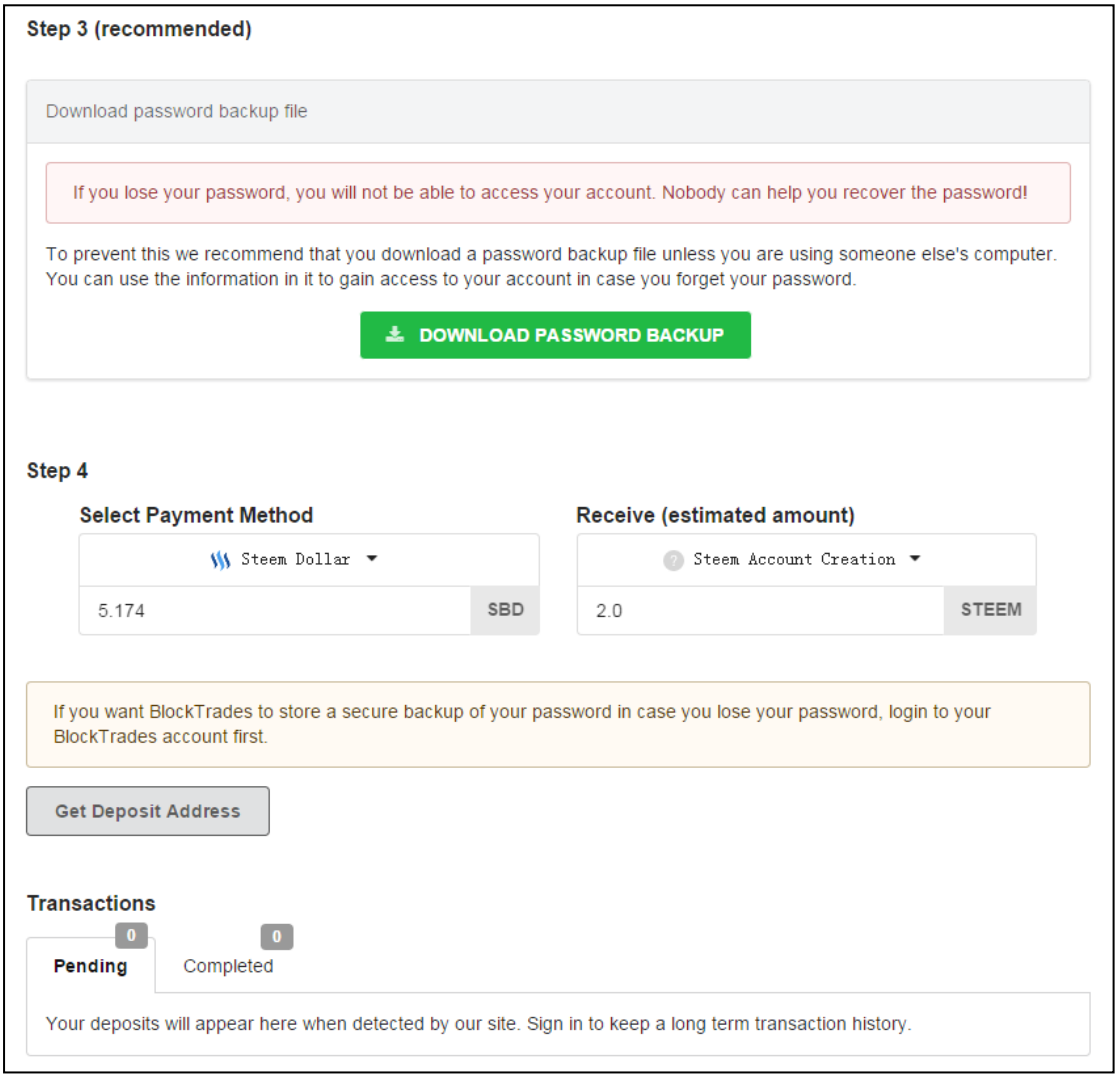


图23-14 下载密码并选择支付方式

4. 选择付款方法。在 select Payment Method 可以看到多种加密货币的付款方式。

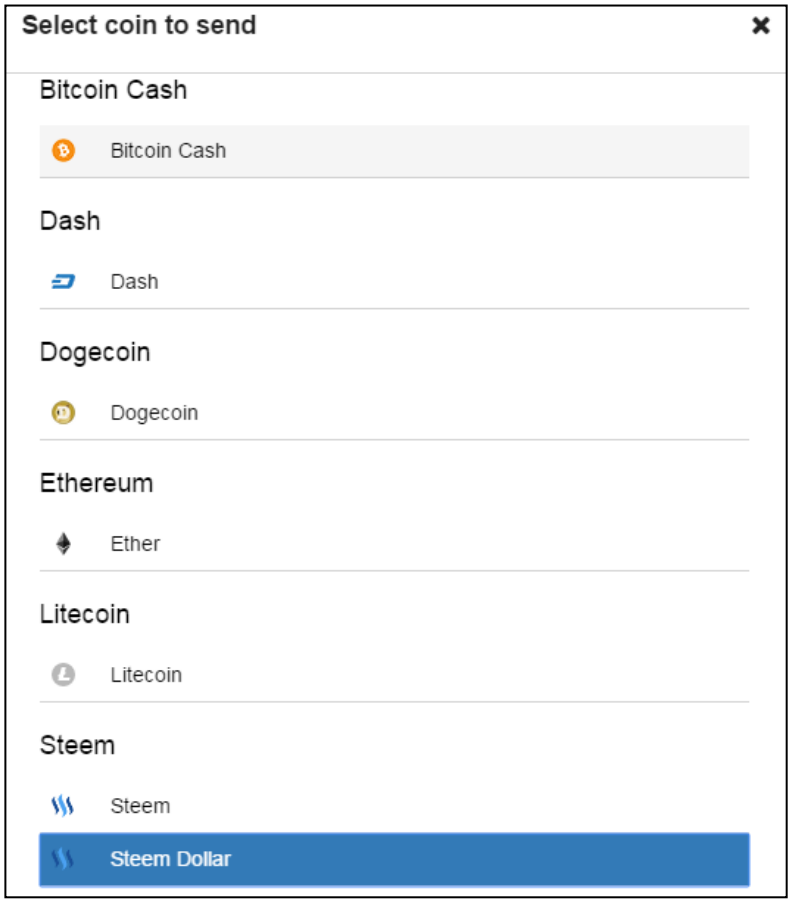


图23-15 可以用多种数字货币来付款

选择付款方式的下面有一行信息，提示可以登录 BlockTrades 账户帮忙保存密码，建议还是个人保存。

5. 点击 Get Deposit Address，得到充值地址信息 Manual Transfer，按照提示给充值地址发送对应数量的加密货币。注意，充值时一定要填上 Memo 信息。

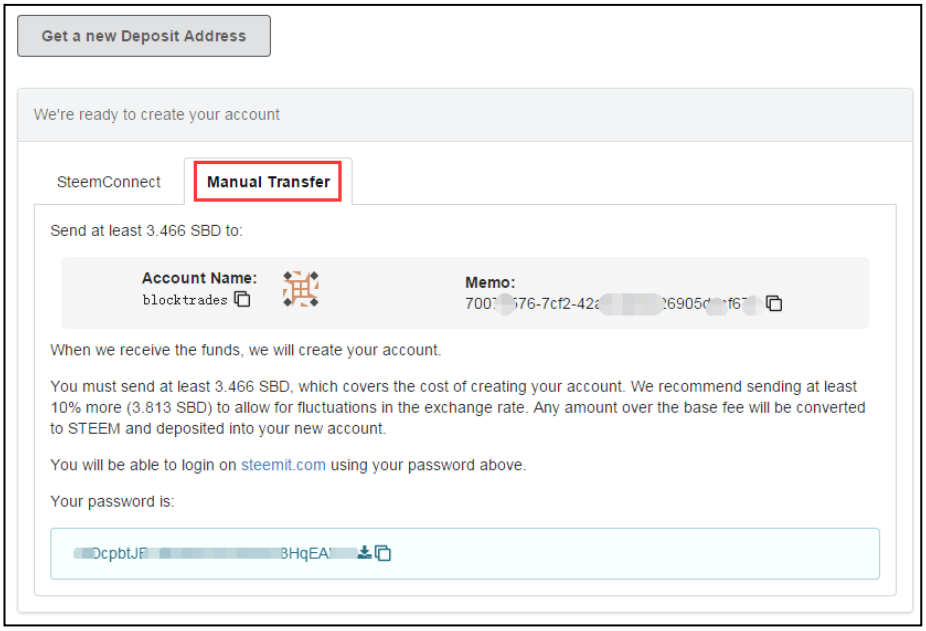


图23-16 充值操作

比如，用已有的 Steemit 账户中的 SBD 来注册为例，通过转账方式给 blocktrades 账户按照提示转账 3.466SBD，务必填写备注信息，点击提交后完成注册。

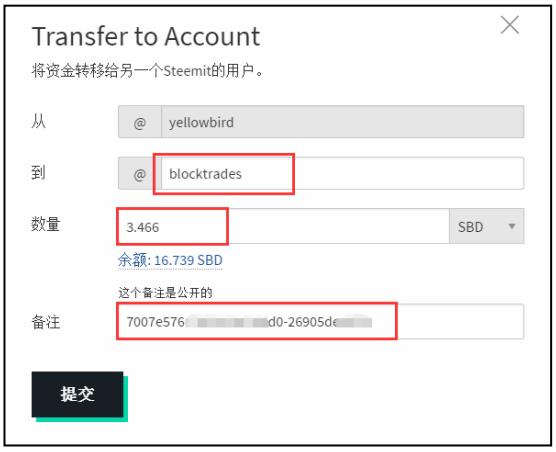


图23-17 转账操作

最后，登录新注册的账户，如果不放心由第三方程序注册的密码安全，可以按照方法二的步骤登录官网 Steemit 重置密码。

小结：方法二及方法三快捷注册相比官网注册需要付出一点费用，这里提供了用法币及其它加密货币付费注册的方法，已经能满足大部分的注册需求。

23.2 Steemit 网站基础常识

23.2.1 小旗是“踩”

图23-18 Steemit 中‘踩’和‘点赞’

每篇文章右上角的小旗图标在 Steemit 里是 downvote，即差评的意思。对于刚踏入 Steemit 的新手极易出错。这样的设计有些反常规，见到 Flag 会本能地想到是给文章做个标记，可能是收藏功能吧，GTD 里把小旗设计为重要事项。

23.2.2 多种密钥

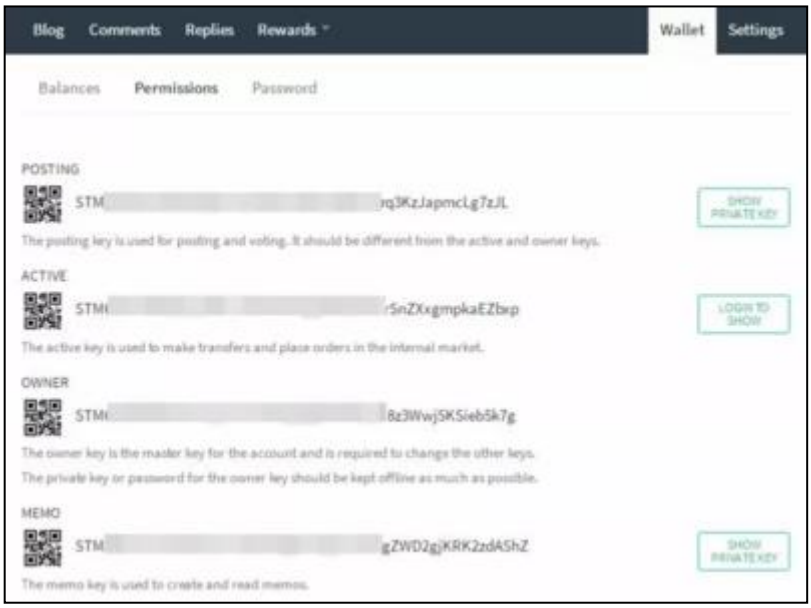


图23-19 Steemit 中多种秘钥

注册 Steemit 时要求**牢记私钥、牢记私钥、牢记私钥**，这种事情在区块链的世界里比较容易理解，因为私钥就是区块链资产的全部，但进入了 Steemit 里的钱包设置时，有 4 个公钥+3 个私钥，分别对应于 Posting、Active、Owner 和 Memo 四种权限，Posting 对应于发文章和点赞的权限 ，Active 对应钱包转账的权限，Owner 权限最高，Memo 是写评论的权限。

23.2.3 向上的箭头是点赞

常见的社交平台中点赞图标是个大拇指，而在 Steemit 里简化为一个向上的小箭头，放在文章的左下角，点赞操作会记录在区块链里，有时候延迟得比较厉害，多点一次可能变为“取消点赞”了。

23.2.4 推广 promote 不是打赏

在每篇文章的右下角有一个大大的“PROMOTE”按钮，容易误认为是打赏功能了，在支付 SBD 操作后。这笔钱送入一个销毁地址，相当于花广告费给文章做了推广。

23.2.5 转发

图23-20 Steemit 中转发、留言

转发别人的文章在 Steemit 里称为 resteem，是在 reply 左侧的一个弯曲箭头的图标，新手开始容易把它当成回复功能。

23.2.6 标签

Steemit 里最多只能设置 5 个标签，在 Steemit 里很多人可以双语写作，英文基础一定要过关，关键词起得好，也能增加一点浏览量，对于中文用户记得常用 cn 标签。

23.3 Steemit 里的三种货币

关于 Steemit 里的三种货币 Steem、Steem Dollars、Steem Power，对于每个新手来说都是个疑问。

这三种币的区别，最官方权威的解释可以在 Steemit 网站里的 FAQ（常见问题）里找到，

英语好的朋友建议自己到官网上去阅读。

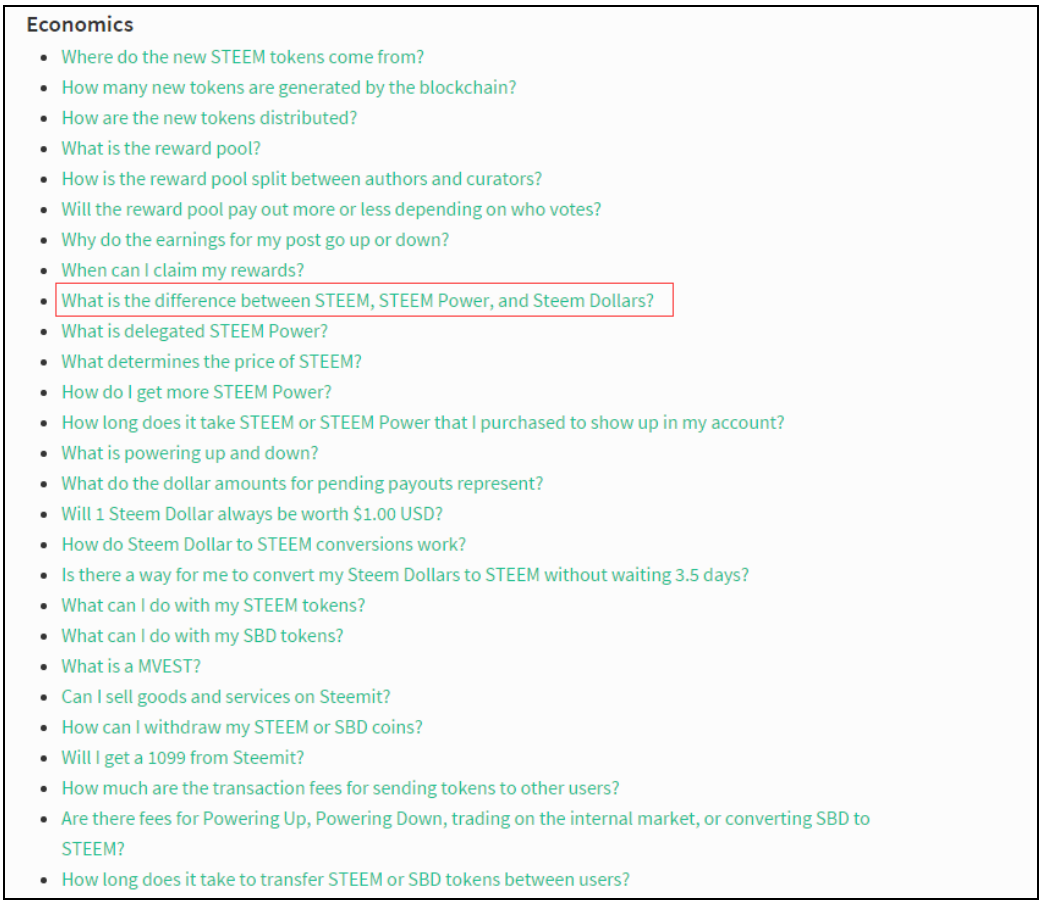


图23-21 Steemit 官网的 FAQ 问题列表

23.3.1 区别 Steemit 和 Steem

对于新手来说，Steemit 和 Steem 有时会傻傻分不清楚。发文时类似于“欢迎来到 Steem”，“我第一次来到 Steem”，“写文章可以获得 Steemit”等都是错误的表达。

Steemit 可以简单理解为网站，我们用来发文的前端网站，它是一个基于区块链的社交平台，在后端它与 Steemit 区块链交互，是一个生态系统（运行着三种货币的生态系统）。

Steem 是 Steemit 的代币，可以把 Steem 理解为比特币、以太坊里的 BTC 和 Ether，它是 Steemit 区块链上发行的虚拟货币。如果你理解比特币和以太坊，那么你就很容易理解 Steem，比特币的区块链在每一个新区块产生的时候就会产生比特币，只不过新产生的比特币是分配给矿工的。在 Steemit 区块链里没有矿工，它是基于一种叫做石墨烯的区块链技术，采用见证人取代矿工来生产区块，分配到系统里。

23.3.2 区别 Steem 与 Steem Dollars、Steem Power

对于一个区块链，有了 Steem 代币本来是没有 Steem Dollars、Steem Power 什么事的，就像比特币和以太坊一样。

Steem 是无限增发的，Steem 以每年 9.5%的膨胀速率产生新代币，只不过这个膨胀速率随着更多区块的产生会慢慢下降，这个速率会一直持续到整体的膨胀率达到 0.95%。它的这种机制不同于固定数量的比特币。所以，我猜是因为价格不稳定，才又创造出 Steem Dollars 和 Steem Power，它们是只存在于 Steemit 系统里的货币，而 Steem 可以在市场上交易。

Steem 与 Steem Dollars、Steem Power 之间可以转换，当然也有一些规则。比如 Steem Power 转 Steem 就不那么容易。

Steem Dollars 是与美元几乎等值的“货币”，在 Steemit 的生态里你可以用 Steem Dollars 买东西，它的价格浮动是与美元挂钩的，有些像一些内盘交易所里的 bitCNY（与人民币等值的平台货币）、USDT（1USDT=1 美元），虽然 Steem Dollars 设计为锚定美元，最后实际情况在 2017 年的牛市里超出的 1 美元的锚定，这或许是它设计失败的地方。

Steem Power 更像是 Steemit 这个去中心化公司的股权，也代表你在 Steemit 生态系统里的权重。Steemit 里的点赞权重越大的，票数越多，这就是为什么一个新手的点赞和一个大鲸鱼的点赞在收益上区别很大的原因。你的 Steem Power 越高，你在 Steemit 生态里的话语权就越大。

Steemit 区块链里每一次产生的新代币，75%发配到奖金池，用于作者的奖励和助力者的奖励（助力者可以理解为点赞、点踩、评论等对文章分发助力的一部分人）。 15%的新代币用于奖励给 Steem Power 的持有者。剩下的 10%奖励给区块链的提供动力的见证人（类似于比特币的矿工，但在原理上不同于矿工）。

所以，基于此，我们大概可以得出结论：

1）Steemit 是希望大家拥有 Steem Power，在早期的版本里，90%的新币是分配 steem power，作者在早期的版本是收益一篇文章的 70%，现在调整到 75%了。目前版本已经迭代了到第 20 个版本了。这是一件好事，系统是可以根据情况来做修正和迭代的。

2)作者发布文章可以选择收益为 100%的 Steem Power 或者 50%的 Steem Power 加 50%的 S

teem Dollars。Steem Power 适合长期看好 Steemit 的，类似于股权，有利息。15%的新币会分配给 Steem Power。所以，也有相当一部分买入 Steem 转化为 Steem Power 拿利息。

3）Steem Dollars 适合短期套现，因为与美元挂钩，也无需担心 Steem 代币的价格过大波动。

23.4 Steemit 里代币交易转账

23.4.1 通过 BlockTrades 交易 steem

Steem 作为 Steemit 平台的代币，可以提升(power up)为 Steem Power。Steem Power 越多，点赞的权重越大，同时 Steem Power 还有利息，如果长期看好 Steemit 可以选择投资购买 Steem Power。

购买 Steem 主要是在国外的币币交易平台，比如 bittrex 或者去中心化的 bitshares，还有币安。对于大额的投资交易，建议去大的交易平台。而对于新手，涉及交易量不大的，这里推荐并介绍一种简单的兑换方式，BlockTrades 平台。

在 Steemit 个人账户页面的钱包下，有一个通道“buy steem or steem power”点击一下就直接进入 BlockTrades。

图23-22 购买入口

BlockTrades 界面如下：

图23-23 进入 blocktrades

首页上的英语介绍非常明了，“快速兑换数字货币”，在 send 和 receive 上，大家可以发现支持多种货币间的兑换。这里的兑换会比交易所的损失高，你输入数值可以查看兑换情况，损失情况可以自行对比。

这里，如果交易量大不建议采用这种方式，如果交易量小，考虑各种平台间的兑换转账损失，其实这种方式的成本会更低。

国内取消了所有的 ICO，之前参与 PressOne 众筹退回来的一些 BTC，现把 icoinfo 平台上的币直接兑换为 Steem。

图23-24 兑换

具体操作：

1）Send 务必选择你手里有的币，比如 BTC。

2）Receive 务必选择你要兑换成的币，我选择的是 Steem。

3）填写你的接收地址，这里只需要填写你的 Steemit 账号，比如 yellowbird。基于石墨烯区块链技术的 Steemit 和 bitshares 的收款地址都是账户名形式,不像比特币那样的一长串字符。在注册时，账户名已经被写入区块链，所以也是唯一的。

4）填写标签，这个随意，主要方便区别。

完成以上操作后，就可以点击获取一个充值地址。如下图，英语提示“使用你的钱包，发送任何数量的 BTC 到下面的地址”。

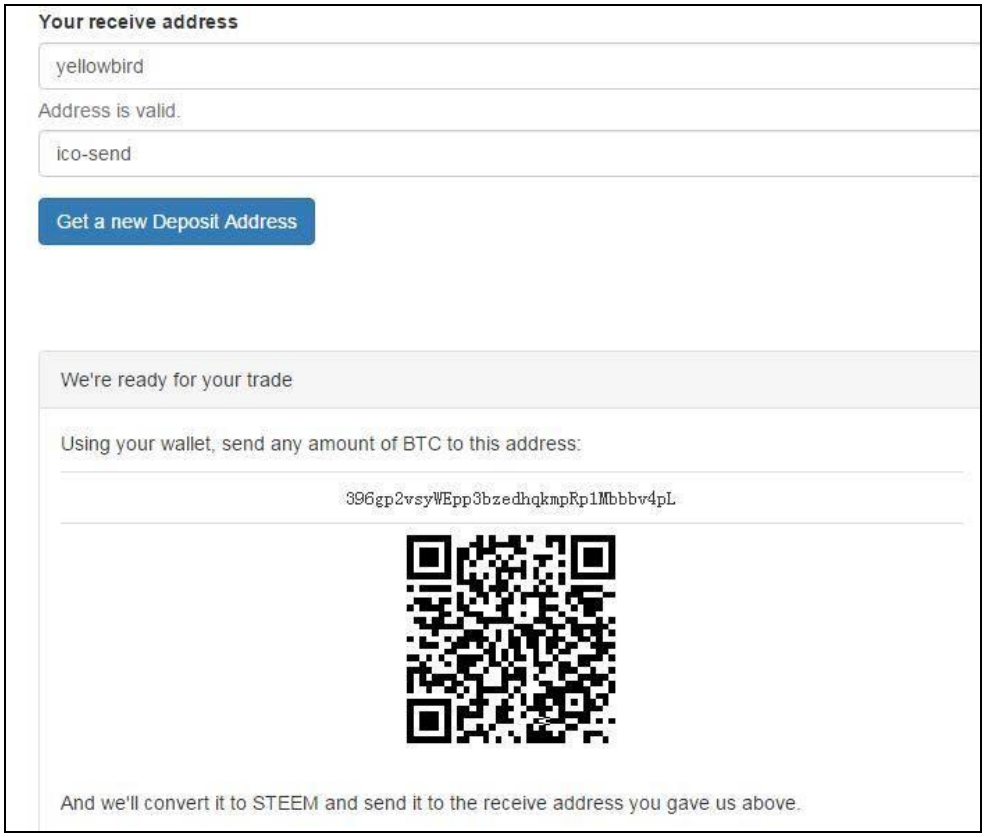


图23-25 发币

再用 BTC 钱包向那个地址转账,或者从交易平台提币到该地址,直接从 icoinfo 平台提币，如下图，填好提币地址之后，确认，然后就是等待了。

图23-26 交易平台提币

这次提币由于平台收取的矿工费很高 0.002BTC，大约 3 个多小时，Steemit 上就收到了兑换的 Steem，在历史信息里可以看到兑换成功的记录。

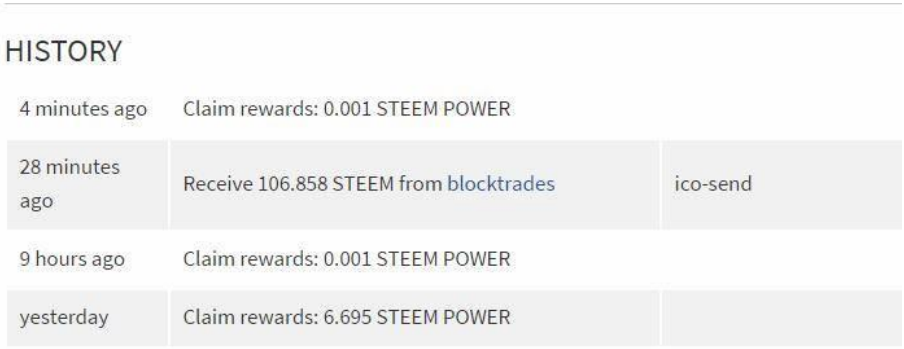


图23-27 兑换记录

至此，兑换成功的 Steem 已经充值到了平台账户，Steemit 就是一个简化版的网页端钱包。

BlockTrades 里还支持把 steem 兑换成 BTC、ETH、BTS 等主流货币，学习一些区块链私钥、钱包地址等基本知识后，大家可自行尝试。

23.4.2 steem 内部交易市场

Steemit 写文章收益的是 SBD 和 SP，通过前几期的文章大家已经知道 SBD 是锚定美元的代币，基本没有价格波动（在 17 年下半年的一波牛市中，SBD 的锚定失效，高于 1 美元很多）。如果看好未来 steem 的价值，可以考虑把 SBD 换成 steem 代币。

那么如何在价格低位时，用 SBD 买入 steem 代币呢？

进入 steem 内部交易所，在 BUY STEEM 输入买入 steem 的价格和数量，点击购买就可以委托交易订单，如图下：

图23-28 steem 交易图

交易订单委托成功后，如图下，显示已经挂单成功。

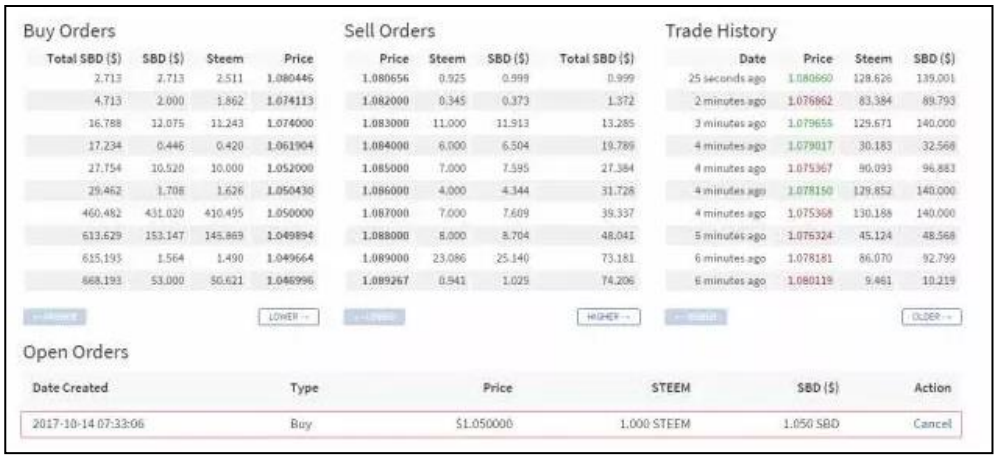


图23-29 steem 交易挂单成功

挂单时 steem 交易所的价格在 1.08 左右，一天后价格降到 1.05，我挂出的交易单成功交易。交易成功后，可以在自己的钱包界面下看到到账的 steem。此处需要说明的是，**steem 的交易所无交易手续费**。

图23-30 steem 交易无手续费

图上的 steem 不等于 SP，SP 是被锁定的 steem。

23.4.3 把 steem 提现到交易所

换成的 steem 可以提现到交易所，换成大家想持有的其他币种，比如比特币等。目前主要有以下几个交易所可以交易 steem，比特股内盘，Bittrex，还有币安。

下面举例实操如何把 steem 提现到币安。

图23-31 Steem 充值地址

登录币安，找到 steem 充值，可以查看到 steem 充值地址及充值备注。

图23-32 在 steemit 里转账

登录 Steemit 账号，在钱包页面的 STEEM 一栏点击“转账”。

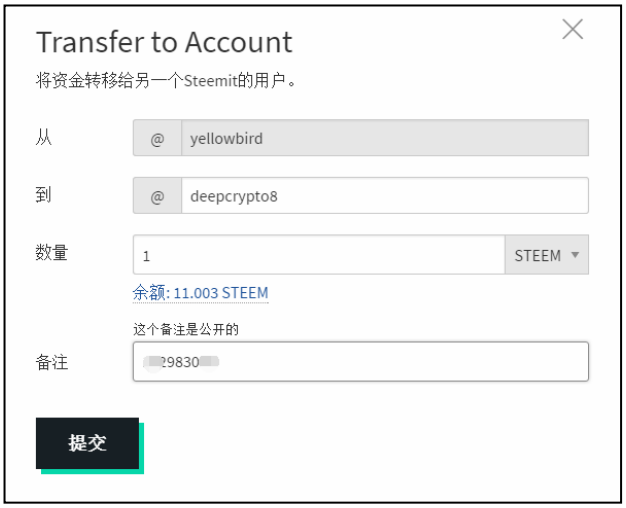


图23-33 填好转账金额和备注

进入转账页面，把币安上 steem 充值地址 deepcrypto8 填入第二行，把 steem 充值备注填入最后“备注”一行。这里需要注意：所有用户币安的 steem 的充值地址是一样的，只是每个人的备注不一样，**充值时必须正确填写充值备注**。

充值信息确认无误后，输入 Steemit 主密码，完成充值转账。完成后，可以在自己的钱包页面下看到转账的历史信息，正常情况下大概 1 分钟左右，就可以在币安收到 steem，steem 充值无手续费。

23.4.4 如何给他人账户转账

在 Steemit 里，和其他区块链资产一样，可以把资产从一个钱包转到另外一个钱包。在 Steemit 的钱包页面，Steem 和 Steem Dollars，下有个 Transfer，点击它。

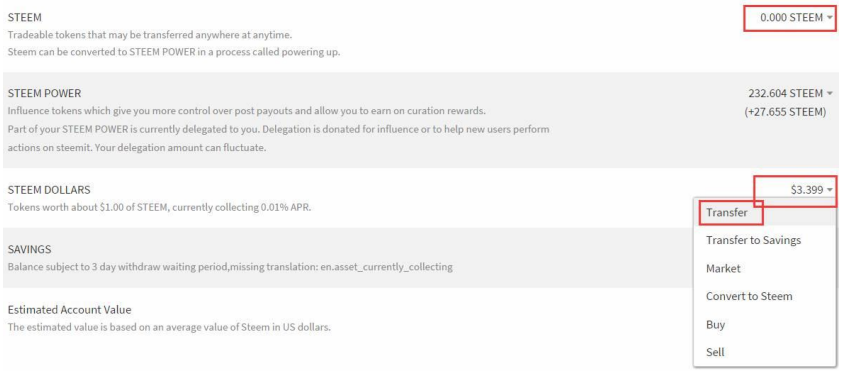


图23-34 给他人转账

在这个界面里，假如要给@speeding 账户（钱包）转账 0.001SBD，操作很简单，填写上接收方的账户名称，输入转账金额，确认。

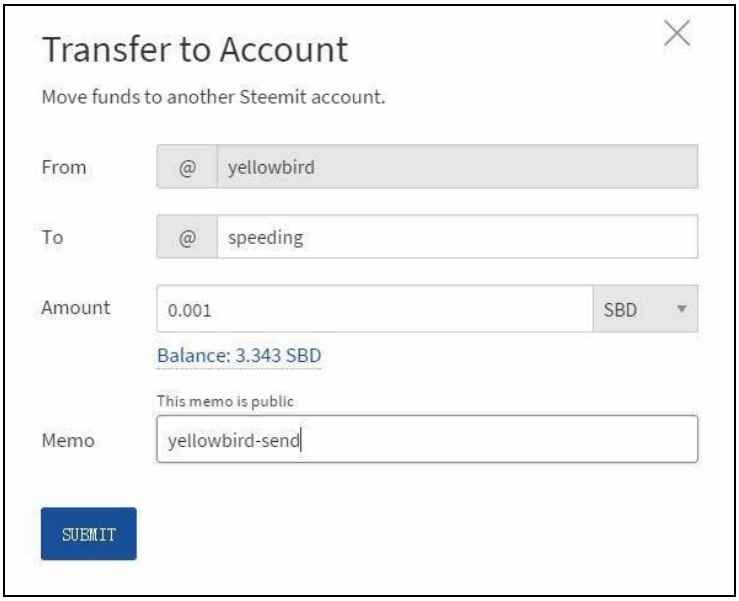


图23-35 转账界面

确认后，就需要你输入密码，就是注册时的私钥。

图23-36 需要私钥

确认之后，在历史信息里就会看到转移了 0.001SBD 到另外一个钱包（账户）。Steemit 是基于石墨烯的区块链技术，转账几乎是秒转，这比比特币和以太坊来说，转账体验真是好了不知多少倍。另外，Steemit 账户间的转账不收取手续费或者类似比特币那样的矿工费。

图23-37 转账历史记录

23.5 Steemit 网站写作

23.5.1 Steemit 写作基本认知

1）Steemit 会被越来越多人知道

李笑来《财富自由之路》40 页写到：微信订阅号培养了无数作者，给更多的文字工作者以更多的机会，已经是不争的事实；国外甚至出现了基于区块链的版权确认和分发系统（例如：steemit.com）——靠创作赚钱，甚至赚大钱，已经成为越来越多人的机会。

Steemit 已经不是一个秘密，随着国内更多类似的区块链（YOYOW，币乎，Ulord）应用起来，基于区块链的内容写作创新模式将会被越来越多人知道和使用，而最早一批接触它的人也必将享受初始红利。

同时，我也发现 Steemit 早一批前辈也在努力致力于 Steemit 中文社区的发展和推广，随着更多的人在这方面的努力，进入的成本也将越来低。

2）Steemit 的区块链属性

（1）信息的不可篡改性

Steemit 里的信息具有不可篡改性，你在 Steemit 上的任何操作（点赞，修改，删除）都会被系统记录下来保存在 steem 的区块链上。当你的文章发表后，7 天之内还可以对文章进行修改，7 天后文章将无法修改。

在 Steemit 里文章修改编辑相当于重新发表一篇文章,任何人可以通过调用数据读取你的原始文章。点赞、点踩、评论、转账，转给谁转多少都被记录到区块链中。所以，Steemit 世界里没有秘密，任何抄袭、谎言等都可以追溯查询。

（2）去中心化——内容无法删除，永久保存。

玩 Steemit 的一位作者曾描述他为什么来 Steemit，他之前是在某个网站上写博客的，写了很多年，后来那个网站倒闭，他的那些文章也无法找回，于是，他来到了 Steemit。

我们现在的世界主要由中心化的系统组成，比如微信靠腾讯，微博需要靠新浪的中心化公司来提供服务。而 Steemit 是去中心化的，不需要这些中心化的公司就能运作。相比中心化的系统，Steemit 里的留存的信息更加安全，理论上所有的信息将永远保存，无法删除。 2014 年 10 月据说有一对新人 David Mondrus 和 Joyce 就把结婚誓言写在了比特币的区块链上，被永远保存，无法删除和修改。

（3）steem 代币的货币属性

区块链代币具有天然的货币属性，解决了交易的信任问题，货币的唯一不可复制性，可以自由流通。

steem 以及 Steem Dollars 是不同于 Q 币的。不过 steem 也不同于比特币，steem 的发行机制是无限增发的，这涉及到 **steem 上的三种代币**的区别：steem 是平台的基础货币，可以在市场上交易。Steem power 更像是这个去中心化公司的股权，Steem Dollars 的存在是为了保证平台经济系统的稳定性与美元基本等值的货币。

（4）私钥

Steemit 注册时，反复强调一定要保存好私钥，这是账户的唯一密码，如果遗失任何人无法找回。

23.5.2 Steemit 写作的心态

Steemit 博主 myfirst 说，以前刷微信时间多，现在刷 Steemit 时间多。Steemit 博主 tumutanzi 说，爱上 Steemit 后，X 生活都没时间了。

刚刚接触 Steemit 是容易让人中毒上瘾的，Steemit 因为创新的内容激励和分发模式，让写作变成一件很容易赚钱的事，这在以前是不可想象的。当很多东西跟钱产生太多联系后，我们很容易忘掉自己写作的初心。

Steemit 博主 tumutanzi 的文章《在 steemit 上写作不要忘了初衷》中提到：通过持续写作输出思想，交结朋友，从而再次扩大知识面和吸收新的思想，至于点赞收入，那些都是水到渠成的事情。Steemit 博主 yellowbird 的文章《Steemit 上写作的“损失厌恶”心理现象》中提到，Steemit 上写作不要因为过分关注收入增加还是减少掉进“损失厌恶”的心里陷阱。

写作迷茫时，都是适合翻出来读一下的。 在 Steemit 上按照正确的方法长期参与坚持下来，我相信一定会有不错的收获。

23.5.3 Steemit 写作的社交性

很多从公众号、简书、微博等其它传统内容平台过来的作者们容易在一开始就对 Steemit 产生一些误读。

误读 1：Steemit 是一个类似微博、微信朋友圈那样的重社交网络。

现象：像微博那样发帖子，一篇文章几句话，或者配一张简单的照片。对于很多刚刚来 Steemit 的新手来说经常可以看到这样的内容。

误读 2：Steemit 是一个类似公众号、简书那样的写作平台。

现象：像公众号和简书那样发长长的一篇文章，文章质量很高，但是关注和点赞确很少。

对 Steemit 的正确理解它是一个“内容社交”网络平台。首先，Steemit 里需要有“内容”，其次，Steemit 有很强的社交性。

在 Steemit 里“内容”与“社交”是相辅相成的，大家通过每个人长期的内容文字，大概了解

在你文字下你是怎样的一个人，大家有共同的兴趣、价值观或者共同的利益（比如赚钱）然后关注（follow）你产生社交，然后由已建立的社交关系，持续关注你的文章内容。对于个人想要提高自己的被关注度，也需要主动去社交，比如主动去阅读他人文章点赞评论留言等。

Steemit 不是一个熟人关系的网络，不能像微信朋友圈那样的发张照片写段简单的文字记录自己的日常生活,在 Steemit 里这样的内容不是优质内容得不到更多的点赞和收益。同样的，一篇长长的有深度有内容的文章而没有因社交传播出去，在 Steemit 也不算优质内容。

Steemit 里的优质内容是跟社交有强烈关联的。Steemit 里常常可以看到一篇都是程序代码的文章，对于不少非程序员的人毫不夸张的来说一点儿都看不懂，这是优质内容吗？对于长期写干货文章的人来说，看到一篇旅游帖的收入很高，完全不能理解，在他们眼里那是优质内容吗？

在 Steemit 里程序代码、旅游帖、绘画等内容都有很强的社交性，都可以通过内容连接起来同样一批兴趣相投的人，这些可以产生社交的内容在 Steemit 里都是优质内容。

所以，对于刚加入 Steemit 的新手来说一篇自我介绍是有必要的，可以介绍下你的职业，你所在的城市，兴趣爱好，写作类型等等。

23.5.4 Steemit 写作的注意力经济

Steemit 上每个作者都在争取获得更多的阅读量获得更多人的注意力和点赞。Steemit 上的文章将会越来越多，大家的注意力将会被分散。所以，Steemit 上的写作需要善待读者的注意力。

（1）不要过于频繁的发帖频率。Steemit 的社区大神 @abit 曾提到过每天不要超过 4 帖，40 个投票。出于减少对大家注意力的干扰，建议发帖频率不宜过大，你可以想象一关注了一个人，一天给你发十多篇文章，刷屏霸屏是多么让人生厌的事。

（2）增加文章的易读性。可以使用 markdown 模式以及多给文章配图来改善文章排版的易读性。

（3）Steemit 上写作建议轻量化写作，建议字数控制在 1000 字左右为宜，大家的注意力很重要，长篇大论影响读者快速阅览。

24 YOYOW 区块链

24.1 YOYOW 是什么

YOYOW 白皮书上是这样介绍的：

> YOYOW 的名称来自英文 You Own Your Own Words，其目标是建立一个利用区块链技术，使用去中心化的共识方式为内容生产领域进行贡献定价和权益回报的网络，使内容生产者，内容投资者、内容筛选者和生态建设者都能得到合理的激励与回报。

YOYOW 的设计初衷是构建一套合理的内容收益分配机制，同时构建一个基于用户内容评价的价值网络。无论是文本、视频、图片、音频甚至直播类为主题的内平台都可以适用 YOYOW 网络构建出对应主题的内容激励平台。各平台之间，使用统一的内容评价算法对内容进行评价。内容生产者、内容投资者、内容筛选者以及平台建设者都将围绕 YOYOW 生态，基于用户对内容的评价来获得相应的合理回报。

YOYOW 背后的团队来自中国。如果你熟悉 STEEM，那么看到上面一段介绍，你可以把 YOYOW 理解为中国的 STEEM。

YOYOW 和 STEEM 一样都是基于区块链技术的内容激励网络，但是从各自的白皮书中，仍然是有所异同。

24.2 YOYOW 与 STEEM 的相同点

1）区块链的共识机制相同

YOYOW 和 STEEM 都是采用的 DPOS 共识算法，区块的产生，见证人制度等都是类似的。区别于比特币的 POW（工作量证明）机制，DPOS 共识算法不需要消耗算力，与全球公司的股份制类似。

2）都是做内容激励平台

STEEM 与 YOYOW 都是专注内容激励的区块链网络，STEEM 和 YOYOW 都是平台生态的发展方向，做基础网络，都具有平台特性。其它内容应用可以在这个网络上搭建。

YOYOW 里提出了社交媒体平台，博客、百科、论坛内容平台，问答类内容平台，门户网站平台，视频点播/直播内容平台，内容聚合类平台，存证服务于版权维权等应用场景。

STEEM 提出 SMTs 也是让更多的内容相关应用公司可以更容易的在 steem 上搭建。

24.3 YOYOW 与 STEEM 的不同点

1）评价权重

STEEM 通过 Steem Power（后简称 SP）来决定评价权重，SP 越多评价权重越大。Steemit 上的评价行为也设计了能量的消耗，可以理解为的能量血条，每评价一次就会消耗血条能量，血条也会随着时间恢复，血条消耗越多，评价权重就会下降，血条恢复的时间就会更长。

虽然 Steemit 设计了能量消耗来应对大户的过大权重的影响,但是 Steemit 的权重没有上限，大户通过持有大量 SP 仍然掌握着绝大部分的评价权重，所以 Steemit 里仍然是大鲸鱼决定了大部分的财富分配。

YOYOW 的白皮书介绍，YOYOW 是通过币天来统计评价权重，有一个最大值的限制。币天跟持有 YOYO 的余额正相关。跟 Steemit 一样持有的代币越多评价权重越大。不同的是，YOYOW 有一个最高的限制，币天达到一个最大值后就停止增长。

2）智能合约

STEEM 和 YOYOW 两者定位都是做一个内容激励平台，而不是定位某个单一的内容平台比如文字博客类，其它内容相关的公司或者组织（文本、视频、图片、音频、直播等）都可以在他们的平台上搭建运营。

STEEM 是通过提出 SMTs 来扩展内容相关的应用，可以理解为一个类似以太坊的智能合约。方便内容相关的公司或组织发行自己的代币。

在 YOYOW 中期开发计划中，允许内容社群平台以 YOYO 代币为基础发行属于自己的社群平台智能代币。这类智能代币的收益分配中设计了一种不能转移、交易的资产。个人理解 YOYOW 的智能代币可能主要存在于 YOYOW 的体系中，有一定的流通局限性。

3）内容审查

STEEM 白皮中介绍，用户的行为皆记录在区块链上，可被公开验证，没有任何一方能够审查 steem 持有人所赋予价值的内容。Steemit.com 或许会审查网站的内容，但是所有内容一旦发布在区块链上，就被广播出去，内容永远存在无法删除。

STEEM 认为言论自由是自由权利的根基，审查意味着限制剥夺了人民的权利，STEEM 致力于围护言论自由，建立自由社会。

在 Steemit.com 上，还是可以通过对内容“踩”的行为来限制部分不好内容，但是个人发表言论自由的权利没有限制，依然可以发表，只是被踩后，内容隐藏但是内容还是存在且可查的。

与 STEEM 不同的是，YOYOW 中注册的账户通过授权注册商进行注册，授权注册商还拥有赋予、收回发帖权，审批、收回账户名称等权利。这等于 YOYOW 设计了一道审查机制，可以通过授权注册商直接剥夺用户的很多权利。

YOYOW 的这种审查机制可以被理解为适应中国的国情。从某个角度来说，在政策上 YOYOW 在国内的大范围推广相比 steem 是有利的。

4）货币体系

Steemit 有较为复杂的货币体系，共三种，Steem，Steem Power，以及 Steem Dollars（锚定法币美元的货币），这让刚刚了解 Steemit 的新手很是困惑。

YOYOW 的白皮书里没有看到类似 Steem Dollars 的代币，YOYOW 里只有 YOYO 代币。

5）广告

STEEM 理念是以基于区块链的内容奖励替代广告。STEEM 认为广告可能会贬损他们的作品在消费者眼中的价值，没有广告，内容更有价值。STEEM 就是要改变传统内容作者需要广告来变现的方式，去除中介者，STEEM 认为区块链内容奖励变现，应该比广告的价值变现更为快捷，而且门槛较低。

Steemit 网站至今也未引入广告。这也让广大 Steemit 用户疑惑和担忧，钱从哪里来，Steemit 如何盈利。

YOYOW 的设计中，考虑了广告系统，平台网站主可以出售按照时长计费的广告位，用户可以直接支付 YOYO 代币进行购买，广告的时长和位置由智能合约执行。按照 YOYOW 的理念，广告系统可以增强 YOYO 代币的流动性，增加平台收入。

引入广告是好是坏，只能交给时间给我们答案，不过广告的引入解决了一部分平台盈利的问题。

6）转账手续费

STEEM 取消交易手续费。YOYOW 增加了跟转账手续费相关的积分系统，也就是 YOYOW 是有手续费的，但是你可以持有 YOYO 代币来获得积分，通过积分来抵扣交易手续费。

7）其它不同

YOYOW 相比 Steemit 增加了对内容的打赏模式，投资模式，另外作者可以设定是否允许文章转载的权限等等。

24.4 YOYOW 的市场定位

STEEM 由于主张言论自由，基本没有审查机制，所以 steem 预计不可能在中国大范围推广，并且 Steemit 的注册对大陆用户也是很不友好，这也妨碍了它在中国市场的发展。

YOYOW 增加了审查机制，可能就是为了规避政策风险适应中国市场的举措。其定位和市场预计也主要以国内市场为主。

中国这几年，涌现出大量的作者，内容社群，中心化的付费知识服务也在蓬勃发展。就微信公众号就有上千万个，某些个人的公众号订阅用户可能都比 Steemit.com 全网的注册用户还多。

所以，内容相关的区块链应用在中国还有巨大的市场，中国的内容市场是可期的。如果以注册用户数来衡量内容网站的价值，鉴于中国巨大的人口基数，YOYOW 这类平台的价值增长或许不是难事。

25 YOYOW 应用生态—币问

25.1 什么是币问

币问跟知乎一样，是一个问答社区，用户发起提问以及分享着彼此的知识、经验和见解。通过“币问”的名字可以知道，跟知乎还是有所区别，**币问是专注区块链的问答社区，可以当做是“币圈的知乎”**。

对于一个小白来说，区块链（blockchain）这个概念还是很难理解，想加入区块链发展的大趋势，做一个专注区块链问答社区的垂直领域还是有很大的市场需求，币圈还是需要币问这

样的社区去培养更多人对于区块链的认知。

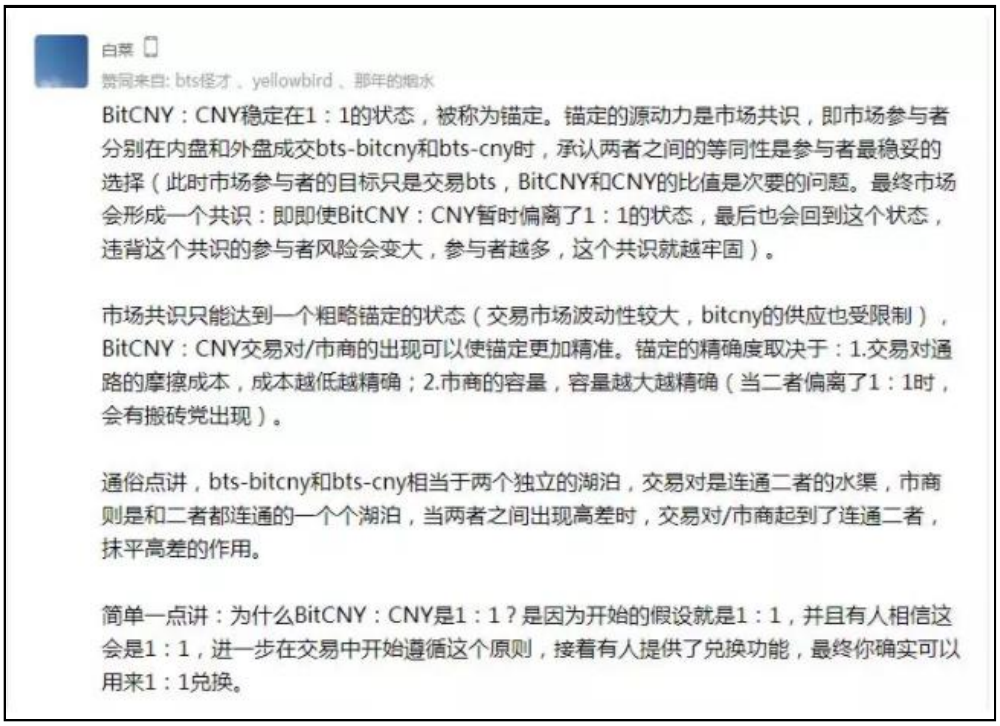
币问会接入 yoyow 区块链，目前还在推广阶段。使用币问提问或者提供优质的回答可以获得 yoyo 代币的奖励。后期的币问接入 yoyow 后就是引入了 yoyow 的内容激励，成为 yoyow 区块链上的一个应用。

25.2 在币问可以做什么

对于想了解区块链的小白用户来说，币问是一个找寻答案的好地方。

币问已经汇集了不少圈内的大佬，牛人。比如 bitshares 社区大神，yoyow 联合创始人，steem 中文区的大神，《精通比特币》中文版翻译的作者等等。对我来说，我更希望在币问社区看到他们观点和看法。

比如 bitshares 社区大神就回答过一个问题：为什么在比特股系统中 1bitCNY 就等于 1cny(人民币)？还是对我有很大的启发。


白菜
赞同来自: bts怪才、yellowbird、那年的烟水

BitCNY：CNY稳定在1：1的状态，被称为锚定。锚定的源动力是市场共识，即市场参与者分别在内盘和外盘成交bts-bitcny和bts-cny时，承认两者之间的等同性是参与者最稳妥的选择（此时市场参与者的目标只是交易bts，BitCNY和CNY的比值是次要的问题。最终市场会形成一个共识：即即使BitCNY：CNY暂时偏离了1：1的状态，最后也会回到这个状态，违背这个共识的参与者风险会变大，参与者越多，这个共识就越牢固）。

市场共识只能达到一个粗略锚定的状态（交易市场波动性较大，bitcny的供应也受限制），BitCNY：CNY交易对/市商的出现可以使锚定更加精准。锚定的精确度取决于：1.交易对通路的摩擦成本，成本越低越精确；2.市商的容量，容量越大越精确（当二者偏离了1：1时，会有搬砖党出现）。

通俗点讲，bts-bitcny和bts-cny相当于两个独立的湖泊，交易对是连通二者的水渠，市商则是和二者都连通的一个个湖泊，当两者之间出现高差时，交易对/市商起到了连通二者，抹平高差的作用。

简单一点讲：为什么BitCNY：CNY是1：1？是因为开始的假设就是1：1，并且有人相信这会是1：1，进一步在交易中开始遵循这个原则，接着有人提供了兑换功能，最终你确实可以用来1：1兑换。

图25-1 币问中的一个页面

对于币圈的老司机来说，币问可以拓展你的圈子建立你的影响力。

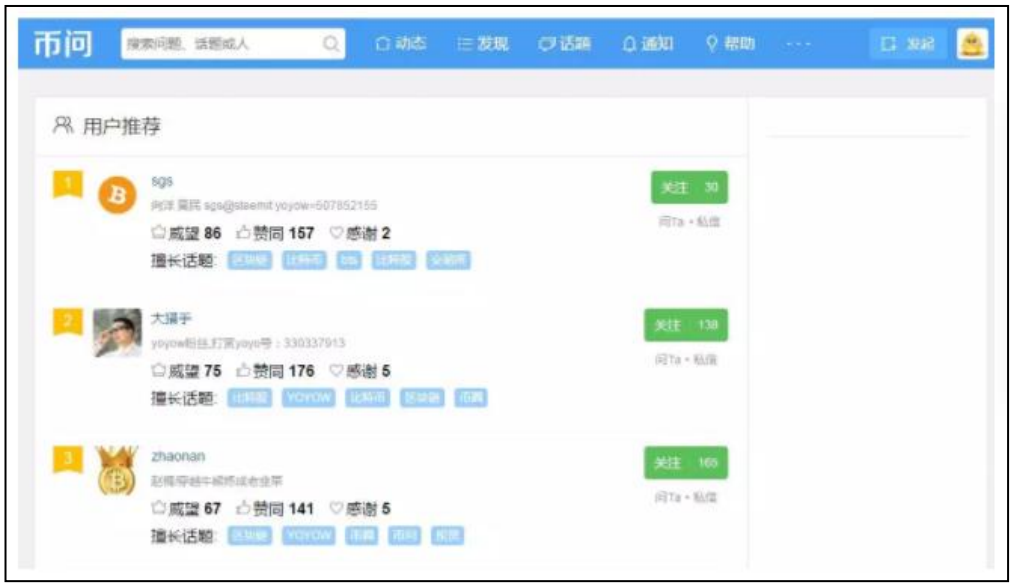


图25-2 币问的活跃用户

图上为币问上排名前三的活跃用户，他们就是币问上的意见领袖。

在币问发起优质问题，提供优质答案可以获得一些 yoyo 代币报酬，目前还未接入 yoyow 主要是人工审核奖励。

26 区块链投资垂直社区——币乎

26.1 什么是币乎？

币乎的白皮书是这样介绍的：

首先，币乎是一个垂直社区，服务区块链投资这个有巨大增值潜力的群体。

其次，币乎是一个代币驱动的内容激励平台。如果你熟悉 steem，那么就比较容易理解币乎的这种模式。

我们知道传统内容社交媒体公司如 Reddit、Facebook 和 Twitter，知乎，微博等这样的平台创造了数十亿美元的价值。参与其中的用户为平台创造内容和价值，但没有获得任何回报。

Steem 和币乎这类平台，通过区块链技术发行去中心化的代币，用代币体系来奖励给平台创造内容价值的用户。

你持有 steem 和币乎的代币意味着就是这个公司的股东，你可以简单把代币理解为这个公司的股票，它具有流通性，可以交易，可以变现成法币，持有它也可以行使一定的股东权利。

图26-1 币乎简介

26.2 币乎的市场定位

目前类似的项目有 steem，yoyow，PressOne。

Steem 和 yoyow 类似，解决的是 Facebook、知乎、微博这样的中心化平台收割用户注意力赚取巨额利润，而用户参与其中并没得到任何回报的问题。市场定位是内容相关的各种平台应用，比如博客、直播、社群等等社交网络。

PressOne 解决的是出版方等中间商赚太多而创作者赚太少的问题，它的目标是通过智能合约把中间商去除掉，把收益直接还给创作者，它的市场定位是内容相关的出版发行。

Steem，yoyow 还有 PressOne 它们的定位大而全，而币乎的定位是：一个垂直代币投资者社区。币乎解决用户三个问题：区块链投资买什么，什么时候买以及什么时候卖。币乎的定位可以理解为小而精，专注服务区块投资这个群体。

未来区块链是一个发展迅猛的行业，区块链投资有着巨大的风险，专注服务区块链投资的币乎社区将会是一个有价值的社区。它通过提供一站式的行业信息，提供意见领袖的看法，让用户慢慢学会独立思考和做出独立的投资决策。

图26-2 币乎的应用场景

26.3 币乎的产品设计

币乎引入区块链代币KEY，用代币激励用户的正向行为，通过奖励做出贡献的用户以鼓励更多的贡献行为，促使平台快速发展，形成网络效应。

1）KEY的功能

KEY可以被用来：

- ✧ 奖励优秀帖子
- ✧ 奖励慧眼识珠
- ✧ 奖励社区管理员
- ✧ 收费看广告
- ✧ 付费私享群
- ✧ 付费问答
- ✧ 付费私信
- ✧ 获得特权

✧ 打赏

2）KEY 是通缩的

KEY 是一个设计为通缩的代币，这个跟 steem 很不一样，steem 设计是一个无限通胀的代币。KEY 总量 1000 亿，通过纳入代币销毁机制，使得 KEY 的供应总量越来越少。持有 KEY 是一种对币乎的贡献行为，通过设计销毁机制来奖励持有者，平台越活跃，通缩的速度越快，销毁的代币就越多。

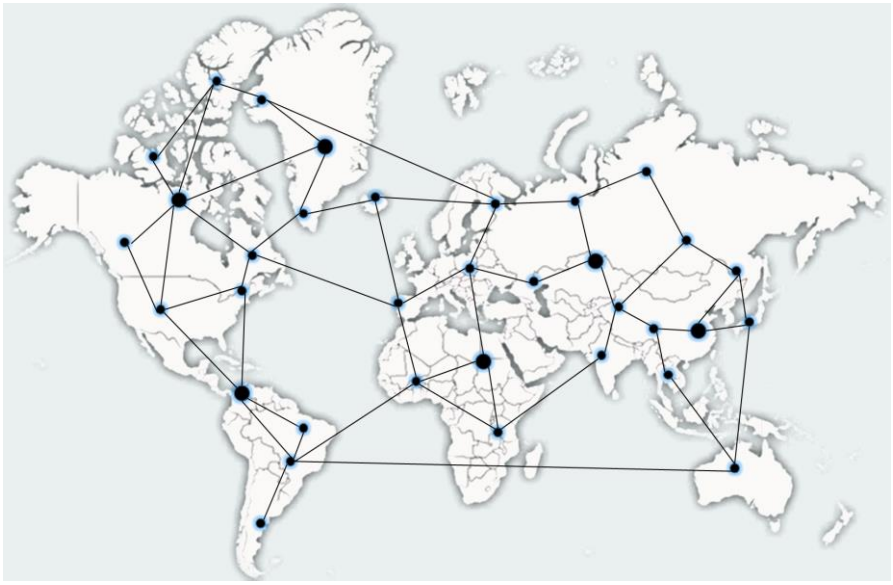
3）中心化应用+去中心化代币

KEY 是以太坊上发行的代币，以太坊的处理速度较慢，这个决定了币乎的实际应用平台可能是一个中心化的平台。

目前区块链的基础网络还很早期，基于区块链实现的完全去中心化的应用体验都还很差，Steemit 就是一个去中心化的应用，Steemit 的应用体验并不好，至今没有一个官方的 Dapp 应用，目前能实现文字发布浏览的流畅性，但是基于 steem 的视频分享如 Dtube 和 Dlive 的使用体验不佳。这很像 97 年的互联网，网速很慢，应用做不了，只有能力发 email。

在中心化的世界里，目前的基础网络能很好的解决各种应用并实现良好的用户体验。币乎应该是一个中心化应用+去中心化代币的平台。在币乎平台里，用户就像中心化的代币交易所那样，把代币发送到平台集中存储，在应用层面通过中心化的方式实现平台的发文，点赞，评论等等各种功能，只有当你需要提取或者转账代币时，才是代币的去中心化价值传输，才会被记录到区块链。

第五篇 其它竞争币



27 笑来 722 分享会上与区块链相关的内容摘要

2017 年 7 月 22 日，李笑来在“人至践则无敌”分享会上，分享了一些与区块链有关的内容。

图27-1 “人至践则无敌”分享会

27.1 区块链的窗口

“**我做过的绝大多数事情都失败了**”这句话是孙正义说的，孙正义真的是一个牛人，不是说他在日本被称为吹牛大王，而是他在小的时候就树立了远大目标，学编程、弄翻译机、追逐互联网的浪潮，为了抓住**互联网的窗口**，去美国买了一家会展公司。现在他去了印度，说下一个崛起的市场一定是印度。

信息流、钱流、物流是商业中的三大流，有商业模式的技术是区块链技术。那么**区块链的窗口**在哪？以前没想通，去中心化的比特币为什么需要一个中心化的交易所？现在发现还是需要的，所以马上弄起了云币、ico.info 和 inblockchain 等——目前云币已关闭交易，ico.info 因某些特殊原因已关站。

27.2 一切才刚刚开始

“活在未来”绝对不是空话，要想尽一切办法让自己活在未来。中本聪的经典白皮书（现在被称为比特币的圣经）只有区区 9 页，当时没有几个人能够看懂，如果你认为它是一篇好论文，就要坚持读完，多读几遍。现在阅读此文已经比以前容易了许多，因为网上可以查到大量的细节解读。

中本聪在设计比特币时，感觉学过密码学、经济学、编程、系统论等学科，做事遵循“奥姆剃刀原理（如无必要，勿增实体）”。只去解决最本质的问题，然后尽量用最简单的办法去解决问题，并且能够让系统自组织地运转。

信息互联网让信息几乎零成本的流动，这些年给这个世界带来的变化太惊人了，想想我们现在社交和购物的方式，再想想20年前的我们是怎样社交和购物的。而**区块链让资产可以无国界、几乎无成本的流转**，不知道又会给这个世界带来怎样的变化。

区块链是人类史上不多见的湍流，这个世界里变化太快，拼的是谁做的事更大，智商和努力反而不是最重要的因素，它一定会改变我们的生活，这一切来自于自己的选择。

人在做选择时往往追求绝对的安全感，明明认同某个道理，但在实际执行时却做出了相反的选择。这说明什么呢？这说明那件尚处于蓬勃发展的事件与你无关。没有未来的眼光，不相信未来会按逻辑发生，财富也会与你擦肩而过。

27.3 锁定资产，握住不放

币市7*24小时全年无休地运转。追涨杀跌，玩K线分析，只会让你沦落成为韭菜。天天盯盘，整天关注那点帐面数字的变化，会让你寝食难安，严重影响生活的质量。更重要的是，让你浪费了宝贵的注意力，失去了场外赚钱的能力。

人在投资时的心理都非常脆弱，大多数人在产生40%的收益时可能就卖了，出现4倍收益时，能够握住的绝对是极少数。投资世界里的一切都是时间的积累，需要长期的思考方式。

区块链世界里，在没有穿过一个牛熊之前，你都不叫入行；穿过两次牛熊，才是专家。

27.4 ICO是机会，但风险特别巨大

区块链的ICO现在很火，是有一些机会，但风险巨大——风险特别大。首先它是全球化的，创始人在美国，做得好大家都不错，如果失败了，一切直接清零，毫无办法。

其次，很多人不懂，连基本概念都不懂，就冲了进去。以前的投资市场中有“合格投资人”这种概念，人为设置了许多进入限制，这些条款都是为了保护这些投资人。但ICO中没有限制，一切的投资行为都要凭自己的选择做出。

这里李笑来现场做了一个测试，让投资了1种以上区块链资产的观众举手（现场应该有2

/3 的朋友抬起了胳膊），然后又说，知道“**区块高度**”的含义的朋友举手（此时不到 1/2），他再问，有谁看懂过两篇白皮书的（此时全场只剩零星的几条胳膊） 。

我对很多人不知道“区块高度”的这种现象还是相当吃惊的，区块高度是区块链里最最基础的概念，BTC 交易中通常认为 6 次以上确认是非常可信的交易，所有的其它概念几乎都与区块高度产生联系，这件事更说明了我开办“区块链生存训练”饭团的意义。

inblockchain 里已经开源了 ICO 的原则，这里又强调了几点：

1、不参加

绝大多数不适合参加 ICO，看不懂的东西不要投。

2、机会有的是

“机不可失”这种说法是骗人的，一件事情如果真的是机会，明天的机会更大。互联网 30 年里，机会一直有。错过了 BTC，错过了 ETH，错过了 EOS，都不要紧，抓紧时间学习上 2 年，机会仍存在。未来的唯一资产是信誉，让别人知道你是一个有作品的人，机会有的是。

3、看团队

看看 ICO 的团队是不是有成绩的；他们是否有真实身份，匿名项目都不要参加；查查这个团队在上个熊市的时候在做什么，识别他们是不是失败的投机者。

27.5 套现

按照这个世界发展的逻辑，区块链资产才是未来的货币，活在未来的人有不同的现金概念。**在这个世界里生存，不要搞错了方向**，短期内找不到这么快的车了——关于现金这件事，老猫的《一切才刚刚开始》这篇文章值得认真阅读。

重视自己的场外赚钱能力，很重要，把为他人创造价值变成自己的刚需，过上好的生活，有稳固的社交关系，有关心你、你也在乎他的朋友，有爱你的、你也爱他们的家人，做有益的事、对他人非常有价值的事情才有可观的收益，才能套现 。

27.6 PressOne 能够做什么

我本想多听一些有关 PressOne 的消息，但笑来透露的并不多。账目公开这件事情运用在商业世界里，会把以前的利益重新分配，把原有的经济体系重新划分，这种划分是不是比以前

更有意义？

有人说李笑来搞 Press.One，那我就要开始写作了。这里需要提醒的是：这种免费的写作是没有价值的，写本书还有可能。例如：有一个去中心化的书店，这里面的版权方式已经确定了，给每一个出版方一个账号，你授不授权我不管了，就开卖了，所有的收益通过智能合约直接打进你的账户。

100 元的书，出版方得 50，50 块留给买方写评论，因为你买了，有资格写评论。从他这里分发出去的订单，也有分成，这些通过智能合约运转，效率极高。即使书价砍一半，也非常有效率。PressOnes 可能会遇到法律问题，但我们已经做好了准备。这里笑来可能故意不透露太多细节，我们只能猜测了。

28 EOS

28.1 EOS 是什么？

从发行上说，EOS 是基于以太坊（ETH）发行的 ERC20 代币；从功能上说，EOS 是 Block.One 公司正在研发的一个区块链底层公链系统。使命是要成为去中心化的区块链操作系统。可以将 EOS 类比成计算机的 Windows 操作系统，支持多种编程语言，为开发者提供底层模块，降低开发门槛。区块链开发人员不再需要从底层编写代码，可以在 EOS 架构上直接开发去中心化的区块链应用（DApp）。

现有的以太坊等区块链就好比只有 DOS 系统的电脑，程序员必须从头编写应用程序。可以说 EOS 就是为 DApp 而生的基础设施，所以有人称 EOS 为区块链 3.0。

block.one 公司注册在开曼群岛，公司创始人和首席技术官是 Dan Larimer，因为他的网名是 Byte Master，大家习惯称他 BM。BM 曾经在 2013 年创立比特股 BTS（去中心化交易中心），2016 年创建了 STEEM（区块链社交媒体）。这两者目前还在正常运作中，总市值在数字货币的前 50 名以内。两次成功的开发经验，给了 EOS 投资者足够的信心。BM 离开 STEEM 团队后，就准备开发一个支持商业级区块链应用的底层平台。这就是 EOS。

28.2 EOS 的特点

相对于比特币和以太坊来说，EOS 有以下几个非常显著的优势：

高性能和易于扩展：目前比特币每秒可以转账大约 7 次，以太坊每秒 15 次，这也是比特币和以太坊经常性交易堵塞的原因。EOS 采用已经被 BTS、STEEM 等项目验证过的石墨烯技术，单线程每秒可以完成 10000 次交易量，在并行处理时可以达到每秒数百万次交易的高性能。在这种情况下，EOS 可以同时支持数千个分布式应用程序（DApp），成为一个性能优秀，高性能的底层公链（操作系统）。

良好的用户体验：免费使用，用户不需要为使用平台或从平台中获得服务而承担费用；在 EOS 平台上的所有帐户名用人类可读的 2 到 32 个字符来命名，而不再是一长串没有意义的数字和字母组合；提供了用户账户钥匙被偷后恢复的方法，账户所有者可以使用在过去 30 天中活跃的所有者密钥，以及他们指定的账户恢复伙伴（如交易所）的批准，来对其账户进行密钥重置。这些特点让 EOS 变得更加具有可用性。

28.3 DPOS 共识算法

DPOS 共识算法是针对 POW 工作量算法的缺陷改进而来。POW 是比特币的算法，需要消耗计算能力，也就需要消耗能源，据说目前比特币挖矿每年消耗的能源相当于一个中型国家的电量，这也是被环保组织严重诟病的地方。当下，相关部门只要停止对比特币矿场进行供电就能完成清理工作。

我的理解是，未来的数字货币不应该再采用 POW 共识算法。比特币已经取得头部效应，不会容许更多的数字货币消耗能源。DPOS 算法应该才会是未来的趋势。

DPOS 共识算法消耗的是 POS 网络内一个叫币天（持有的币乘以在系统里面的未被使用的天数）的概念。当记完账之后你的币还在，未被使用的天数会被清零。

EOS 系统规定每 3 秒产生一个区块，区块生产者的个数为 21 个。由 21 名生产者轮流产生新的区块。区块生产者由 EOS 持有者进行投票选择。任何人也都可以选择参与区块生产，并有机会生产与总票数成正比的区块。

目前使用 DPOS 算法的项目有 bts、steemit 以及公信宝，这几个项目已经稳定运行非常长的时间了，看来该算法还是比较经得起长时间考验的。

28.4 EOS 众筹问题

EOS 这个项目（eos.io）的 ICO 众筹模式非常烧脑，无上限吸进 ETH，众筹期长达近 1 年

——前无古人，后无来者。

开始时间：2017 年 6 月 26 日 13:00:00 UTC

结束时间：2018 年 6 月 1 日 22:59:59 UTC

众筹时长：346 天，切分为 350 个区间(Period)，每个区间是 23 个小时。

发行代币：10 亿枚 EOS

第 0 区间：前 5 天，发行 2 亿 EOS，当时共筹到了 65 万个 ETH，以 7 月 1 日的当时单价 2000 元计算，约 13 亿人民币。我当时参加了前 5 天的云币代投，1 个 ETH 大概换 306 个 EOS，我当时 ETH 的买入单价为 2334 元，这样我的 EOS 成本是 7.6 元/个。由于以前 ETH 在 1400 多的时候我也买入过，所以平摊下来成本也就是 7 元左右。

以后的 341 天里，按 23 个小时为一个区间，共划分为 350 个区间，每个区间筹 2 百万个 EOS，350 天共要筹 7 亿个 EOS 。每个区间的分发代币数的计算公式：

$$\frac{\text{你参与的ETH数量}}{\text{总的ETH接收数量}} \times \text{可认筹的EOS代币数量}$$

以 7 月 27 日刚刚完成的区间来举例吧，标准记法为：27/351 period，913 个人发送了 19102.59 个 ETH，相当于 1 个 ETH=104.7 个 EOS。这些数据可以在 eoschart 这个网站上查到。

我查了一下 EOS 当时在云币网的单价，大概是 12.75 元，而 ETH 当时为 1403 元，如果事后计算，1 个 ETH 换 110 个 EOS（注意，这里没有包括交易的手续费）。但还有一点需要注意，上面的数据来自于事后计算，每个区间有 23 个小时，你不知道最后 1 分钟内会有多少人杀入（几乎 50%左右的 ETH 都是在最后几分钟杀入 ），所以价格很难估计。

刚才说了，总共 10 亿，前 5 天 2 亿，后面 341 天 7 亿，还剩 1 亿留给 EOS 团队（block.one）。

这篇经验贴（http://www.bitett.com/forum.php?mod=viewthread&tid=5486）认为众筹后的第 3 至第 10 个月进入比较好，但我感觉问题在于：如果 EOS 在不到 3 个月的时候就放出公测版，那么行情会高涨。总之，世事难料。写这段文字是在 2017 年 7 月，没想到 9 月遭遇了中国全面叫停 ICO 事件，EOS 一度跌到 3 元多，后来又一度高涨到 100 多元。

长达 341 天里无上限地接收 ETH，有人说 EOS 是 ETH 的吸血鬼，此话不假，事情如何发展，我们只能慢慢观察了。

Period	No. of EOS Tokens Distributable	Duration	Open	Close
0	200,000,000 (two hundred million)	120 hours (5 days)	June 26, 2017 13:00:00 UTC	July 1, 2017 12:59:59 UTC
1	2,000,000 (two million)	23 hours	July 1, 2017 13:00:00 UTC	July 2, 2017 11:59:59 UTC
2	2,000,000 (two million)	23 hours	July 2, 2017 12:00:00 UTC	July 3, 2017 10:59:59 UTC
3	2,000,000 (two million)	23 hours	July 3, 2017 11:00:00 UTC	July 4, 2017 09:59:59 UTC
-				
-				
-				
350	2,000,000 (two million)	23 hours	June 1, 2018 00:00:00 UTC	June 1, 2018 22:59:59 UTC

图28-1 EOS 的 ICO 进度状态

如何了解 EOS 的开发进度

EOS 文档：https://eosio.github.io/eos/

EOS 代码：https://github.com/EOSIO/eos

EOS 是基于 C++ 14 进行开发并使用 CMake 进行编译管理，据 git 上的信息，EOS 开发者使用 clang 4.0.0 和 CMake 3.8.0 进行开发编译。EOS 使用 WebAssembly 对编译和运行智能合约，因此需要使用 WASM 编译器。除此之外 EOS 还依赖：Boost 1.64，OpenSSL， LLVM 4.0 和 secp256k1-zkp。

28.5 如何参与 EOS 众筹

请注意，EOS 众筹在 2018 年 6 月 1 日截止，通过众筹购买到的 EOS 不一定比直接从交易所买到的便宜，请谨慎参与。

这里介绍的众筹方法是 EOS 官方网站推荐的，使用谷歌浏览器以及以太坊网页插件钱包 metamask。由于网站对中国和美国地区的 IP 地址进行了限制，必须使用在这两个地区以外的服务器作为梯子(科学上网并使用全局模式)访问 EOS 官网才可以进行众筹及其后的相关的操作。

确保 metamask 钱包里有参与众筹的 ETH 和手续费。使用谷歌浏览器登录官网 https://eos.io，找到如下页面：

图28-2 EOS 众筹首页

点击上面图片中的“GET EOS”，就出现确认选项页面。这 5 个选项的意思是确认你不是美国人；确认你不是中国人；确认你同意众筹协议，确认你同意使用条款，确认你阅读过白皮书。如果你确认要进行众筹，当然都打勾，然后点击“continue”继续向下操作。

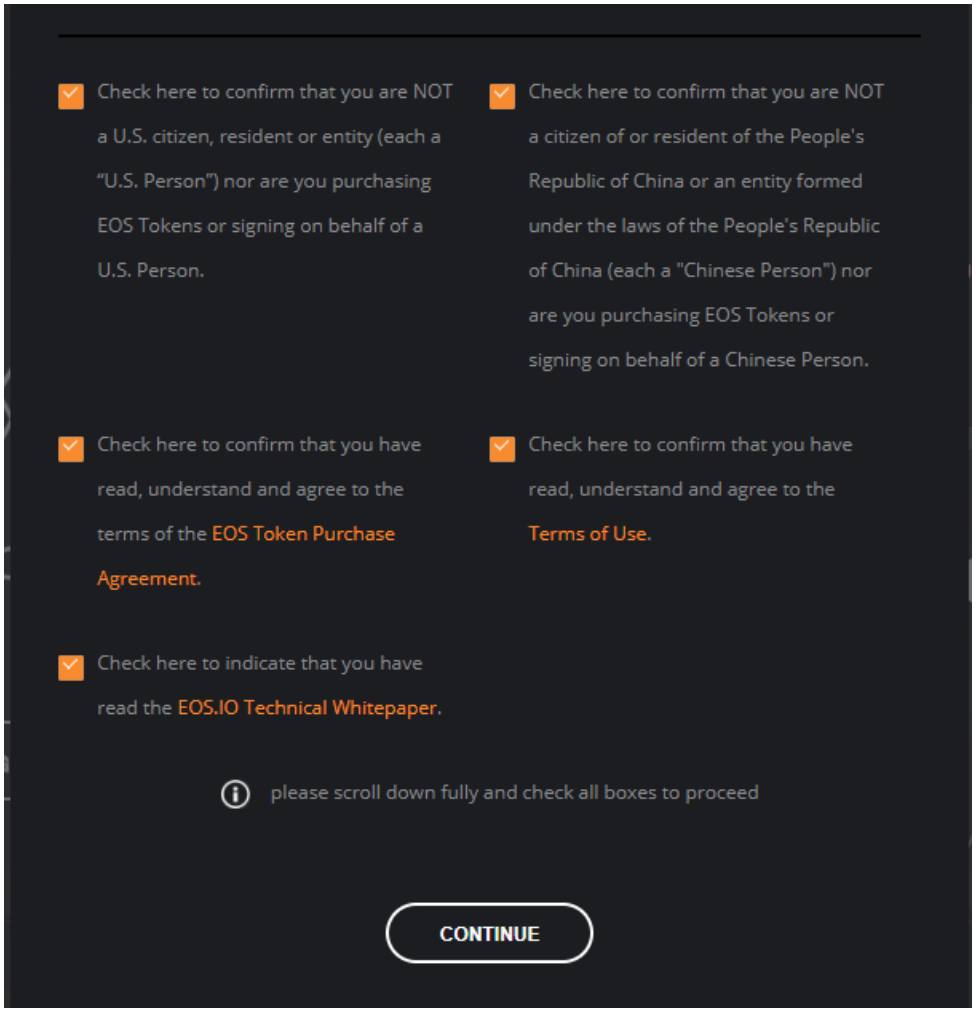


图28-3 同意众筹协议

经过确认后，点击“continue”，进入下一个页面，并往下滚动。见到下图的界面：图形的上面部分有 4 个功能菜单，分别是 buy（众筹）、register（注册）、claim（认领）、transfer（交易）。进行众筹时选择 buy（众筹），出现了 EOS 官方推荐的 metamask 钱包的小狐狸头像图标。

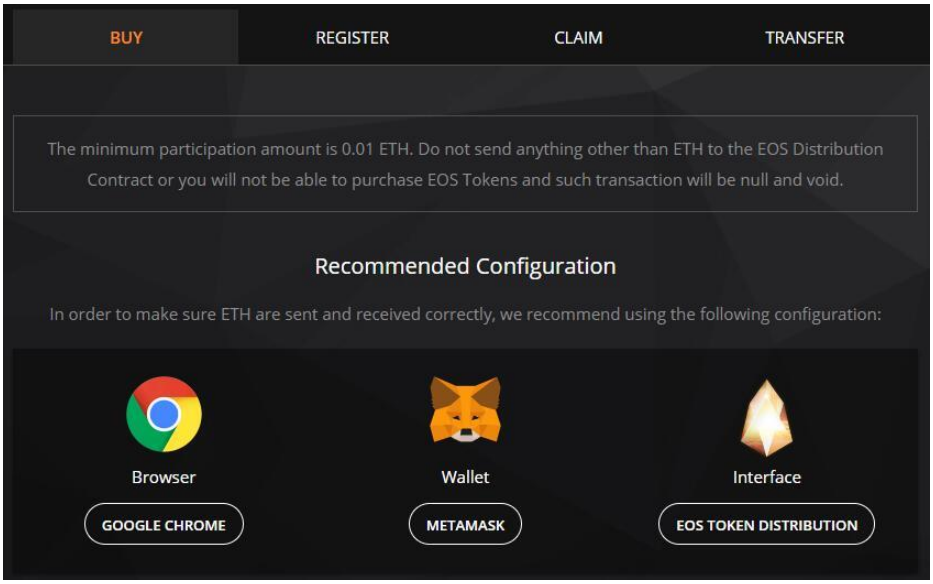


图28-4 选择钱包

点击最右边的按钮“EOS TOKEN DISTRIBUTION”，然后进入到下一个页面。这个时候必须使用安装 metamask 钱包时的密码给钱包解锁，否则钱包无法和网页关联，进行下一步操作。在用密码解锁 metamask 钱包后，刷新页面就可以了。（红色字体是对相关内容的解释和说明）。

图28-5 EOS Token Distribution

点击“GET EOS TOKENS”后，出现下面的界面：

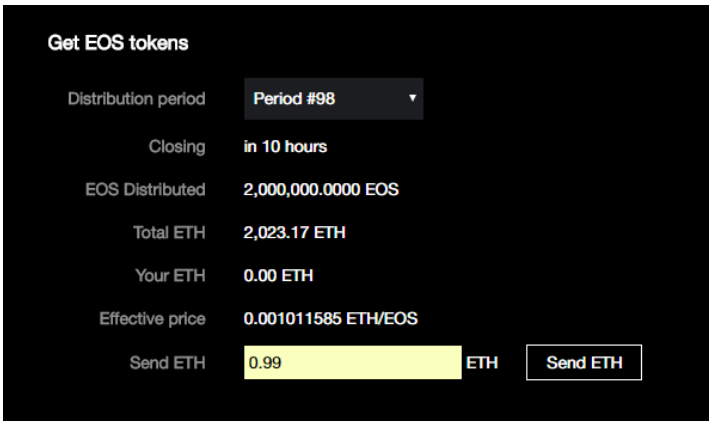


图28-6 Get EOS tokens

在输入框中输入你要投入的 ETH 的数量。点击“Send ETH”。等待 metamask 钱包装载交易。装载成功后，钱包会弹出一个转账交易页面。再次确认转账金额和转账地址，在这个过程中不需要输入转账地址，由系统自动生成。但是还是有必要检查一下地址是否正确，否则将收不到 EOS。官方众筹地址为（0xd0a6e6c54dbc68db5db3a091b171a77407ff7ccf）。

28.6 EOS 代币的领取

在某个时间区段参与 EOS 众筹后，还需要一个认领的过程，EOS 代币才会到你的钱包。这里还是以 metamask 钱包为例，介绍认领的步骤如下：

第一步和第二步和前面众筹的步骤一样，在第三步时，选择 claim（认领）。在选择（点击）下面的 metamask 钱包的小狐狸图标。

解锁 metamask 钱包，并选择当初参与 EOS 众筹的 ETH 账户。

点击小狐狸图标下面的按钮“EOS TOKEN DISTRIBUTION”，进入到下一个页面，和众筹第 4 步骤（图 28.4）相同。

点击“CLAIM EOS TOKENS”，出现认领的界面：

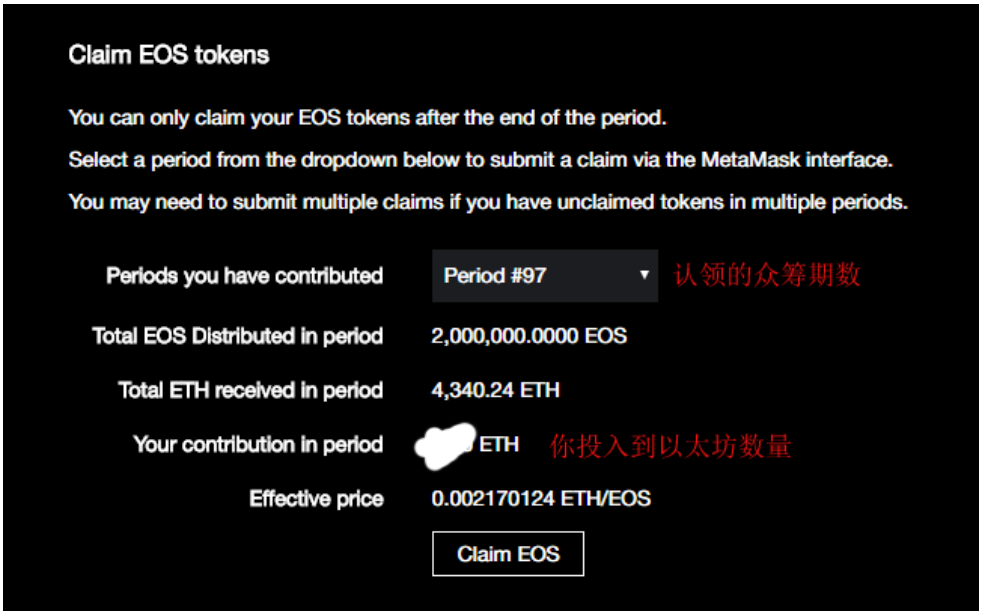


图28-7 认领 EOS

点击“Claim EOS”， 等待 metamask 钱包装载交易。装载成功后，钱包会弹出一个转账交易页面。因为这个认领过程也是要交 ETH 手续费的，而且不同的众筹区间要分别交手续费。在钱包交易页面点击 “SUBMIT”提交交易，等待交易被矿工打包，认领就结束了，认领成功后在 metamask 钱包中或者官网上可以查询到 EOS 的数量。

28.7 EOS 的注册（映射）

在 EOS 官网上进行众筹后，或者钱包里有从交易所购买的 EOS 代币后，一定要进行注册（register），这样才能映射到未来的 EOS 公链上。

基于规避美国法律风险的原因，block.one 公司在官方网站中声明：在完成 EOS 软件开发后，不对 EOS 代币的价值做任何保证，不负责，不保证 EOS 临时代币会变成 EOS 公链上的 EOS 代币。也不会启动 EOS 公链，EOS 公链将由第三方启动。2018 年 6 月 1 日前，EOS 只是由 ETH 上派生出来的临时代币，Block.one 公司在众筹结束后的 23 小时内冻结 EOS 的一切交易，对已经注册的 EOS 进行快照。第三方根据快照的结果启动公链，将快照中已经注册的 EOS 映射到公链中。如果你在之前没有注册，公链里就没有你的 EOS 代币，你的 EOS 代币就消失了。所以在 2018 年 6 月 1 日前一定要完成注册。

大概率情况下，交易所会做好映射的，就像在比特币分叉时，交易所会帮用户领糖果一样。否则这么简单的事情都不做，实在是赶走用户的一种最好方式。所以，在 2018 年 6 月 1 日之前，关注交易所的公告，将 EOS 存入交易所，就不用进行下面的映射操作了。

注册步骤如下：

第一步和第二步和前面众筹的步骤一样，在第三步时，选择“REGISTER”（注册）。再选择（点击）下面的 metamask 钱包的小狐狸图标。

解锁 metamask 钱包，并选择当初参与 EOS 众筹的 ETH 账户。

点击小狐狸图标下面的按钮“EOS TOKEN DISTRIBUTION”，进入到下一个页面，和众筹第 4 步骤的（图 28.4）相同。

点击右上角“REGISTER EOS KEY”按钮（如果注册过，相应的按钮就是“CHANGE EOS KEY”）。出现如下界面：

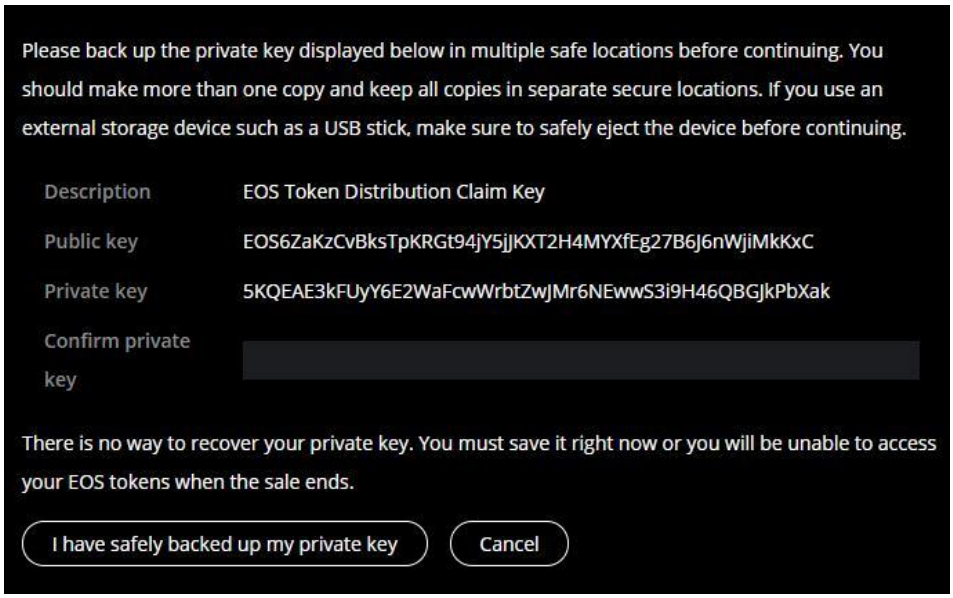


图28-8 EOS 的注册

如上图已经出现了 EOS 公钥和私钥（为了写教程，我用了另外一个空的以太坊地址进行操作），请立即用纸张将私钥记录下来，并保存在安全地方。未来私钥就是决定你 EOS 归属的关键。如果丢失了，你的 EOS 就消失了。

将私钥输入“confirm private key”中，点击”I have safely backed up my private key”。

等待 metamask 钱包装载交易。装载成功后，钱包会弹出一个转账交易页面。因为注册过程也是要交 ETH 手续费的。在钱包交易页面点击“SUBMIT”提交交易，等待交易被矿工打包。

注册成功后，注册页面的右上角“REGISTER EOS KEY”按钮就会变成“CHANGE EOS KEY”

按钮。在页面左边，也可以看到 EOS 公钥序列号和钱包中的 ETH 和 EOS 数量。

29 Zcash

Zcash 的中文名为“零币”，代币代码为 ZEC，官网地址：https://z.cash。

BTC 的区块链里虽然没有记录持币人的身份特征，但是记录了比特币地址、数量、交易对手地址等详细信息。但只要持币人还与其他人交易，根据这些交易信息，就能够追查到更多的信息——这说明 BTC 并不是绝对匿名的。

对于亿万富翁或者商业公司来说，交易地址、交易金额绝对是商业私密，并不想公开在区块链上。

Zcash 就是针对这种需求来设计开发的，它在原来 BTC 源代码的基础进行了修改，使用“零知识证明”技术，既支持 BTC 这种公开所有信息的交易，又支持隐藏信息的交易。它可以隐藏交易地址和交易数量，如果交易双方的信息都不公开，外人能够查到的仅仅是某两人之间发生了一笔交易。谁参与了交易？多少钱？这类关键的信息无法查证，连矿工也不知道这些信息。

29.1 Zcash 曾经是史上最高价格的数字货币

这个号称匿名性最高的数字货币在 2016 年 10 月 28 日横空出世的时候，一个币的单价最高时达到 3300 个比特币，相当于 200 万美元，简直不可想象。Zcash 就此一骑绝尘，成了币史上的传奇。然而疯狂的开始注定了接下来的一地鸡毛，几天后，Zcash 价格急剧下跌至 0.1 比特币，从 200 万美金左右，直接跌到 75 美金。无数人因此损失惨重……

SELL ORDERS ⇌ Total: 0.08914328 ZEC

Price	ZEC	BTC	Sum(BTC)
1888.00000000	0.00044454	0.83929152	0.83929152
1888.00000001	0.00031640	0.59736320	1.43665472
2500.00000000	0.00008668	0.21670000	1.65335472
2850.99999997	0.00011469	0.32698119	1.98033591
2900.00000000	0.00033251	0.96427900	2.94461491
2900.00000001	0.00408065	11.83388500	14.77849991
3000.00000000	0.07666471	229.99413000	244.77262991
3100.00000000	0.00015187	0.47079700	245.24342691
3296.99999999	0.00039474	1.30145778	246.54488469
3300.00000000	0.00030321	1.00059300	247.54547769
3400.00000000	0.00295000	10.03000000	257.57547769
3500.00000000	0.00083194	2.91179000	260.48726769
3850.00000000	0.00066523	2.56113550	263.04840319
3960.00000000	0.00069691	2.75976360	265.80816679
4000.00000000	0.00086598	3.46392000	269.27208679
4660.00000000	0.00043559	2.02984940	271.30193619

BUY ORDERS Total: 689.46303656 BTC

Price	ZEC	BTC	Sum(BTC)
2000.00000004	0.00000449	0.00898000	0.00898000
2000.00000003	0.00021141	0.42282000	0.43180000
1849.99999999	0.00138100	2.55485000	2.98665000
1799.99999999	0.00053573	0.96431400	3.95096400
1600.00000001	0.00011904	0.19046400	4.14142800
1508.00000000	0.00010000	0.15080000	4.29222800
1500.00000108	0.00065666	0.98499000	5.27721800
1500.00000107	0.00000100	0.00150000	5.27871800
1500.00000104	0.00000333	0.00499500	5.28371300
1500.00000103	0.00006479	0.09718500	5.38089800
1500.00000102	0.00017333	0.25999500	5.64089300
1500.00000101	0.00091364	1.37046000	7.01135300
1500.00000100	0.00096635	1.44952500	8.46087800
1500.00000001	0.00003413	0.05119500	8.51207300
1500.00000000	0.00104327	1.56490500	10.07697800
1471.00000000	0.00094978	1.39712638	11.47410438

Throttle Updates 1s ▼ Order Grouping 6 decimals ▼

图29-1 Poloniex.com 上 Zcash 的价格

我在网上没有找到 2016 年 10 月 28 日的交易曲线，但是在 https://coinmarketcap.com/，找到了 10 月 29 日及之后的部分的交易图表。

图29-2 Zcash 最初的交易图表

从图表中可以看出，10 月 29 日，Zcash 最高价格是 5130 美元，随后一路走低，在 11 月 15 日价格为 0.17 美元。云币网上 2016 年 10 月 29 日的交易信息显示，最高价格 140001 元人民币一枚 Zcash。

从可以找到的信息来看，Zcash 当之无愧的是史上“曾经”最高价格的数字货币。Zcash 最

大的特点就是匿名性及其关键的实现方法：零知识证明。

29.2 什么是零知识证明？

零知识证明（Zero-Knowledge Proof）的数学过程和比特币加密算法一样非常复杂，不过这不影响我们对其概念的理解。零知识证明也是一种密码学技术，允许两方（证明者和验证者）来证明某个提议是真实的，而且无需泄露除了它是真实的之外的任何信息——信息在数字货币和区块链中，这通常是指交易信息数据。

举个例子来说明这个概念。

如果有一个密码门，你知道密码，但是验证者不知道密码，如何验证你知道密码？你让验证者呆在门里面，你使用密码将门打开。验证者通过猫眼看到没有其他人帮助你，只要你能够将门打开进去并见到验证者，就说明你掌握了密码，验证者也能够确认这一点，但是整个过程，验证者并没有接触到密码，也不知道关于密码的任何信息。这个过程就是零知识证明。

29.3 零知识证明有什么作用呢？

主要是匿名性和隐私性。

比特币虽然也有匿名性，但这种匿名是建立在帐户匿名性上的。比特币区块链的信息是完全公开的，任何人都可以查询每个地址的所有交易信息。尤其是 2017 年之后，各国政府都要求数字货币交易所对所有用户进行 KYC（实名认证），所以，比特币几乎没有匿名性。

达世币（Dash）和门罗币（Monero）在比特币的匿名性上做了进一步的改进，也是属于隐私类别的数字货币，匿名程度各不相同。

Zcash 使用了零知识证明的技术，从而使 Zcash 达到了绝对匿名的效果。Zcash 通过零知识证明，实现了对交易记录和金额的彻底隐藏，只有掌握了私钥的人才能够查询到相关信息。

除了黑客和洗钱，零知识证明（匿名性）在商业上也是有用处的。作为公司的商业机密，肯定是不想让竞争对手知道自己的资产具体情况的。

目前，摩根大通，这家世界上最大的银行已与 Zcash 的创造团队达成了合作，为该银行的企业级区块链 Quorum 提供一层新的隐私层。

Zcash 首席执行官 Zooko Wilcox 在 Consensus 2017 年大会上公布了这一消息，摩根大通

将整合这种零知识证明安全层，旨在进行安全且匿名的区块链结算交易。而零知识安全层正是匿名加密货币 Zcash 的关键所在，这项技术本身的目的是让网络安全地解决数字资产的移动。

29.4 Zcash 的风险在哪里？

由于完全匿名性，Zcash 的币总量是不可观测的，因此一旦发生刷币，将血洗所有 Zcash 持币人。Zcash 持币人既然要享受完全匿名性，那就要承担相应的代价。

任何代码都可能存在 BUG，哪怕是代码并不复杂的比特币，都曾经因为整数溢出漏洞，被刷出过 1844 亿个比特币。比特币刷币能被迅速发现，并回滚（作废），是因为比特币区块交易公开可查。如果 Zcash 也发生类似的漏洞，那所有 Zcash 持币人都将成为黑客刀下的肥猪，甚至被长时间割肉，流血至死都还一无所知。

关于这一点，目前还没有找到任何比较有效的方法。或许，这世界上原本就没有完完全全安全的地方。

30 Siacoin

早期应用区块链方式实现分布式存储方式并发行数字货币主要有 3 个：Sia，Storj，MaidSafe。长期以来，Sia 的市值在这三个数字货币中排在首位。今天我们来一起了解它。

30.1 Sia 简介

30.1.1 Sia 的历史

Sia 的创始人是 David Vorick，他早在 2013 年就提出来这个项目的设想，并找到 Luke Champine 等志同道合的人共同进行开发工作。

- 2014 年 10 月 29 日发布了白皮书，正式命名为 Sia，货币代码 SC。

- 2015 年 6 月 6 日 10:13，创世区块产生，同时发布了第一个 Sia 软件版本。

- 2017 年 4 月，Sia 宣布和开源云技术供应商 Nextcloud 合作，nextcloud 使用 Sia 的技术推出基于区块链的云存储服务。

Sia 的最新的版本是 2017 年 10 月的 1.3.1 版，名为 duplicati。Sia 会持续修订软件，改进用户体验。

30.1.2 Sia 的主要目的

从时间上看，Sia 是非常早的数字货币了。主要的目的是作为一个去中心化的数据加密存储平台，利用全球范围没有充分使用的空闲存储空间，建立一个比 Amazon 存储云或者百度网盘等中心化公司更加可靠和更加便宜的数据存储市场,同时被租用的空闲存储空间会给其拥有者带来收益。

可以将 Sia 存储方式类比为滴滴打车的共享经济模式。滴滴打车让你的私家车的空余时间给你带来收益，Sia 分布式存储让你的空余存储空间给你带来收益。而且目前这个项目还正在成长过程，随着租用者和提供者的增加，网络协同效应的叠加，未来的增长一定是非线性的。

到目前为止，Sia 的托管主机超过了 1000 台，合约使用存储空间 240TB，主要分布在欧洲和美国。

30.1.3 Sia 的盈利模式

Sia 目前是公司化运作，公司名字是 Nebulous，David Vorick 是公司的 CEO 和创始人。

Nebulous 公司通过接受投资和捐赠获得部分资金。参与种子轮投资的有 Raptor Group, First Star Ventures, Fenbushi Capital 公司和李笑来。2017 年 7 月 11 日，李笑来转账 173 个比特币给 Sia 团队，当时的金额大约是 40 万美元，所以 Sia 网站上的文章声明收到 INBlockchain 的资助 40 万美元。从 CrunchBase 网站上查询这笔金额并没有列入投资中，只是一笔捐赠。

Nebulous 盈利的方式是这样的：Nebulous 建立“sia 基金”，并拥有其 88%的股份。每当存储空间的托管主机和租用者签订合约的时候，3.9%合约资金分配给“Sia 基金”。因此，Nebulous 公司就能获得其中 88%的收益，其他的收益分配给早期的 Sia 众筹者。

30.1.4 安全、高效的分布式存储的策略

Sia 使用了 3 个策略来确保存储数据的安全。

第一个策略是加密。在数据上传之前就经过了加密，只有在下载后才进行解密，而且每个主机保存的数据只是全部文件的一个碎片部分，托管主机无论如何都看不到解密的数据。

第二个策略是备份。文件经过切割后，再做多重备份，传给很多主机同时保存。比如，将

数据做 2 重冗余备份，也就是说在网络上有 3 份相同的文件，同时将每份文件分割为 10 份，这样就有了 30 个文件碎片分布在网络中。如果按照 Sia 的要求，托管主机必须在线率大于 95%的情况下，这个 10 对 30 搭配所提供的文件在线率将达到 99.999999999%。

最后的策略是区块链的文件合约。通过签订合约让托管主机和租用者对于文件存储达成协议；托管者同意在一段时间内储存一个文件，然后收取一定的费用。租用者一开始支付所有的币，区块链作为第三方托管。如果托管者保存了文件并在最后发出了一个储存的证明，文件合约就会自动启动，他就会取得付款。反之，这些支付会被退回给租用者。所有的支付都用 Sia 代币（Siacoin）完成。

30.1.5 Sia 的应用场景

设想一个场景，你不在办公室的时候，你的老板打电话给你：你把昨天写的报告发给我。你说：好的，但是我在外面，回到办公室再发给您，行吗？老板说，不行呀，我正在向领导汇报工作，马上要看到。

文件不在身边，而且也不可能随时随地将所有文件放在手机上，手机容量肯定是不够的。这样的尴尬情况在工作中可能经常出现，为什么一定要回办公室，因为文件在办公室的电脑上，这样的信息，就是存储在“信息孤岛”上。在今天这个网络和空气一样渗透在我们身边的时候，还是这样存储信息的话，就太过落伍了。

所以，在未来，云存储服务就会像现在的电力服务一样变得随手可得。如果你还需要更加便宜、更加快速、更加保密的服务，Sia 将会是一个非常好的选择。

Sia 或许对普通人存储照片和电影没有太多的吸引力，但是对于提供网络服务的公司来说，保密、快速和安全的特点还是非常有用的。

Nextcloud 社区发言人 Jos Poortvliet 告诉 iTWire，融合 Sia 技术便提供了一种通过加密的分布式冗余全球存储技术来扩展存储的方法。他表示：“与亚马逊、谷歌和其他公共云相比，Sia 是完全开源的，其区块链基础能够节省一笔可观的成本费用。”

如果当年 Sia 能够提供希拉里加密的邮件服务，估计就不会有“邮件门事件” 了。

30.2 Sia 钱包安装及其注意事项

30.2.1 软件下载

Sia 官网现在是全英文界面，而且界面过一段时间就会有所变化。软件下载地址为 http://sia.tech/get-started。为了使用方便，要选择图形界面的钱包。图形界面的钱包有 Windows、mac 和 Linux 三种版本。目前对于 windows 系统的钱包软件是 Sia-UI-v1.3.1-win32-x64.zip，从软件名字可以看出来只是适用于 64 位的操作系统，目前 Sia 没有适用于 32 位操作系统的钱包软件。

该软件是一个绿色免安装软件，只要将其解压缩在你的硬盘中，运行其中的 Sia-UI.exe 即可。如果文件无法下载，请考虑使用科学上网方式。

30.2.1.1 创建钱包

1）运行时必须有计算机管理员（adminstrators）的权限，否则会出现错误报警。

图2. 1 sia 钱包安装错误报警

2）启动 Sia-UI.exe，稍等一会，出来一个主窗口。

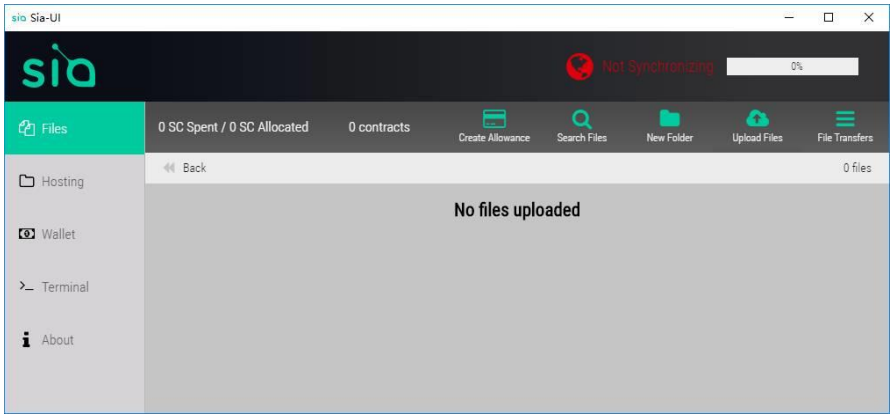


图30-1 Sia-UI 的主界面

3）点左侧的 wallet 钱包，**勾上“use custom passphrase”这个选项**，再点“create a new wallet”。

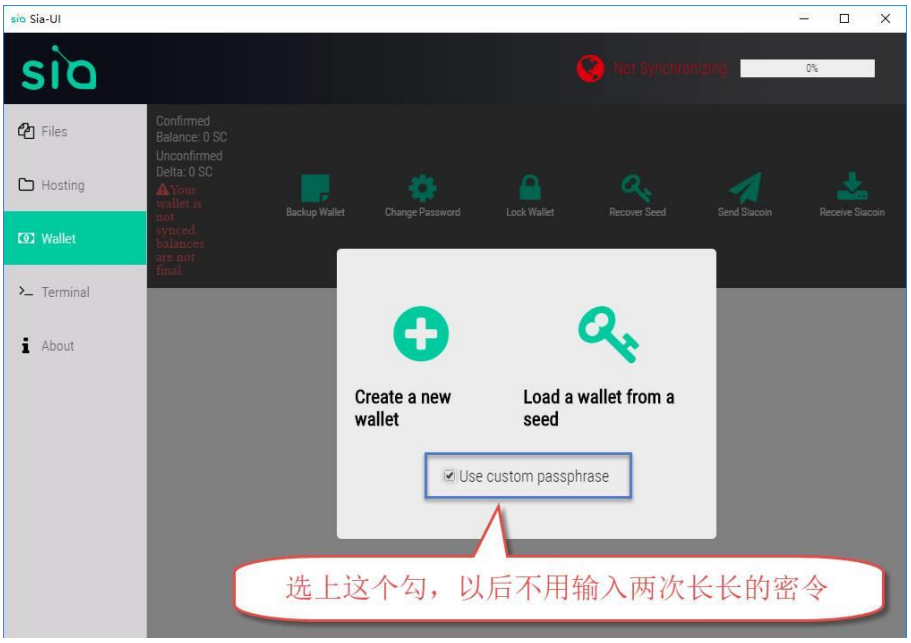


图30-2 新建钱包

软件会提示你输入密码，再让你抄下许多英文单词（seed），**请把这个长长的字符串认真地、只字不差地抄下来**——不要拍照、不要发邮件、微信、QQ 等。放到安全的地方，将来你的 Sia 货币（代币名称 SC）就靠这串密令打开了。

切记、切记、切记，牢记 seed 和 password：

如果遗忘它(seed, password)，谁也无法帮你找回；

如果被别人偷走，你的 SC 也就没了。

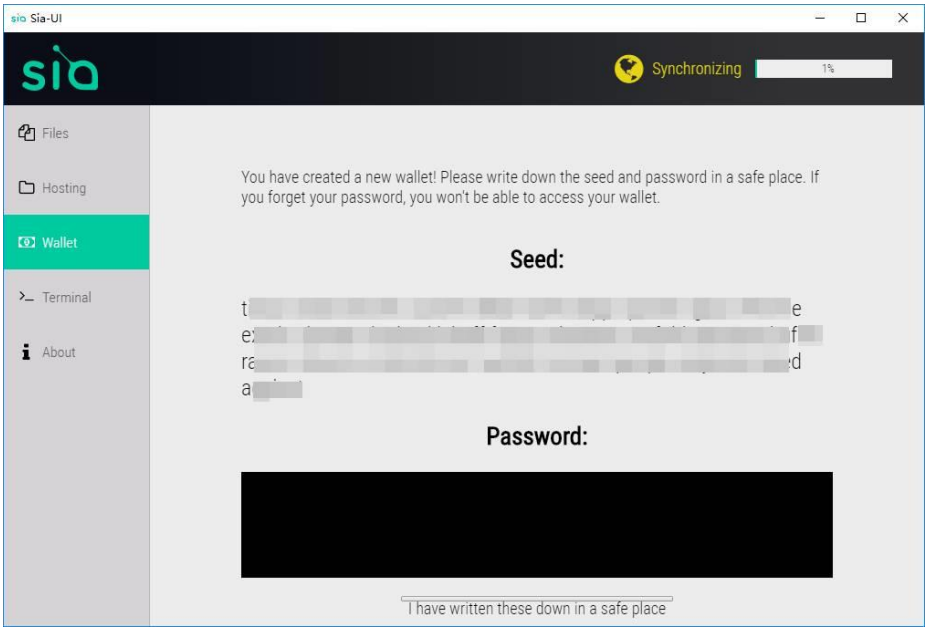


图30-3 种子和密码

程序为了确认你已经正确地记住了密令，会马上让你再输入一遍 seed 和 password（一个字母也不能错）， 这样钱包就建立好了。

30.2.2 软件与安全或杀毒软件的冲突

Sia 官方目前没有轻钱包，上面使用的钱包软件必须同步区块链全节点数据文件。目前 Sia 区块的高度是 *14187*，区块链的文件大小约 8G，随着时间的推移，区块高度会不断增高，文件也会越来越大。第一次运行钱包软件，建立钱包的同时，软件就开始进行数据文件同步。同步的时间根据你网络的带宽会有不同——一般来说 2-3 天时间就可以完成了。

在这个同步过程中，如果安全软件和 Sia 钱包软件有冲突，而你又不在电脑旁边（2-3 天，谁也不会守在电脑旁的），这时数据文件的同步就会停止在某一个阶段。软件同步界面显示错误。“Access is denied”是其中一条。这时候，软件无法继续运行和同步了。

关闭钱包软件，再次启动后软件也无法正常运行，会出现下面的故障，如下图：

图2. 2 sia 钱包错误报警

报警的意思是 Siad.exe 文件找不到了，无法正常运行。解压缩后的 siab.exe 文件本来是在\ Sia-UI-v1.3.1-win32-x64\resources\app\Sia 文件夹中，但是被安全或杀毒软件（比如 360 杀毒软件或网络安全卫士）判定为危险文件，被当作病毒软件删除了。

解决办法：重新将 Sia-UI-v1.3.1-win32-x64.zip 解压缩覆盖到原来的文件夹中，恢复被删除的文件;同时退出杀毒软件或者将 Sia-UI-v1.3.0-win32-x64 文件夹列入杀毒软件的白名单中，避免被误杀；删除%UserProfile%\AppData\Roaming\Sia-UI 目录下的文件，重新启动 Sia-UI.exe，重新设定钱包，重新开始。

30.2.3 Sia 区块链全节点数据文件

对于 Windows 系统，Sia 区块链全节点数据文件默认保存在“%UserProfile%\AppData\Roaming\Sia-UI\sia\consensus”目录中的 consensus.db 文件内。由于全节点数据文件比较大，而且随着时间的推移会越来越大，会对系统盘的使用有影响，所以有必要将其转移到硬盘其他地方。转移的方法如下：

（1）彻底退出 sia 钱包软件；

（2）备份 sia 文件夹（C:\Users\INSERT_YOUR_USERNAME_HERE\AppData\Roaming\Sia-UI）

（3）将上述文件夹拷贝到新的地方（目标文件夹）；

（4）删除原来的文件夹（C:\Users\INSERT_YOUR_USERNAME_HERE\AppData\Roaming\Sia-UI）；

（5）打开命令行模式（cmd），使用如下命令：mklink /J “原文件夹”“目标文件夹”（注意要在管理员权限，这个命令的运行结果是在原来的文件夹中建立一个文件指针，指向新

的目标文件夹，所以这种方法适用于任何软件或钱包的文件转移）。

同步区块链全节点数据文件的时候，如果中途中断后无法正常启动 Sia-UI 软件，比较简单的方法是重新开始。将 C 盘中的文件夹%UserProfile%\AppData\Roaming\Sia-UI 全部删除，重新运行 Sia-UI 文件。如果想从刚才中断的数据文件进度中开始，可以将未同步完的全节点数据文件 consensus.db 另存并保留下来。重新启动钱包软件后可以将其拷贝回原来的目录，减少同步时间。

这时候需要注意的是，由于更换了全节点数据文件，运行软件时会显示正在同步最新版本，而且需要比较长的时间，甚至需要几个小时。但是对于下载了 1-2 天的文件，还是值得等待的。

30.2.4 不断变化的 Sia 的钱包地址

Sia 的钱包每次生成的地址都不一样，官方的解释是，基于私密和安全的要求，每次都生成一个新的地址，不过旧地址一直是有效的。所以你可以保留原来的地址，也可以每次用新的地址进行收币，Sia 都在你的钱包里。

30.2.5 查看结果

SC 的区块数据同步很慢，如果等不及，可以到这个网站查询交易的确认情况：https://explore.sia.tech。

31 Press.One

31.1 Press.One 解读

李笑来的 Press.One 是在 2017 年 7 月 12 日开始 ICO 的，但根据国家政策，在当年的 9 月 6 日已经完成退币。抛开火热的 ICO 不谈，从官网上发布的 Slide（PPT 的幻灯片）中，我们看看这个 Press.One 到底想做什么？

Slide 1

如果说，世界上第一个成功的区块链应用，比特币，本质上是使用去中心化的方式颠覆了银行的商业模式。

那么，PressOne，就是使用去中心化的方式颠覆出版发行，进而彻底改变每一个内容创作者的商业模式.....

以前的商业活动的交易中心是银行，而内容出版发行的中心是出版社，这个去中心化的应用就要让作者与读者直接相连，实际上 steem（https://steemit.com）当前正在做这件事，内容的创作者、分发者和读者都有利可图——虽然李笑来不承认 Press.One 是 steem 的本地化，但它的运营模式肯定会大量参考 steem。

Slide 2

PressOne 可能会成为互联网上最大的公链，因为互联网本来就主要由内容构成，无论是图文、声音、还是影像……

颠覆原有的发现途径、分发渠道，很可能等同于“重建整个互联网”。

PressOne 很可能会成为 DAPP 最自然、最丰富的公链。

公链：就是公有区块链，全世界的人民都可以使用。

发现途径：由于内容的转发、评价等都用代币 PRS 来参与，没有免费一说，有价值的内容自然会发现。

分发渠道：分发者会消耗 PRS，但如果带来了阅读量，他会有可观的收益，所以促使他分发有价值的内容。

重建互联网：整个互联网不再是充斥着垃圾内容的信息互联网，而是价值互联网。

DAPP：去中心化应用，PressOne 本身也会开发一款重量级应用，感觉前期会类似 steem，但肯定会按国内行情改造。

Slide 3

一切内容产业中都有三个环节，制作、发现、分发。

制作，必然是优秀个体或团体所为，不需要去中心化完成；然而，发现与分发，去中心化网络一定更有优势……

手里握着好内容，或者可以写出好文章的人，将来大有可为。

发现与分发：想想数亿用户在利益的驱使下自组织地进行这个活动，会促进好内容的传播，也就是促进价值的传播。

Slide 4

这是内容创作者的商业模式革命，不再被中心化机构所限制。

创作完成之后，一切都可以交由市场处理。每发布一个作品，就相当于发布了一个“资产”（作品证券化），至于它的价值，无需中介，直接由市场来检验。

创作者、发现者、分发者，这三个角色可能相互重叠，但无论哪一个都应该有利可图。

不需要出版机构了，一个内容的好坏全部交给市场去决定，充分利用了系统论中的自组织概念。

Slide 5

实名制不仅不像一些人想象得那么可怕，很可能恰恰相反，它更可能鼓励人们发表负责的言论……

如果有匿名的需求，无需担心，因为原本的互联网上有无数的地方、无数的方式可以匿名。

全部实名，更符合中国的行情。

Slide 6

审查机制同样并不一定是洪水猛兽，有共识机制辅助的审查，同样可能会提高内容质量。

它不一定会限制自由，理由还是一样的：如果创作者讨厌审查，互联网上有很多其它地方、很多其它方式可供使用。

所有的读者本身就是审查员，可以用举报+投票机制，举报成功，侵权的内容所得的非法收益会被重新分配，我猜的。

Slide 7

PressOne 并非一个“中国本地化”项目，它所提供的机制，对内容创作者来说，不分国界，不分种族，不分性别、不分语言……

感觉前期就像 steem 的中国本地化项目，脑洞会比 steem 开得更大。

Slide 8

PressOne 正式上线之前并不提供所谓的“白皮书” —— 那个通常即便是提供了也没多少人看得懂，甚至就没几个人看的东西。

正式上线之后，项目本身会有不断完善的文档（Documentations），为后继的开发者们提供完善的支持。

白皮书确实看不懂，但文档必不可少，以笑来的风格，估计他以后会补上的。

Slide 9

在 PressOne 的基础上，开发者和运营者们可以很容易地启动各种内容社群，社交媒体……

这不再是只属于技术极客的机会，这也是内容创造者们运用最新趋势的宝贵机会。 他们不需要了解技术，不需要了解区块链，正如每个人其实并不需要完善的金融知识也一样可以正确使用钞票一样……

感觉像是点击几下按钮，就建立起一个付费社群，内部流通的货币全部是 PRS。

Slide 10

也可以把 PressOne 想象成一个巨型孵化器，对每一个垂直方向的开拓，我们都会组织“竞选”，由社区成员选择出尽可能最合适的人或团队去“征战”。

这部分与平常的项目不同，看公布的 ICO 方案，有一部分 PRS 就是留着做这件事用的，

留给好的项目。

Slide 11

PressOne 不是一个公司 —— 区块链的世界里，理论上并不需要一个公司主体存在。

一个好的区块链项目，理想目标是创造一个去中心化的自治企业（或组织），一切的规则，尽可能都写进基础协议（或智能合约）， 而不是靠所谓的“强运营”去完成。只有这样，它才是真正可持续的、可扩展的。

就像中本聪建立了比特币系统之后隐退一样，没有他比特币系统仍在发展，系统通过**自组织**的机制来持续发展。

Slide 12

为什么我们最适合来做这件事儿？

首先，我们在中国，地球上互联网用户最多的国家； 其次，我们的开发团队来自世界各地，在区块链世界里的开发经验加起来超过一百年，用户体验设计也是全球领先； 还有就是，我们有太多的相关资源，想象一下“一块听听”建立在 PressOne 之上，想象一下 Knewone.com 建立在 PressOne 之上……

有关 PressOne 开发团队的信息并不多，这是最让我担心的。

我很害怕腾讯公司发力，但腾讯是中心化的公司，与这种去中心化的理念本不相容，腾讯会发起一个私链？做出一个去中心化的微信？

31.2 李笑来的 Press.One 设计理念

2017 年 7 月 11 日，李笑来在“一块听听”分享了 PressOne 的设计理念，本文是申龙斌的理解。

31.2.1 投资方面

投资人的逻辑要好，不能靠信仰，靠信仰的人不需要逻辑。

投资是一个不断学习的过程，自己要形成自己的投资逻辑，区块链技术很好，但不能仅靠单纯的信仰冲了进去，而要有自己的投资逻辑。

投资是一个长期的过程，这个长期可能不是 1 年，而是 4 年。

李笑来在这里讲到了与 Daniel Larimer 结缘的故事，这个 Daniel Larimer 是个非常了得的人物，又称 Bytemaster，代号 BM，在区块链世界中做了三个项目（Bitshares、Steemit 和 EOS），每个都非常成功。想与他套近乎的可以看看他的 Linkedin 主页：http://www.linkedin.com/in/daniel-larimer-0a367089/

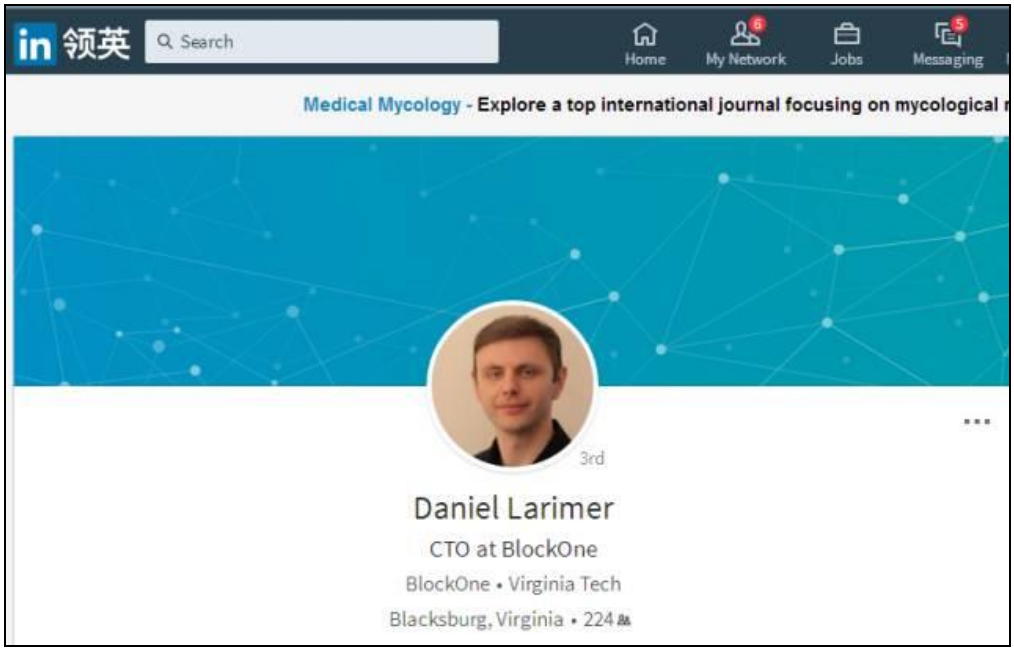


图31-1 Daniel Larimer 的领英页面

但从李笑来的这个故事看来，投资一个靠谱的人更重要。虽然 BM 与两个 CEO 闹掰了，但 BM 并没有损害投资人的利益。

投资领域中有许多机会，不是你的，你别要，也别懊恼。

李笑来虽然是币圈的老江湖，仍然错过了以太坊的投资。我感觉现在的市面上已经有上千种币，机会肯定有，但更多的是坑。

31.2.2 PressOne 设计原则

Steemit 是 Press.One 的前期 MVP

MVP 即 Minimum Viable Product，最小化可行产品，我在《Press.One 解读》已经猜到李笑来的这个项目将会大量参考 Steem，所以现在多研究一下 Steem，肯定会发现将来 Press.One 的不少机会。

Press.One 的设计原则：简单。

有些事情想得复杂了，就没有了答案，碰巧“分享与成长群”里的一位朋友今天发了一个四方块问题，与这种思想挺类似。遇到一个问题时，由于人脑的思维定式，都会去寻找复杂的解决办法，以至于对显而易见的解决办法视而不见。

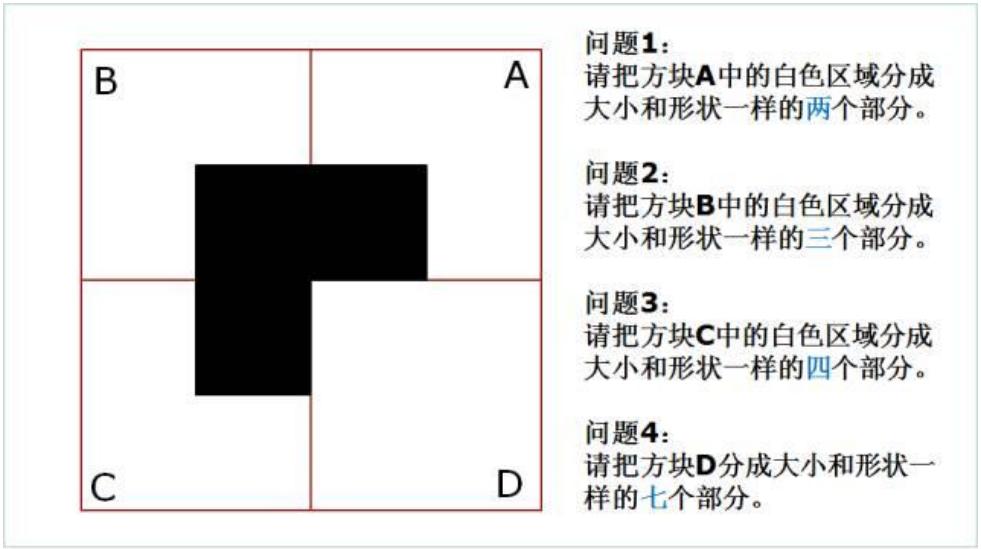


图31-2 一个思考题

（在微信公众号“申龙斌的程序人生”里回复：四方块，看问题的答案）

想把系统设计得简单并不容易，中本聪在设计比特币系统时，他的源代码写得不是非常优秀，但他把整个系统设计得非常精练，多一分则肿，少一分则缺。

严格的实名 + 严格的强关系 = 和谐社会

PressOne 坚持实名制，李笑来更喜欢微信上的和谐，不喜欢微博上的混乱。

不一定都要去中心化

实名认证适合中心化来解决，有些内容的存储也适合中心化，并不一定非要用去中心化的方案。比如，一些违反社会道德伦理的内容，如果写入区块链，将永远存在，本身并不是一件好事，这种东西需要一种机制（HASH+智能合约）来解决。

关于盗版认定的事情，交给市场来解决

因为这些记录会被区块链永久地保存下来，该实名作者的信用记录会受到严重影响，以至于影响他将来的收益。

更合理的利益分配

参考 steem 的机制，writer 和 reader 都有利可图。

writer 负责内容的发行，虽然一些内容仍会放在一些大平台上，超链接则通过 HASH 加密保存在 Press.One 的公链上（笑来老师原来说，PressOne 的底层链将基于 EOS，后来又说基于 Xin 开发，所以还得研究一下 Xin 的具体技术方案），这样区块链并不臃肿，毕竟大量用户点赞、转发的行为都要消耗 PRS，这种高并发量不能用以太坊——估计在以太坊（ETH）建立 PressOne 会卡爆以太坊。

Reader 购买内容需要消耗 PRS，分发也需要 PRS，但如果这种分发带来了更多的购买和再分发，则会给这个 Reader 带来可观的分成。

2016 年“分答”中对提问者、回答者的利益分配创新，造成了分答当时的火爆场面。

共赢

并不是与一些常规的内容发行方抢食，而是一种共赢机制，这些中心化的平台可能会过得更好。

31.2.3 区块链的生存原则

要等到下一个牛市，才算是真正入行.....

现在的行情，在几年前也是惊人的相似，能够穿越熊市的人并不多。

31.3 PressOne 进展

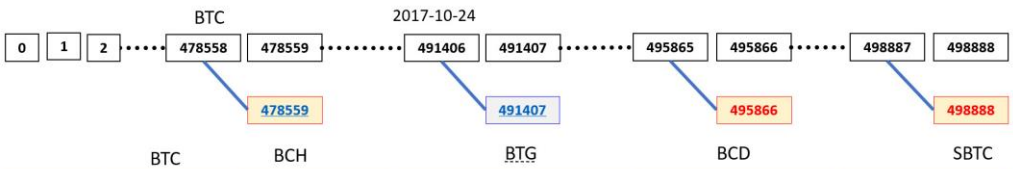
PressOne 的消息不多，曾经还出来一个网站 B.Network，出现过这样的介绍：

> B.Network 是去中心化的内容分发平台，是一个内容分发公链，人们可以在这里创建各种各样基于内容的去中心化应用，比如博客、论坛、微博、电商、音乐分享、图片社交、视频直播.....

2018 年 2 月，press.one 上线，当前功能非常弱，只是绑定了一个身份，其代币 PRS 可以在 big.one 交易，期待其后续有更好的表现吧。

32 BTG 比特黄金？

2017 年 10 月底，比特币分叉出 Bitcoin Gold(BTG)，2017 年 11 月 12 日，BTG 的全节点的客户端才出来，2018 年 2 月 23 日的价格为 130 美元。2017 年的 11 月和 12 月，比特币分叉泛滥，市面上主要流行的分叉币见图 32-1。



中文名称	比特币	比特币现金	比特币黄金	比特币钻石	超级比特币
分叉时间		2017-8-1	2017-10-25宣布分叉 2017-11-12正式出块	2017-11-24	预计2017-12-17
数量	2100万	2100万	2100万	2.1亿	2121万
挖矿算法	SHA256	SHA256	Equihash	SHA256	
区块大小	1M	8M	1M	8M	8M
出块速度	10分钟	10分钟	10分钟	10分钟	
SegWit	支持	不支持	支持	支持	
难度调整	2周	DAA	EDA	2周	
口号	正宗比特币	真正的比特币	让比特币回归去中心化		拯救比特币

图32-1 几种主要的比特币分叉币

32.1 BTG 分叉的目标

官网上声称要让比特币重新回归“去中心化”。现在挖比特币的机器都配备了专业的 ASIC 芯片，普通用户根本没机会，背离了中本聪的“一 CPU 一投票权”的初衷。比特币已经被矿池老板绑架了，中心化趋势非常严重，BTG 想改变这种状况，让用户回归 GPU 挖矿。

32.2 几个事实：

1）工作量证明机制由 SHA256 改为 Equihash（即 Zcash 使用的算法），这是最大的变化

2）Bitcoin gold 项目由香港挖矿公司 LightningASIC 首席执行官廖翔主导

3）每出一个块就进行一次难度调整

4）开发人员预挖了 10 万枚 BTG

5）分叉高度为 491407，在国际标准时间 2017-10-24 01:20:39，也就是说在这个时间之前如果拥有 BTC，就应该拥有 BTG，除非交易所或钱包公司耍流氓

32.3 几点有争议的地方

1）关于工作量证明算法的调整，采用 Equihash，当前世面上并没有支持该算法的 ASIC 矿机，但是，如果需求足够强劲，支持 Equihash 算法的芯片很快也会被做出来，而 BTG 的去中心化的目标就是空话了。

2）即使用 GPU 挖矿，确实不被矿池绑架了，但 GPU 市场被英伟达和 AMD 所控制，也无法去中心化。

3）开发团队被质疑水平不够，曾经悬赏实现重放保护功能

32.4 提醒

Bitcoin Gold（BTG）的官网是：https://bitcoingold.org 。市场上出现许多假冒网站，小心被骗，不要没领到糖果，丢了大西瓜。

参考阅读：

- Bitcoin Gold（BTG）：对抗挖矿中心化，比特币分裂的新思路，http://www.cheekr.com/P/76382
- 继 BCC 之后，又一个 Bitcoin gold 比特币硬分叉即将到来 https://www.sohu.com/a/195196118_325319
- BCC 之后，BITCOIN GOLD 又是什么鬼？真怕比特币被你们玩坏了 http://www.jinse.com/news/bitcoin/74555.html
- 比特币硬分叉 BTG 存在诸多问题 社区质疑该分叉为欺诈 http://www.jinse.com/news/bitcoin/78566.html
- Bitcoin Gold to Launch on November 12, But Will Anyone Care?https://www.cryptocoinsnews.com/bitcoin-gold-to-launch-on-november-12-but-will-anyone-care/
- Bitcoin Gold: What you need to knowhttps://bitcointechtalk.com/bitcoin-gold-what-you-need-to-know-8b3e645be409
- Bitcoin Gold Sets Sunday Date for Cryptocurrency Release，https://www.coindesk.com/bitcoin-gold-release-cryptocurrency-sunday/
- 比特黄金的官方博客，https://bitcoingold.org/blog/
- NOT official websites & SCAMS，https://bitcoingold.org/not-official-websites/

33 BIG

33.1 BigONE 是什么？

BigONE 是 INBlockchian（硬币资本）旗下全球区块链资产现货交易所。其前身是云币网。云币网于 2014 年 4 月正式上线，2014 年 10 月 8 日正式命名为云币网，国内早期进行区块链投资的人都比较熟悉，云币网曾经做到 EOS 交易量全球第一。

2017 年 7 月份，Bigone 作为云币网国际版在 ico.info 网站上进行众筹，发行 BigONE 代币，据说在 20 分钟内就众筹到了 1.5 亿美元。9 月份，由于政策原因云币网停止了交易，BigONE 众筹的所有代币也原路退还给投资者。

Bigone 没有完成众筹，但是在 10 月份，BigONE 交易所还是如期上线。

33.2 不众筹，代币从何而来？

自从 BigONE 退回众筹的 EOS 代币后，就没有再开展众筹活动。2017 年 11 月 25 日，BigONE 资讯公众号发布公告：*同行们占领宇宙，我们只准备了一堆糖果.*

前期参与过 BigONE 众筹的白名单用户以及在 BigONE 交易所存有各类区块链资产的用户等都可以分到相对应的 BIGONE 代币（代号 BIG） 。

一个月下来，BigONE 发出来近 2000 万个 BIG 代币（数据来源 BigONE 的 CEO 老猫公众号的留言）。但是通过区块链查询，第一个地址拥有约 1.5 亿个 BIG，应该是 BigONE 团队拥有。第二个地址拥有约 5000 万个 BIG，推测是交易所分发给大家的糖果，依然放在交易所的钱包中。所以，具体数据不是太明确，但是可以肯定的是超过 1.5 亿个代币是在团队手里的。

至于没有分发出来的 BIG 如何处理，是否每年按照一定比例释放出来还是其他方法，不清楚。按照交易所 CEO 老猫的答复是：会用这些代币让更多人一起创造更大价值。

社区和市场给出的回应是肯定的。12 月 25 日，BIG 代币在 BigONE 自己的交易所上市，开盘就 30 多人民币 。就当时面言，2 亿个代币的市值就是 60 亿人民币了。

33.3 BIG 的价值何在？

一句话就是：BIG 代币就是 BigONE 交易所的权益证明。为什么这样说？我们看一下代币的规则（BigONE 目前官方的说明和早期白皮书的说法是一致的）。

BIG 代币回购机制:

为保证 BIG 代币足够的市场深度与稳定的价格增长,无论现有二级市场所流通的 BIG 代币数量多寡，BigONE 团队都将对 BIG 代币进行回购。

BIG 上线后，回购销毁分为两阶段：

第一阶段为六个月，BigONE 团队将在每个自然月拿出平台 40%的手续费收入用于回购 BIG

代币。

第二阶段为 BIG 上线六个月后，BigONE 团队将视平台的发展状况，逐步调整至每个自然周拿出平台 40%的手续费收入用于回购 BIG 代币。

回购的 BIG 代币将会发送到一个没有任何人掌控私钥的地址直接销毁,任何人都可以通过以太坊区块链浏览器查询，以确保公开透明。

正是这个回购机制，BIG 代币的持有者就拥有了 BigONE 交易所的股权收益。为什么这样说呢？每月或者每周交易所 40%的手续费收入用于购买 BIG 代币，就等同于每月或者每周 BIG 的净值增加。相对应的 BIG 的价格就会升高。代币的持有者就可以通过出售代币兑现收益。

40%的手续费收入是明显比 40%的利润更高，那就是相当于股权收益大于 40%。但是无法确认到底占比多少，因为不知道 40%的手续费到底和利润是什么关系，但是基本上可以肯定大于 40%的利润的。

因此这 2 亿个代币所占有的 BigONE 交易所的股比大于 40%。也就是说交易所的估值小于 60 亿除以 0.4，小于 150 亿人民币，这就是 BIG 的价值所在。只要数字货币或者说区块链成长的趋势确立了，未来交易所的手续费大概率是越来越高的。

33.4 为什么要做 BigONE 的股东？

除了前面所说的代币回购以外，还有 2 个比较大的特点或者优势：

（1）公开透明和诚信（这一点我认为是最重要的）

BigONE 的 CEO 老猫在公众号所说，**公开透明和诚信是交易所的原则**。BigONE 将公开平台所有区块链资产的冷，热钱包地址，每天公布平台当日所有交易数据及平台账户资产余额。通过账户资产余额总数可以核对是否与冷，热钱包资产数量一致。同时，平台用户可以在公开的数据列表中以加密方式查询自己的交易数据与账户资产余额。一一对应，人人可查，以确保公布数据真实可信。通过每日交易总量可以计算平台每周分红，监督回购金额是否足额。

（2）用户上架资产

团队除采用 INB 原则挑选优质区块链资产，还将以 ULA (User Listed Assets) 方式上架区块链资产，即当某一区块链资产在 BigONE 用户与存量达到一定数量时启动交易。

33.5 BIG 有没有让人感觉不放心的地方呢？

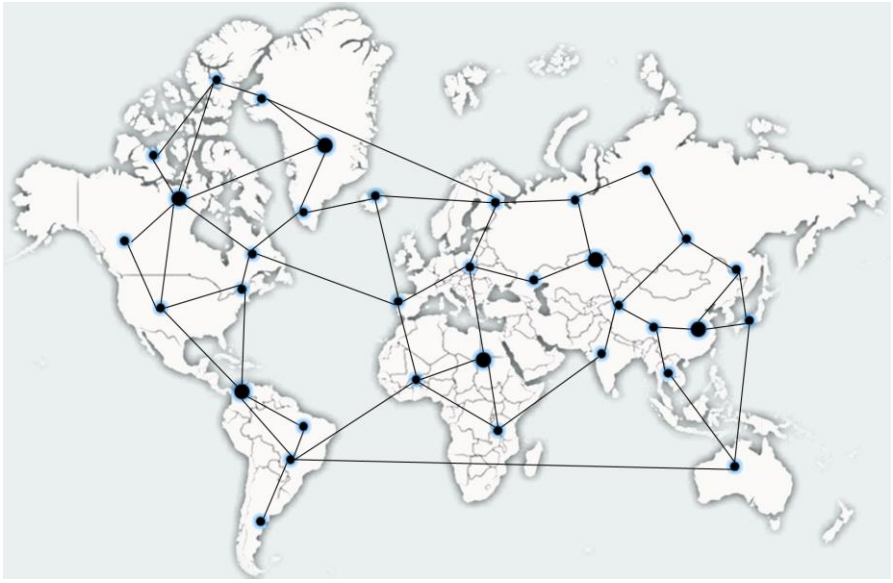
在网站 https://coinmarketcap.com 上能查到的数字交易所超过 400 家，BigONE 要在其中厮杀出来，到达其白皮书所说的第三名，需要时间的考验。目前在 https://coinmarketcap.com 中查询到 BigONE 的日成交额离其白皮书所说 3 亿美元还有不少差距。

团队中持有的超过 1.5 亿个 BIG 代币，处理方案不明确，也会是投资者心中的一个疙瘩。比如前段时间在火币网上线的 WAX 突然增发 10 倍代币，WAX 价格从最高 10000 元掉到最低 5 元左右，投资者损失惨重。

33.6 结论

区块链世界本来就是高风险的，哪里有什么确定的百倍币，哪里有百分之百可以赚大钱的数字货币。但是成为数字货币交易所的股东，是一种比较简单的分享数字货币经济繁荣的方法，拥有 BIG 就能分享到 BigONE 成长带来的收益，就好像股市的牛市行情会给股票交易所带来大量的收益是一样的道理。

第六篇 投资实操篇



34 参与区块链投资的几种方式

关于区块链投资，涉及的内容很广。很多新人不敢入场，不知道如何入场，入场了不知道买什么……进场之后，有些人是看到哪个币便宜就买哪个，看到号称私募的项目就跟着上，以为自己捡到了宝。之所以会这样，其实是大家比较心急，怕错过车。还有一些人呢，则是以为自己进入了区块链投资领域，而实际上是进入了披上了区块链外衣的传销组织。比如 3M、以太坊贸易、Zcash plan 等， 甚至很多人去买老牌的传销币、很多都是 2013 年那个时期流行的山寨币，比如雷达币、无界币、公牛币……有些一听名字就知道没多少价值，不过这个市场最不缺的就是进来接这种盘的钱。

所以除了自己在这个行业盲目摸索外，还需要一位能为你指明方向的人，本章节尝试从一个新人的角度来看待这个行业的机会，希望帮助朋友们发现新机会以及避开一些坑。

区块链投资是非常个人化的话题，区块链行业中的玩法众多，每个人都可以选择适合自己的方式去参与区块链投资，并不一定非得听从一些人的意见，按照别人的想法去投资。不过，投资中的个人心得可以作为一种思路，以供朋友在进入区块链投资领域时借鉴。

34.1 囤比特币

参与区块链投资有很多种方式，而不同的方式有不同的利弊。每个人因为时间、空间、地点的不同导致其擅长的的东西也各不相同。

假设我们本来擅长另一种方式投资方式，但是我们并不知道，导致只能使用单一方式进行投资，而且这种投资方式并不适合我们。其实我们稍微想一下就能明白，本来我们擅长另一种投资方式，但用的是我们并不擅长的投资方式，虽然也有些收益，但是相对来看，我们的投资就变成了事倍功半的投资。

所以，既然打算参与区块链投资，那么就很有必要了解一下区块链世界到底有哪些投资方式，看看究竟哪种投资方式最适合自己，怎样做才能最高效。

比特币已经经历了九年的发展（2009 年至今），数百万倍的涨幅早就证明了一个道理：尽早买入比特币，并拿着不动，是获得这个行业增长带来红利的最好方式之一。实际上，自比特币出现以来，一直都有人这样怀疑：比特币已经涨了这么多倍，现在还能买吗？他们普遍认为现在比特币价格已经很高了，后期很难再涨，从而更倾向于买便宜的山寨币，因为他们认为

这样的方式翻很多倍的机率更高……

怀疑是人的直觉，是人的本能，但不妨逆向思维地想一想，比特币已经翻了百万倍了，它还在乎再翻两三倍么？

比特币在现实生活中没有什么可以锚定的东西（黄金都不是它所能锚定的），所以贸然给它贴上一个价格范围标签是不太合适的——甚至是比较愚蠢的。

囤币的优点：方法极其简单。

囤币的难点：守币难。都说守币比守寡难，几乎没有人能做到买完就忘记这笔投资，能守住比特币百倍千倍不放的人真的少之又少，正因如此，我们也没有必要去羡慕那些早期参与比特币投资的人——因为能守住的其实没几个。

34.2 挖矿

早期能进入挖矿领域，是很需要胆识和见地的。很多人无法理解虚拟货币为什么要挖矿，而挖矿的巨大投入也着实让人怀疑，这么大的成本是否可持续？未来政策对挖矿会不会有很大的影响？

图34-1 比特币矿场

专业挖矿需要场地、电力和矿机等几个要素的支撑，一般人搞不定这些事，风险很大，但还有一种参与办法，叫联合挖矿。有专业的团队帮你把这些琐碎细节搞定，收益和风险共同承担。你的投资策略只有一条，把钱投给靠谱的团队。而那些无诚信的矿池、矿场老板会克扣你

的算力，让你一直蒙在鼓里。

随着币价进一步的上升，到了现在（2018 年），比特币仅仅剩余四百多万个没被挖出来，获得比特币也变得越来越难……如果真是比特币的信仰者，相信比特币一时半会不会失败，那么，参与比特币的挖矿可能是一个非常不错的选择。

挖矿优点：用相对便宜的成本获得比特币。

挖矿难点：

前期需要巨大的投入（主要是矿机设备）；

矿场维护成本也不小，而且还要花上不少心思来保持矿场的持续稳定运转。

短期看，挖矿的收益可能跑不过囤币的收益（人民币计价的话）。

34.3 搬砖

搬砖是币种倒买倒卖的别称，比如同一个币种在两个交易所之间的价格不一致，于是就有机会可以低价买高价卖，这种行为通常被称之为搬砖。

过去比特币独霸市场，币种少、平台少，搬砖机会不多。搬砖这种活通常很容易就被专业的大公司团队与搬砖机器人把市场差价给抹平。如今币种越来越多，交易所也百花齐放，各币种的计价方式也千差万别，出现了以法币计价，以 BTC、ETH、QTUM、EOS、平台币等多种方式计价，市场价格经常出现短暂的不平衡现象，所以会有各种各样的搬砖机会：

跨国搬砖。地域之间存在价格差异是有它的道理的，唯有能打通这条神秘通道的人能吃上这杯羹，这其中涉及到跟法币打通的问题，所以有很大的政策风险。

炒新币。很多新币上新平台都会出现一波不正常的涨跌，很多人就趁那几分钟做一做短线，也能获得不少收益。

暴涨暴跌中找机会。平静的市场搬砖机会少，大起大落之下经常出现一些币种价格不正常的情况。

优点：技术好的话，收益非常可观。市面上也有一些自动搬砖的软件，运用得当可以获得不少的收益。

难点：

很少人能有这种敏锐的洞察力。

手动搬砖特别消耗个人注意力。

搬不好容易砸脚（亏损）。

34.4 OTC 场外交易

由于国内法币买币的通道被禁止，让人不得不学习场外交易的技能，如果想成为职业的场外交易员，其实这跟搬砖并无两样。

做场外交易，最好要有两条优势：

自身声誉：尽管自己的价格比别人高，但别人就是愿意从你这买，这靠的是信任。

找到更便宜的买币渠道：币卖掉容易，关键能找到更低的价格渠道再把币给买回来，才能保持你生意的持续运转。

场外交易的优点：人品好才能赚钱（币）。

场外交易的难点：

容易形成赢家通吃的局面，对于没影响力的新手来说其实挺难。

同样有渠道壁垒，需要把买币卖币的渠道打通，普通人没有这样的渠道。

34.5 参与 ICO

参与 ICO 相当于购买了潜力新股，新股的优势相对于已经在市场流通的股来说，更有可能出现相对更被低估的品种，如果能看得懂项目逻辑，并且有一定的市场敏锐感的话，投 ICO 仍旧是一个不错的选择。

操作方式：

寻找优势项目、被低估的项目，参与私募或者 ICO，买入项目代币，一旦获得预定的收益，就部分撤出、剩余留作长线投资或者干脆全部撤出。

ICO 的优点：拥有很多行业新机会。

ICO 的难点：

非常考验一个人的眼光。目前 ICO 已经五花八门，十里挑一变成了百里挑一。

碰上熊市，上线破发机率大，风险非常大。

未必能跑得过主流币。长期来看，大部分币可能都跑不过比特币或以太坊本身的涨幅。

目前参与 ICO 有门槛，会碰到各种身份认证问题，普通人可能无法直接参与 ICO。

34.6 炒币

也就是低买高卖，这个并不是我们要在这个章节所讨论的，但值得一说的是，炒币基本就注定与十倍币、百倍币无缘。一般炒币的话，币涨了百分之三五十就会撤离，炒币的心态无法承受数倍的涨幅，股市与币市的逻辑不同，短线看 K 线的方法也许逻辑相通，但炒短线很难抓住整个行业上升的机会，而且，短线技术不好的话十有八九的结果是币越炒越少的。

34.7 做项目

自己开交易所、或者自己做区块链项目去融资也是参与区块链投资的一种方式。但这是一个门槛极高但是做好了回报巨大的事情，只有极少数人会（能）选择去做的。实际上，现实中创业者占总体人群的比例其实也不大，但如果你是个技术宅，非常推荐你扎根到这个领域中去——因为这样更为划算。

34.8 其他

除了上面列举的几项，另外还有很多可以做，比如期货、杆杠、大资金自己控盘做庄(俗称"割韭菜")、专业 ICO 代投、基金+私募等。互联网创业如自媒体、周边资讯、信息论坛等，传统实业如矿机研发生产，矿机贸易、矿场运作、出售云算力等。还有些依靠真正的区块链应用来赚钱的，如 Steemit 写作、玩 CryptoKitty"加密猫"游戏、甚至虚拟货币赌场、亦或是成为某区块链全节点进行 PoS 挖矿、加入到任何区块链生态中都可能能寻找到新的赚钱机会，而且长期来看，以后这方面的赚钱机会会越来越多。哦，对了，技术厉害、野心大点的还可以自己造山寨币，分叉比特币、以太坊……等等。

35 搬砖

35.1 区块链低风险套利——搬砖篇

搬砖：利用数字货币在不同交易平台的价差，从一个平台买入，再搬到另一个平台卖出进行套利的行为。由于现在价差很小，每次搬砖利润微薄，需要通过量的积累来获利，并且还要承担价格剧烈波动产生的风险，所以形象地用“搬砖”来类比。

有了上面的定义，我们不难发现，**搬砖的本质是低买高卖。**

搬砖有单向搬砖（硬搬砖）和双向搬砖（对冲搬砖）：

单向搬砖（硬搬砖）需要在不同交易所转账；

双向搬砖（对冲搬砖）不需要转账，需要在两个交易所配置同样的币种。

目前更多的是赚取 BTC 和 ETH 等区块链中的币种，其实 BTC 和 ETH 目前就是区块链的法币，你可以用它们来买其它币种。

任何两个币种都可以用来搬砖，只要有相应的交易对转换就行。

比如 BigONE 上 INK 和 QTUM 两个交易对，gate.io 上也有这样的交易对，那有价差就可以考虑搬砖，赚取 INK 或 QTUM 都可以。

35.1.1 搬砖准备工作

1）注册交易所，国内主流交易所有 OKCoin、火币、比特时代、比特儿、聚币等等，国外主流交易所有 poloniex、coinbase、kraken、bitflyer、bitfinex 等等。

2）注册 btc，eth 钱包，比如：imToken，覆盖以太系品种的钱包，jaxx，目前支持币种包括比特币、以太坊、Zcash 等数字币的钱包。

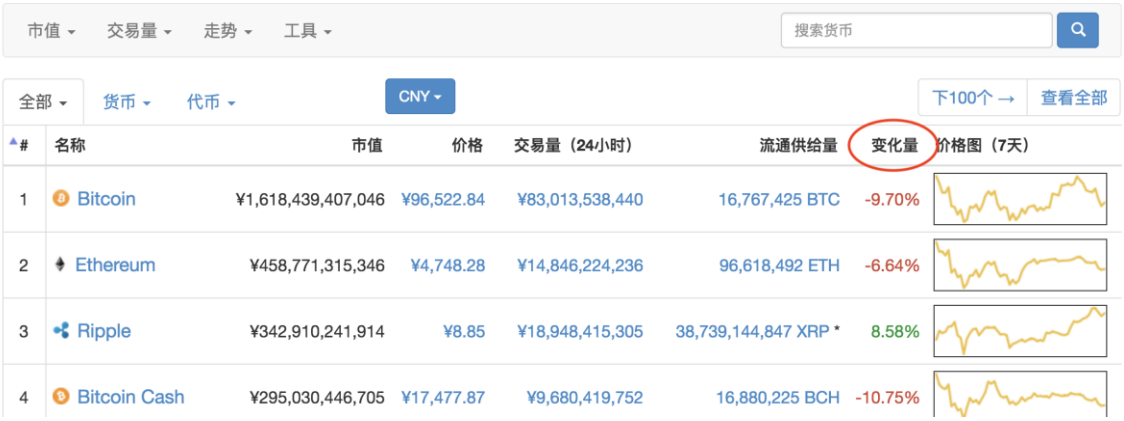
3）科学上网，国外交易所需要科学上网。

35.1.2 价差发现方法

寻找价差可以通过网站 https://coinmarketcap.com 和 http://www.feixiaohao.com ，优先推荐第一个，因为更新很及时。

如何找差价呢？大家可以打开第一个网站，在首页显示的是市值前 100 的币种，然后点击变化量，那这 100 个币种就会按涨幅大小来排名，一个个点进去看看是否有利差。如果找不到再点下变化量，会按跌幅来排名，再找找。

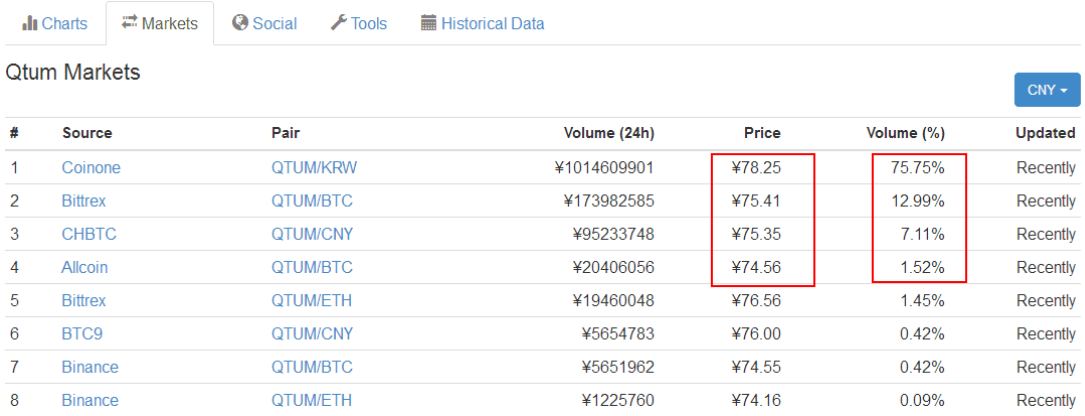
选择市值前 100 名会相对有保障；最好从涨幅里面选择，因为币种在涨的过程中你去搬砖会更加安全。



#	名称	市值	价格	交易量（24小时）	流通供给量	变化量	价格图（7天）
1	Bitcoin	¥1,618,439,407,046	¥96,522.84	¥83,013,538,440	16,767,425 BTC	-9.70%	
2	Ethereum	¥458,771,315,346	¥4,748.28	¥14,846,224,236	96,618,492 ETH	-6.64%	
3	Ripple	¥342,910,241,914	¥8.85	¥18,948,415,305	38,739,144,847 XRP *	8.58%	
4	Bitcoin Cash	¥295,030,446,705	¥17,477.87	¥9,680,419,752	16,880,225 BCH	-10.75%	

图35-1 从 coinmarketcap 找价差

以量子链为例，2017 年 9 月 13 日交易量前四的交易所之间差价达到了 4 块钱，存在 5% 存在套利空间，波动期的价格差距会很容易超过 10%。



#	Source	Pair	Volume (24h)	Price	Volume (%)	Updated
1	Coinone	QTUM/KRW	¥1014609901	¥78.25	75.75%	Recently
2	Bittrex	QTUM/BTC	¥173982585	¥75.41	12.99%	Recently
3	CHBTC	QTUM/CNY	¥95233748	¥75.35	7.11%	Recently
4	Allcoin	QTUM/BTC	¥20406056	¥74.56	1.52%	Recently
5	Bittrex	QTUM/ETH	¥19460048	¥76.56	1.45%	Recently
6	BTC9	QTUM/CNY	¥5654783	¥76.00	0.42%	Recently
7	Binance	QTUM/BTC	¥5651962	¥74.55	0.42%	Recently
8	Binance	QTUM/ETH	¥1225760	¥74.16	0.09%	Recently

图35-2 Coinmarketcap 上找量子链的价差

35.1.3 搬砖策略

对于搬砖党来说，能够做好搬砖这件事需要满足以下几个条件：

1）市场震荡

搬砖这种投机套利者最喜欢市场震荡的时候，有利好，有利空就会有差价，有差价搬砖党就有机会，比如品种上新交易所，产品发布新版本，签约合作伙伴等利好消息出现，就是搬砖党套利的好时机。对消息反应的灵敏性是搬砖党的基本技能。

2）套利空间测算

交易所利差出现时，算清楚利差大小，确认好有足够的交易深度，确保有利可图后，就大胆的开始吧。

3）快速执行能力

天下武功唯快不破，相对稳定利差的搬砖机会总是转瞬即逝，搬砖党发现机会后的快速执行决定了到底能不能赚到钱。

4）铁一般的纪律

牢记自己就是搬砖投机党，快进快出是搬砖党的基本素质，坚持纪律，赚了止盈，亏了止损，要是因为搬砖过去砸了自己的脚而变成价值投资者放弃搬砖，那无疑是搬砖界的笑话了。

5）良好的心态

搬砖投机时有发生从 A 站搬到 B 站时，利差已经消失甚至为负的情况，不要因为一次的亏损而忘记了长期搬砖带来的收益，良好的心态，清醒的头脑有助于我们抓住一波又一波的套利机会。

35.1.4 搬砖实操

搬砖 1.0：法币利差

比如比特币 BTC 在交易所 A 价格是 4 万人民币，在交易所 B 是 4.1 万人民币，那在 A 买了 BTC 之后到 B 去卖，一个就能赚 1 千元。

搬砖 1.0 的操作方法是人人都能看到的，利差出现后很快就消失了，而且国外交易所的搬砖，往往无法兑换美元等，所以搬砖 1.0 的操作空间不大。

搬砖 2.0：币本位

搬砖原则就这一个**低买高卖**，玩法却可以千变万化：

1）比如我不想赚人民币，我想赚 BTC 可以吗？假设我有 1 个 BTC 在交易所 B，以 4.1 万价格卖出，然后拿这 4.1 万到交易所 A 可以买多少个 BTC 呢？4.1/4＝1.025，多出 0.025 个 BTC！

2）你肯定想说，现在除了场外交易，用人民币购买 BTC 的交易所都关了，那我把人民币换成其它币种可以吗？比如交易所 A：1BTC＝20ETH，交易所 B：1BTC＝20.5ETH，同样我可以 20 个 ETH 在 A 买入成 BTC，转到 B 再换成 20.5 个 ETH，多了 0.5 个 ETH。

到这里可能就有点绕了，很多人转不过弯，这就有点像物物交换，**原则还是一个，便宜的地方买，到贵的地方卖。**原来中国有段时间红薯非常多，大家就用红薯来换其它东西，比如张三家 1 斤红薯＝1 斤面粉，而李四家 1 斤红薯＝1.1 斤面粉，你有 1 斤面粉，先到张三家换成 1 斤红薯，然后到李四家就可以换成 1.1 斤面粉，这样就多了 0.1 斤面粉。

理解这个例子后，现在，你把红薯和面粉换成区块链市场的任意两种币种，还是一个原则，低买高卖，那就可以赚取利润。比如红薯换成 ETH，面粉换成 ZEC，交易所 A：1 个 ETH=1 个 ZEC，交易所 B：1 个 ETH＝1.1 个 ZEC，那用 1 个 ZEC 在 A 处换成 1 个 ETH，再把这 1 个 ETH 转到 B 可以换 1.1 个 ZEC。

国外单据语言问题可以通过翻译软件轻松解决的。搬砖 2.0 的关键在于币本位，坚持以 btc 或者 eth 作为法币来操作，就越过了人民币和美元兑换的鸿沟。以赚 btc 或者 eth 为主的，一波行情来临，投入几万块，赚到几个 eth 不是难事。

搬砖 2.0 的核心是坚持币本位的思维，合理利用翻译软件，国际化投资，哪里有利差就往哪里去。

搬砖 3.0：自动对冲

如果说搬砖 1.0 和搬砖 2.0 是小米加步枪的体力活，而且一旦时机把握不好就会搬起石头砸了自己的脚，那么搬砖 3.0 的自动对冲则解决了搬砖过程中耗费体力的问题，而且同时买卖的操作也保证了每一波的利差都会被搬砖党吃掉，价值投资的同时不放过市场波动的收益。

自动对冲是通过调用交易网站的 api 来打造一个自动化交易的搬砖机器人，全年无休的为我们提供源源不断的“睡后”现金流，所以自动对冲代表的搬砖 3.0 才是无风险套利中的最高武功，后续章节会详细讲解如何用软件进行自动对冲。

35.2 区块链搬砖要避免哪些坑

35.2.1 搬砖的坑

搬砖的前提是找价差，找到后最需要注意的是要有足够的交易深度，也就是说要足够支撑你买卖的量，否则你用越多的钱投入，亏的越多。其它常见坑如下。

1）转账问题

搬砖需要转账，从交易所 A 到交易所 B 在转账上有可能有各种坑。

（1）币种转账打包处理时间

不同的币种转账时间各不一样，其中目前发现最快的是 EOS 和 ETH，而 ETH 像 BTC 一样可以称为区块链的法币，所以用搬砖者喜欢用 ETH 转账。

BTC 有段时间因为分叉币 BCH 大涨导致大量算力切换到 BCH 上，转账非常慢，有时候要一两天，而正常大概半小时左右。BCH 正常也要 1 小时，大算力切换可能会快些。

自己搬过的币种中，ZEC 转账 2 小时左右，BCY 要 2 小时以上。小伙伴曾经搬过一个叫 UNO 的币种，要 300 个确认，转账至少要 1 天，这些转账慢的币种是要上搬砖黑名单的。

（2）交易所处理时间

好不容易发现 SC 在云币网（现已关闭）与 B 网上有价格差，然后就去云币网用 ETH 买入大量 SC 之后，准备转账到 B 网，结果等了十来天才到账，价格差早就没了。我的第一笔搬砖就是砸在云币提现太慢的问题上。

有些交易所提现是需要人工审核的，有天晚上发现 HSR 在 EXX 交易所 https://www.exx.com/和币安上有超过 10%的价差，就去买入提现，结果提现状态一直是等候审核，当时晚上客服不上班，等到上班之后再处理价差早就没了。这种每一笔提现都需要审核的也应该进入搬砖黑名单！

还有些网站提现额度较大时也会人工审核，需要注意，厚道的网站会在你提现时告诉你，比如 BITZ 提币 GXS 数量大于 2000 时需要人工审核。不厚道的网站像 CHAOEX 提现不明说，有一次我提现 NULS14420 个竟然也需要人工审核。这种情况的解决办法就是小批量多次提现。

（3）钱包维护

有一次看到 XCP 在 P 网上和 B 网上有价格差，就在 P 网买入之后准备提现，结果发现 P 网 XCP 钱包在维护，直接傻眼，只能原地卖掉。以后搬之前一定要看下两个钱包是否都可以正常提取，否则就会砸脚。

2）时间差问题

搬砖很多时候是利用消息市，比如某个币种要在一个新的交易平台上线，那么刚开始的时候价格肯定是偏高的，你就可以提前埋伏，但也有不少坑要注意。

（1）买入时已经涨太高

假设当你得到这个消息时，发现这个币种已经涨了很多，比如 20%以上，那说明你的消息已经晚了，这个时候买入再转账可能就没有利润了。

（2）等待时间太长，忽略配置

因为听说 GXS 要在 BigONE 或者 B 网上线，我在 BTC 价格为 2.8 万时用 BTC 买入 GXS，当时 1GXS＝0.006BTC，折合成人民币约 16.8 元，然而上线的消息过了好多天还没来，而 BTC 的价格从 2.8 万很快涨到近 5 万，但是 GXS 的价值还是在 16 块左右，此时 1GXS 的价格变成 0.003BTC，我当时用 2 个 BTC 买入的直接亏损 1 个 BTC，就算 GXS 涨到 16 块，也不会变成 0.006 BTC 的价格。

当然这次的教训除了等待时间太长，还有：

买入时已经涨太多，GXS 要在 BigONE 上线的消息出来后已经涨了近 8%；

忽略配置，搬砖也需要考虑配置，至少保持 BTC 在 50%以上，因为现在基本上是币币交易，比特币涨对其它币种有虹吸效应，其它币会跌。

3）心态问题

虽说搬砖行情时间不长，个把小时，但有时候买卖也不能太急，要稍微给点缓冲时间，让别人把单子放上去。

比如下面的行情，要买入 NULS，深度足够，别人卖出委托如下，如果出价 0.000159 把上面几个全买了之后，再想买要等会，让别人把卖出委托重新放出来，否则你急着买只能出比这个价更高的 0.00015793 才能成功，那利润就大大降低了。前段时间搬砖 NULS 因为这个太急这

个原因直接损失 0.25BTC，这是个 1 万的教训。

卖出委托

价格	NULS	BTC	累计(BTC)
0.00015290	637.0709	0.09740814	0.09740814
0.00015300	500.0000	0.07650000	0.17390814
0.00015788	888.0000	0.14019744	0.31410558
0.00015880	850.0000	0.13498000	0.44908558
0.00015900	3000.0000	0.47700000	0.92608558
0.00015973	850.0000	0.13577050	1.06185608

图35-4 区块链货币价位委托图

投资很多时候就是反人性的，如果发现搬砖失败，砸到脚了，怎么办？是继续持有等待再涨上去吗？不是，赶紧割肉也要处理掉，并且去寻找下次机会，而不是在那伤心。吃过亏，伤过心，但投资是最能锻炼人性的地方。

而且搬砖的同时也要学着了解下所搬品种，继续去学习，并且尽量向价值投资上靠。

最后说一点，搬砖需要耗费大量时间和精力，需要考量和权衡，平衡注意力问题。虽说我入过这么多坑，但是经过这么多次洗礼，我对这种新的投资行为越发感兴趣。

4）法币入口导致虚假价格差

有段时间发现 ZB.com 的 BTC 比其它交易所都高约 10%，想尝试搬砖，一试发现他的 USDT 无法提现。原来是它开通 USDT 与人民币的场外交易，所以 ZB 上 BTC 对 USDT 价格其实是场外价格，高出 10%属于正常，无法搬砖，当恢复 USDT 提现后，这个价差就没有了。

类似情况在 BigONE 上的 BTC/BITCNY 也比场内价格低出约 10%，那是因为购买 BITCNY 时和 RMB 比例并非 1：1，而是会收约 10%的手续费，也是无法搬砖套利的。

35.2.2 探路方法

能否有个途径可以先探下路，尽量避免以上的大部分坑呢？

在发现行情并且深度足够的情况下，有个方法就是先买入少量，比如人民币 500 元之内，然后开始转账，看看能否到账？如果能到账，那风险就小很多。

因为你要转账，你就可以确认两个交易所是否钱包维护、检查交易所是否审核、检查转账打包时间。但这样就一安全了吗？

有一次我看到 INK 在 BigONE 价格比 EXX 低很多，有近 40%，就在 BigONE 上先买了 73 个 INK，然后开始转账，过几分钟就出现了 txid（转账的 ID），过个把小时转账成功。

感觉没问题了，我开始买了几万个，继续提现，然而问题来了，久久出现不了转账的 txid，就是在下图中红圈部分点击并没有有效的 txid。

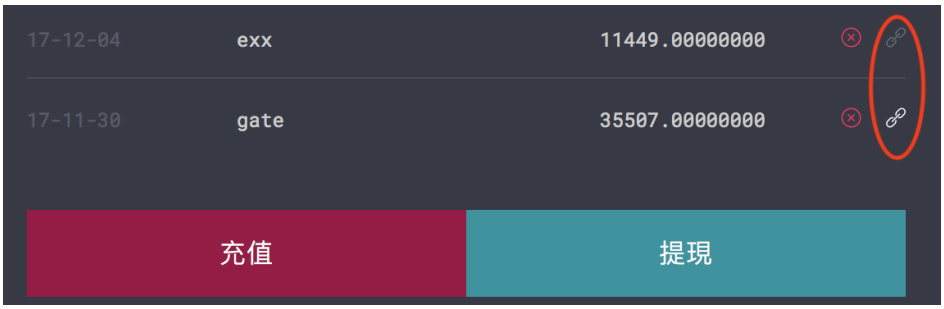


图35-5 txid 无法显示

联系 BigONE 客服说 INK 钱包维护，再联系 INK 客服他们说没问题，返回来联系 BigONE 说自己钱包维护。一直出现不了 txid 那说明就是 BigONE 这边的问题，后来被我问急了，客服说是热钱包里没有 INK，就是说他们手里没有足够的 INK 可以用来提现，而这个 INK 拖了我十几天才提出去。

那回到我们的探索途径，怎么来优化呢？刚才说先买入少量之后如果转账正常，对于量大的建议还是要分批购买，至少要等到提现时确认有转账 ID，这个时候才更安全。再进行大量买入。

总结下这个探索路径就是：

在发现行情并且深度足够的情况下，先买入少量，开始转账，转账成功之后尝试分批买入，并且分批转账，第一批转账之后等到有转账 ID 之后再买入第二批。

你可能会说，这样操作下来，可能时间过去，价格差就没了。有道理，但这种方法尤其适合在以前没搬过的币种和以前没用过的交易所，用过这个方法之后，第二次就轻车熟路那就没必要那么谨慎了。或者你对所搬币种和交易所的时间处理都了如指掌，那就可以直接上路搬。但对不熟悉的币种和交易所，这是一种很好的探路，毕竟，搬砖路上安全才重要。

搬砖路上有些坑只有自己走过之后才会更加深刻，但提前了解这些坑会让你更加从容面

对，即使一不小心掉进去，也能清楚问题出在哪，多试几次之后你就会更加得心应手了。

35.3 如何用软件自动搬砖实现睡后收入

35.3.1 自动搬砖的原理

经过前面的分析：大家会发现，手动搬砖浪费大量的注意力，大部分人没那么多精力和时间，那可不可以自动搬砖呢？

我们希望自动搬砖的初衷就是在不同的交易所有价差时，它可以实现自动交易，在便宜的地方买，在贵的地方卖，实现有两种方式：

- ✧ 从便宜的交易所买之后转账到贵的交易所，需要软件实现转账功能
- ✧ 两个交易所同时进行买卖，不需要转账

第一种方式要实现转账会牵涉到一个很重要的安全问题,万一软件方把资产转走怎么办？行不通。

第二种方式不需要不同的交易所转账，只需要交易所内部交易，可以利用软件的 API 功能把提现功能关掉，从而解决安全问题。这种方式需要每个交易所都有资产。

比如你在币安和火币两个交易所都有 ETH 和 EOS，当币安上 EOS 价格低时，让软件在币安上用 ETH 买入 EOS；同时让软件在火币上卖出同等数量的 EOS，这样实现赚取 ETH 的差价。这就需要币安上 ETH 的资产价值与火币上 EOS 的资产价值相同,才能实现买入和卖出的 EOS 数量相同。

每个交易所的币种价格会波动，如果币安上 EOS 价格高时，软件在币安上卖出 EOS，火币上再用 ETH 买入同样数量的 EOS，这样就又赚取了 ETH 的差价。

同样的原理扩展，如果你在不同的交易所都放置不同的币种，比如 ETH 和 EOS，软件自动捕捉价差，不停进行量化交易，从而实现自动搬砖，躲着赚钱，实现睡后收入。

经过上面分析，你会发现，这样自动搬砖不会改变你原有的配置比例，其核心是赚币，用哪个为基准对就赚那个币种，比如用你 ETH 买卖 EOS，那就赚 ETH；如果你用 EOS 买卖 ETH，那就赚 EOS。

35.3.2 软件自动搬砖的使用前提是什么？

首先，你得有不同的币种，首先是基础货币，比如 ETH，BTC，USDT 你至少得有一种。除了基础货币外要有交易的币种，比如 EOS，否则是没法交易的。

其次，资产的价值得到一定级别，比如合人民币的价值在 5 万以上，否则你交易还不够手续费和软件使用费。

再次，不同的币种最好能有个配置比例，比如前面 EOS 交易的例子，如果 EOS 和 ETH 的价值不一样，那就没办法在不同的交易所实现同样数量的 EOS 买卖。

因此在初始配置不同的交易所的时候最好把每个币种平均分到不同的交易所。

以上条件不满足，你可能没法用自动搬砖收益，或者收益不高。

当然我们投资会有自己的币种配置，最好不要为了搬砖而去改变配置。自动搬砖只是为了赚外快，是对 BTC 和 ETH 等的再利用，如果你都没有这两种资产，别急，不看好的币种买来为了搬砖更是划不来的。

35.3.3 软件的实现

有个软件叫比特币精灵（目前只支持 window）可以实现上述的功能。

可在官方网站 http://www.btcjl.com/下载，注册。新注册用户会送 2 万对冲额度，可以先尝试下。超过之后就需要付费购买，价格是按对冲金额收取手续费，费率为 1.5/10000，就是每对冲 1 万元，收费 1.5 元，购买多了之后会有少量优惠。

先看一张我 40 天（2017.11.20～12.30）来的收益图，我的主要交易币种：BTC ETH ZEC EOS BCH（BCC），当时总资产价值在 40 万左右。

图35-6 搬砖利润额

上图中**利润额**就是你赚到的币种折算成人民币的价值。

交易额是每次买卖资产的价值汇总，不是你币种的价值，收费也是以交易额度的万分之 1.5 计算的。

利润率就是利润额除以交易额，大家看我上图，利润率在千分之二，而收费是万分之 1.5，所以还是有利润的。

35.3.4 软件具体操作步骤

第一步：确定你要对冲的交易所和币种

作为举例，我们这里选择在火币和币安两个交易所之间对冲 EOS。

注：实际对冲中，为了提高资金周转和利润，建议至少选择 3 家交易所进行对冲。

但有些交易深度不够，不建议选择，比如 gate.io，hitbtc 和 liqui 等。

第二步、交易所资金准备

在火币和币安充入资金分别充值 EOS、ETH 和 BTC。

注：充值时，为了提升资金利用率，建议 ETH+BTC 价值=EOS 价值，这样可以提高资金利用率，但若已经配置好之后，也不用特意去更换。

第三步、交易所 API 账号配置

API 是应用程序接口（Application Program Interface）的简称。简单来说，当你在比特币精灵上接入交易所的 API 后，就可以在比特币精灵上进行买卖，从而实现自动化交易。

建议至少配置三个交易所进行对冲。特别注意的是在申请 API 时只允许查询和交易，不要勾选提现转账等，以保证资产安全。

以币安为例申请 API 方法如下：（注意火币专业站的 API 申请需要到火币站 huobi.com 申请，BigONE 目前还未开放 API）

币安 API 配置方法

配置步骤

（1）登录币安，注意现在火币专业版网站也需要回到火币网去申请 API

（2）进入 用户中心-->API 管理

（3）创建新 Key

图35-7 创建 key

（4）申请成功后获得 Apikey、secretkey（只在申请成功的时候显示，刷新页面后就无法看到，所以请申请成功后马上拷贝记下）

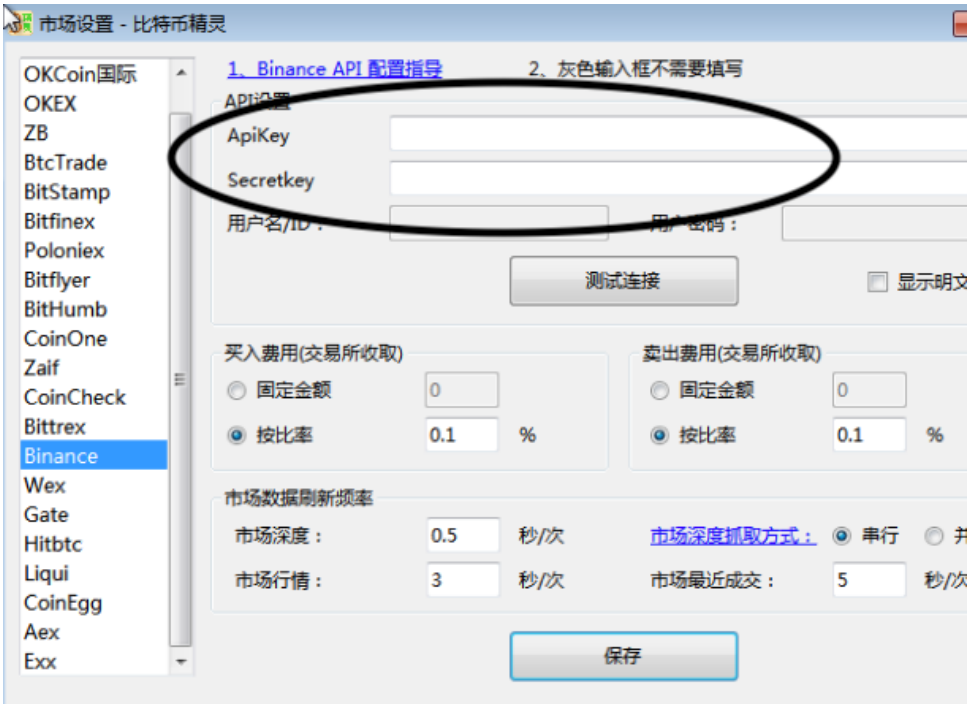


图35-8 记录 Apikey、secretkey

（5）将 Apikey、secretkey 配置到 【比特币精灵 客户端-》市场设置】 功能的相应输入框中，测试连接成功后保存即可。

第四步、设置交易对及对冲策略

进入 【自动对冲-对冲策略设置】，找到对冲策略，比如火币和币安的 EOS

（1）设置对冲方向的利润率阀值，即两个市场差价达到多大进行对冲，以及每次对冲的最大最小数量。默认设置为 0.02%，如果你想设置高点，那可能会导致交易次数变化，因为不一定有那么大的价差。

（2）启用火币和币安的 EOS 对冲策略，两边都放有 BTC 和 ETH，所以我都勾选了。

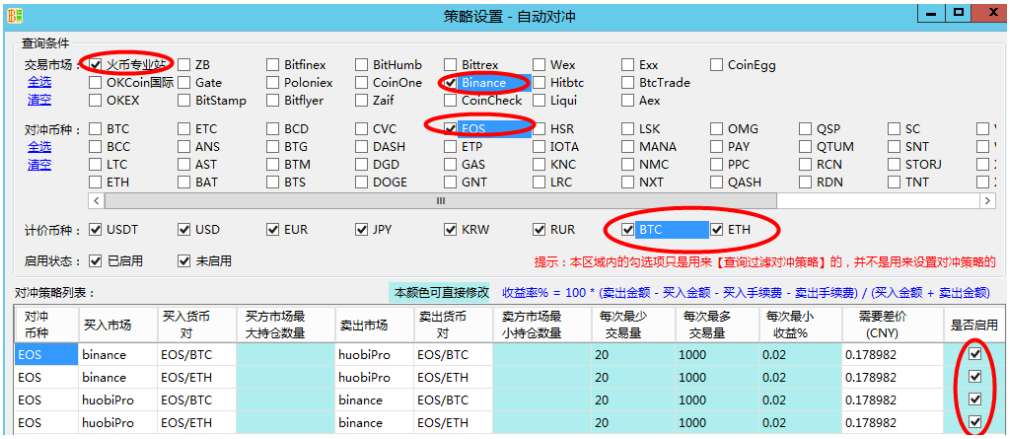


图35-9 选择对冲策略

最后、对冲执行

点击【自动对冲】功能中的【开始】按钮即可

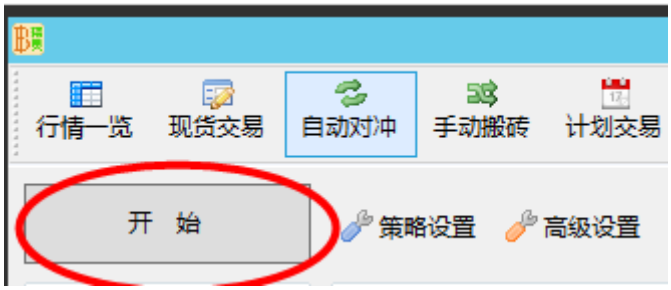


图35-10 开始自动对冲

这样就可以实现软件的自动对冲套利运行，有几个规律

- ✧ 一般建议做 5 个或以上的交易所，5 个以上的品种。开的越多，机会越多。品种价差越大越好，价差越大，利润越高；
- ✧ 多开几台机器，每台机器跑 1-2 个品种，效果比一台跑多个品种好很多，否则会出现很多类似【深度数据是 xxx 秒之前的】的问题；
- ✧ 币种选择：大币种配小币种，usdt 计价，btc 计价，eth 计价的一起跑，机会多。找活跃的币种（波动大的）

这种方法软件需要一直开：

（1）可以把自己电脑 24 小时打开，但电费或许不少，或者使用时会不方便

（2）建议直接买个云服务器，比如阿里云，就相当于租一台 24 小时可以远程控制的电脑，让软件 24 小时不间断运行，会更加省心。详细设置会在下节文章中阐述。

这样我们就可以实现“睡后收入”，什么都不用管，让他自动运行，搬砖套利。

35.4 如何在阿里云上部署比特币精灵实现躺着搬砖赚钱

35.4.1 注册购买

进入网站 https://www.aliyun.com/注册阿里云账号，登录之后，根据下图一步步选择到

云服务器 ECS，。

自己尝试使用淘宝账号登录，一直有如下提示，找客服也未解决，最后重新注册了阿里云账户：

你的帐号未添加手机号码，帐号无法激活。建议你注册阿里云账号。

图35-11 注册阿里云账号

进入之后选择入门级——1 核 2G 内存的或 1 核 1G 的 CPU，官方推荐购买 1 核 2G 内存的，运行效果更好。

图35-12 选择阿里云服务类型

不过现在有一个活动，非常实惠，一年的费用只要 660 元（2G 内存）或 330 元（1G 内存），大概是原来 1/3 的价格，链接如下：

https://www.aliyun.com/chinaglobal/promotion/overseaall2017?spm=5176.8112568.738194.4.7bfe9d91W9SGvz （如果活动结束请按上述方法选取）

进入之后选择入门版——香港——公共镜像即可

图35-13 选择云服务镜像

两种方法进入之后选项类似，以前者为例，选择一键购买——香港——共享基本型——Windows Server+2012 R2 数据中心版 64 位中文版。下面的默认选择即可。

为什么一定要选择非大陆服务器？原因是有些区块链网站在国外，有可能国内上不了，选择香港，新加坡等都可以。

图35-14 选择服务器类型

35.4.2 设置密码

购买成功后，回到阿里云首页，进入控制台。

图35-15 阿里云控制台

进入后选择最近使用的产品：云服务器 ECS，或者通过我的资源：云服务器 ECS 进入。

图35-17 进入云服务器 ECS

进入之后再点击云服务器。

图35-18 设置云服务器

进入之后，在云服务器界面，点击“更多”，需要设置密码，这里有两个密码：

- 重置密码指登录这台服务器的密码，相当于**电脑登录密码，**可记为密码 A；
- **远程连接密码**指的是过程控制的密码，可记为密码 B。

图35-19 修改控制密码

点击重置密码（或设置密码）就是电脑登录密码，简记为密码 A，设置要求如下

图35-20 重置控制台密码

点击修改远程连接密码要求如下：只要 6 位数字，为密码 B。

图35-21 修改远程连接密码

35.4.3 连接云服务器

点击远程连接，然后弹出一个**远程连接密码**框，这个密码为刚才设置的 6 位数字密码 B。

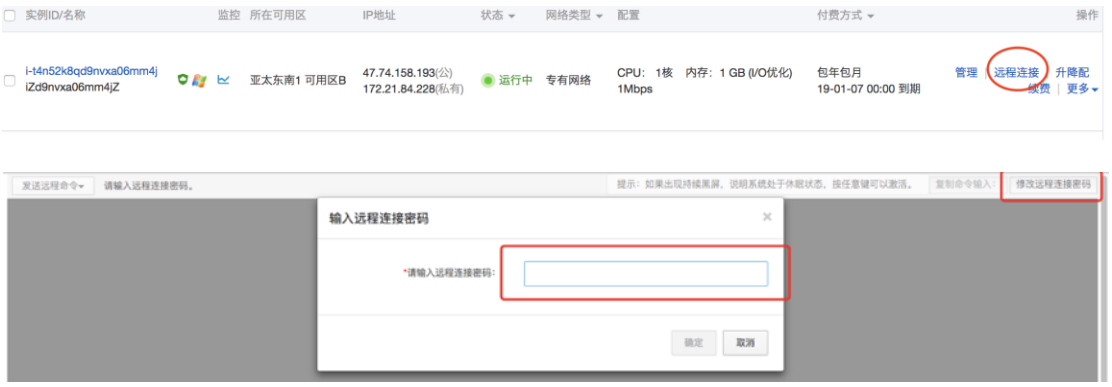


图35-22 连接云服务器

输入远程连接密码之后，会出来 win 的登录界面，提示按 CTRL+ALT+DELETE 登录

进入 win 的界面之后，点击左上角发送远程命令，选择 CTRL+ALT+DELETE.

图35-23 CTRL+ALT+DELETE 发送远程命令

这个时候需要输入电脑登录密码，即密码 A。这样就能进入云服务器了。

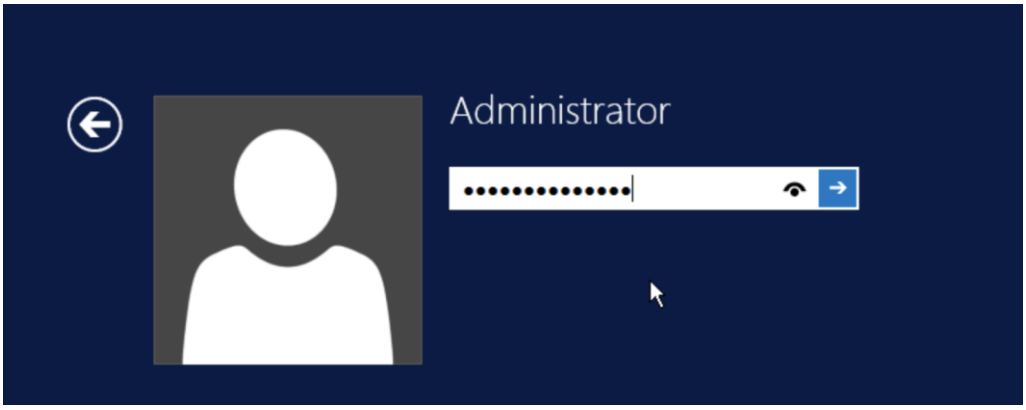


图35-24 登陆云服务器

35.4.4 部署比特币精灵

登录后，就和自己的 window 电脑差不多了。下载比特币精灵，并安装，然后在一个个设置不同网站的 API，参考上篇如何用软件自动搬砖实现睡后收入。

但默认的 IE 浏览器十分不方便，建议在里面下载谷歌浏览器。

另外因为这个服务器配置比我们自己电脑低很多，所以在里面运行起来很慢，建议比特币精灵在自己电脑里面配置好 API 之后，直接生成个压缩包（如果运行过一段时间，压缩包比较大，可以把安装文件下面的 Log 文件夹删除），然后用邮箱发给自己。再在阿里云服务器上打开就行了。

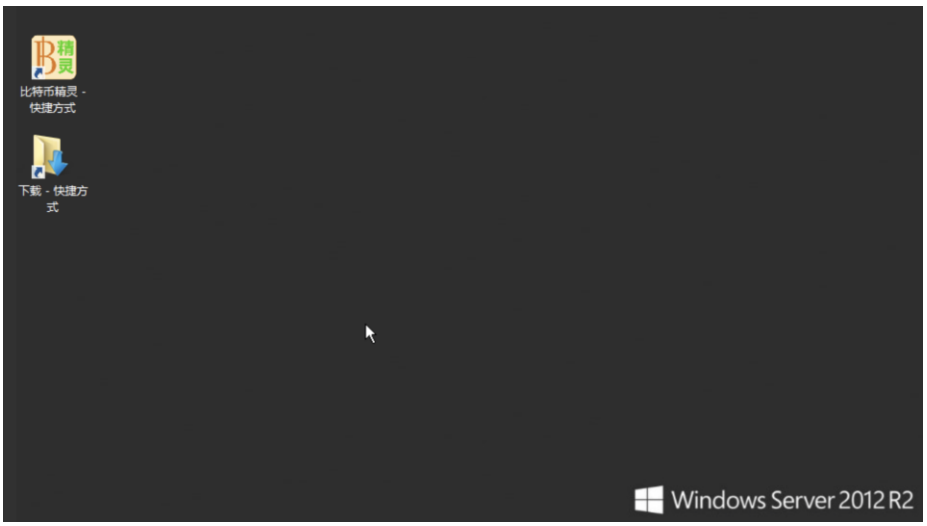


图35-25 云服务器界面

设置好之后打开比特币精灵就大功告成了。软件就会 24 小时不间断运行，实现躺着赚钱。

不过前期有可能不稳定，最好每天登录查看下运行情况。

36 挖矿

36.1 挖矿那些事

36.1.1 挖矿相关概念

1、什么是挖矿？

精通比特币中对比特币挖矿的解释如下：

挖矿是增加比特币货币供应的一个过程。挖矿同时还保护着比特币系统的安全，防止欺诈交易，避免“双重支付”。矿工们通过为比特币网络提供算力来换取获得比特币奖励的机会。简单理解，挖矿的过程实际上是银行发币的过程，矿工除了发币之外，还承担了打包交易记账的工作。

矿工们验证每笔新的交易并把它们记录在总帐簿上。平均每 10 分钟就会有一个新的区块被“挖掘”出来，我们把包含在区块内且被添加到区块链上的交易称为“确认”交易，交易经过“确认”之后，新的拥有者才能够花费他在交易中得到的比特币。

矿工们在挖矿过程中会得到两种类型的奖励：创建新区块的新币奖励，以及区块中所含交易的交易费。为了得到这些奖励，矿工们争相完成一种基于加密哈希算法的数学难题，这些难

题的答案包括在新区块中，作为矿工的计算工作量的证明，被称为“PoW 工作量证明”。

简单理解：比特币是一家区块链世界的银行，矿工就是比特币银行的工作人员，矿工挖矿的过程中完成了比特币银行铸币（发行比特币）和记账（打包交易）的全部工作。

有人工作，就要有人支付费用，区块奖励和交易手续费支付了矿工工作的全部费用，挖矿模式保证了比特币系统的安全、去中心化的自动运行。

2、比特币总数、区块减半和矿池

比特币总数：比特币在设计之初总量约为 2100 万个。

新币减半：矿工通过创造一个新区块得到的比特币数量大约每四年（或准确说是每 21 万个块）减少一半。开始时为 2009 年 1 月 3 日每个区块奖励 50 个比特币，然后到 2012 年 11 月 28 日减半为每个区块奖励 25 个比特币，2016 年 7 月 9 日再次减半为每个新区块奖励 12.5 个比特币。基于这个公式，比特币挖矿奖励以指数方式递减，直到 2140 年。届时所有的比特币（20,999,999.9769）全部发行完毕。换句话说在 2140 年之后，不会再有新的比特币产生。

矿池：由于有大量的矿工竞争挖矿，导致单个矿工的产出不稳定，为了获得稳定的挖矿产出，聪明的矿工设计了通过矿池把大家的算力集中在一起，在全网中占据一定的份额，这样就保证了稳定的挖矿产出。分配产出时，矿池会根据单个矿工贡献给矿池的算力按照比例分配，矿池收取少量的手续费。

排名前三的矿池都是中国的，全球算力已经达到了恐怖的 4381PH/s，可访问以下网站查看矿力分布情况：http://www.qukuai.com/pools。

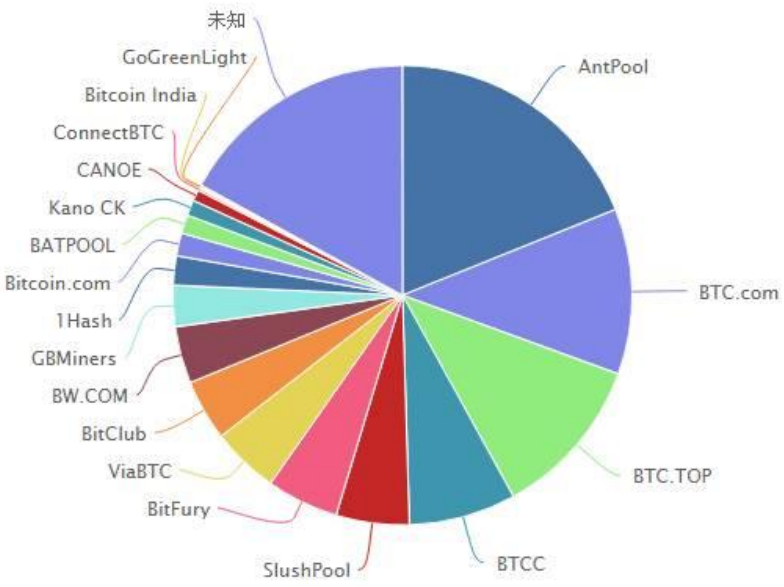


图36-1 矿池算力分布图

3、挖矿品种及矿机种类介绍

主流的矿工都是以 ASIC 矿机挖比特币为主，莱特币为辅，随着 ETH、ZEC、SC 等其他区块链品种的出现，也有一部分矿工开始选择使用显卡矿机挖 ETH 等币种。

ASIC 矿机：

比特大陆生产的蚂蚁 S9 是现在市面上最主流的矿机，以功耗小著称产出大。其他厂商比如阿瓦隆、翼比特、神马矿机等。

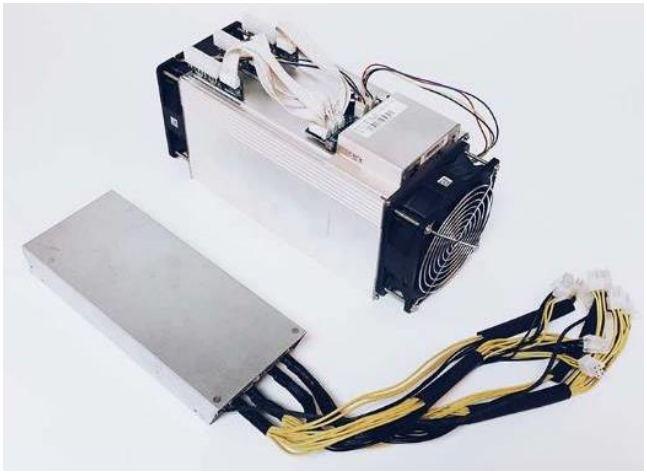


图36-2 ASIC 矿机

显卡矿机：大多都是矿工用显卡自己组装，专业矿机厂商有熊猫矿机等。

图36-3 显卡矿机

36.1.2 挖矿投资的成本、收益和风险

1、挖矿成本

1）矿机成本

矿机成本属于固定的一次性支出，蚂蚁矿机现在最先进的机器为14nm的S9，硅芯片的预计极限是7/10nm，再往下就会碰到难以逾越的量子效应右墙，因此有可能7/10nm是终极矿机，短期内下一代矿机还无法上市。

从S9上市时的效应看，淘汰的是S5矿机，在现在很多电价便宜地区S7还在工作，所以一台机器可以挖很长时间。从硬件性能看一台机器至少可以正常工作3~5年，也就是说矿机的一次性投入，在算力不暴涨的情况下，至少可以提供3~5年的相对固定的产出。

蚂蚁S9矿机单台成本现货14000，期货9400，但是期货通常在2个月后上市，且很难抢购；显卡矿机以rx470为例6卡矿机成约15000元，2017年5月之后挖矿显卡长期缺货。

2）电价成本

电价成本属于长期固定支出，电价越低，成本也就越低。以蚂蚁S9为例，每天耗电量36度，电费5毛每天电费支出18元，每月电费支出540，中国四川、云南拥有丰富的水电资源，内蒙、新疆拥有丰富的火电资源，中国的大多数矿场分布在以上几个省份，长期投入的话，最好找到便宜的电力资源。

3）其他成本

比如维护成本：矿机故障维修，非正常状况下的停机等，比如场地成本、矿场租赁场地需要支付的成本等，比如维护人员的工资成本等。

2、挖矿收益

挖矿收益来源分两部分，即新区块奖励和交易手续费奖励。

一开始交易手续费的奖励占矿工收入的 0.5%或更少，大部分收益仍来自挖矿所得的比特币新块奖励。然而随着挖矿奖励的递减，以及每个区块中包含的交易数量增加，交易费在矿工收益中所占的比重将会逐渐增加。在 2140 年之后，所有的矿工收益都将由交易费构成。

投资挖矿之所以风险低是因为在牛市可以卖币直接套现法币，熊市可以屯币等待币价上涨。挖矿带来的收益来自于以下几个部分：

1）卖币收益

挖出来的币按照现价卖掉换取法币，可保证资产稳步增加。

2）屯币收益

等待币价上涨带来的收益，以比特币为例，年初至今上涨了约 5 倍，ETH 年初至今上涨了 30 倍，如果是投资买币的话，很少有人可以拿的住手中的币。但是，同样的资金，如果投资矿机挖矿，按照比例一部分币卖掉，一部分币囤积起来，是可以享受到币价上涨带来的红利的。

3）ICO 收益

挖出来币直接拿来做 ICO，其实是用低风险来博得高回报。比如用 ETH 参加 EOS 的 ICO，是低成本在一、二级市场套利办法，比如挖出来的币在年初投资了公信宝或者量子链。

挖矿获得的币如果按照比例配置为 50%卖币，30%屯币，20%参加 ICO，其实为我们提供了源源不断的现金流（卖币收益）+资产（屯币收益）+子弹（参加 ICO 的子弹）。

3、挖矿的风险

1）算力暴涨

算力暴涨是挖矿投资最大的风险，算力增加导致挖矿难度增加，导致收益减少，但由于自由市场中，无法避免竞争，算力增加的风险是可以被接受的。

2）币价下跌

币市和股市一样也存在涨跌，牛市价格高，熊市价格低，当价格低到无法承担电费时，挖矿就无利可图，挖矿投资就无法继续。不过根据测算，电费 5 毛，币价 6000 以下才可能亏本，现在的币价接近 30000，除非有特殊原因短期内币价下跌到 6000 的可能微乎其微。

3）系统风险

比如分叉，比如最近从 BTC 分叉出了 BCC，由于分叉的风险导致币价下跌，挖矿收益锐减。

但是由于铸币和记账是整个系统中最重要的工作，分叉之后的竞争币也是需要矿工来完成铸币和记账的过程，所以为了争取到更多的矿工来工作，相应的币种就会提供的更多的区块奖励和交易手续费。实际情况来看也是如此，BCC 分叉后矿工在 BTC 和 BCC 中间切换来保证了利益的更大化，系统风险反而成为了矿工增加收益的机会。

4）政策风险

由于越来越多的国家公开支持比特币，比如日本，韩国等已经承认比特币的货币属性，中国央行等五部委在 2013 年 12 月 5 日下午发布《关于防范比特币风险的通知》，虽然定义比特币不是货币，只是一种虚拟商品，但承认了投资比特币的合法化，即：比特币交易作为一种互联网上的商品买卖行为，普通民众在自担风险的前提下拥有参与的自由。内蒙乌海等地区政府牵头支持成立挖矿为主的大数据产业园，也反映了政府对于区块链投资的支持态度。

综上，投资挖矿的风险除了算力暴涨之外，其他的几种风险同样也是区块链投资中所要承担的风险，系统性风险中由于工作量证明的币种中都需要矿工，反而给矿工提供了更多盈利机会，保证了挖矿收益的相对稳定，所以投资挖矿是区块链投资中相对低风险的投资。

36.1.3 普通人如何参与？

挖矿已经不是 2013 年时随便一台电脑就可以挖出比特币的时代了，大量专业矿场利用四川，云南的便宜水电，冬天又迁徙到新疆，内蒙使用便宜火电。散户想要参与有以下几个方法：

1、联合挖矿

图36-4 联合挖矿

币信的云算力，莱比特矿池的联合挖矿，比特大陆的算力托管合约都是散户参与的机会。优点：方便投资，不需要管理，缺点：手续费支付较高，没有矿机所有权。

2、自建矿场

图36-5 专业矿场

自建矿场的优点：矿机 100%所有权，收益有保障。缺点：投资大，风险大，需要寻找便宜的电力资源，自行维护成本也会高些。前段时间在四川考察过水电资源，合适的资源下，自建矿场挖矿的收益是超越很多投资品种的，对于普通的散户，自建矿场+联合挖矿也许是低成本低风险参与的一个机会。

36.1.4 以太坊挖矿

区块链的生态系统中挖矿也是其中的一种投资方式，如果有朋友资金充足敢于冒险，也可以一试。

挖矿考虑到的因素有：回本周期、电费、矿机成本、当前币价、算力变化、挖矿协议等，

用以太坊挖矿为例：

（1）回本乐观估计大概 200 天，做好 1 年的心理准备。

（2）电费：在四川、云南、新疆等地方电费便宜，大概每度三毛多，与发电场谈好协议，有时电场不讲信誉，突然变卦收你 5 毛，你就没法玩了。

（3）矿机成本，这些都是市面上一搜就可以搜到的，算力越强，价格越贵，但这些机器如果不坏，是一次性的固定投资。

（4）当前币价 2000 元左右，如果突然翻倍，你可能 100 天回本。

（5）算力变化，如果竞争的矿场增多，算力增大，挖矿难度变化，你的收益也会受到影响。

（6）当前以太坊用 PoW 工作量证明机制，**可能 2018 年改为 PoS 机制**，这是最大的风险，你的以太坊矿机如果不能挖其它币很可能会变为一堆废铁。

参与这种行业，有一个优点，数字货币当前不算资产，好像不收企业所得税。

有一个投资回报测算的网站：http://www.unminer.com/tools/eth/calculator

小结

投资挖矿是区块链投资中相对低风险，稳定收益的项目，提供了除了期待暴富而浮躁的 ICO，忽上忽下的币价起伏之外另一种平稳的选择，在资源允许的情况下，作为区块链投资避险的投资是值得尝试的。

36.2 使用公信宝 DAPP 进行数据挖矿

·1）下载安装挖矿软件

公信宝 DAPP 挖矿软件下载地址如下：https://blockcity.gxchain.org。

2）开始创建自己的区块链身份

图36-6 公信宝布洛克城界面

3）输入自己的手机号码开始注册

图36-7 注册布洛克城

4）填写自己的真实姓名与身份证号码

图36-8 填写注册信息

5）开始创建自己的区块链身份

图36-9 创建布洛克城身份

这时你会收到一笔 GXS 奖励，标志这你的区块链身份已经生成。

图36-10 获取 GXS 奖励

你可以看到你区块链身份的详细信息。

图36-11 查看布洛克城个人信息

6）如何进行数据挖矿？

（1）你现在看到的是数据挖矿的主页面，你能看到矿产、算力、算力提升、自动挖矿等按钮。

图36-12 开启自动挖矿

（2）开启自动挖矿，点击“开始赚钱”。

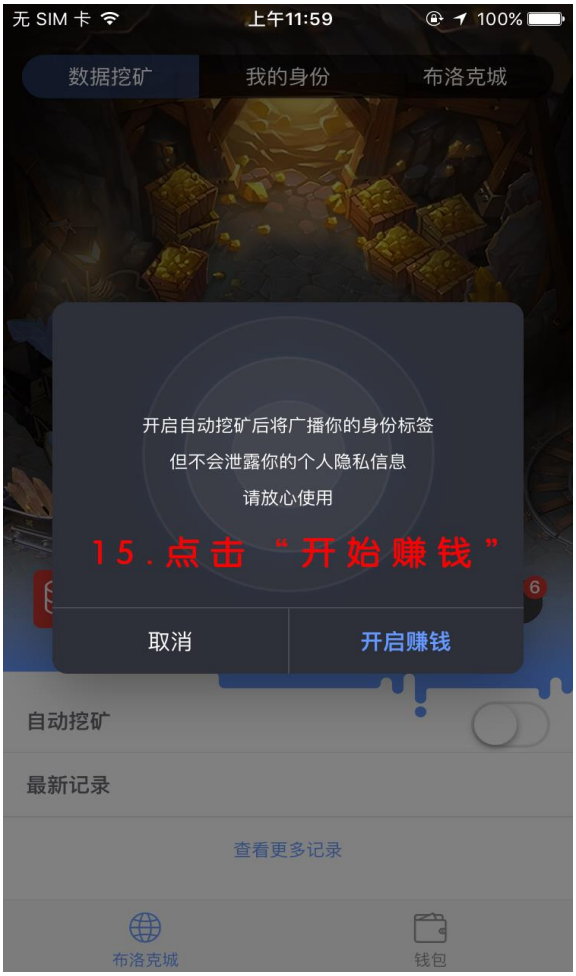


图36-13 确认挖矿

（3）当出现“挖矿中”这个标签时，说明你已经开始数据挖矿

图36-14 查看挖矿详情

（4）过一段时间登录点击挖矿页面的矿产资源即可获得数据挖矿的代币。

图36-15 点击收取矿藏

7）如何进行算力提升？

（1）点击进入算力提升区

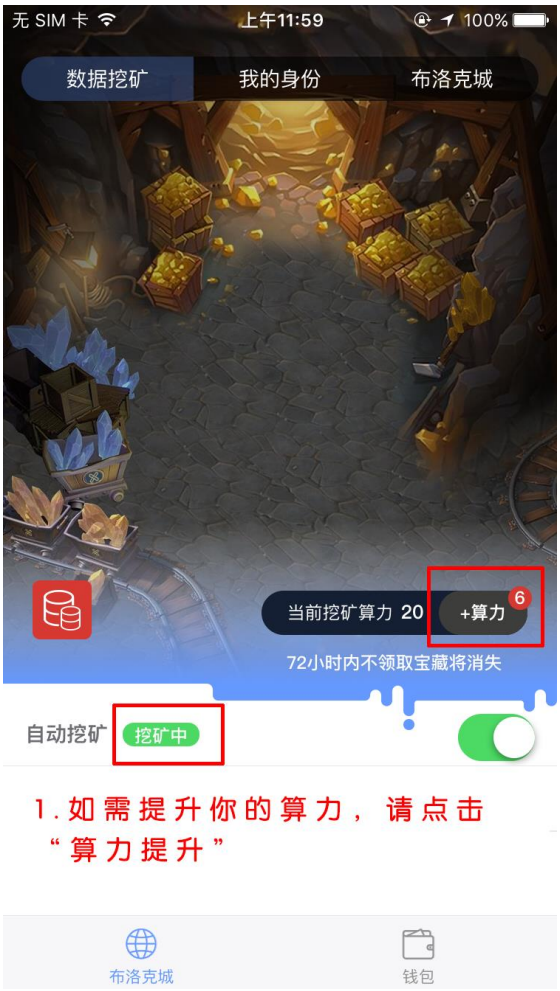


图36-16 提升挖矿算力

（2）选择你想要授权的数据类型，按要求填写账户信息

图36-17 授权信息提高算力

（3）数据采集将持续半分钟到 2 分钟不等

图36-18 授权认证采集

36.3 IPFS 挖矿

36.3.1 IPFS 基本概念

IPFS：InterPlanetary File System 是一个分布式文件系统，它综合了以前的对等系统的成功想法，包括 DHT，BitTorrent，Git 和 SFS。 IPFS 的贡献是简化，发展和将成熟的技术连接成一个单一的内聚系统，大于其部分的总和。 IPFS 提供了编写和部署应用程序的新平台，以及一个新的分发系统版本化大数据。 IPFS 甚至可以演进网络本身。

IPFS 是点对点的;没有节点是特权的。 IPFS 节点将 IPFS 对象存储在本地存储中。节点彼此连接并传输对象。这些对象表示文件和其他数据结构。 IPFS 协议分为一组负责不同功能的子协议：

身份 - 管理节点身份生成和验证。

网络 - 管理与其他对等体的连接，使用各种底层网络协议。可配置的。

路由 - 维护信息以定位特定的对等体和对象。响应本地和远程查询。默认为 DHT，但可更换。

交换 - 一种支持有效块分配的新型块交换协议（BitSwap）。模拟市场，弱化数据复制。贸易策略可替换。

对象 - 具有链接的内容寻址不可更改对象的 Merkle DAG。用于表示任意数据结构，例如文件层次和通信系统。

文件 - 由 Git 启发的版本化文件系统层次结构。

命名 - 自我认证的可变名称系统。

这些子系统不是独立的;它们是集成在一起，互相利用各自的属性。但是，分开描述它们是有用的，从下到上构建协议栈。

Filecoin：

Filecoin 是一个去中心化存储网络，它让云存储变成一个算法市场。这个市场运行在有着本地协议令牌（也叫做 Filecoin）的区块链。

区块链中的矿工可以通过为客户提供存储来获取 Filecoin,相反的，客户可以通过花费 Filecoin 来雇佣旷工来存储或分发数据。和比特币一样，Filecoin 的矿工们为了巨大的奖励而竞争式挖区块，但 Filecoin 的挖矿效率是与存储活跃度成比例的，这直接为客户提供了有用的服务

36.3.2 IPFS 挖矿机制

从 filecoin 的白皮书可以看到 filecoin 的挖矿机制基于存储和检索服务,任何用户都可以作为客户端、存储矿工和/或检索矿工来参与 Filecoin 网络。

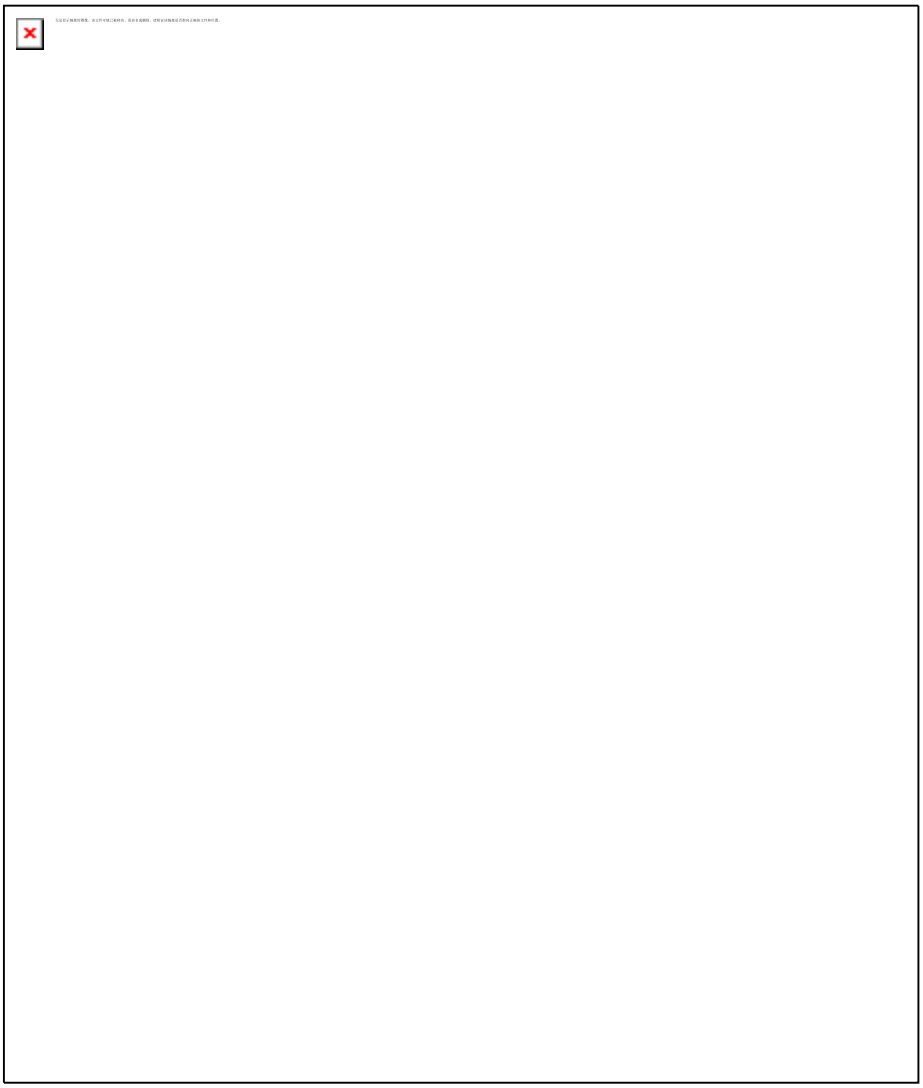


图36-19 filecoin 协议

挖矿流程如下：

1）由去中心化存储网络(Decentralized Storage Network)(DSN)：提供存储和检索服务两种独立服务市场。

2）网络用户和矿工设定所要求服务的价格和提供服务的价格，并将其订单提交到相应的服务市场。

3）网络使用者会在 DSN 中通过 Put 和 Get 请求存储数据或者检索数据，并为此付费。

4）存储矿工为网络提供数据存储。存储矿工通过提供他们的磁盘空间和响应 Pug 请求来参与 Filecoin。要想成为存储矿工，用户必须用与存储空间成比例的抵押品来抵押。存储矿工通过在特定时间存储数据来响应用户的 Put 请求。存储矿工生成"时空证明”，并提交到区

块链网络来证明他们在特定时间内存储了数据。假如证明无效或丢失，那存储矿工将被罚没他们的部分抵押品。存储矿工也有资格挖取新区块，如果挖到了新块，矿工就能得到挖取新块的奖励和包含在块中的交易费。

检索矿工为网络提供数据检索服务。检索矿工通过提供用户 Get 请求所需要的数据来参与 Filecoin。和存储矿工不同，他们不需要抵押，不需要提交存储数据，不需要提供存储证明。存储矿工可以同时也作为检索矿工参与网络。检索矿工可以直接从客户或者从检索市场赚取收益。

5）矿工通过复制证明和时空证明两种方式来进行挖矿：

“复制证明”（Proof-of-Replication）允许存储提供商证明数据已经被复制到了他自己唯一专用的物理存储设备上了。执行唯一的物理副本使验证者能够检查证明者是否不存在将多个数据副本重复拷贝到同一存储空间。

“时空证明”（Proof-of-Spacetime）允许存储提供商证明在指定的时间内存储了某些数据。

36.3.3 IPFS 机会与风险

1）IPFS 的机会：

从 Filecoin 的挖矿机制看，这种需要磁盘空间的挖矿形式和比特币挖矿有很大的区别，btc 挖矿是个减量市场，挖一个少一个，而 Ipfs 挖矿是个增量市场，随着项目应用的增多，项目方会上传大量的数据，数据市场的价格也会水涨船高。逻辑是不一样的。

ipfs 个人挖矿由于网络条件的原因，并不能提供专业矿场的上行下载的速度，所以个人矿工现在看并没有什么优势，而所有的区块链项目都需要节点，专业矿场会直接和项目方谈节点更容易卖出存储资源。

ipfs 挖矿的赚的是资源的钱，即使没有代币，存储资源也值钱，所以代币化之后，存储资源依然值钱，在行业早期能够提供专业化存储的团队一定会有生存空间，这是 IPFS 挖矿的基本逻辑。

2）IPFS 挖矿的风险

首先，早期并没有足够多的用户租用网络资源是 IPFS 挖矿最大的风险部分。

其次，IPFS 挖矿是网络资源所有者的竞争，谁拥有更低成本且优质的网络资源，谁就更容易获得网络资源带来的红利。如果算力的竞争变成网络资源的竞争，那么并不是有矿机就可以保证收益的，这也是挖矿的风险之一。

36.4 利用空闲的 CPU 挖点 XMR

BTC、BCH、ETH 等主流数字货币的竞争已经白热化，一般配置的机器直接不能玩，而 ZEC、XMR 等匿名类数字货币由于其本身的加密特性，算法复杂，而且需要较多的内存，并且价格还不高，这类币的专业矿机还未出世，所以普通机器还可以尝试。下面我以 XMR 为例说明具体的步骤。

36.4.1 挖矿软件

现在世面上有许多开源的挖矿软件，速度参差不齐，我试验了 claymore、eqm、nheqminer、sgminer、xmr-stak 等几款软件，最后选择了这两款软件。

1、xmrig2.3.1

这是一款利用 CPU 挖矿的软件，如果大家下载不方便，直接点这里：https://files.cnblogs.com/files/speeding/xmrig2.3.1.rar

2、ccminer64

这是一款利用 nvidia 显卡的 GPU 进行挖矿的软件，我用的版本是 2.2，下载链接：http://pan.baidu.com/s/1eRFpBs2

36.4.2 钱包地址准备

挖出来的币得放在钱包里，或者放在交易所里，如果你在 poloniex 等交易所有账号，可以申请一个 xmr 充值地址，然后记下来，xmr 的地址非常长，比如：

43haAx81nYteyA3VQcj8XQBorEkAo9Bm7Xh7DLgdWoCtQsRWj2ma9V7WvLjV7gVM7iSzQ5ydg5G3dLhpwJkj8QK8GgfZPw5

门罗币自己也有全节点的钱包，叫 monero-gui，我用过 0.10.3 版本的钱包，不用同步也

可以生成地址。

36.4.3 配置参数

1、先说 xmrig 软件的参数

这个软件中只需配置一个 config.json 文件，用文本编辑器打开后是这样：

```
"algo": "cryptonight",
"av": 0,
"background": false,
"colors": true,
"cpu-affinity": null,
"cpu-priority": null,
"donate-level": 1,
"log-file": null,
"max-cpu-usage": 75,
"print-time": 60,
"retries": 5,
"retry-pause": 5,
"safe": false,
"syslog": false,
"threads": null,
"pools": [
    {
        "url": "pool.supportxmr.com:7777",
        "user": "43haAx81nYteyA3VQcj8XQBorEkAo9Bm7Xh7DLgdWoCtQsRWj2ma9V7Wv
LjV7gVM7iSzQ5ydg5G3dLhpwJkj8QK8GgfZPw5",
        "pass": "cpuxmrig:slofslb@qq.com",
        "keepalive": true,
        "nicehash": false
    }
]
```

其它不懂就不用懂了，max-cpu-usage 表示占用 cpu 的百分比，最重要的是 pools 里面的参数，支持 xmr 的矿池挺多的，我选了功能不错的 supportxmr 矿池，url 是连接地址，user 是前面介绍过的 xmr 钱包地址，pass 的设置有一个规则，用冒号分为两部分，冒号前面是一个 worker 名称，如果你有多个机器或 CPU 都在挖矿，设置不同的名称。冒号后面是邮箱名。

运行程序时，直接启动 xmrig.exe 即可。

2、再说 ccminer64

ccminer 也可以用一个配置文件，也可以直接用命令行搞定，比如：

```
ccminer-x64.exe --algo=cryptonight --url="stratum+tcp://pool.supportxmr.com:7777" --user="
43haAx81nYteyA3VQcj8XQBorEkAo9Bm7Xh7DLgdWoCtQsRWj2ma9V7WvLjV7gVM7iSzQ5ydg5
G3dLhpwJkj8QK8GgfZPw5" --pass="nvidia:slofslb@qq.com"
```

--algo 后面的参数是 xmr 的算法名称

--url 是矿池连接方式

--user 是 xmr 的地址

--pass 是与 xmrig 类似的 worker:邮箱，这里的 worker 取不同的名字即可

36.4.4 查看挖矿进度

在 https://supportxmr.com 网站上可以看到自己挖矿的主要指标和收益，步骤：

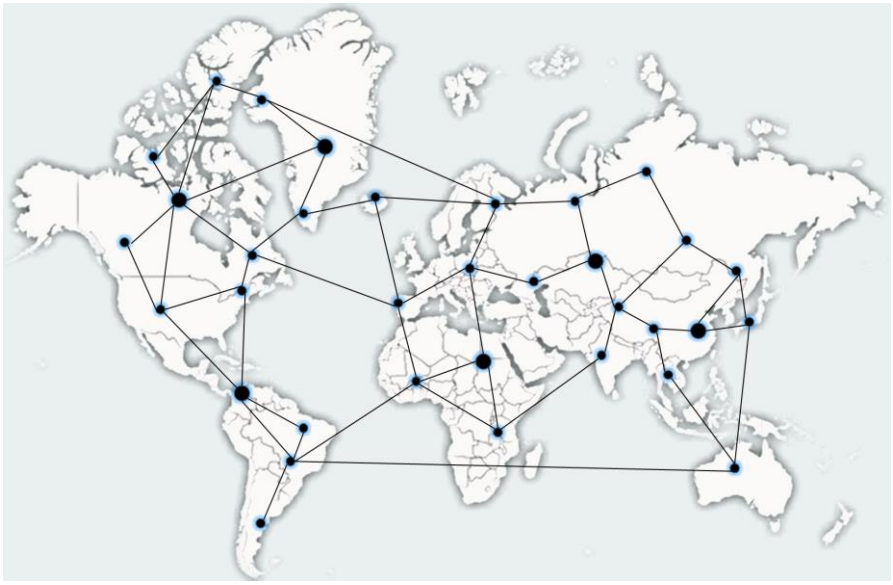
1）登录 https://supportxmr.com

2）点击左侧的 Dashboard，在 Enter Payment Address 中输入长长的 xmr 地址，点 Track Live Stats，就可以看到挖矿进度了。

该矿池最低 0.3XMR 才发币，如果你的算力仅仅为 100H/s，那估计得挖上 6 个月左右吧。

如果你的 CPU 本来就闲着，那就让它用 75%的时间挖着玩，也不会影响其它事务。

第七篇 投资原则篇



37

38 区块链投资生存指南

本章内容是在苏江 2018 年 2 月 12 日做的一场线上直播的基础上增改而成的，仅供参考。

38.1 当前区块链市场的现状

38.1.1 疯狂的 2017 年

很多人已经见证了 2017 年数字货币的盛况，2017 年的疯狂可谓史无前例，整个区块链的市值从年初的最低几百亿美元市值左右，上升到了最高时的八千亿美元市值左右。

从 GBI 指数，也就是区块链全球指数上来看，从一开始的一千多点，涨到了最高时的两万多点，这就意味着，如果 2017 年年初按照一定的配置，买入一些前二十名的主流币种，最少应该有 20 倍左右的收益。如果你一年没有赚到 20 倍的收益，就算没跑过大盘。不过也很正常，90%以上的人都没跑过大盘，这是个很有意思的现象，很努力炒币的人可能真没有那些放长线的人收益高。

而一年下来，我们能观察到的是，无论好币还是差币，一年涨幅达到 100 倍的，应该也有 100 个币种以上。这个数字是很惊人的，但也不用羡慕，因为不大可能有几个人能拿这么多倍，多数人都会在涨涨跌跌中被甩出去。也不用羡慕 13 年前进入币圈的人，他们可能更悲惨，大部分人在经历暴跌的洗牌后，就再也不敢碰比特币了，多数人也并没有因为进入早而获得更高的收益。

所以说，没有一定的投资策略，你很可能连大盘都跑不过，辛苦炒币可能也只是白忙活一场。

38.1.2 疯狂是否已经结束了？

2017 年发生了很多事情：央行约谈交易所、比特币病毒、纽约共识大会、94 政策、比特币分叉潮……在 2018 年初还经历了一场暴跌，很多人可能对区块链世界失去了信心（或许已经离场了），开始有些恐慌了，所以有很多朋友问我，这次熊市会熊多久，2018 年，会不会是一个大熊年？区块链行业的红利是不是已经结束了？

我的回答也很干脆，没有，绝对没有，区块链行业最少还有 2 年的红利期。最起码对于比特币、以太坊这些主流区块链来说，它们从无到有地向世人展示了价值传输协议是什么样子，而真正的区块链应用仍未出现，所以现在仍然是早期，一切才刚刚开始，这句话放到今天仍然适用。

很多人把区块链产业的泡沫与 90 年代末的互联网泡沫（也叫 dot-com 泡沫）来相比较，我想告诉大家的是，两者目前真的是没发比，要知道，今天(2018 年初)的区块链总市值也就 4000 亿美金。据可查数据，互联网泡沫的奔溃是在 2000 年 3 月到 2002 年 10 月间。总共约 5 万亿美元的凭空蒸发。

一个是千亿级别的市场，一个是数万亿级别的市场，差距仍不小。

全球黄金的市值在 2017 年底是 7 万亿美金，更不用说股票，房地产和对标的法币市值。在你的心里，加密货币总市值才值黄金市值的 1/10 都不到？

如果非要问，2018 年初这个阶段可以类比于互联网发展的那个阶段？笔者的个人观点仍然把他算作 90 年代早期，2018 年年初的泡沫破裂仅仅是历史上的一个小插曲，过后肯定还会继续酝酿出前无古人的史诗级大泡沫。

即便现在伴随着小泡沫的破碎，但也破碎得并不彻底，一点都不彻底，跌的居然只是比特币，其他各种劣币依然这么顽强，

所以，笔者的逻辑也很简单，泡沫固然存在，远离泡沫（同时也远离了机会）才是最大的风险，在大趋势出现的时候，如果能看清趋势的走向，判断出当前时刻所处趋势的位置，只要还是早期，那么，坦然拥抱泡沫才是更正确的姿势。也可以预料到，极有可能的是，当史诗级泡沫破裂的时候，大家 90%的可能性依然躲不过，但也不需害怕，如果持有的都是具有长期价值的投资物，能经得起泡沫的洗礼，风雨之后依旧会起来，泡沫之后才能见到真正的"谷歌、亚马逊"。

对于已经离场，不再相信区块链技术这种巨大威力的人说，只能祝他们好运吧。

而对于一个月前才进场，一进场就"被套"的新人来说，也没有什么必要惊慌，"被套"是再也正常不过的事了，作为投资者，唯一要想清楚的是，你现在买的是不是垃圾币？如果不算是垃圾币，那么迟早会有重见光明的一天。现在你就把你的这笔投资当作丢进了一个黑盒里，要一定的时间才能解封，这段时间不管它就是了。

可能有人认为笔者没"被套"，觉得笔者站着说话不腰疼，但个人也的确就是这么过来的，笔者也被套过好几回，但在时间的沉淀下，再垃圾的币都解套了，比如 Status，bancor。尤其是 Status， 破发了半年之后，居然又涨了十倍呢，谁都很难搞清楚这里面的逻辑。

38.1.3 All in 的悖论

投资有很多大道理，说多了大道理，很多人也不愿意听，但还是不得不说一些道理（因为真的很重要）——懂一些投资道理跟完全不懂还是有本质上的区别的。

很多人最近被郭宏才(币圈网红宝二爷)的视频刷屏，二宝在视频里提到，最好拿闲钱投资，因为用闲钱投资时，哪怕是腰涨，大熊市来了，心理也不会受太大影响，因为反正钱也不多，亏了就亏了嘛。

不过他说完就画风一转，他说，如果拿闲钱投资，你亏的时候不会亏太多，那也意味着你不可能赚太多。你拿个资产的百分之一在投资，就算涨了 100 倍，对你的财富结构也不会有太大的影响，你不拿出自己资产的 90%来投资，怎么可能翻身呢？

"同志们，这是一场千年难遇的机会，难道只是随便投投而已吗？"

但，无论是拿闲钱投资，还是拿自己 90%的资产近乎 all in 了进去，请记住，只投自己能完全承担得起的钱，这是你自己所做的选择，你要（学会）为自己的选择负责——毕竟大家都是成年人了嘛！

之所以说承担得起，因为这完全是一个个人的度量，有的人亏一万就跟要了老命似的，有的人亏一千万都没感觉（这类人的赌本非常大）。不过还是有一点值得建议（强调）：千万不要借钱投，不要贷款投，不要卖房投，不要去搞期货加杆杠投——因为加期货杆杠极有可能让你走到亏得承担不起的地步。

这是投资区块链的悖论：无论是哪个大咖，他们都会告诉你，只用闲钱投资，只用能赔得起的钱去投资。

实际上，真弄懂区块链的人，了解趋势的人，都是 all in 进去的。

郭宏才说话只是相比其他人太实在了，总是粗糙地道破事实，但话糙理不糙。

大范围的分享，只能说说普世的道理，而投资这种事情，对于个体来说，只能针对性地讲

针对性的道理。李笑来和老猫等大咖也只会跟大家讲一些普世性的道理，最起码符合大众的三观，如果私下间，才有可能跟你说他们自己的一些实际操作。哪怕是李笑来，经常宣称说拿着不动，坚持守币，其实他早期也做波段——只不过他醒悟得早。

老猫会明里会跟你说，要配置 70%的比特币，20%的其他白马币种，这样能助你更好地度过牛熊。说他看好 eos，要合理的做好配比，谁知道他实际有多重仓 eos 呢？人的看法会变，个人的认知、实际操作也都在变化，只有那一层普世的道理不变。

所以说，普世的道理针对大众，具体的道理要针对实际的个人情况。不同人需要根据各自的资金量，年龄阶段，风险承受能力，制定不同的投资策略。

38.2 区块链投资的本质

进入区块链投资，你要搞清楚投资区块链的目的是什么。

答案一，当然是赚钱：绝大多数人的想法是，现在有区块链这么个玩意，普通老百姓都可以参与进来投资，而且没有门槛，多好的一件事，那就趁着这波浪潮，能捞上一笔算一笔，赚到了就赶紧撤。

就算是认真地投一些区块链项目，可能你也是想着，这一波捞个千百万就撤，然后就回老家买个房子安顿养老……

答案二，是赚币：这里说的币一般是比特币，当然也有一些人的目的是赚以太坊（甚至 EOS），不过一般来说还是以比特币为最基础的投资标。

从稍微长远一点的角度来看，作为一种世界货币，比特币是有理由在一定程度上在这个世界拥有一席之地的。当然，你也别指望它会替代法币，它没必要替代法币，它仅仅是一个作为世界银行所发行的货币而已。或者说，它就是存在于互联网这个虚拟世界的虚拟银行，买比特币买的就是虚拟世界里面的虚拟银行的股票，因为它是相对于发币波动的，它具有股票的一些性质。

不过说虚拟也并不完全虚拟，就像过去人们对“软件是否该收费”这样的争执一样，软件虚拟吗？软件不值钱吗？认为只有现实物体才值钱，那是农耕文明的思维方式。你也可以称比特币为数字世界的数字货币，如果你认为虚拟的东西太虚无缥缈的话，那么，请问你天天用手机电脑，你是在现实世界中活着的时间比较长还是虚拟世界中活得比较长呢？实际上，我们这代

的年轻人，起码精神上都已经向互联网移民了。

于是我们的目标就很清晰了，为了在这个虚拟世界生存，你要用的就是虚拟货币，比特币就是虚拟货币之王，所以在这个世界你的投资目的只有一个——**赚比特币**。

无论是投资其他数字货币，还是投资 ico，你的唯一目的就是赚比特币。毕竟你法币就只有这么多，都入场了就没钱了。

所以，投资区块链的目的就只有一个，赚更多的比特币。

而投资的本质就是：**将成长速度慢的资产转移到成长速度快的资产上**——这件事值得长期重复做。

从趋势上看，尽管比特币本身的市值是在不断扩大的，但比特币所占区块链市场的份额却是在逐步降低的，在这一个过程中，会有一些其他币种涨得比比特币还快，所以其中还是有不少投资机会的。

所以说，作为一个投资者，真正值得我们追求的应该是“长期成长率”——我们不断地寻找成长率更好的投资标，从这辆车跳到另一辆车，其实就是为了追求“长期成长率”。

38.3 区块链投资策略

当你弄清楚了区块链投资的本质后，思考得再深入点，你要判断的是，什么是（长期）增长速度快的资产，什么是（长期）增长速度慢的资产。

这一定程度上就取决于你的见识了。不过，这一定程度上是可以量化的，有个别较真的投资者甚至会把各个币种，各个 ICO 项目给量化成一个个具体的指标，用可能性这样的概率来给项目评分，以方便做决策。

38.3.1 拼概率

不夸张地讲，投资就是一场概率游戏，我们所进行的所有投资活动就是从各个方面搜集更多的信息来分析，从而提高我们决策成功的概率。

从另一个角度来看，投资其实跟赌博没什么本质区别，只不过，赌博一般都是你只有低于 50%的成功机会，而投资，则是你要不断去寻找成功率高于 50%的事，投资也就是赌概率。

你只要尽可能多的去对你要投的项目多了解一点点，各方面信息多知道一点点，就能很大

地提高成功的概率。

之所以说概率这么一回事，是因为“概率”这个概念在投资中占了一个非常重要的位置。

举个例子：

在 2018 年初这场暴跌时，很多人都知道要抄底，他们问我该抄什么币的底？

我的回答是：只抄主流币，而且谁跌得多，就买谁。

整体上来看，是比特币领跌的，跌的幅度最大，而其他币种相对于比特币来说价格也没怎么跌，所以我说抄底比特币就够了，毕竟比特币是到过 12 万一枚的品种，从概率上来讲，比特币未来回归到原来最高点的概率就是比其他币回归到最高点的概率要大。

38.3.2 无情绪

下一个要说的点就是：要做到投资时没脾气。实际上，投资最忌讳的就是情绪波动，尤其是对新人来说，这一点最难克服。

当你买了一个品种后，你可能每天没事都会想要打开行情软件来看一看，每天睡醒的第一件事就是看行情。说实话，一开始笔者也是这样，一年后才真正地进入佛系状态（就是少动，少看）。2018 年初的这次暴跌，起码自己的心境还是很平静的，别人不说自己都不知道比特币跌到了四万多。

而你事先对自己的投资物早就有了期望设定，如果目标是 10 万美金，那么中间过程是如何达成的就没那么重要了。

情绪是投资者的敌人，甚至不夸张地说，人性常常是“成功投资”的绊脚石。投资通常是反人性的，当市场整体涨的时候，你会认为形势大好，赶紧加仓（这个时候我们靠感觉判断），稍微有点风吹草动的小跌，你就会觉得形势不妙，急着抛盘（这个时候我们也靠感觉判断）。

但这样做的结果常常（真的是常常）就是你加完仓就跌了，跑完盘就涨了……

币圈里，你会发现一个常见的错误逻辑，很多人是这样一个情况：一个币因为涨的好，所以才看好它。一个币因为跌了，从而对它失去信心，进而对它更加看跌。

还有一个现象就是，一个币，或者一个项目，你对它研究得越多，了解得越深，很有可能你就会更加认可它，更加对它深信不疑。这就好像你喜欢某个人，虽然她/他事实上不是世界

上最漂亮（帅气）的女生/男生，但是在你眼里她就是最漂亮（帅气）的……——这种带有主观的意愿在日常生活也许没事（有时甚至还有好处），但这在投资中常常就是十分危险的一件事。

这也算是一个悖论吧。如果你一开始感觉一个东西好，你可能会不断地刻意寻找证据来证明它好。

这都是人情所致，所以我要说：“千万不要对一个币产生感情”。

笔者就是对公信宝（GXS）动了真情，上线翻了几十倍也还一直坚守着（真爱，但在这个领域里真爱可能会伤了你，甚至毁了你），以至于也损失了不少的机会成本。

38.3.3 讲原则

另外一点就是，在你投资之前，就要制定好投资策略，你所做的策略，就是你的投资原则。

郭宏才说他自己投项目的时候从来不看白皮书，投项目时自己也不懂，都是凭感觉，感觉哪个项目不算太差，就扔些 ETH 进去。

我前段时间偶然有机会私下跟郭宏才交流过，他在硅谷的两天时间，投了三个项目，而且都是 几千个 ETH，他每天看超过 10 个项目，我们普通人难以想象。不过，他能看懂吗？郭宏才也很实在，他说他看不懂项目，只是凭感觉，照样广撒网地做投资。不过，获得那么大的财富，他也很识趣，他说自己就是个卖牛肉的，很清楚自己是什么位置。他最起码相信区块链技术正在改造这个世界的趋势，所以他有理由盲投，只要是在风口上，猪都会飞起来。所以为了减小风险，无论是什么项目，他都会上线后卖一点，先把成本收回，然后零成本地玩。

但是毕竟人家是大佬，人家的成本多低，别人的策略我们没法学。处境不同，策略不同。我们可以制定自己的投资策略，为自己的投资行为制定原则。如果你想赚短线的钱，每天做做波段，那你就必须接受自己跟百倍币无缘的这个现实。如果你想赚长线的钱，想抓住一两个百倍币，那么你没必要去羡慕那些每天炒短线赚钱赚到手软的人，他们短期赚钱的诱惑力可能会对你影响很大，但你必须清楚你选择的是一条怎样的路线。

笔者这里说几条自己的投资策略和投资原则：

1、由于所有的投资行为都是攒比特币，或者可以加上以太坊和 EOS，那么短期来看买其它币都是临时行为。

2、配置最少 xx 个比特币（无论是五个还是十个），作为长期屯币的最少标准，多余的用来投其他币或者 ICO。

3、其他任何决定长期持有的币都给自己设定一个最少屯有量，如有必要可屯到钱包，而非平台，以防止自己的手贱行为。

4、握紧主流的几个币，其他币未必要长期持有。

5、目前的长期持有主流币种包括：BTC、ETH....（还有更多，但无法公开做投资建议。）

6、通过参与 ICO 换来的代币，在能交易的一段时间后，通常慢慢地卖掉一半，换回主流币——除非遇到个别极其看好的项目。

7、任何币种在买的时候，就设定一个预期的目标价格，不达到不卖。

8、坚决不碰没有价值没有意义的一些品种，包括传销币，以及没有任何创新的山寨币，哪怕它涨了 100 倍，也不羡慕。

9、将自己的币种控制在 20 个左右（主要是为了省心）。

很多人没有什么原则，做事很随意，经常发生这样的情况，比如某个币突然暴涨，或者出乎意料的暴跌，问笔者怎么办，笔者通常会回答，当你不知道该怎么办的时候，那就卖掉一半吧。

在无法预知未来的盲目状态下，减仓一半是最好的避险办法。

38.3.4 看准后重仓

下一个要说的是重仓（重点投资），重仓是我们重点讨论的一个部分。有的朋友说了，不对呀，不是说鸡蛋不要放在一个篮子里吗？话是这么说，但你也应该明白之前说的一个道理，即：不同的人情况不同，应该制定不同的策略。

李笑来的硬币资本，在去年一年里投了 100 多个项目，平均每两天一个项目，而且每个项目的投资规模都不小。硬币资本的前负责人易理华说，总结下来，百分之二十的项目盈利超过尾部的百分之八十项目。

大资本大基金采取的是广撒网的策略，对于手头数亿规模的资金来说，也不得不采取这样的策略，一个项目能投几千个 ETH 就已经算很多了。

而对于我们普通人来说，资金极其有限，可能广撒网也能碰到几个百倍币，但资金太分散很难获得较高的收益回报。

所以对于资金量不是很大的个人来说，尤其是年纪不大的年轻人，风险偏好很高，能承担得起较高的风险,所以这类人还是宁愿在确定性大的项目上多投点，这是基于概率的基础上来讨论的。如果说同时有三个项目摆在你的面前，一个 30%的成功率，一个 60%的成功率，一个 90%的成功率...那么你会选择广撒网吗？无疑，选择重仓 90%成功率的那个项目将是更明智的选择。

查理芒格（股神巴菲特的合伙人）基本上也是这样的观点，伯克希尔哈撒韦公司（Berkshire Hathaway Cooperation）过去几十年积累的数千亿美金，很大程度上依赖于 10 个最好的项目带来的，其中包括可口可乐，富国银行等。

当发现好的机会之后，就应该狠狠地下注，把赌注押在有把握的事情上，其他时间则按兵不动。其实说来投资就这么简单。

在逻辑上，笔者有无数的理由 all in 到区块链里的，最起码在当前的历史阶段是这样。

在概率上,我们要不断地去寻找那些成功概率相对更大的项目,下更多注在这种项目里面。

38.4 如何筛选优质区块链项目

38.4.1 概念炒作

很多人问我这个项目怎么样，那个项目怎么样。说实话，我看过的项目也实在有限（主要真心看不过来），当他们问我这个项目怎么样的时候，我可能十有八九连名字都没听过（主要是这个世界里面的项目实在是太多了），更有可能的是，有一些项目一听名字就能察觉有些不太靠谱，根本没兴趣去看，但很多人就是很感兴趣，也不知道为什么。

来说说个人投 ICO 的逻辑，笔者投 ICO 的逻辑一直也在变。一开始，我们看项目的重心在于看项目逻辑，看白皮书写得好不好，再后来，主要看的维度是，众筹的估值高不高，上涨空间如何，最关键就是团队懂不懂营销，再到后来，ICO 项目井喷式大量出现，全球到处都在搞区块链孵化器，我开始发现很多团队都仅仅是在玩概念而已。

在什么都没有的情况下，任何一个创业团队都可以发表自己的 idea，通过发布 token 来进行融资。这在过去实在难以想象，光一个 idea 就能值好几个亿？疯了吧？

笔者在硅谷的期间，看了很多项目，发现了一个让人有些诧异的事情，就是很多项目是中国的项目,然后他们跑到硅谷来路演——他们在演讲能力上表现倒是都不错。只不过深入发现，居然超过半数的区块链创业团队连一个技术人员都没有,只有创始人在台上描绘他对自己项目未来的设想。

很多项目甚至是技术人员都是共用的，大家都出自一个孵化器嘛。当然，技术人员也分好多种，笔者也是技术人员，也是学计算机专业的，但在编程这方面，只是略知些皮毛，做做网页跟搞区块链开发完全是两回事，离区块链应用编程还太远，区块链这行的技术人员通常都是全能型人才，所以千万不要太高估了那些说自己是搞技术的——个人认识很多搞技术的，但对区块链却也是一窍不通的人。

38.4.2 寻找技术人才

基于区块链技术人员极其稀缺的这个现实，我看项目的逻辑就简单了很多。主要就是看团队，看人，这一点的权重应该超过 80%。

1、看创始人靠不靠谱，过去有没有做过什么成功的项目。通过 google, linkedin, 各种渠道了解这个人，能线下见到就最幸运了。

2、其次就是看这个团队是否真有技术人员，是不是懂行的技术人员。

3、再进一步就是看这个项目是否有 github 代码，github 上是否有项目的原型，以及最近有没有更新。

剩余就是看项目逻辑，以及一些零散的指标，比如：社区的热度，包括 telegram、slack、twitter 的热度，以及对未来热度的预测。再比如：项目的硬顶高不高，什么时候上交易所啊.....

38.4.3 看懂项目逻辑

最关键的一点还是项目逻辑，很多人看不懂项目，一看到官网介绍就一头雾水，更别说白皮书了，大家千万别紧张，白皮书这东西本来就不是一般人能看懂的，十有八九笔者也看不懂。

当前的市场环境下，多数区块链项目是拼概念的，概念写得深奥一点才更好糊弄人吧，大家也都能看到一个现象，越是简单易懂的项目，大家越容易相信，越轻易去投。大家千万别因为“只投自己懂的东西”这句话而掉进坑里，你能看得懂的大家可能都看得懂，但这并不意味着

这就是一个好项目。

有些描述深奥的项目介绍也可以简化,尽可能用自己的第一性原理去解读这个项目是不是扯淡（忽悠人）。

区块链项目可以简单粗暴地分成两种，一种是作为区块链基础设施的一些东西，可能是一个公链，也可能是某些服务。

如果是公链， 你就带着几个问题去质问就好了：

（1）该区块链项目能解决现有基础设施的哪些问题？比如解决了比特币交易慢，以太坊拥堵，还是什么其他问题？

（2）凭什么世界一流的比特币和以太坊团队没解决你们能解决？

（3）这个项目对区块链生态世界以及对现实世界有什么影响？是否有技术突破或者有其它方面的创新？

当然，现在区块链这个世界仍处于一片蛮荒之地，仍然需要人进来开疆拓土，搭建基础设施，在基础设施这方面仍然是 2018 年的重点，仍然存在着巨大的机会。

另外一种就是应用币。应用币大都是以 dapp（去中心化应用）的形式建立于智能合约之上。区块链之所以被认为是直接改变了社会的生产关系，是因为很多商业事务都可以用智能合约来重新分配利益。所以说，优秀的区块链应用项目，本质上是建立了一种新的优秀的商业模式。

区块链的商业模式改变了以往中间商获取绝大部分利润的现状,由智能合约来替代原有中间人的角色，利益能够更广泛地分配到各个参与者手里。

比如：

Sia coin, 做分布式存储商，人人可以通过分享存储空间来获得回报。

对于应用类型的项目，主要就是理解它是如何改变原有的商业模式的，想想它在逻辑上通不通。是否真的有必要通过区块链技术来解决。

38.5 ICO 的现状

38.5.1 私募盛行

除了买币，再进一步说就是投 ICO。自从 2017 年的 94 事件后，ICO 在国内被禁止了，ICO 虽然在明面上被禁止，但在地下却更盛行了，几乎每天都有人问有没有私募渠道。个人的渠道也有限，而且自己的渠道也不适合推荐给别人，如果没有投成功，"翻车了"，甚至跑路了，谁又能承担起这个责任呢？

找代投其实是个风险很大的事情，一方面，你不知道代投方会不会跑路，代投方不跑路不代表渠道方不跑路，渠道方不跑路不代表项目方不跑路；另一方面，如果对方币保管不善，或者投错了，或者项目方被黑了，投到了黑客地址，其中的利益责任关系无法说清，报警可能都没用，很难走法律程序解决。

另外，目前的代投鱼龙混杂，里面暗藏了很多套路和猫腻，如果不跑路的话，代投方明里收些代投费，暗里还可能扣一些比例。这都还好，毕竟是市场交易，你情我愿的事情，最可怕的是某些代投机构，提早筹到参与者的币，用去临时炒其他币。这种借币炒币的风险是非常大的，也不是没见过这样的事情，想想作为手里拿着几百上千 ETH 的代投方,这其中的诱惑实在太大了。

所以未来，想要有安心的渠道来投项目越来越难了...如果不是自己熟悉的朋友，我也不敢轻易找人代投。

38.5.2 整个市场的焦虑

越到后期，参与私募、参与 ICO 将会越来越难，天使投资人王利杰发了篇文章，说得挺好的，他说以后就不会有私募轮了，以后只有天使轮+ICO 轮，意思就是说，现在的私募其实跟 ICO 轮区别已经不大了。币圈的人疯了一样地找私募，实际上层层分销，已经被刮了几层利润了，就跟商品有代理价、批发价、零售价一样，私募正向对公众的 ICO 轮无限靠拢，之间的价格差也将不断被压缩。

2018 年的 ICO 趋势，对于任何人来说都不算乐观：

- 知名度高，能给项目方带来品牌正面影响的资金机构，将继续获取头部的项目资源。

- 没有优势的传统资本机构难以入场，最多跟着喝汤。笔者在硅谷见到很多传统投资人，

其实都能看得出传统投资人们的焦虑——都是因为抢不到额度而烦恼吧。

- 小散户们相对还好，只是在这样的特殊国情之下，只能寻找到外部渠道。小散户们要么通过不大正规的基金参与，要么通过某些二道贩子接手分销。

- 外国项目大都需要提前注册白名单，提前进行 KYC 认证，这是主流模式。只不过 KYC 一直是这行的安全隐患，若是某项目方将护照等信息泄露的话，恐怕对我们这些老百姓参与者来说，隐性损失可能不止亏钱这么简单。

- 真正优质项目的额度将少得可怜，很可能会出现很多项目只会给白名单个位数数量的 ETH 额度，比如每人只能参与 1ETH 这样。对于优质项目，土豪们想重仓恐怕也没法总仓了。

- 反而弱一些的项目（说白了就是一些垃圾项目），可能不会有那么严格和麻烦的参与要求……但这对于小白们来说，将很容易中招。

过去小白们一入场喜欢投一些便宜的山寨币，现在，小白们可能喜欢投一些没有什么门槛参与的所谓私募或者 ICO（好的项目小白们基本是没有办法在初期参与的），所以这个行业里其实到处是坑。

行业发展到这样的一个阶段，前方依然有着巨大的机会，只是参与者们的门槛提高了些，但是我们依旧足够幸运，能够踩上这波时代的浪潮（参与不了 ICO 还有二级市场嘛），见证区块链技术对于整个世界的影响进程。

38.6 持续学习

38.6.1 相信逻辑

当人们谈论比特币时，经常见到两种反应，一种是依赖直觉的人，他们的第一反应就认为这个东西就是骗人的。另外一种人，他们倒是不像前一种人那样，但是他们会长时间犹豫不决，自己的心里也没有定论，更愿意多听从一些所谓的专家的意见。意见领袖的言论对他们的认知会有非常重要的作用，大佬大咖们说买什么他们就买什么，说卖什么他们就卖什么……这些人更倾向于跟从，而不是先经过自己的大脑思考再做决定。他们称比特币是他们的信仰，喊着什么时候要上多少万的口号，而信仰从何而来，他们自己也说不清楚。

之所以会出现信仰这么一回事，是因为人们无法用现有的认知来理解事物，于是，就想办法用简单的因果把事物给联系起来，同时也节省不少脑细胞死亡了——实际上，脑细胞是可以

不断再生的。

人类活着的首要推动是为了求存，而非求真。真理对于身体机能来说从不重要，耗费最小的能量将生命存续下去才是硬道理，所以，人类本身并不善于思考，能不动脑的事情就尽量不动脑——使用逻辑来思考很难（特别是正确地思考），简单地依赖信仰则很容易。

用信仰来生活其实是因为想偷懒。信仰有时的确能带你度过难关，但如果方向错误的话（投资靠信仰其实就是方向错误），会让人陷入到一种执着，容易陷入不愿承认错误的一种状态——历史上各种宗教极端分子就是这样。

投资就是做买卖，你的每一次交易应该都有你买入和卖出的理由，交易就是不断跟自己对话，自我怀疑，自我审视。交易多了，自我思考多了，就会越来越懂你的内心世界，经验丰富了，逻辑也会更加清晰。

投资尽量不要靠信仰，更应该依赖的是逻辑，你必须弄清楚事物背后的道理，根据当前的情况，分析出未来的可能性。依靠逻辑，进行预判，一定程度上是可以活在未来的。用逻辑推理出来的未来，其成功的可能性将会更大。当你自我怀疑的时候，不但需要为信仰充值，更需要重新审视自己的逻辑判断。

38.6.2 紧跟趋势

趋势是正在发生的事情，TCP/IP 协议使得不同的主机之间可以相互通讯，从此人们开始放弃了使用电报；SMTP 实现了个人的私密信息在不同服务器之间收发，从此去邮局寄信的人越来越少；HTTP 协议实现了人们通过一个浏览器就能访问几乎全世界电脑上的文件信息，从此开辟了一个全新的互联网时代。

区块链技术本身是一种价值传输协议，比特币的区块链底层技术实现的是点对点的价值传输，这是过去信息互联网一直没有解决的问题，它意味着不需要任何第三方就可以实现价值的传送。人类数千年来一直在寻找可被信任的中间机构，信任的成本是巨大的，而这样一种价值传输协议已经稳稳地运行了长达九年时间，人们都很期待它未来会发生些什么。

它必然会发生些什么，因为这就是趋势，趋势是客观正在发生的事，它不以个人的主观意识而改变。

趋势是事关起码五年十年的事情，底层协议被缔造的时候，任何人都很难想象未来会发生

什么，就像过去互联网刚进入人们视野的时候，只知道它能用来收发信息，谁也想不到后面的移动互联网、甚至是物联网会如何改变世界。

如果从应用的角度看待区块链行业时，加密货币相对于区块链，仅仅相对于电子邮件相对于互联网，一个是实现了个人信息的点对点传送，一个是实现了价值的点对点传送，而电子邮件出现后的互联网发展，远远超越于因信息交换而生的 Email 本身。对于区块链来说，区块链后期的发展也远远超越于以价值交换而生的加密货币。

革命性的理念和新的技术带来了无穷的想象空间，尽快里面夹杂着投机、欺诈、贪婪，但这不能作为你远离它的理由。

如果因为一些风吹草动，就让自己离开风口，显然这样格局很小。我们要做的就是紧跟趋势，稳稳地站在风口。

38.6.3 独立判断

许多人很依赖专家大牛，喜欢听专家牛人们的意见。当自己看到一个项目的时候，通常会去问，你怎么看？这个能投么？什么时候卖呢？

认真的大牛也许会好心帮你看看是否靠谱，而更可能的是，大牛的判断也不一定准确，投资这种事情本身是靠自己对项目信息的了解程度，如果你愿意深入研究某个项目，很快，你就能成为这个话题的专家，事实上，区块链项目实在太多，没有人能同时研究太多东西，每个人都是根据自己的情况和兴趣，钻研自己偏好的领域。

你所认为的大佬，未必是真大佬，也许只是一次或者几次的投机成功的，假装懂区块链的，在商业里叫幸存者偏差；其次，行业整体上升时，也有闭着眼投都能赚的窗口阶段，幸存的机会很大，再说，区块链行业很新，哪来的那么多大佬呢？

而长期问别人怎么看、怎么做的人，最恐怖的结果是自身的大脑会退化，越来越不擅长于思考问题，从而进一步更依赖于别人。

学习区块链投资，也没什么技巧，就是要硬着头皮地学，不懂就搜索，一定要学会独立判断，自己做决策，并且为自己的决策负责。

在这个领域，没有什么专家，只有自己是自己的专家。

38.6.4 持续学习

巴菲特说，投资最重要的事就是弄明白所投股票的价值所在。如果你不清楚这只股票的价值在哪里，你就不能碰。如果你明白它的价值，就没什么可怕的。比如你在股价 10 元时买入，但股价跌到 5 元时，因为害怕会继续跌，所以你可能把它卖掉。按巴菲特的理论，一个东西 10 元时你想买，5 元你反而想卖，这很可笑对么？

同样在区块链投资领域，这个现象就太正常了，没有搞懂自己投资的东西是什么，只是跟风买卖，最终很有可能在市场回调的时候恐慌性割肉——这就是常见的割韭菜。不过刚进入区块链投资的这个圈子，几乎人人都会有这样的经历，正因为意志的不坚定，虽然有着大部分人都会经历所谓的“韭菜”行为，多数人最后也会意识到这个深刻的道理——投资最重要的事情就是要弄懂你所投的东西价值所在。没有这个前提，谈什么长期持有？

要搞懂区块链是什么，本身就要费上不少心思，更何况看懂那么多的 ICO 项目呢？要想做一个真正的价值投资者，恐怕要踏上一条学无止境的路。这也是为什么说进入到区块链行业，能深刻地感受到知识是真的可以变现的，这个领域绝大多数的机会，都给了那些勇于探索研究、不断提高认知的人……

39 财富大爆炸

本文取自苏江 2018 年 1 月的文章。

2017 年恍如隔世，发生了很多事，而对于自我来说，最重大的影响是对金钱、对财富的理解有了巨大的改变.....这种转变，很大程度上也都是从接受李笑来老师的一些思想所引起的。

从 2016 年开始，我开始在知识付费上花了很多钱，单单在“得到”上就付费订阅了十多个专栏，结果不出所料，超过一半的专栏内容我都没看完，意外的是自己对知识的焦虑已经大大减小.....

人的注意力一时只能针对性地专注在一个领域，只有闲暇之时才能随机地学习一些内容……对于这么便宜的专栏价格，花钱购买了一个随机的知识库也无可厚非。

而李笑来老师让我最兴奋的一个观点不只是**“付费就是捡便宜”**这么简单，只是隐约记得在他的一次活动现场曾说过这样的一句话：

如果你还在 30 岁以下，建议你花光你手里的每一分钱。

这种观点让人感到兴奋，于是让自己有理由让自己对钱不吝啬，开始舍得为自己在不少工具上付费....开始平和地接受各种付费软件，甚至用起了两千多块的机械键盘，这事一直被我女友吐槽....花钱是任性了一点.....但还是得讲原则，因为李笑来的原话观点也是有前提基础的：

若是认为自己还有学习、成长的空间，就不要给自己留退路：**在不负债的情况下，花光手里的每一分钱，也即，在还有成长空间的时候把资金全部投入到成长与极致体验中去。**

于是我真想过这么做，在成长上花钱再不吝啬，可实际要做到却也不是一般的难，因为如何花钱也是一门技术，如何花好钱更是一门艺术，每个人都是自己的老板，行使这一套个人的商业模式，它关乎的是**资源配置**的问题。

把金钱这种资源都花在对自己成长有利的事情上，等于是一直在为自己的财富道路上打下基础，在此基础之上，就可以实践**复利**的模式……

财富 = 本金 * (1 + 投资利率)^n

说复利是这世界上最恐怖的工具，一点都不为过。它是公开的工具，但鲜有人能够利用它。

本金越高越好，富二代相比常人具有巨大的优势....不得不承认，有钱的人大多数只会更有钱，这个世界本身就是这样，就像《圣经》里说的，“凡有的，还要加给他，叫他有余”。这就是**“财富黑洞效应”**，这是自然的结果，并非资本家刻意剥削穷苦大众，这个说法很恐怖，我们必须接受这个现实，尽快积累原始的资本，在困难中寻找翻身的机会。

投资利率是个变量，这对所有人都是公平的，我们每个人都有机会去寻找那些投资回报高的产品，甚至这一生都应该持续做这件事，因为你不得不接受一个现实，**劳动的回报永远跑不过资本的回报**。最起码过去几年就是这么个现状.....正如我之前所说，打工是几乎不可能实现财富自由的.....

时间是一个既公平也不公平的变量，财富的效应要到越往后越能显现，前期大部分的时间都是在酝酿，10%的回报率下，10*(1+10%)^n，10 万元需要 7.3 年翻倍，而 50 年呢？就变成一千多万了.....巴菲特和查理芒格之所以那么牛逼，因为他们能”坚持“，巴菲特大部分的财富也都是在它 50 岁之后才积累的...在这个份上，财富能达到多少量级基本就取决于**谁能活得更**

长……

这是个公开的武器，但大部分人都败在了自己对获得**即时享受**的贪婪上了，将本金拿住很难，忍着不吃利息更难…持续赚钱+延迟满足真不是一般人能做到的。但为了逆袭，除非你是个幸运的创业者，就很难再找到更好的实现路径……

除非….

除非….

除非你恰好遇上了百年甚至千年一遇的**财富大爆炸**……

财富爆炸是很罕见的，一次新的技术变革就有可能引发原有财富分配的重组，如铁路的出现、互联网的发明，都是一场场**造富运动**。

而毫不隐晦的说，正在发生的区块链技术所带来的革命也同样是一场造富运动…而且它将比历史上的任何时候都要来得猛烈。

从原子到比特：人类的财富长期以来都是以”原子“来体现的，无论体现为贝壳还是黄金，随着人类信息革命的到来，现实的一切信息都开始向互联网转移。传统的互联网只实现了**信息**的自由流通，却一直没有实现**价值的传递**……直到比特币的出现。

所谓的”价值传递“指的是，你拥有的一串比特信息（私钥）仅仅只有你拥有，并且能够通过整个网络来承认你所拥有的”比特信息“的价值，当你进行转账（”价值传输“）后，你所拥有”比特信息”则被自动赋予了全新的价值，这样就实现了无中介的价值转移功能。

在这一场革命中，以比特币为代表的价值传输系统已然成为互联网原生的货币……人类财富的“比特化”趋势已然不可阻挡。

生产关系的改革：以以太坊为代表的智能合约技术的成功运行让人看到了无限的前景，智能合约指的是通过计算机程序提前写好一份电子合同，它包括事件触发机制、以及利益分配计划。当所约定的事件被触发时，整个网络将自动实行利益的分配…这个过程不再需要任何第三方机构来干预，而程序将被强制执行，没人能够违约除非网络自身漏洞…. 利益的分配则都是通过代币的形式来体现的。

人类继工业革命之后，生产力得到里爆炸式的发展，而生产关系却一直能未有改变…. 当人类的生产关系开始通过程序代码来体现时，必将掀起一场前所未有的金融革命。

确权运动：人类经济的运作还得从“私有制”说起，私有制的产生体现为了人所拥有的财富的不可侵犯，以此为基础人们才有劳作、交易的意愿，否则财富不被承认便是徒劳。

1998 年中国的房地产改革就是通过“房产证”的形式，将房产确权与个人，房产本来不适合当作资本，但在中国有了明确的确权之后，受到了法律保护，于是房地产行业迅速发展，其本身也远远超出了使用价值，只有在被承认的基础上，才有可能变现（透支）其未来的价值。

如今，区块链技术提供了更好的**确权方案**，将你所有权写入区块链大账本，获得全网的承认是最好的方式。而这一技术的奠定，将会对经济引发多大“变现未来”的可能呢...

毫无疑问，我们十分有幸正在经历一场史无前例的财富大爆炸.....而这里最恐怖的是，这三重财富革命正同时发生.....

抓住机会，拥抱新技术，可能是我们这代人缩短复利效应、实现财富爆发的最好路径，就像加拿大的喻颖正所写的文章：《幸福取决于较多的小高潮，财富取决于极少的大高潮》...

致富不取决于你判断对了多少次，而是取决于你在对的时候敢不敢下注，在错的时候能不能止损。也就是说，财富取决于单次的幅度，不取决于频率

与查理·芒格的观点类似.....如果碰到了这种极少的“大高潮”，在关键时刻就应该下重注。

同样，如果热爱了一样事物，就应该全心地投入，拥抱它，认真地对待它，而不只是玩玩而已。

40 区块链投资近期的思考

本文来源于金炜 2017 年 10 月初的文章。

> 人们之所以不愿改变，是因为害怕未知。但历史唯一不变的事实，就是一切都会改变。
>
> ——尤瓦尔·赫拉利《未来简史》

40.1 国内的市场

2017 年 9 月注定是区块链史上值得记录的一段时光，国家央行等七部委连续出台文件，从禁止 ICO 到关停交易所，中国区块链行业一夜之间进入寒冬。然而利空尽出之后的市场行情依然稳定在 BTC 价格 25000 元人民币，风暴过后的市场底部应该就是这里吧，btc 下一次考验在 11 月份的 SegWit2x 区块扩容。

随着国家不断进行的监管政策，中国的 btc 交易从最高的占据全球 90%的交易量到现在的不到 6%的交易量，而邻国日本在 4 月份宣布比特币的货币属性合法之后，近日第一家合规的比特币交易所 coincheck 也通过了日本金融厅的批准，而等待审批的日本交易所已经超过 50 家。第一家合规交易所 coincheck 的单日交易量也一举超过了中国三大交易所的总和。

中国政策对 btc 价格的影响越来越小，持续封闭之后，也许会暂时错过区块链技术带来的金融创新，但对于普通投资者来说，btc 代表的区块链投资属于全球化的投资品，区块链带来的高增值的空间，会让投资者无法抑制内心的本性，紧盯着可能的机会。恐慌离场的韭菜也许永远不会回来了，但已经熟悉市场规则的成熟投资者，一定会蛰伏下来，耐心等待下一次爆发。

市场中唯一不变的是变化，市场会变，政策也会变化，个人认为如果把监管前的区块链行业比喻为一辆刹不住车的跑车，那么这次监管并非要让跑车报废，而是一次强制的停车检修，再次上路之后也许会更快更好。

40.2 疯狂的套利

巴菲特说过：别人贪婪时我恐惧，别人恐惧时我贪婪。疯狂的暴跌危机中，除了被割离场的韭菜外，大量火中取栗的套利者踩着钢丝疯狂收割着廉价的筹码，云币，火币，ok 禁止充值之后一边是韭菜们的恐慌性抛售，导致的 btc 价格和海外交易所价差一度超过 3000，更有 SC 之类的币种一夜之间暴跌又暴涨几倍，另一边是贪婪的套利者疯狂的买入，提币，收割利润，各交易所陆续关闭之前，最后的日子依然会是手工搬砖和机器套利者们的狂欢。

仔细思考区块链投资品种，长期看，由于天生的程序属性给了机器交易很大的空间，在国内市场停机检修之时，提供给看好区块链行业未来的投资者足够的时间去打造自己的交易策略，自己的交易程序。

40.3 未来的投资

中国防范的是去中心化的比特币带来的金融风险,没有任何一个中心化的政府会欢迎去中心化的比特币成为法币，除非对比特币带来的金融创新另有企图，比如，日本，韩国。

但是比特币带来的区块链技术，有可能给传统的互联网带来改变性的革命，比如去中心化存储的 sc，比如做数据交易的公信宝，比如出师未捷的 pressone，传统互联网中可能存在的隐私、版权、价值分配的问题，被区块链技术完美的解决了。这才是区块链行业除了货币属性的比特币之外最大的价值，能够解决互联网中遇到的实际问题的应用类项目，才是区块链的未

来！

未来能够有很强增值价值的项目有三类：

（1）区块链底层操作系统类项目比如 eth，eos，neo，qtum

（2）金融创新类项目，比如金融交易所的 omg，比如黄金交易的 dgd

（3）实际应用类项目，比如数据交易的 gxs，比如价值传递类 btm

除了 btc 之外，以上三类区块链品种对我们日常生活的改变将是巨大的，区块链操作系统提供的底层操作系统，就好像 windows 带我我们进入了 pc 互联网时代，iPhone 带我们进入移动互联网时代一样。金融创新的产品是超越支付宝的创新品种，由于数字置产转换流通的便捷具有不可比拟的优势。应用类项目的丰富则可以提供给我们升级版的互联网生活。

但是由于政策的管控，投资区块链项目一级市场的 ico 可能转入私募与海外，二级市场的投资需要出海或者等待政策调整。

未来的投资机会依然存在，只是离普通人越来越远了……

40.4 不死心的拓荒者

早上看到笑来老师的微博：哀大莫过于心死。只有那些不死心的人，才对此其实最深有感触。

就是那些不死心的人，那些相信未来的拓荒者们，才能赢得未来给予的惊喜与机会……

40.5 不成熟的投资者

上面的文字写于 2017 年 9 月 4 日的监管暴跌后，之后的日子区块链行业才开始了真正大爆炸的发展，随着对区块链行业的理解的深入才明白区块链最大的价值在于：

区块链把任何有真实价值的东西，通过区块链“无限分割并确权”且随时随地可交易，全球流动，即时变现。

回头再看去年暴涨暴跌的市场，个人认为源于区块链行业中的两个变化：

（1）投资关系的改变

传统投资面向机构，机构更理性，靠数据事实决定投资，ico 面向个人，个人更感性，太多人靠理想和情绪决定投资，可投资不是买彩票，机构也不是慈善机构，于是发生了机构利用情绪收割韭菜的一级市场，引发郭嘉监管。

（2）二级市场流通

在区块链这个不可篡改的数据库世界里，传统的行业的积分被改名为代币，在没有任何盈利证明的情况下，这些项目仅仅靠想象空间就开始了二级市场的流通，泡沫期迅速引来各种各样的投机者/投资者

对于自由经济美好未来的想象，让市场疯狂起来，被情绪和理想点燃的大量的不成熟投资者被成熟的韭菜收割机收割，一个个创富故事之后是一大堆带血的筹码。

40.6 仍然美好的未来

未来简史中提到：“如果说第一次认知革命是因为智人的 DNA 起了一点小变化，让人类拥有虚构的能力，创造了宗教、国家、企业等概念，使其成为地球的统治者；那么未来，算法和生物技术将带来人类的第二次认知革命，完成从智人到神人的物种进化。”

“人类将把工作和决策权交给机器和算法来完成，大部分人将沦为‘无用阶级’。只有少数精英才能真正享受到这些新技术的成果，用智能的设计完成进化、编辑自己的基因，最终与机器融为一体，统治全人类。”

技术是人类社会进步的第一生产力，而金融领域除了为资本家服务之外，并不产生更多价值，靠区块链所谓的数字货币来改变世界的“神话”已经过去，区块链技术革命对现实社会的改造才刚刚开始！

41 五天的海上区块链盛宴之感悟

本文节选自杨卫祥的文章。

2018 年 1 月中旬破天荒请了一周长假，带着家人出去旅游+学习：第一次坐游轮，最兴奋的莫过于 5 岁的孩子，提前一星期天天念叨，一切都是新鲜刺激的，就连第一天晚上的讲座也能从头撑到尾。

游轮很慢，1 千公里，上海到日本福冈，海上漂 2 天；在日本呆一天后再漂 2 天回来。然

而区块链却很快，常说“币圈一天，人间一年”，正好在船上又经历了一次大跌，由于公海上网络实在太差，超过 1 千多的币圈人士在游轮上干急也没办法，索性享受这次“Block Hot—For The Future 驶向未来”海上区块链盛宴。

这次海上峰会活动，由 BTC123 主办，邀请了上百位大咖，联合多个区块链项目方、交易所、媒体、顶级投资机构、开发技术团队等，意在打造专为高净值人群定制的区块链盛宴，共同开启驶向财富巅峰的旅程。

经过这次洗礼，自己认知也有进一步的提升：

41.1 更加坚信区块链的未来

区块链除了是个去中心化的分布账本外，它还有哪些意义：

经济学人把它定义为“信任机器”，目前多个产业都在引入区块链的概念来解决信用问题：物联网、支付、游戏、投资等，区块链不是一个产业，而是一种社会业态，现在已经在开始打造一个生态系统。

区块链技术已经成为新风口，**全球市值排名前七的互联网巨头都已经布局了区块链。**

2017 年 12 月，**苹果**公司创建了一个使用区块链技术验证时间戳（timestamp）的系统；

2017 年 6 月，**Google** 宣布领投比特币钱包公司 Blockchain4000 万美元；

2016 年 7 月，**微软** Azure 平台发布首个区块链解决方案，为终端用户提供分布式账本技术；

2017 年底，**Facebook** 创始人扎克伯格表示将深入研究加密货币及相关技术；

2017 年 11 月，**亚马逊**注册了三个与区块链有关的新域名；

而国内的**腾讯**则发布了区块链平台 TrustSQL，并注册“以太锁”的商标；

阿里在诸多领域都布局了区块链，特别是 2017 年 11 月 8 日，阿里巴巴集团、蚂蚁金服集团与雄安新区签署了战略合作协议，承建数字雄安区块链实施平台。

对于我们个人来说，我觉得徐小平前段时间流传出来的聊天记录同样适合我们每个人：鼓励大家拥抱区块链革命。

真格基金创始人徐小平在微信群中的聊天记录，称区块链革命已到来，这是一场顺之者昌，逆之者亡的伟大技术革命。对传统的颠覆将比互联网、移动互联网来得更加迅猛，彻底。他希望在做好现有模式的同时，了解区块链，理解 ICO，进入区块链时代。对区块链不要有怀疑，不要有迟疑，立即动员全体员工，学习如何拥抱这场革命。

而真格基金早在 2013 年就投资了交易所火币。不但不佩服其眼光，如果你到现在还对区块链视而不见，把比特币当骗局，那你迟早会后悔的。

这场区块链革命会成为一场财富再分配的革命，现在的首付已经不是比尔盖茨了，而是比特币的创始人-中本聪。

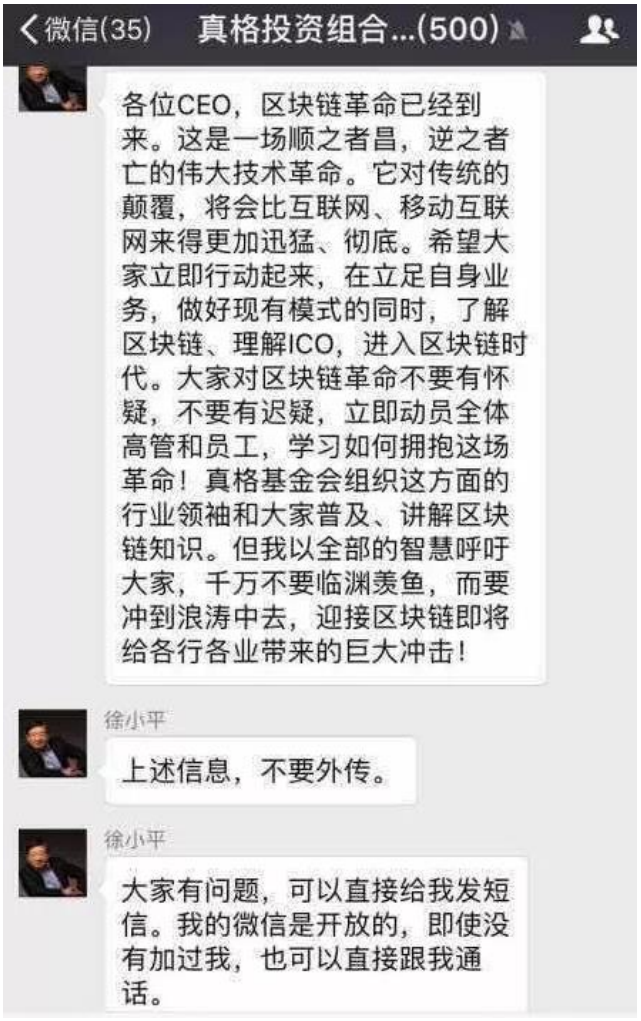


图41-1 被疯狂传播的徐小平微信

41.2 如何判断项目好坏

不得不说，区块链在 2017 年火的不行，在 2018 年还会火下去，很多人都会说这里面的泡

沫很大。确实有不少项目在骗钱，不管什么东西都想和区块链沾上关系，不管逻辑通不通就想改变世界，圈钱之后不思进取，甚至跑路，有些直接就是传销模式发展下线并绑定利益关系，这样的项目就是泡沫。

据说 99%的 ICO 项目都死了！

薛蛮子提到**区块链及数字货币投资是带泡沫的啤酒。不尝泡泡喝不上啤酒，但是泡泡占了百分之九十**。真正的啤酒少之又少，现在的项目绝大部份是空气币。

但是我们也应该辩证看待泡沫这个问题，有泡沫就一定是坏事吗？据统计，目前中国了解参与区块链的人数大概在千分之六，而泡沫要达到千分之十才会足够大。同时有泡沫才会吸引更多的人关注及进入，也会反向促进行业的快速发展。

我们要做的就是鉴别好的项目，这次峰会上火币首席战略官**蔡凯龙**分享了火币是如何鉴别项目的模型。他就是那个网传年薪 120 个比特币的蔡总，虽然他解释这是个美丽的误会。

这个模型称为火币 **SMARTChain 区块链资产评价模型**，分为五类

- ✧ Strategy 战略定位
- ✧ Management 项目管理
- ✧ Activity 市场活跃度
- ✧ Reliability 团队可信度
- ✧ Technology 技术先进性

从**风险分析**角度把五大类分成 14 个指标，从**成长潜力**角度把五大类分成 37 个指标，如图 41-2。每个指标有不同的打分比例，以此来判断这个资产到底如何，来决定火币是否要上币。

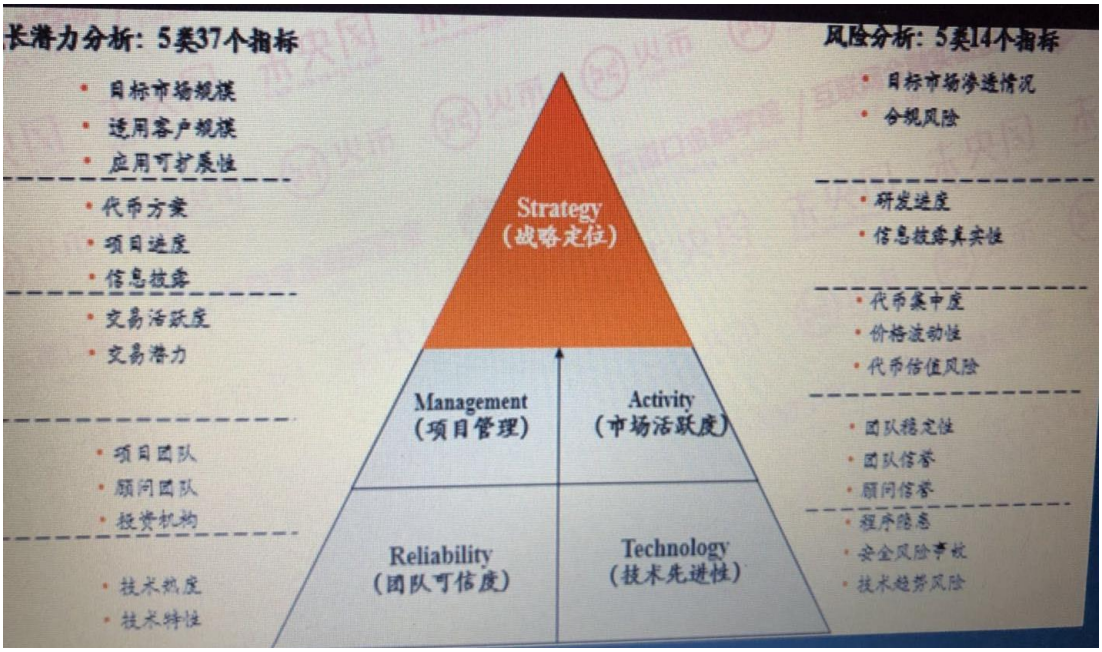


图41-2 区块链资产评价模型，来源于火币网蔡总的分享

蔡总又讲到火币对项目尤其关注三点：

✧ 技术创新突破

✧ 用户量&应用场景

✧ 合规

其他大咖也表达了他们的观点：

✧ 比如对应用类项目资金量在 1 个亿左右合适，太大有圈钱嫌疑，太小则可以考虑不周；

✧ 这个项目能否解决实际问题，改变生活；

✧ 投资重要的还是投人。

通过对项目的判断，学会鉴别，能让我们识别其中的骗局，提升赚钱的概率。

42 每次大跌了，就回来看这篇文章

本文内容由苏江参考 Youtube 上《Ready for Crypto》的视频翻译而成，视频网址：https://www.youtube.com/watch?v=9i6II8A5ACY。

已经不是第一次经历大跌了，为什么我们还是感到恐慌？

首先，我们看到一个奇特的现象，人们身处数字货币市场预测未来，喜欢指点江山挥斥方遒预测未来，但往往到最后发现自己是错的，而大部分人也从不去深入思考、分析为什么要投资数字货币，数字货币的本质是什么？而且为什么有些人总是抓不住机会，总是慢一拍，总抱怨大跌，而与暴涨失之交臂，总是完美地避开所有的正确选项呢？

其次，为什么人们在面临熊市时，总是表现慌张，并不善于冷静下来思考这些话题？如果能够深入内心，体会自己对数字货币失去信心的感觉，亦或是依旧对它的未来坚信不疑，那样你能更理性地看待市场，也能更加最大化个人的收益。

好么，让我们首先说说，一个人在受过良好教育的情况下，为什么预测未来时仍然做得这么一塌糊涂……

42.1 只用直觉，而不是理性

人们了解虚拟货币时，对它的第一反应总是错的，对它的未来看法也是错的离谱，那是因为他们通常只用不超过**五分钟去理解一件事物**，并且立即形成自己的看法。

这不是思考，这仅仅是直觉，而这种直觉往往是不靠谱的。生物学上来说，这使用的依旧是我们上古时期的**猴子**的大脑机制，它毫无任何防备，它是我们大脑中被称为下丘脑的部分，它所有的应激反应都是为了求存，几万年进化到今天，在生存相关的基本生物本能方面发挥着重要作用。而在现代已经基本脱离那种可能随时有生命危险的年代，仍然使用这部分大脑功能可能就并不是那么有效了。

这种生物本能，也叫鳄鱼（爬行动物）大脑，没有情绪，没有理智，全靠身体完成各种应激反应，当鳄鱼遇到入侵者时，只有四种反应，它有所谓的 4F 特性：

- ✧ Fight 如果是同性，就是打~
- ✧ Fleeing 如果体积比自己大，那就溜~
- ✧ Feeding 如果是体积比自己小且不是同类，那就吃了。
- ✧ Fucking 如果是异形鳄鱼，那就干~

使用大脑的这个部分，那就不可能理解任何新鲜事物，唯有不断训练我们的大脑，才能慢慢把这部分训练成一个生存机器。

42.2 用过去的思维模式思考未来

想想一百多年前，人们第一次看到汽车时，是什么反应？

“哦，这是啥机器？太不靠谱了吧……你看看它吭哧吭哧到处冒出黑烟，跑得比驴还慢，动不动就陷入淤泥无法自拔，我有什么理由放弃我那可靠的马车呢？”

很多人对未来的判断简单粗暴地进行否定，大多是它与自己所理解的世界产生了冲突。

人们总是用过去的思维模式来理解未来，想想 Sears 和 Blockbuster 这样的公司的命运，他们错误地认为未来依旧会是过去的样子，而没有想到未来社会将产生巨大的变革，过去身为巨头，他们最终失去了自己的皇冠，主宰行业数十年后轰然倒下。

人类社会就是这样，人或者公司不能自我**范式转移**，新的就会一直在颠覆旧的。

如果想通过过去来看未来，那么你应该脱离你现有的位置，放到更广的角度去看现状，使用超乎现有的理解能力去讨论 Sears 和 Blockbuster 公司为什么会失败。

42.3 捍卫现有的权益，害怕被颠覆

人们未能看到数字货币未来的第三个主要原因，是因为数字货币挑战一些人的权力地位。

正如首席执行官杰米·戴蒙（Jamie Dimon）和其他许多银行家，都宣称比特币或其它数字货币是彻头彻尾的骗局，他们想要消除任何可能引发争议的东西，以及银行和金融业这样强大的机构，他们每天都在主要的新闻网络上大肆渲染，刻意唱空，并且怀疑数字货币的潜力，而另一方面，当他们开始意识到自己的错误时，他们则也很鸡贼地发布了自己的版本的数字货币...

42.4 把自己所认为的当作现实

人们看不到数字货币的潜力的第四个主要原因呢，是因为他们喜欢把自己的观点当作是现实。因为你自己所理解的事情并不意味着你能看到他的全部，如果说我相信数字货币的未来，相信他们的潜力，并不意味着它保证成为现实。

我们一些人也可以承认自己的无知，但不是所有人愿意承认...很多人就是不愿意承认自己在某些方面有了错误的见解，于是就将错就错，自我圆说。不过这完全是人类生物自我保护的**本能**。

42.5 太缺乏耐心

新事物出现时，很多人完全没有耐心，要知道，**等待**才是最难的部分，它需要耐心让事情自然地发展。

很多人质疑，**比特币已经存在近十年了，区块链技术发展到现在还没有出现任何杀手级应用，还没有解决任何现实中有意义的问题**....他们列出了区块链技术现有的各种毛病，以此质疑它的前景... 抛开这个不说，他们显然没有一点耐心...

很多新技术创新，总是会经历各种不顺，以及人们的失望，在时间的打磨下慢慢显现光芒。

例如：TCP / IP 协议是在 70 年代发展起来的，但是互联网并没有立即就进入大多数人的生活，直到数十年之后...

42.6 总是尝试用现有的办法解决未来的问题

事物的发展当然需要时间，但很多人看不到数字货币的未来，是因为他们总是局限于现有的技术发明，就地采取了现有的一些技术方案，将其推进，并将它们也想象成未来问题的解决方案，但这是完全错误的。

在莱特兄弟发明飞机之前，过去的人总想着模拟鸟儿的翅膀来实现飞行...

当前的发明大都只能解决了目前的问题，**未来的问题可能需要用未来的方案来解决。**

你知道吗，历史上第一辆车是没有方向盘的，方向盘是在汽车出现后的第八年才发明的。

螺丝出现了 300 年之后，才出现了螺丝刀这个东西。

罐头开瓶器被发明也是罐头出现 45 年之后才被有的。

从现在的角度，你几乎不可能知道未来的解决方案将会是什么样子。但是我们现在可以尽最大努力找出解决方案将具有的特性，以便我们能够在接近它。

42.7 如何应对市场暴跌走熊

回到最开始的主题，即在市场暴跌走熊时，如何才能不傻呢？

对于那些愿意投资于数字货币市场的人来说，市场暴跌时会给一些投资者带来幻想破灭以及失去信仰的感觉....因为有些人还真是这么想的，他们以为投资了数字货币，它就会一直上

升，起初他们可能还有信仰，还很傲慢，但他们很快意识到，他们在高处买进了，现在已经下降了 50%，马上就傻了...

聪明的投资者并不会刻意地去避免每一次暴跌，所以当市场恢复正常时，他们确保他们仍处于一个合适的位置，因为这也是可以接受的。

很具讽刺意味的是，人们会因为**惊慌失措过度反应所产生的损失，远比他们丢币被盗的要多的多**。把你的币存储在自己钱包里比存在交易所里有个好处就是，大跌时可能你也懒得把币转到交易所卖掉，这样还得多一道程序，所以你还有能空来再三考虑一下。

42.7.1 不恐慌

我们的规则是不要恐慌，除非你喜欢赔钱。不要相信我们，也不要随意信任何人。即使数字货币并没有很长的历史，**还真没什么真正的专家**。

从股票市场上来说，那些把自己的账号密码遗忘，或者交给经纪人，会比那些经常出现恐慌而频繁交易的人表现要好得多。当市场下跌时，你可能无法承受持有的痛苦，如果不保持情绪镇定，可能你将会为此付出代价。有一个被称为交易悖论的事：

The best trades feel the worst and the worst trades feel the best

所以我们需要去理解这种心理，市场总是反直觉的。而我们本身都只是动物，人性所在，我们总觉得自己的反应行为是很正确的，并且经常在脑中选择性地思考，刻意搜集相关信息，只听你想听的意见，寻找那些符合你的范式的信息，忽略矛盾的信息，并加以确定自己是正确的，但这就是所谓的**确认偏见**（Confirmation Bias）。

42.7.2 不要跟市场过不去

我们的第二条不让自己变傻的规则就是——不要跟市场过不去，否则你就是跟自己过不去。

Do not trade against the market, you’re trading against yourself.

这句话是绝对正确的，顺市者昌，逆市者亡。市场试图给你提供各种信息，在某一个时刻，它试图告诉你一些信息，让你感觉你知道了你所想知道的，然而你不能看到全部，因为你只是从你自己有限的视角来看待事物。所以说，终究你看到的仅仅是你所能看到的，在所知所见之

处交易。

市场“操控”着人们“痛苦的感觉”，已被研究证实的是，当自己**没赶上一趟（上涨）的车时所导致的痛苦，可能比自己亏钱时还要来得痛苦**。为什么亏钱时要怨市场呢？其实多数亏钱都是由一些不合理的行为导致的，要么投入过多，要么破坏了自己的风控准则。

42.7.3 只投你能亏得起的钱！

Only put in what you’re willing to lose.

如果你投入了整个家当，而不是用闲钱投资，用自己能承担得起的钱来投资，你可能会到凌晨 4 点睡不着觉，模模糊糊时不时打开手机看看行情走线...

如果是新入的投资者，总是会表现得比老手更情绪化，市场下跌了，他们更容易慌张，慌张可是投资的大忌。

如果新人决定要入场时，最好在投资之前就做好一些决策，比如只用小额进行投资，并且要确保出来的时候比进去的时候多，每个月做好记录，花了多少钱，不管市场发生了什么。

42.7.4 不要尝试高抛低吸，或是追涨杀跌

所以这是第四个也是最后一个规则，不要试图掌控市场，算计上涨下跌的时间。投资之前，每个人都知道投资的基础原则是低买高卖，但是实际投资时，如果市场真的来一场暴跌呢，你想的不是不是“该不该清仓离场呢”？然后再找机会又抄底回来呢？

可能你很聪明，也许实际上你并不够聪明，也不是有意冒犯说你不够聪明，几乎每个人人都自认为自己是股神。

想知道市场什么时候会涨会跌？除非你是一个机器人，并且不断获取整个市场的每一件事情并加以分析...聪明的投资者只要保持原来的状态，并保持原有的原则，就能避免任何市场扰动。

研究显示，试图盯紧市场往往导致更糟糕的回报，随着投资策略稳定下来，收益才更稳定，除非你真是幸运的或天赋异禀之人……

附录：作者的微信公众号

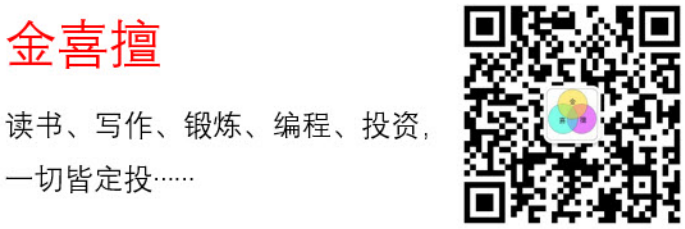
申龙斌

在博客园上写博客已经有 10 多年，2016 年 7 月底开通了微信公众号“申龙斌的程序人生”，订阅李笑来的《通往财富自由之路》1 年后，写了一篇践行笔记《人至“践”则无敌》，被李笑来的公众号“学习学习再学习”转发。

践行 GTD(Getting Things Done)有六年多，在新生大学、一块听听分别做了一场直播，点击《5 年 GTD 自我管理经验，一块听听》，可以回听。

对 Python 编程感兴趣的朋友可以看看 40 多篇的《零基础学 Python 编程》系列文章。

个人独立博客：http://shenlb.me



苏江

我是苏江，一个不思考就会死的家伙。2015 年因韩峰教授进入区块链世界，开始意识到区块链技术是一项伟大的技术革新，并同时买入人生中的第一枚比特币。从此开始思考区块链和这个社会以及自身的关系，践行自己的财富自由之路。

之后开始提笔写作，试图通过写作倒逼输出来加深自己对这个全新世界的理解。至今已经输出几十万字，现在是巴比特专栏作者，同时也是这本书的作者之一。

2016 年有幸加入了老猫 BCA 俱乐部后，开始区块链项目的大范围投资，同时也是量子链、公信宝、亦来云、IPFS 等项目的早期投资人。

2018 年决定要在这个全新的世界里面去做一点自己的事情，希望可以带领大家一起践行财富自由之路。现已经运营超过 2000 多人的区块链社群，欢迎有你加入一起搞事情。大家可

以关注我的微信公众号：苏江。

金炜

区块链投资者，比特币矿工，巴比特专栏作家，区块链自媒体路可比特创始人

区块链投资以来研究过区块链行业各种赚钱门道，ICO，二级市场投资，挖矿，搬砖，场外交易，略有一些心得，曾在一块听听上进行过《区块链低风险投资之挖矿》和《区块链低风险套利之搬砖》，经营的社群帮很多成员在 2017 年完成了 7 位数的投资收入。

2017 年上半年，在成功参与量子链的 ICO 并取得超额回报之后，发现区块链行业可能会是一场改变现有世界的技术革命，迅速的寻找行业机会。切入挖矿领域之后，成功在国内和东南亚建设了自己的比特币矿场项目，目前已建成矿场 2 个，在建矿场 1 个，托管矿场 3 个，矿场运营状况良好。

2017 年下半年年组织路可比特新媒体团队完成了上百篇区块链项目的评测文章，相关文章收录在《全球 top50 价值币种分析》书稿中。帮助 oraclechain、uip、tokenclub、WaykiChain 等多个项目完成线上推广、线下 meetup 及社区建设等工作。

2018 年希望把自己在区块链世界探索之路变成带领一群人财富自由的创造之路，新世界的惊喜才刚刚开始。

黄黎

Steemit 资深用户，写了不少 Steemit 的教程文章，《steem 指南》众创作者之一。弄了个知识星球上第一个 Steemit 相关的免费社群“Steemit 抱团成长群”旨在帮助更多喜欢写作的人，可以通过写作在 Steemit 里赚些零花钱。

在区块链投资方向上主要关注可以通过“脑力挖矿”零资金成本参与的区块链项目，更多的分享可以关注微信公众号：零成本参与区块链。

苏耀勇

传统武术（包括太极拳）的习练和传承者，尤其擅长秦汉大剑（短兵）。从传统武术阶跃到区块链这个未来世界的新潮流，对于终身学习者来说并不是一件奇怪的事情。希望通过我的学习和研究能帮助到更多的人。

杨卫祥

公众号思考与践行，深入思考、知行合一；在学习中思考，在思考中践行，在践行中提升。从 2016 年 9 月开始业余写作，已发布原创 70 多篇，其中区块链相关文章 30 多篇，创办知识星球区块链接财富自由，志力于推广区块链相关技术，识别风险与骗子，把握机遇与机会。

图表目录

术语表

1Password：一种密码管理软件，用一个主密码去管理其它密码

51% Attack：51%攻击，矿池算力超过51%之后，能够威胁区块链的安全

AES：Advanced Encryption Standard，高级加密标准，一种对称加密算法

API：Application Programming Interface，应用程序编程接口，许多交易所提供量化交易的API

Asymmetric Cryptography：非对称加密

BCC：Bitcoin Cash的代币曾用名，现在常用BCH

BCH：Bitcoin Cash的代币名称，以前称为BCC

BIG：BigOne交易所发行的一种代币

BigOne：一个国际化的数字货币交易所

BIP：Bitcoin Improvement Proposal，比特币改进提议，比特币社区提出的许多改良建议，有一套流程来处理这些提议

Bitcoin：比特币，缩写为BTC

Bitcoin Address：比特币地址，用于收款

Bitcoin Cash：比特现金，货币代码BCC

Bitcoin Core：一款全节点的钱包软件

Bitmessage：去中心化的通讯软件

Block：区块，记录着一组交易数据

Block Height：区块高度

Blockchain：区块链，一个全球共享大账本

BTC：比特币的货币单位

btc-e：一个已经关门的交易所

Byzantine Generals Problem：拜占庭将军问题，解决去中心化的网络中如何达成共识的问题

Chain：链，每个区块与上一个区块有链接关系

chain code：链代码，在HD钱包中根据主私钥生成子私钥

CNY：人民币元

Coinbase Transaction：创币交易，挖矿产生的第一笔交易记录在这里

DApp：去中心化应用

Decenteralization：去中心化

Deposit：存款

Difficulty：难度，比特币系统每 2016 个区块会自动调节难度

Digital Signature：数字签名

Double-Spend：双重支付，有些书中翻译为“双花”

Emergent Consensus：涌现共识，一种扩容方案

EOS：ByteMaster 正在打造的一款区块链底层操作系统，与以太坊有竞争关系

ERC-20：一种以太坊的代币标准

ETH：以太坊的缩写，也是 ETHER 货币单位的缩写

Fork：分叉，当多方无法达到共识时，区块链会分叉

GAS：以太坊的燃料

Genesis Block

GPU：显卡中的一种计算单元

GTD：Getting Things Done

GUI：图形用户界面

Hard Fork：硬分叉

HASH：哈希

Hash Rate：哈希率，算力

HD Wallet：分层确定性钱包

ICO：初始代币发行 Initial Coin Offering

Imtoken：一款以太坊的钱包软件

IPFS：InterPlanetary File System，一种点对点的分布式文件系统

KeePass：一款开源免费的密码管理软件

KEY：币乎发行的一种代币的名称

Keystore：以太坊用于导出、导入私钥的文件

KYC：Know Your Customer，了解你的客户，通常指实名认证

Lantern：一款 VPN 软件

Merkle Tree：默克尔树

Miner：矿工

Mining：挖矿

Mining Pool：矿池

MyEtherWallet：一款以太坊钱包

NameCoin：域名币，代币为 NMC

New York Agreement：纽约共识

Nodes：节点

OTC：Over the Counter，场外交易

Peercoin：点点币，代币为 PPC

Poloniex：排名第一的国际数字货币交易所，简称 P 网

PoS：Proof of Stake，股权证明

PoW：Proof of Work，工作量证明

PressOne：李笑来准备实施的去中心化的版权发布系统

Private Key：私钥

PRS：PressOne 发行的代币名称

Public Key：公钥

Replay Attack：重放攻击

RSA：一种非对称加密算法，用到大素数分解理论

Satoshi：聪，比特币的最小货币单位

Satoshi Nakamoto：中本聪，比特币的创始人

SC：Siacoin 的代币名称

Script：脚本，一段简单的程序，比特币区块中用于锁定、解锁比特币

SegWit：一种比特币扩容办法，隔离见证

Segwit2x：一种比特币扩容办法，先隔离见证，再从 1MB 扩到 2MB

SHA256：一种 HASH 算法

Siacoin：一款去中心化的存储产品

Sidechains：侧链

Smart Contract：智能合约

Soft Fork：软分叉

Solo Miner：独立矿工，自己独立挖矿，不与矿池相连

SPV：Simple Payment Verification，简易支付验证

Steem：一种数字货币

Steemit：ByteMaster 以前打造的一款区块链产品，去中心化的社交应用

Stratum：一种矿场与矿池的通讯协议

Token：代币

Transaction：交易

Transaction Fees：交易手续费

UGC：User Generated Content，用户生成内容

USD：美元

UTXO：Unspent Transaction Output，未花费交易输出

VPN：Virtual Private Network，虚拟专用网，代指科学上网

Wallet：钱包

WEI：以太坊的最小货币单位，为纪念一位名人 Dai Wei

Withdraw：取现

Yours.org：一款支持 BCC 支付的类似博客系统

Yoyow：一种基于区块链的内容分发平台的代币

Zcash：一种加密货币，可以隐藏币的地址和数量

1.0 版后记

2017 年十一国庆长假八天，孩子刚刚踏入大学校门，没有回家，我也不愿意去景点给全国人民添堵，想想做点什么呢？突然想起来李笑来说过，利用长长的假期可以写书、开公司，我正好已经在“区块链生存训练”饭团里积累了 200 多页的素材，平常没有时间整理，那就在这个长假整理出一本书吧。

正好在 Steemit 微信群里看到有人聊到，写作是普通人实现财富自由的机会，我真没敢有这样的奢望，但感觉“写书”这件事还是值得一做的，毕竟这是有“**复利**”效应的一件事，即可以将一份产品卖出去许多次。

虽然已经有了 90 多篇文章，200 多页的素材，但出书仍然不易，国庆长假闷头整理了 8 天，认真检查每一段文字、梳理各个知识点的逻辑关系、编辑插图、更新编号与交叉引用、保持一致的排版风格，终于在 12 日完成了全部整理工作。

我在高中之前的作文成绩基本上都是刚及格，人生从没想过会写出一本书，今天能够完成这样一本书也多亏了一年多在公众号上的坚持写作。2017 年 9 月底，我正式加入了 007 写作组织，也把此书当作给 007 战友们的一份见面礼，与大家共勉。

申龙斌

2017 年 10 月 11 日 山东东营

2.0 版后记

区块链的世界，每天都有新知识要学，1.0 版问世后 4 个多月，我也知道许多内容已经跟不上形势变化了，可惜平常没空修订。

我是李笑来的脑残粉，知道李笑来经常把假期用来写书、开公司等，所以我在 2017 年国庆期间编写出了 1.0 版，2018 年的春节也是这样度过的。

2.0 版的所有素材来自于几位共创作者在最近几个月里的分享与文章，我一开始严重低估了整理的工作量，样稿汇总出来后，原来的 200 多页变为近 400 页，好在整个期间，苏江、金炜、黄黎、苏耀勇和杨卫祥给予了密切配合，让我能在 2 月的最天一天如期交工。

这里要特别感谢郑成文对本书第五篇的细致审阅,感谢零月浅浅在制作封面的过程中忍受我可怜的审美观点，感谢林旷野牺牲大量时间维护微信群、修改 DOC 格式。

四天前，我收到了硅谷 Live 举办的《智能合约开发课三期》的助教邀请，书稿完成之后，我要按计划继续学习智能合约开发了，万一“神龙币”开发成功了，就送知识星球里每个支持过我的朋友各 1 万枚“神龙币”吧。

申龙斌

2018 年 2 月 28 日 山东东营