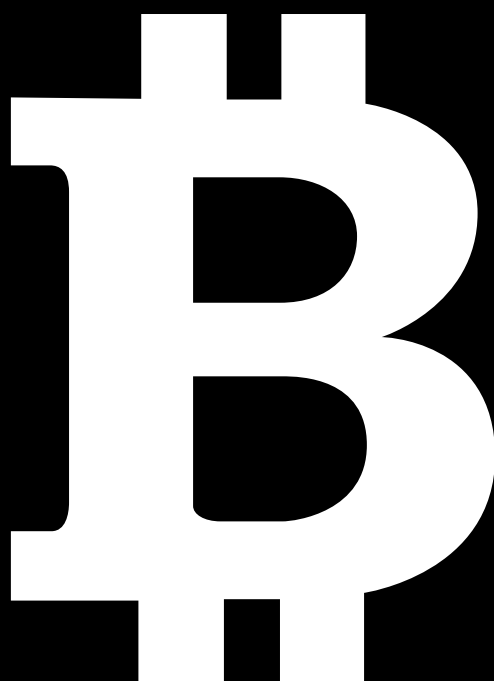


比特币囤



HODL  
BITCOIN

@AHR999

《囤比特币》会分享我在过去几年囤比特币过程中的思考和经验。写它的目的不是宣传比特币，而是帮助那些已经准备囤比特币的人。如果不看好比特币，最好取关我。是否看好比特币很大程度上与价值观有关，我无意改变任何人的价值观。

序章：

## P6 《知之非难，行之不易》

为什么我要写这个系列。

入门：

## P12 《比特币与理想主义》

我们在参与一场社会实验，它存在失败的可能性，但是我们无怨无悔。

## P19 《下车太早只因愿景太小》

这场实验的目标很大，如果一切顺利，比特币的价格可能会在 20 年后涨到 1.6 亿人民币。

## P25 《囤比特币：你离财富自由还有多远？》

我们没有其他能耐，只能靠囤积比特币，并耐心地等待属于自己的财富自由。

## P32 《囤比特币：冲动、孤独、无聊与矛盾》

虽然会经历冲动、孤独、无聊和矛盾等心理考验，但是我们已经做好准备囤币。

## P39 《囤比特币：手握私钥的快感》

虽然掌握私钥有点麻烦，但是我们仍然准备自己对自己负责。

## P46 《囤比特币：如何管理私钥？》

管理私钥其实并没有想象的那么麻烦，但我们需要把握好几个原则。

进阶：

## P55 《囤比特币：基本价格模型》

囤币是比特币一切价值来源，长期囤币者关心的去中心化和安全性是比特币首先要保证的特性。每次产量减半，囤币需求不变，但比特币供应减少，价格必涨。

## P62 《囤比特币：寻找合适的够买时机》

我们都希望使用有限的投入获得更多比特币，那么何时是合适的买点呢？

## P70 《囤比特币：唯有比特币》

除了比特币，我不持有任何其它数字币。但是，我也不反对任何人持有任何币，哪怕是传销币。

## P77 《囤比特币：不要跟着感觉走》

囤比特币其实是反复决策的结果，别人觉得简单是因为只看到结果，而看不到决策的过程。

## P85 《囤比特币：币本位思维》

比特币创造了一个全新的世界。在这个世界里，只有一个标准——比特币。

## P93 《囤比特币：心中无币》

当理解上升到一定程度，我们不再需要关注任何比特币相关的信息。

贡献：

## P101 《囤比特币：打造强节点》

成就最好的自己就是对比特币最大的贡献！

## P106 《囤比特币：运行全节点》

私钥决定比特币所有权，全节点捍卫比特币规则。

终章：

## P111 《不忘初心》

序章：

知之非难，行之不易

为什么我要写这个系列。

2018 年的国庆节，阳光明媚，秋高气爽。我最喜欢北京的秋天，原本这是个应该进行户外活动的好日子，我早早的起床。却临时决定宅在家中，写点东西。

最近一段时间，我把全部业余时间都用来写《囤比特币》系列了。

写作自然希望有人读。很庆幸，《囤比特币》系列确实有读者。咱们真的跟四年前不一样了，那时我写的文章最多三五条评论。

当然，也不能因为有人愿意读，我就去写，10 万 + 的垃圾文章比比皆是，我并不希望再为这个世界多创造垃圾。我必须要有实实在在的干货可以分享。很庆幸，我确实有。谈起囤比特币这个话题，我就思如泉涌。

原本已经不写关于比特币的文章很久了。机缘巧合写了一篇回忆的文章《四年一个轮回，不光有世界杯，还有比特币》，居然获得了 25 万的阅读量（我感觉微博数据有水分）。我没有做过任何推广，这个阅读量大大出乎了我的预料。表面上看，现在和四年前都是熊市，但是形势或许真的与四年前不一样了，至少关注度是不可同日而语的。

最近，我花了点时间重新关注比特币圈子里的动态，感觉也与当年有了巨大差异。

就从币圈媒体说起吧，虽然各类公众号一大堆，但是发的全是些没营养的内容。很多文章，随便瞟一眼就知道作者是个小白，啥也不懂，瞎扯淡。其它的要么搞行情分析，明天币价除了涨就是跌，要不就横盘；要么就推销币，错过了比特币，不能再错过 ABCDEFG，全是一

个套路。

读这些东西，难道不会让人变傻么？那些比特币早期玩家都去哪里了？就没有人能够给大家写点干货么？

环顾四周，大家不是忙着发币，就是忙着推销币。有良知的，会告诉你，仍然看好比特币。没良知的，基本提都不提比特币，全部推销各种垃圾。

任何一个流量入口，无论是媒体，交易所，还是所谓的钱包，全都在发币。

作者们已经不能踏踏实实的写作了，一看就是个卖软文的；媒体已经不能踏踏实实的做资讯了，一看就是个卖站台费的；交易所已经不能踏踏实实提供交易了，一看就是个卖上市费的。

能圈到钱当然也是本事。但是，我很奇怪的是，难道就没有人还记得当初的情怀吗？

好吧，我错了，情怀确实不能当饭吃。

在中文比特币圈里，我们不仅仅是缺少程序员，缺少自愿维护比特币的核心开发者，而且我们缺少布道者，缺少像 Andreas M. Antonopoulos 这样的灵魂人物。

当然啦，我自己也要检讨。虽然比特币带给我巨大的经济回报，但是我却没有为它做过太多有意义的事情。

我总想等待别人出头。



因为我知道我不可能成为 Andreas M. Antonopoulos 那样的人。我的所有收入都不是来源于圈内，我还需要赚更多钱，囤更多币。比特币不是我的主业，我还有其它梦想要实现，而实现那个梦想不仅需要大量的钱，而且需要了解很多领域的技术储备。

但是，如果我不站出来试试的话，还有另外一个人会站出来吗？虽然我知道比我更适合做这事的人大有人在，但是，我又完全看不到有人要站出来的迹象。

同时，我过去一直很怀疑，我站出来就有意义吗？从大的方向看，很多事情的结局是注定的。我知道很多人会倾家荡产，这种事过去四年一直发生，多少人含泪流血离场。我写还是不写，并不可能影响事情的发展。是的，我其实有些麻木。

但是同时，我也很乐观，因为来一轮熊市，等牛鬼蛇神全部死翘翘，必然又迎来新的春天。我写还是不写，比特币都会自顾自的发展，高速的发展。

你看，结局是注定的，我理应什么都不做，耐心等待。

但是，有时候我会很难过。全局的发展从来不关心个体的死活，伴随着成千上万人倾家荡产，比特币仍旧高速发展，这很残酷。

如果我写的东西能够挽救那么 3-5 个人呢？虽然对全局而言没有任何意义，但是或许可以挽救某个个体的一生。

好吧，哪怕挽救 1 个人也是好的，这是我决定写《囤比特币》的初衷。

我写得内容，要么是我一直坚信的，要么是我亲身经历的。是我希望分享的经验和思考，也是我对比特币倾注的全部感情。

刚开始我以为我只需要写几篇，后来我发现能写的内容越来越多。已经完成的有 6 篇，它们构成第一个部分：入门，目的是帮助大家入门。

《比特币与理想主义》我们在参与一场社会实验，它存在失败的可能性，但是我们无怨无悔。

《下车太早只因愿景太小》这场实验的目标很大，如果一切顺利，比特币的价格可能会在 20 年后涨到 1.6 亿人民币。

《囤比特币：你离财富自由还有多远？》我们没有其他能耐，只能靠囤积比特币，并耐心地等待属于自己的财富自由。

《囤比特币：冲动、孤独、无聊与矛盾》虽然会经历冲动、孤独、无聊和矛盾等心理考验，但是我们已经做好准备囤币。

《囤比特币：手握私钥的快感》虽然掌握私钥有点麻烦，但是我们仍然准备自己对自己负责。

《囤比特币：如何管理私钥？》管理私钥其实并没有想象的那么麻烦，但我们需要把握好几个原则。

囤比特币，入门的标准是：明确比特币的目标，愿意参与实验，自愿承

担风险，并开始利用比特币储值，自己掌握比特币私钥，并进行冷储存。

后面的内容，我大概列了个清单，发现还可以写 10 篇左右。考虑到写作过程中还能产生新的思路，而且不断的有人问我问题，内容只会更多。

囤比特币绝对不是一件轻松的事。知之非难，行之不易。所以，我才会有这么多的内容可以写。

我的目标是写出永不过时的经典。所以，我尽量写与时事无关的事情，越是热点事件，我就越不会写。我希望，多年以后，当你再次拿出我的文章时，仍然觉得它不过时，而且愿意把它分享给那时的新人。

写作也不是一件轻松的事。知之非难，行之不易。我希望自己能把这个作品完成。

祝大家国庆节愉快！

2018 年 10 月 1 日

于北京

入门:

# 比特币与理想主义

我们在参与一场社会实验，它存在失败的可能性，但是我们无怨无悔

比特币是人类历史上第一次，用技术手段实现了私有财产神圣不可侵犯。----- 李笑来

在真正读懂比特币白皮书的瞬间，我的感觉是无法用文字来形容的。充满了惊叹、兴奋与懊悔。惊叹于中本聪巧夺天工的设计，兴奋于比特币即将引发的社会巨变，懊悔于自己竟然没有在第一个人第一次听到这个词的时候就来读白皮书。

我是个理想主义者，我的初衷其实只是想参与这场史无前例的社会实验。但也不可否认，比特币价格的暴涨是当初驱使我阅读白皮书的主要动力。

没想到的是，参与这场社会实验也改变了我的认知，我的人性和人性也遭受到了巨大的考验。

人性是脆弱的，往往经不起考验。有那么一段时间，我一度对自己产生了怀疑，因为我本身陷入了巨大的矛盾之中。

我近乎疯狂的囤积着比特币，这到底是因为理想呢，还是因为贪婪呢？我已经分不清了。一方面，我仍然坚持着理想，或许实验最终会失败，但我无怨无悔；另一方面，我如此坚信它会成功，于是囤得越多，财富自由就会越快，我完全控制不住自己囤币的冲动。

最终，我不得不给自己订下一条死规则——不卖币。不卖币就意味着，我赚不到法币，也就意味着我的投入跟这个实验共存亡。

但是，我依然无法控制自己囤币的冲动。我只能这样安慰自己，其实我

是中本聪，比特币就是我的孩子，我需要不断投入，以帮助它成长。

在投资和金融领域，理想主义者是无法存活的。比如：李笑来老师的经典录音中有一段经典的话：

我操，你妈的整天讲价值投资，那他妈的，我就这么跟你讲个例子就知道了，我他妈天天骂中医，中医就是傻逼，但是中医上市公司股票，我真买了，为什么道理很简单，我知道傻逼信，傻逼众多，然后我知道我不买，别人会买，这钱我为什么不赚？在商言商。到最后没有什么世界比金融的世界更成王败寇的。

话糙理不糙，理想主义者怎么可能在投资和金融领域成功呢？

你看，我不看好中医，我绝对不会买中医股票；我憎恨某幼儿园虐童事件，我绝对不会去抄底它的股票；我厌恶分叉币空气币，哪怕明知赚钱概率很大，我也绝对不会去炒。

我有时候也纳闷，我怎么就这么傻，怎么就这么倔呢？我也不知道。

还好我有比特币。不得不佩服比特币，它居然就是这么优待理想主义者。前段时间，李老师的基金兑现了，但 5 年收益率只有 40 多倍，收益尚不如我这个傻傻囤币的理想主义者高。想想都觉得好讽刺。

这说明，哪怕你牛逼如李老师，粉丝无数，挖过“烤猫 7BTC 以下随便买”大坑，和 BM 大神一起割完 BTS 割 EOS，给无数币站台，折腾得

死去活来，号称自己很忙，七年就是一辈子，每天都兴奋地干活，为了利益与合作者撕逼。最终，收益还是没跑过比特币。

但是，如果你以为理想主义者就一定能很滋润，那你又错了。

事实是，很多理想主义者并没有撑到现在。他们待了一段时间之后，完全看不到圈子里其他人有任何理想，放眼望去全是贪婪，满眼绿光，伤心失望至极，选择退出。非常的可惜。

能坚持到现在的，或许都是因为能分得清失望的对象，到底是失望币圈的人呢？还是失望比特币本身呢？

很多人会把币圈的人做的坏事都算在比特币头上，比如：宋欢平和VV酱。这当然是不对的，我们不能把杀人犯做的坏事都算到枪头上，也不能据此认为枪不是技术革新。

比特币是人性的放大器，你想得到的骗局，你想不到的骗局，都会在这里发生，而且层出不穷。更可气的是，骗子骗完一次，还可以骗第二次，比如：朱荣。有时候想想也很无奈。

但不管怎么样，最初的理想我还在坚持。而且持有比特币时间越久，我就越乐观，我对比特币能够成功深信不疑。我希望大家也能坚持下去。

圈子越是混乱，越说明比特币系统的抗冲击能力很强。有人不遗余力的黑比特币打压比特币；有人不遗余力的骗人，割韭菜把圈子搞得乌烟瘴气；有人不遗余力的想要控制比特币，却恶人自有恶人磨。但是，比特币只管自顾自的发展，高速的发展，加速的发展，完全不受影响。

会有越来越多的人加入我们，趋势是无法阻挡的。

如果你也跟我一样，是个理想主义者，那么我也有几条经验可以分享。

### **首先，不要过于兴奋。**

不要逢人便夸比特币，不要谈任何话题都扯到比特币上，没必要把自己整成一个神经病，也没必要搞得跟个传销分子一样。而且，越是开头热的人，持久力越差，这样的先例真的很多。

有时间静下心来学习一些经济学和密码学课程，网络课其实很方便，深刻理解比特币是需要时间的。既需要理论指导，也需要自己的实践，但不管怎样，都比民科科普和炒币攻略要靠谱得多。

实话说，我的兴奋劲不会弱于任何一个人，而且我很持久，多年过去，我仍然很兴奋。也许在字里行间，你也能体会到我的兴奋。但是，除了写文章，我平时是不谈比特币的。

### **其次，不要问底在哪里。**

想像一下，若干年后，你已经从新人变成了老人，有新人私信你，请问大神，底在哪里？你该如何回答？

对于一个上不封顶的东西，没有必要总是纠结于底在哪里。你们来得虽



晚，但并不用懊恼，来得晚是运气不好。

只有运气好没抓住的人，才该懊恼。知道吗？很多人在这里待了好几年，但手上仍然没币。从 8000 元到 900 元，他们在纠结底在哪里。从 900 元到 130000 元，他们还在纠结底在哪里。从 130000 元到 40000 元，他们仍然在纠结底在哪里。你应该庆幸，他们一直在纠结。

5000 元的币我买过，1000 元的币我买过，130000 元的币我也买过，40000 元的币我仍然在买。我只关心终点的美景。

如果实在想低成本持币，猜底还不如定投。从 8000 元定投到 900 元，平均成本大概是 2000 元，虽然是最低点的两倍，但是只有最高点的四分之一，应该可以接受罢。

### **第三，不忘初心，保持耐心。**

不要明知分叉币、空气币没前途，却去跟着炒一把；不要坑蒙拐骗，即使那样能赚钱；不要没完没了的撕逼，我们不需要打嘴仗，时间终能证明比特币的伟大。

一路走来，我感觉到很多人都变味了。近朱者赤，近墨者黑。在大染缸里呆久了，想独善其身很难。局外人看得很清楚的坏事，局内人总会编织各种理由来麻痹自己。

时常回想一下，自己当初为什么要来。努力在理想和贪婪之间找到一个平衡点，理性的逐利。

路遥知马力，日久见人心。我期待 4 年以后，8 年以后，12 年以后，N 年以后，我还能在这里见到你们。那时，你们经受住了人性的考验，实现了财富自由。我们是从未谋面的老朋友，或许不能一起喝酒，不能一起撸串，但是我们心意相通，隔着网络也能感觉亲切，只因为我们都是中本聪。

入门:

下车太早  
只因愿景太小

这场实验的目标很大，如果一切顺利，比特币的价格可能会在 20 年后涨到 1.6 亿人民币。

比特币十年，有的人来了又走了，有的人走了又来了，有的人来了就不走了，有的人走了就不来了。

绝大多数比特币早期玩家都已经下车，还有很多人眼睁睁看着比特币暴涨就是没上车。这对我们来说是好消息，因为如果他们现在都在车上，币价还能是几万块吗？

犹犹豫豫不上车，迫不及待要下车，原因或许是多方面的，但最主要的，还是因为心中的愿景不够大。

**愿景决定了视野，视野决定了行动。**

比特币价格 10 元时，他们说，太贵了。

比特币价格 100 元时，他们说，太贵了。

比特币价格 1000 元时，他们说，太贵了。

比特币价格 10000 元时，他们说，太贵了。

**比特币似乎永远都太贵，他们永远不舍得买。**

比特币价格 10 元时，我们说，它还早。

比特币价格 100 元时，我们说，它还早。

比特币价格 1000 元时，我们说，它还早。

比特币价格 10000 元时，我们说，它还早。

**比特币似乎永远都还早，我们永远不舍得卖。**

心中没有愿景，或许还能扛过熊市，但绝对守不住牛市。一涨你就会卖的，千万不要不信，48 万哥就是活生生的例子。

要做到无论牛熊，我自岿然不动，最需要想明白的问题是，它的未来到底有多大？

再涨个百倍？你太悲观，百倍太少，让我来分享我的愿景。

**比特币最核心的应用是储值，它的未来目标就是成为人们的储值首选。**

那么，在比特币出现之前，我们都用什么东西储值呢？也就是说，我们赚了一笔钱，除去消费余下的部分，我们会以什么形式来保存财富呢？它们主要是黄金、货币和不动产。

下车太早只因愿景太小

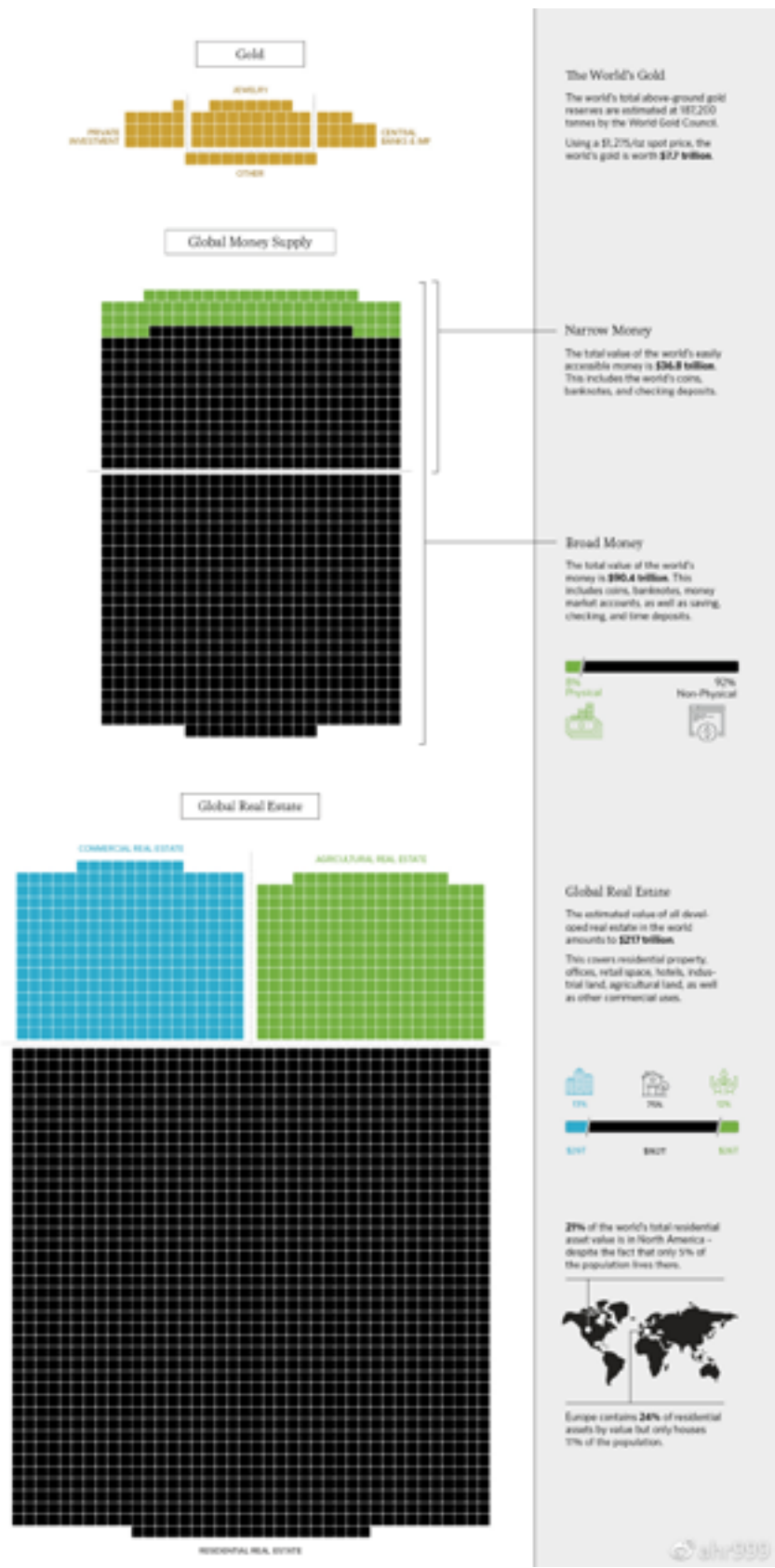


图 1. 世界黄金、货币和不动产总量（修改自 <http://money.visualcapitalist.com/>）

全球黄金的总市值是 7.7 万亿美元，广义货币总量是 90.4 万亿美元，不动产是 217 万亿美元。

黄金现在的主要用途就是储值，而论储值，比特币各方面都强于黄金，市值超越黄金只是时间问题。

广义的货币包含：现金、定活期存款、证券公司客户保证金，等。除了现金（占比 8%）用于流通，其余部分都是用于储值。

不动产主要用途应该还是居住和使用，但是肯定也有相当大的比例是用于储值的。如果不是因为比特币，我应该也会把我的大部分资金用于买房子。由于没有比例可以查，我们暂时假设 20% 比例的不动产是用于储值的（这个比例不影响最终结果的数量级）。

**那么，全球总储值市场有多大呢？  $7.7 + 90.4 \times 92\% + 217 \times 20\% = 134$  万亿。**

**而比特币总量只有 2100 万，大约有 300 万永久丢失。考虑到比特币储值相对于黄金、货币和不动产的绝对优势，每个比特币将涨到 750 万美元，折合 5000 万人民币。**

这就完了？当然没有。

**世界财富总量在以每年 6% 的速度增长，10 年以后总量是现在的 1.8 倍，20 年以后总量是现在的 3.2 倍。因此，假设 20 年后比特币的储值功能得到广泛认可，那时它的价格应该是 1.6 亿元人民币。**

以上计算，仅仅考虑了比特币的储值功能，如果考虑其它因素，比特币的总市值会更高。

换句话说，比特币依然有千倍的增长空间。每 4 年，当产量减半，供应突然减少之后，都会迎来新一轮暴涨。

有时候，我经过城市中最繁华的地段，穿梭于人流，看着人来人往。我就会想，这些人都是做什么工作的？他们的家庭怎么样？他们整天忙忙碌碌追求的是什麼？他们中有多少知道比特币？又有多少能理解比特币的未来？

虽然比特币最高涨到过 10 万人民币，但是很显然，人群中的 99% 仍然不理解比特币，仍然没有持有比特币。这当然是好消息，这同样意味着，比特币的上涨空间仍然巨大。

目前，Bitcoin Core 客户端的版本号是 v0.16.2，虽然比特币网络稳定运行了近十年，客户端却仍然没有升级到 v1.0 正式版。

**我们其实只是一群测试版用户，真正的用户还没有来呢。**

如果把比特币比做一个孩子，那么这个孩子现在还没有出生，还只是个腹中胎儿。虽然，从一个受精卵成长为胎儿，已经长了千万倍，但未来从胎儿到婴儿到儿童到成年，仍有无穷的成长空间。



入门:

囤比特币：  
你离财富自由还有多远？

我们没有其他能耐，只能靠囤积比特币，并耐心地等待属于自己的财富自由

哪怕明知囤比特币可以实现财富自由，你可能还是囤不住，因为你不想等，你还想走捷径。

读这篇文章之前，你应该首先认同我前面两篇文章的观点：

《比特币与理想主义》，我们在参与一场社会实验，它存在失败的可能性，但是我们无怨无悔。

《下车太早只因愿景太小》，这场实验的目标很大，如果一切顺利，比特币的价格可能会在 20 年后涨到 1.6 亿人民币。

如果你不认同上述观点，你就没有必要往下读了。

很多人读了《下车太早只因愿景太小》，留言说，我的预测太大胆。这篇文章会告诉你，我的预测有多么保守。

**如果 20 年后比特币可以涨到 1.6 亿元，那么它每年需要涨多少呢？**

我们都知道，比特币的供应每 4 年就会减半，每 4 年供求关系的平衡就会被打破，供应变得紧缺，而需求仍然持续增加，因此币价会迎来一次暴涨。过去的两次减半，都导致了暴涨。

如果 5 个周期后，也就是 20 年后，比特币可以涨到 1.6 亿元，每个周期需要涨几倍呢？

我做了两种计算：

一种我称之为“线性增长”（其实数学上并非线性），认为每个周期增长的倍数一样；

一种我称之为“指数递减”，认为刚开始增长倍数高，后面增长倍数低。

结果如下：

年份	2018年	2022年	2026年	2030年	2034年	2038年
倍数 (线性增长)		5.25	5.25	5.25	5.25	5.25
比特币价格 (万元)	4	21	110	579	3039	15954
财富自由需要比特币	4000	762	145	28	5	1
倍数 (指数递减)		11.8	7.20	4.85	3.54	2.75
比特币价格 (万元)	4	47	340	1650	5838	16043
财富自由需要比特币	4000	339	47	10	3	1

表 1. 两种增长模型的比特币价格预测

**如果是线性增长，每个周期仅仅需要涨到 5.25 倍。**

4 年后，比特币价格 21 万元；8 年后，比特币价格 110 万元；12 年后，比特币价格 579 万元；16 年后，比特币价格 3039 万元；20 年后，比特币价格 1.6 亿元。

**每个周期 5.5 倍，意味着，每年比特币只需要相对于上一年增长 50%。**

请问，现在还有人认为我的愿景很大么？我真的很保守耶！

为什么 20 年涨到 1.6 亿元，人们会认为激进；而每年增长率 50%，

人们会认为保守呢？

**因为，人们往往会低估复利的威力。**

当然，线性增长模型并不合理，事物的发展总是开始快，后来慢，最终趋于平稳。

如果是指数递减增长，每个周期的倍数依次是：11.8 倍，7.2 倍，4.85 倍，3.54 倍和 2.75 倍。这个模型预测，下一个周期（到 2022 年）比特币会涨 12 倍左右。考虑到上一个周期涨了几十倍，这个增长速度基本也是合理的。

**囤币：我们需要多长时间可以实现财富自由？**

一线城市财富自由的门槛是 2.9 亿（请自行百度）。在这里，我们放宽一点要求，把门槛降低到 1.6 亿元，也就是 20 年后 1 个比特币的价值。

根据指数递减增长模型：

如果你想 4 年后实现财富自由，你需要拥有 339 个比特币；

如果你想 8 年后实现财富自由，你需要拥有 47 个比特币；

如果你想 12 年后实现财富自由，你需要拥有 10 个比特币；

如果你想 16 年后实现财富自由，你需要拥有 3 个比特币；

如果你想 20 年后实现财富自由，你需要拥有 1 个比特币；

**很多人会告诉你，拥有 1 个比特币，未来你就可以财富自由。我认为我百分比认同。**

但我的问题是，你是否愿意等 20 年？或者你到底愿意等几年？或者你现在能买得起几个币？

现实是，以今天的币价，绝大多数人拿出 10%-30% 的资产，只能拥有 10 个或更少的比特币。因此，想要通过囤币实现财富自由，需要至少 12 年。你是否已经做好了长期囤币的打算？

**所以，哪怕你明知囤币可以实现财富自由，你也囤不住的，只因为你等不了这么久。**

矛盾之处恰恰也在这里。你买 1 个币，需要等 20 年才能财富自由，你觉得太久，不愿意等，很懊恼。但是，如果你不买，4 年之后，你可能连懊恼的机会都没有了，因为那个时候，你连 1 个币都买不起了。

**我们是否有捷径可以走？**

首先，你可能需要反省一下，是不是自己的要求太高了？绝大多数人，这辈子都没有实现财富自由的可能性，能够实现财富自由的是极少数。囤 1 个比特币，等上 20 年，除此之外啥都不需要干，已经是捷径中的捷径了。

其次，疯狂提升圈外赚钱能力，多赚法币多囤币，可以缩短实现财富自由的时间。但是，要缩短 1 个周期，币量大约要翻 3-4 倍，对每个人来说都是很艰难的。我选择的的就是这条路径，至少很稳。

再次，快速实现财富自由的途径永远存在，也可以不局限于币圈，但总体上概率极低。万众创新，那么多企业，又有几家能成为拼多多呢？

我也在践行这条路径，但是我不抱什么希望。

人往往就是这样，其实已经走在捷径上了，还在拼命的到处找捷径。

### **在币圈各种折腾，行不行？**

当然也行。很多币圈老人都在折腾，但是除去少数人，绝大部分人的结果并不算理想。

你需要明确一点，在币圈想赚币往往更难，甚至不如从圈外赚钱来买币。原因很简单，比特币总量有限，固定 2100 万。

圈内每个人都想赚币，而且入圈人数越来越多。10 万人玩的时候，平均每人 210 个币；等到 100 万人玩的时候，平均每人只有 21 个币。这就是为什么，玩着玩着，大家手上的币都越来越少了。反而是那个在圈外赚钱来买币的人，啥都不干，币却越来越多，成了收益最高的人。

很多人玩亏了币，不甘心，就需要做一些事情找补回来。这很容易理解的，原来几千币，玩了一段时间变成几百个，是你甘心吗？于是，你开始想办法赚回来，可是想赚回来又谈何容易呢？于是你不得不去想一些损招。

圈内有几类人是赚币的，大家其实也都知道是哪几类，所以，下面是我的个人建议：

如果想玩山寨币空气币，你应该去发币，而不是给别人发的币接盘，帮别人实现财富自由。很多币圈老人都在发币，虽然我很反感，但是

我不反对，因为人人都有骗傻逼的自由，而道德只能用来约束自己。如果想玩杠杆期货，你应该去开交易所，在自己的交易所割韭菜，而不是去别人的交易所，被别人割了还是小事，关键还要被别人骂傻逼，就很憋屈了，更有甚者，输得要死要活的，就更不值了。

如果想玩挖矿，你应该去造矿机，或者建矿池，或者有电厂，而不是买矿机或者云挖矿，行情好的时候赚一点点辛苦钱，行情不好的时候自己承担了全部风险。

总而言之，在圈里混，你需要想方设法把别人的币弄到自己兜里来，争取早日实现财富自由。如果你没这些能耐，那你或许应该像我这样，耐心地等待。

**最后，衷心祝愿我的每一位读者都能最终实现财富自由。**

入门:

囤比特币：  
冲动、孤独、无聊与  
矛盾

虽然会经历冲动、孤独、无聊和矛盾等心理考验，但是我们已经做好准备囤币。



*What doesn't kill you makes you stronger.*

如果你认同前面三篇文章的观点：

《比特币与理想主义》我们在参与一场社会实验，它存在失败的可能性，但是我们无怨无悔。

《下车太早只因愿景太小》这场实验的目标很大，如果一切顺利，比特币的价格可能会在 20 年后涨到 1.6 亿人民币。

《囤比特币：你离财富自由还有多远？》我们没有其他能耐，只能靠囤积比特币，并耐心地等待属于自己的财富自由。

那么你或许已经下定决心囤比特币了。从过往的经验看，绝大多数人没能成功。外部因素当然很重要，比如，出了一点意外，你需要急用钱。但是，决定性因素还是心态。

你可能以为最需要克服的是恐惧，其实不是，因为你早就对币价暴涨暴跌有了准备。

## 冲动

比特币价格的巨大波动，山寨币动则十倍百倍的涨幅，常常会让我们产生进去炒一把的冲动。这是一种非常非常不理性的冲动，但是我们常常难以抵抗。

**人们天生对赌博就缺乏抵抗力，明知是个零和或者负和游戏，却常常忍不住要去 ALL IN，多少人因此而倾家荡产。**

炒山寨币就像是买彩票，中奖了十倍百倍千倍都有可能，但是概率极低。少数币确实收益很高，但是大多数最终都会归零。而且认真你就输了，你认为的“价值币”就是不涨，反倒是那些垃圾币涨得稀里哗啦的，他们管这个叫“市值管理”。

杠杆炒币就像是赌大小，赢了十倍百倍，输了倾家荡产。我不否认这里面可能有些技术含量，但是这明显是个零和或者负和游戏，你赢的必然是别人亏的币。

囤比特币则是个正和游戏，所有人都会随着比特币的发展壮大而获利。过去十年里，比特币从未辜负任何一个相信它的人。

但是，我也很清楚地知道，说这些道理都没用，赌博这玩意历史悠久，多少血的教训，却依然火爆异常。人们骨子里的赌性是与生俱来的，我们常常难以与之对抗。

**我的策略是，交易所不放钱也不放币，把私钥藏得深一点。每当行情到来，冲动的时候，我没法立刻操作私钥；而当可以操作私钥的时候，行情已经过去，理性又占据了上风。**

## **孤独**

相信比特币的人都是孤独的。

你爱上了一个姑娘，她美丽温柔且善良，但她穿着前卫，特立独行，于是其他人就认为她品行不端，你的家人反对你们在一起。你该怎么办？

你相信自己的眼光，坚信自己是对的，别人是错的。但是，你同时又发现，讲道理根本没人认真听，你站在了所有人的对立面。时不时还有好心人来劝你，让你回头是岸，号称是为你好。你该怎么办？

我从未跟周围的人提过比特币，这是一段地下感情，是一段煎熬。更煎熬的是，在长达三年的时间里，周围的人也没有跟我提过比特币。

我是个双面人。一方面，我在网上很活跃，学习很多比特币相关技术，写很多的文章；另一方面，我在一个完全没有比特币的圈子里生活，也很活跃。

我时常会想象中本聪的生活状态。一方面，他在网上是神一般的存在；另一方面，在他的生活圈子中，恐怕没有一个人知道他就是中本聪吧。

我甚至能感受到你们的痛苦，即使非常认可我的文章，也不能点赞，更不能转发，因为你们不想让朋友圈知道你们囤币的秘密。

很多人感到孤独的时候，就会去参加币圈各种聚会。但是，相信我，那并没有什么卵用。你会发现，圈内跟圈外一样，真正的信仰者寥寥无几。

到了2017年，居然出现了那么两次，别人在我面前主动提比特币。但是，那时的我已经习惯了孤独，甚至开始享受孤独。

一次是公事会议。结束后闲聊，话题不知道怎么谈到了外汇管制问题，C 老板年龄 50 左右，中年油腻男，一家连锁酒店的董事长，提到了比特币。另外有几个人似乎也感兴趣，就开始问问题。我装作一脸茫然的样子。C 老板兴致勃勃的告诉大家，这玩意可以买一点，正在涨，估计还会涨。

另一次是私人饭局，老 G 管理一个私募基金，正在介绍他最近关注的机器学习和量化交易。他提到说，他有很多同行在进行数字货币的交易。

他们讲的时候，我就认真的听着。我发现他们的理解都非常的肤浅，有些甚至是错误的，但是我也不能打断他们。他们或许永远想不到，我才是对这事理解最深的人。

不过那种感觉超好，因为傻子也能判断，牛市真的来了，赶紧回家再买两个币，呵呵。

对于孤独，我的建议是，疯狂写东西。有的事情你想跟别人说，别人又不认可，你憋着又难受，你就把它全部写下来。等到你适应孤独的时候，你会发现，不仅你的思维更成熟了，而且你的文笔更好了。

## 无聊

囤比特币这个行为本身是极其无聊的。

你喜欢一个姑娘，你却要把她晾在一边，什么也不干。这 TM 是反人性的！

你热爱比特币，你觉得自己一定要做点什么。这种心情我很理解。但是，请相信我，囤币行为本身已经对比特币网络做出了巨大的贡献。

只有你相信比特币的去中心化，你相信比特币的安全性，你相信比特币的前途无限，你才有可能长期囤币，你才有可能把自己辛辛苦苦赚来的财富，保存在比特币那一串“虚幻的”私钥字符串上。

你的这种行为，你对待比特币的态度，已经远超你对待爱人的态度。请问有多少人愿意把自己辛辛苦苦赚来的财富，无怨无悔的交给自己的爱人？

所以，你真的不需要再做什么了。如果实在感觉无聊，就去健身去养生，别等到财富自由的时候，你身体也挂了。给你嫩模，你也只能看看，那还有什么意义呢？

## 矛盾

这是一种很复杂的心情，你既希望比特币涨，又希望比特币跌。

我曾经希望自己不要看行情，于是把所有比特币行情相关的 APP 都删了。但是，发现自己根本做不到，因为手机或电脑浏览器打开网站也能看行情。

对于囤比特币而言，币价涨是没用的。长期囤币，又不准备卖，涨多高都是“浮盈”。但是，涨意味着自己的坚持是正确的，总是另人高兴的。

反过来，币价跌虽然心情上会有些郁闷，但是有机会抄底补仓，币量将成倍增长。

人会变得有些分裂。这是正常现象，你去看看某些币圈老人。他们一会儿跑出来唱多，一会儿跑出来唱空，被粉丝喷得不要不要的。

我个人的判断是，他们绝大部分币都是囤住不动的，既没有在做多，也没有在做空。之所以变来变去，是因为他们自己也搞不清楚，到底想要涨，还是想要跌，矛盾得很。

这种矛盾的心情我也不知道该如何解决，因为我至今也还是矛盾的。不过似乎问题也不大，因为并没有影响我囤币。

我们会经历心理上的考验：冲动、孤独、无聊和矛盾。但是，那些没有打倒我们的，终将帮助我们成长，就像那些没有打倒比特币的，终将让比特币变得更强大。

**几年过去了，我跟随比特币一起成长，如果你一直读我的文章，你或许能感受到思维方式、写作风格和文笔上变化，甚至连我的性格都变得越来越温和呢。**

入门:

囤比特币：  
手握私钥的快感

虽然掌握私钥有点麻烦，但是我们仍然准备自己对自己负责。

把财富储存在一串“虚幻的”私钥字符串上，是人类储值方式的重大革命。

如果你认同前面四篇文章的观点：

《比特币与理想主义》我们在参与一场社会实验，它存在失败的可能性，但是我们无怨无悔。

《下车太早只因愿景太小》这场实验的目标很大，如果一切顺利，比特币的价格可能会在 20 年后涨到 1.6 亿人民币。

《囤比特币：你离财富自由还有多远？》我们没有其他能耐，只能靠囤积比特币，并耐心地等待属于自己的财富自由。

《囤比特币：冲动、孤独、无聊与矛盾》虽然会经历冲动、孤独、无聊和矛盾等心理考验，但是我们已经做好了准备囤币。

**那么接下来，你会遇到一个问题：你到底应该把比特币储存在哪里？**

如果我们囤积黄金，我们可能有两种方式。一种是在银行租个保险柜，把黄金存进去；另一种是在家里买个保险柜，把黄金存进去。答案可能需要视情况而定。

**但是，对于囤比特币而言，答案永远只有一个——囤在自己手里。**



**什么叫囤在自己手里？有且仅有你掌握了能够动用这些比特币的私钥。**

需要特别说明的是：

此处特指囤币，而且是长期囤币。如果你只是想炒币，那么你可以把币存交易所，毕竟对交易者来说，时间就是金钱。

市面上有很多所谓的“钱包”，并不是严格意义上的钱包，因为你并不掌握私钥。它们容易跟真正的钱包混淆，因为界面可以做到完全一样，甚至易用性还要更好一些。我不推荐你使用这类“钱包”囤币。【注：不是说这类“钱包”不能用，它们有它们的用途，比如放少量币供平时消费时使用。】

还有一些“钱包”会付给你利息，你需要时刻想想 p2p 理财的风险。感兴趣也可以百度“比特币存钱罐”。

**如果你不愿意自己掌握比特币私钥，或许是两个原因，一怕风险，二怕麻烦。**

所谓风险是与技能相关的，对于掌握了私钥管理方法的人而言，其实没什么风险，反而是不掌握私钥更具风险。曾经有个哥们存了 900 个币在 Mt.Gox，当然那会儿币也不值钱，后来币价涨到了 1000 美元，这哥们才发现 Mt.Gox 发生了挤兑，提不出币。原本是个美好的故事，结局却很悲惨，Mt.Gox 宣布倒闭，这哥们自杀了。

所谓麻烦是与意义相关的，对于有意义的事情而言，我们从来不会感到麻烦。关于私钥管理有多麻烦，我们以后再谈。本文想表达的是，无论

掌握私钥多麻烦，都值得拥有。你之所以怕麻烦，仅仅是因为还没有意识到这件事情有多重要罢了。

李笑来曾经说过：

比特币是人类历史上第一次，用技术手段实现了私有财产神圣不可侵犯。

我非常赞同这句话，但它并不太好理解，尤其是对于那些从来没有接触过比特币私钥的人而言。我个人的理解如下：

比特币第一次使得我们可以把财富储存在一串“虚幻的”私钥字符串上，这是革命性的，它意味着人类社会最大的需求之一，每个人都有的储存财富的需求，其方式发生了重大革新。

如果你用现金储存财富，当拥有巨额财富时，你的现金可能会放满 1 间屋子。实际上，你并不拥有这些财富，因为你拿不走。你的现金会慢慢发霉，或某天被人开卡车拖走，并且烧坏几十台验钞机。

如果你用银行存款储值，提取转账都很方便，但你的账户存在被银行冻结的风险。

即使你现金不多，能随身携带，存款也不被冻结，你依然存在被增发货币稀释财富的风险。20 年前的 1 万元存单，放到今天还剩下多少购买力？

如果你用黄金储值，你同样无法拿走，于是你可能会跟某证券大佬一样，偷运 44 公斤黄金出海关被查。

如果你用不动产储值，那就不仅仅是无法带走的问题了，还有被强拆强征的风险。

如果你用股票储值，你也很危险，弄不好会意外死亡，股份被捐给慈善机构。

**只有比特币，完美的解决了上述问题。**

无论是把私钥藏在书里，还是记在脑子里，你都可以携带财富，全球畅通无阻。而且，这些财富是正在属于你的，只要你不说，就没人能抢走，甚至都没人知道你拥有这些财富。

俗话说，钱财乃身外之物。这话其实只适用于 2009 年之前。比特币诞生之后，钱财不再是身外之物。虽然生，还是不能带来，但是死，你却可以带走。

如果你不想把比特币遗传给子孙后代，你只需要毁掉私钥，其结果等同于捐了，因为全世界持币者都是受益者。

因此，如果说这世界上还有一样东西是真正属于你的，那它就是比特

币。当然，这里有一个前提条件，那就是你自己掌握了私钥。

如果你不掌握私钥，你就无法享受这革命性的储值方式。

如果你不掌握私钥，你就无法真正理解这场社会实验的意义。

如果你不掌握私钥，你就没有真正的拥有过比特币，更不要说什么长期囤币。

如果你不掌握私钥，你就体会不到那种“你再也不能把我怎么着”的快感。

当然，自由是要付出代价的，掌握私钥也有代价，那就是一切后果自负。听起来很吓人，其实也没你想象的那么严重，我就从来没有丢过币。

假如你生活不能自理，那么放手让你自己照顾自己，风险确实很大。但是当你学会自己照顾自己时，放手就没什么风险了。

现在问题来了，你是想永远生活不能自理，一直依赖别人，还是想尽快学会自己照顾自己，以便放飞自己，享受真正的自由呢？

几年前，我第一次制作冷钱包的场景，仍然历历在目。作为一个小白，我当时使用了最笨的办法，在一台废旧笔记本电脑上重装了系统，下载 Core 钱包（那时候叫 QT），断网之后安装钱包，生成新地址，备份钱包到 2 个格式化过的 U 盘，然后发币到钱包地址。从此，我拥有了冷钱包，我掌握了私钥，而且还有两个备份。我对当时既兴奋又怀疑，还有一点不安的心情，记忆犹新。

直到很久之后，我才终于弄明白哈希函数、不对称加密和椭圆曲线，那种对安全性的怀疑和不安逐渐被打消。而随着时间的推移，1 年，2

年，3年，它一直很安全，我对它的信心越来越强，对私钥管理越来越有心得。

掌握私钥，你会渐渐对比特币产生全新的认识。你会不由自主地关注比特币的去中心化和安全性，因为对于你而言，这些才最重要。去中心化保证比特币不被增发，不被冻结，安全性保证比特币不被破解。而所有其它那些花里胡哨的属性全是次要的。你也终将明白，币王就是币王，其它那些花里胡哨的币，绝大部分是垃圾，是一些踏空比特币的人创造的垃圾。

你会打开一个全新的世界，你真正拥有了自己的财富。你甚至会开始怀着怜悯的心情看待旧世界的人们，他们忙忙碌碌，却仍没有意识到，并没有什么东西是真正属于他们自己的。

他们依然对比特币的价值持怀疑态度，或许是因为他们从来没有体验过手握私钥的那种快感罢。

入门:

## 囤比特币： 如何管理私钥？

管理私钥其实并没有想象的那么麻烦，但我们需要把握好几个原则。

通过囤比特币实现财富自由，私钥管理是唯一需要掌握的技能。

通过前面几篇文章：

《比特币与理想主义》我们在参与一场社会实验，它存在失败的可能性，但是我们无怨无悔。

《下车太早只因愿景太小》这场实验的目标很大，如果一切顺利，比特币的价格可能会在 20 年后涨到 1.6 亿人民币。

《囤比特币：你离财富自由还有多远？》我们没有其他能耐，只能靠囤积比特币，并耐心地等待属于自己的财富自由。

《囤比特币：冲动、孤独、无聊与矛盾》虽然会经历冲动、孤独、无聊和矛盾等心理考验，但是我们已经做好准备囤币。

《囤比特币：手握私钥的快感》掌握私钥有点麻烦，但是我们仍然准备自己对自己负责。

我们终于下定决心要自己掌握比特币私钥了，于是我们立刻就会面临下一个问题：如何管理私钥？

这个问题很重要，不过我原本是不准备回答的，因为如果你不能通过自己搜索找到问题的答案，那么你不配拥有比特币。但是，因为问的人很多，最终我还是决定分享一些心得。

本文不会介绍详细的教程，也不会推荐任何钱包。这是因为比特币发展很快，各类钱包软件更新迭代也很快，教程也很快就会过时。如果你一

定要教程，网上也是有的，虽然我也不知道它们是否过时了，你姑且可以尝试一下。

《比特币冷钱包到底应该怎么做？》

《“比太钱包”用户体验报告》

本文的重点是，分享私钥管理的一些原则，无论软件如何更新迭代，这些原则是永不过时。

### **根据安全性需求分级管理私钥**

每个人对安全性的需求是不一样的，而同一个人在不同应用场景对安全性的需求也是不一样的。因此，不可能有一种通用的私钥管理方法适用于所有人或所有应用场景。

另外，安全性与易用性通常是一对矛盾，任何私钥管理方案其实都是在安全性和易用性之间进行平衡和取舍。

于是我们就需要分级管理私钥。对于普通比特币用户而言，通常分两级就够用了：高安全等级和低安全等级。

比如，你现在拥有 10 个比特币，其中 9 个准备长期持有，几年都不会动，另外 1 个需要经常拿出来使用。现在，你有三种方案可以选择：

把 10 个比特币全部放在 1 个冷储存（安全）；

把 10 个比特币全部放在 1 个热储存（易用）；

把 9 个比特币放在冷储存（安全），把 1 个比特币放在热储存（易用）。



第三种方案，就是分级管理，既保证安全又兼顾易用。第一种方案使用起来很不方便，第二种方案将那 9 个长期持有的币置于不必要的高风险之中。

由于我们是囤币用户，大部分币都要囤到 10-20 年之后，因此接下来，我只介绍在进行高安全等级私钥管理时的原则。

### **管理私钥而不是管理钱包文件**

长期囤币，必须直接管理私钥。很多人虽然已经开始使用比特币，但是仍然不知道私钥为何物。关于私钥是什么，私钥和地址的关系是什么，请参考：

《精通比特币 - 第 4 章 密钥、地址、钱包》

《比特币的私钥，公钥和地址是什么？》

在《囤比特币：手握私钥的快感》中，我简单讲述了我第一次制作冷钱包的方法，那时我还是小白，所以我在管理钱包文件。这个方案至今仍是安全的，但是我现在已经不用了。

为什么我们要直接管理私钥呢？因为软件迭代速度非常快，升级频繁，消亡也快。

4 年前，我们很多人用的是一款叫作 multibit 的钱包 (<https://www.multibit.org/>)，现在这款钱包已经停止更新了。如果你当年存的是 multibit 的钱包文件，现在你就打不开这个文件了。就算你当时也备份了软件，仍然存在风险，因为软件长时间没人维护，漏洞也没人修复。

没有人能预测 10 年后的景象，也没有人能知道我们今天使用的钱包能否活到 10 年后。也没有人知道这 10 年间，比特币还会发生多少次分叉。

所谓得私钥者得天下，这天下也包括分叉币的天下。你在高点卖掉你不看好的分叉币，既可以获利，又可以让该分叉的操纵者痛不欲生。

所以，请直接管理私钥，而不是钱包文件。事实上，你甚至都不需要一个钱包，你需要的只是一个能随机生成地址和私钥的工具。这个话题要稍微高级一点，大家有空可以自学，其实也不麻烦。

### 冷私钥管理的基本方案

制作冷私钥的步骤如下：准备设备（废旧手机或废旧笔记本电脑），下载软件（钱包等能离线生成地址和私钥的工具），断网（甚至可以把网卡毁掉），离线生成地址和私钥，加密并备份私钥（直接存文本并加密）。

完成冷私钥制作之后，你只需要向该私钥对应的地址转账比特币，并使用其它联网设备在区块链浏览器中查询该地址的交易记录和余额即可。

至于选择哪个钱包工具，可以参考 (<https://bitcoin.org/en/choose-your-wallet>)，它对每个钱包都有一个简单的介绍：



图 1. Bitcoin Core 钱包简介

最重要的是第一条，一定要选择“Control over your money”的钱包，凡是第一条不是这个的钱包都不要用。

### **实战之前一定要测试**

由于冷储存的币一般数额都比较大，一旦出错，损失也非常高。所以，无论你选择了什么方案，你都需要先使用少量的币，进行测试。测试也是加深理解的过程，通过反复测试你还可以不断地改进方案。直到你非常确定，方案安全可靠，就可以正式使用了。

### **需要几个备份？**

备份少了很危险，因为私钥一旦丢失，比特币就全部损失了。备份多了也很危险，因为备份越多，私钥越容易暴露。经过我个人的长期摸索，3个备份应该最合适。这3个备份在形式要有差异，储存地点也要分散。

电子备份和纸质备份各有优劣。电子产品长时间放置，可能会出现故障而打不开。纸质版虽然不会出现故障，但可能墨迹会消失或者模糊。建议：2个电子版+1个纸质版。

如果3个备份放置在同一个地点，一旦发生火灾，或者遭遇盗贼，很可能一锅端了。建议：3个备份分别存在3个安全的地点。这一点很难，既要足够分散，又要足够安全。

### **私钥是否需要加密？**

私钥加密有风险，因为一旦忘记密码就全部损失了。私钥不加密也有风险，因为一旦被盗就立刻损失了。建议：使用自己最常用、记得最清楚的密码加密。

你不必担心这密码不够强不够安全。加密的目的是防贼，密码并不需要特别复杂，能拖延足够时间即可。比如：某天你发现家里被盗了，由于盗贼破解密码需要时间，这样就为你争取了时间，去用其它备份把币转移了。加密工具有很多选择，即使使用压缩软件自带的加密也够用。

### **需要管理多少私钥？**

随意。你既可以把币都存在 1 个地址，这样管理 1 个私钥就够了；也可以把币分散到 N 个地址，管理 N 个私钥。管理难度本质上没有差别，多 1 个私钥也就多 1 串字符。

把币分散到 N 个地址有优点。比如，你有 9 个比特币，分散到 9 个地址。某天你需要使用  $<1$  个币时，你可以直接把某 1 个私钥导入热钱包使用，而完全不影响其它 8 个私钥的安全性。对于囤比特币而言，大量卖币的可能性不存在，所以推荐把比特币分散到多个地址中。

### **防范自己出意外**

什么叫囤在自己手里？有且仅有你掌握了能够动用这些比特币的私钥。这意味着一旦你发生意外，你的比特币也跟着全部损失了。这就是比特币的特性，真正属于你个人的财富，不能与他人分享。

但是，你仍然可以选择把私钥备份交给一个你百分之百信任的人。你需要特别叮嘱他，只有你出意外，他才能动私钥。

为什么呢？因为私钥管理是有难度的，共用私钥最终极有可能导致信任关系破裂。比如，某天你发现比特币被盗了，可能是你的疏忽，但你并不知道，你就会开始怀疑对方。当然，也有可能是对方背叛了你，但不承认。总而言之，这事就说不清了。

所以，对方在保管你的私钥时，需要非常明确的知道，他所承担的风险和责任。反之亦然，如果你获得别人的信任，帮他保管他的私钥，你也需要非常明确的知道，你所承担的风险和责任。

而且，一旦你决定要把私钥备份交给他人，你不仅仅需要绝对信任对方，也需要做好心理准备，万一被背叛了，你也无怨无悔。否则，你就不要把私钥交给任何人。但这并不代表，你不能把比特币分享给他人，你可以把比特币转给他人，让他自己保管自己的私钥。

### **还是觉得太麻烦？**

那你就用硬件钱包吧，要买就买2个，加上1个种子卡，正好3个备份，有电子版有纸质版。

硬件钱包最大的风险是硬件被人做手脚，尤其是在运货阶段。曾经就有人购买二手硬件钱包，结果被人做了手脚，导致丢币。因此，请原厂下单，收货的时候仔细检查包装和封条是否完好，收到之后，先少存点币玩上个半年，币量逐步增加。

你仍然需要明白，硬件钱包还是没有直接管理冷私钥安全。但是，对于一个啥都不想学的人来说，已经是最好的方案了。

### **后记**

刚开始，我是拒绝写这篇文章的。因为我始终认为，如果连这都需要我教，可能也不适合比特币吧。看起来，财富自由的吸引力还是不够大嘛。

但是，问这类问题的人又很多。我也曾经小白过，也很希望得到前辈们的指点，这样就不用走弯路了。我能理解大家的心情，于是就硬着头皮写了。或许还是没有大家想象的那么详尽，真的很抱歉。

我已经很长时间没有使用过钱包软件了，所以我也不知道该如何推荐。除了电脑上还保留 1 个热钱包，用的是几年前版本的 Electrum，存了点币以备不时之需，其它所有钱包全部卸载了。

**事实上，囤比特币也不需要任何钱包软件，你们终究会明白的。**

进阶：

## 囤比特币： 基本价格模型

囤币是比特币一切价值得来源，长期囤币者关心的去中心化和安全性是比特币首先要保证的特性。每次产量减半，囤币需求不变，但比特币供应减少，价格必涨。

比特币的价格到底由什么决定？为什么产量减半会导致比特币价格暴涨？

现在，我们已经达到了囤比特币的入门标准：明确了比特币的目标，愿意参与实验，自愿承担风险，并开始利用比特币储值，自己掌握比特币私钥，并进行冷储存。

那么，接下来，我们什么都不用做了，等着就行了。

但是，傻傻的等确实太闲了，所以我们继续学点东西，本文分享我个人理解的比特币价格模型。需要指出的是，我并非经济学科班出身，所以你可以认为我是民科，欢迎批评指正。

首先，我们看看比特币过去的价格走势（图 1）。

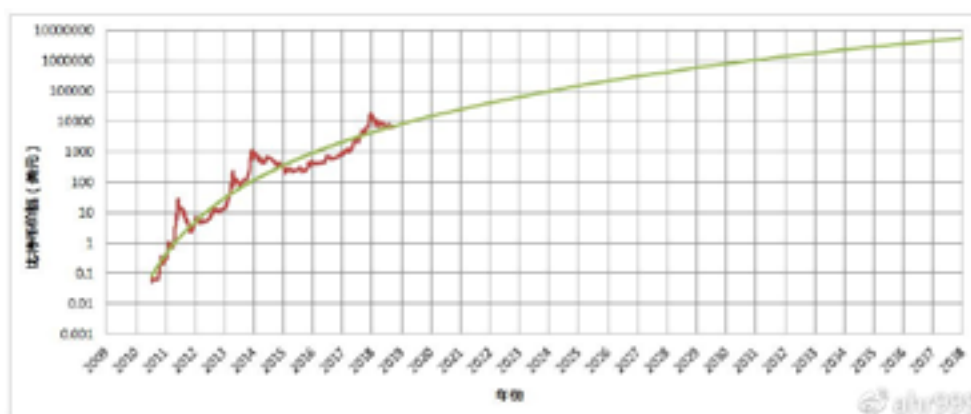


图 1. 比特币历史价格拟合和未来价格预测（数据源：bitcoinity）

这个走势完全可以用指数级上涨来拟合，并且根据拟合结果，预测 20 年后的比特币价格应该在 700 万美元，即 5000 万人民币左右。与我们在《下车太早只因愿景太小》中预测的基本一致。



考虑到比特币储值相对于黄金、货币和不动产的绝对优势，每个比特币将涨到 750 万美元，折合 5000 万人民币。

那么到底比特币价格的根源在哪里？答案是：你。

我们可以简单把比特币市场分为 3 类参与者：囤币、矿工、炒币（图 2）。

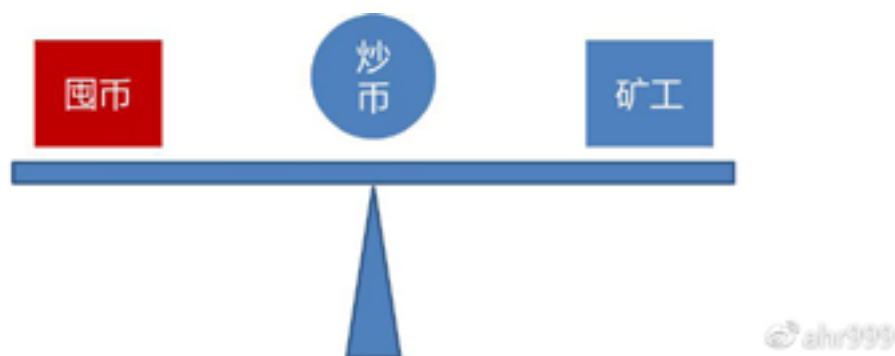


图 2. 比特币市场参与者示意图

囤币是买方，矿工是卖方。最初也只有这两类人，由于这两类人有交易需求，才产生了交易所和第三类人：炒币。炒币摇摆不定，行情向上就去滑到囤币一边，行情向下就滑到矿工一边。

当然，某一个人可能同时是囤币、矿工和炒币。但是，为了简化模型，我们可以把他拆分成 3 个人来考虑。

囤币是比特币一切价值得来源。有人囤，才会有人挖；有人挖，才有了交易；有了交易，才有了炒作，才有了资讯、商家等等。如果没有人囤币，市场马上就会崩盘，也就不会有现在的比特币了。

比特币持续不断流入囤币者手中。这是必然趋势，因为囤币是只买不卖的。在总量被限制的情况下，流通比特币只会越来越少，只有 9% 的币，其币龄小于 1 个月，只有 2% 的币，其币龄小于 1 天，（图 3）。

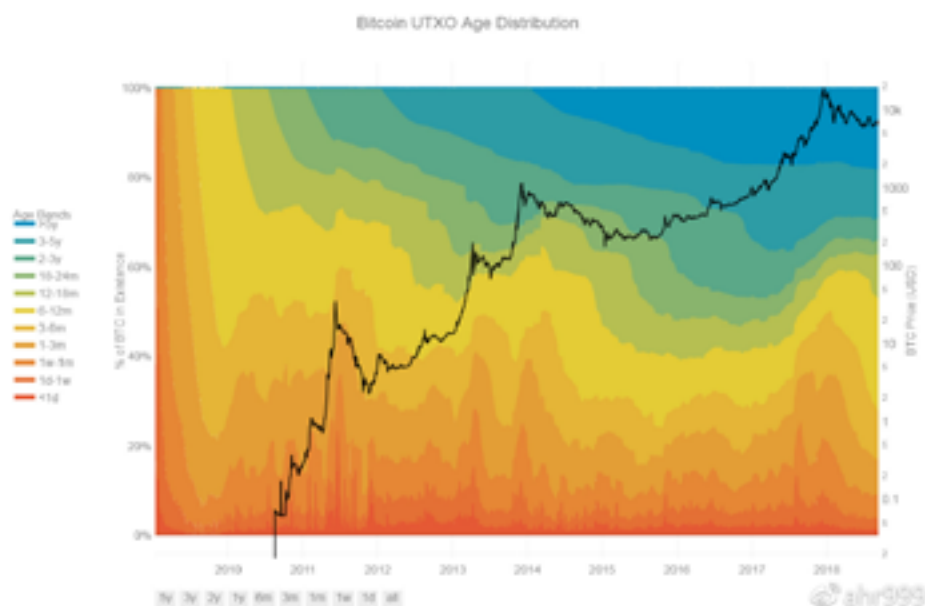


图 2. 比特币市场参与者示意图

那么，为什么会有人囤币呢？由于现在的你已经是个合格的囤币者了，你肯定有自己的答案。

我的答案是，我们的储值需求是与生俱来的。我们努力赚钱总会有一些消费不完的钱，这些钱总是需要存起来以备不时之需。我们越是富有，这个需求就越大。而比特币的去中心化和安全特性，使得它成为了我储值的第一选择。

世界上最大的囤币者是谁？是中本聪。据不完全统计，中本聪囤积了超

过百万比特币，从来没有动过。

理解了比特币的一切价值来源是囤币，我们就应该自豪，因为我们自己就是比特币一切价值的来源，我们赋予了比特币价值，我们都是中本聪。

而且，一旦开始囤币，很多长期困扰你的疑问就有了答案。

比如：既然囤币是比特币一切价值的来源，那么作为一个长期囤币者，你最关心的问题是什么？

你一定最关心去中心化和安全性，去中心化保证比特币不被增发，不被冻结，安全性保证比特币不被破解。而主链交易是否够快，是否便宜，你其实是不太在乎的，毕竟你一年也转不了几次帐。这就是莱特币、狗狗币、XXX 币、等等，永远无法超越比特币的根本原因。

对于这个问题，如果你不亲自囤币，你是理解不了的。随便被人忽悠一下，你就跑偏了。不要看了中本聪的白皮书，就开始抠字眼。你不应该看中本聪怎么说，而应该看中本聪怎么做。

我们也很容易理解，为什么每次产量减半，比特币价格必涨。

一般情况下，如果没有人炒来炒去，比特币的价格应该是囤币和矿工之间的平衡。例如：现在每天产出 1800 个比特币，那么每天囤币者需要 1000 万美元的投入，才能维持比特币 6000 美元的价格。1000 万美元实际上非常少，如果全球 100 万囤币者，每人每天只需要投入 10 美元。

假设比特币价格原本处于平衡状态，现在开始产量减半，每天产出 900

个比特币，请问价格会如何变化？价格由供求关系决定，囤币者的投入又不会变，傻子都知道会涨。

上面我们只是考虑了每天的产量，你可能会问，难道存量比特币就不会被抛售吗？

图 3 显示，90% 以上的币超过 1 个月没有动过，75% 以上的币超过半年没动过，其实大家都在囤，根本就没有什么存量币会被抛售。

接下来，我们再分析下一个问题，为什么每次产量减半比特币都不止涨一倍，而是涨很多倍？

这就要从比特币的奇葩供求关系说起了。

首先，比特币的供给是完全固定的。任何一个实体商品，都是价格越高，供给越大。这很好理解，商品价格涨，利润空间变大，促使更多的人投入生产，于是就有了更多的产出，增大的供给会遏制商品的暴涨。黄金就是这样，价格涨导致供应增加。经济学上有个名词描述它，叫作供给的价格弹性，指的是由价格变化引起的商品供给的变化。比特币的供给的价格弹性是零，无论价格怎么涨，供给始终不变，这非常变态。

其次，比特币的需求更变态。任何一个实体商品，都是价格越高，需求越小。这也很好理解，商品价格升高会逼迫人们寻找替代商品。举个例子，你每天都吃肉，如果肉价涨了，你可能就会改变习惯，减少吃肉，隔天吃一次鱼，所以，你总体上对肉的需求就降低了。这个叫需求的价格弹性，比特币的需求的价格弹性居然是负的，也就是说币价越高，需求越旺盛。因为盘子越大，越适合储值。

再加上每一次产量减半，人们都预期比特币会暴涨，于是炒币大军疯狂涌入，推波助澜。

总而言之，每一次减半都打破了供需平衡，而一旦平衡打破，供给不变，需求反而增加，再加上炒币大军涌入，怎么可能不暴涨？

那么反过来也是一样的。如果泡沫形成，比特币价格太高，矿工的抛压超过了囤币的投入，币价就会下跌。一旦价格下跌趋势形成，需求就会开始减少，因为盘子越小，越不适合储值。从而造成，比特币价格的进一步下跌。

囤比特币是只买不卖的，我们总是希望能用有限的资金购买更多的币。那么比特币的基本价格模型，能否帮助我们寻找合适的比特币购买时机呢？请看下回分解。

进阶：

囤比特币：  
寻找合适的够买时机

我们都希望使用有限的投入获得更多比特币，那么何时是合适的买点呢？

我们都希望使用有限的投入获得更多比特币，那么何时是合适的买点呢？

很多比特币脑残粉会告诉你，在任何时候都可以买入比特币。这话既是正确的，也是不正确的。

正确是因为，放在一个大的时间尺度，任何时间购买比特币，都能获得巨额回报。比如上一轮牛市的顶点是 8000 元人民币，或许真的套住了一批人，但是只要拿到了今天，仍然是 N 倍收益。

不正确是因为，每一个囤币者的资金量都是有限的。这意味着，如果你控制得好，可以多获得好几倍的币，例如：你通过定投把平均成本降到 2000 元人民币，那么你的币量会是高点买入的 4 倍。那么，根据我们前面的计算，你可以提前 1 个周期（4 年）实现财富自由，这显然也很重要。

我希望所有囤币者都能够以最低成本持币。为什么呢？囤币者是市场上的硬手，都是只买不卖的。我当然希望更多的币集中在硬手们的手中，而不希望那些炒来炒去的人拿到太多币，因为他们拿到了也没意义，迟早要吐出来的。

那么，问题来了，我们如何判断购买时机呢？

李笑来在《比特币世界简明生存指南》提出：

长期来看，我认为可以把矿工成本看做基本面。

但是，他从来没有解释过原因，因此很多人并不认同他的观点。

我认为这句话是有道理的。上一轮熊市最低点的币价是 900 元，当时吴忌寒接受采访的时候透露，生产一个币的边际成本是 800 元。这其实间接支持了李笑来的观点。

我们先看看比特币的难度增长（图 1），虽然比特币价格起伏很大，但是难度基本没有出现过回调，而是单向上涨。



图 1. 比特币的挖矿难度增长（数据来源：btc.com）



这说明，比特币的价格从来没有跌落到当时主流矿机的电费成本之下，否则就会有大规模关机现象出现，算力就会下降，从而造成挖矿难度下降。因此，电费成本是比特币价格的硬支撑，这一观点，至少在历史上，都是有效的。

但是，这种现象在经济学上是不合理的，因为价格是需求决定的，与成本无关。在理论与事实矛盾的时候，我们需要修正理论，下面我个人的解释。

比特币的特别之处在于，任何一个人，包括你和我，在准备持有比特币的时候，都会考虑它的生产成本。因为每个人获得比特币都有两种途径：买币和挖矿。如果你可以通过挖矿以 5000 美元的成本获得比特币，你就不会用 6000 美元去买。

在这一点上，比特币与其它商品有本质区别。如果你要购买苹果手机，或葡萄酒，你主要关注的是商品的品质，而不是成本。但是，如果你要购买比特币，你主要关心的则是成本。

成本又是因人而异的。每个人的成本不一样，如果我去挖矿，成本可能是 10000 美元，所以，对于我而言，当然是直接买划算。

但是，总会有人掌握矿机或电力资源，越大的资金，越有动力与资源结合，实现低成本。而一旦比特币价格接近最低成本线，原本准备投入矿业的资金就不会再投入了，而会选择买币。于是，就解释了为什么比特币的价格从来没有跌落到主流矿机的电费成本之下。

根据这个现象，我们可以做出这样的判断：比特币价格的下限是当前

主流矿机的电费成本。

但是，即使知道这个，也仍然没有太多可操作性。如果这一轮熊市没有跌到成本线，怎么办？毕竟像上一轮那样跌到 900 元，是可遇而不可求的机会。

因此，我们必须在币价相对较低的位置先购买一些比特币，再留一些钱，或者去赚更多的钱，等待可遇而不可求的机会。

什么叫相对较低的位置呢？我们再来看看比特币的历史价格（图 2）。

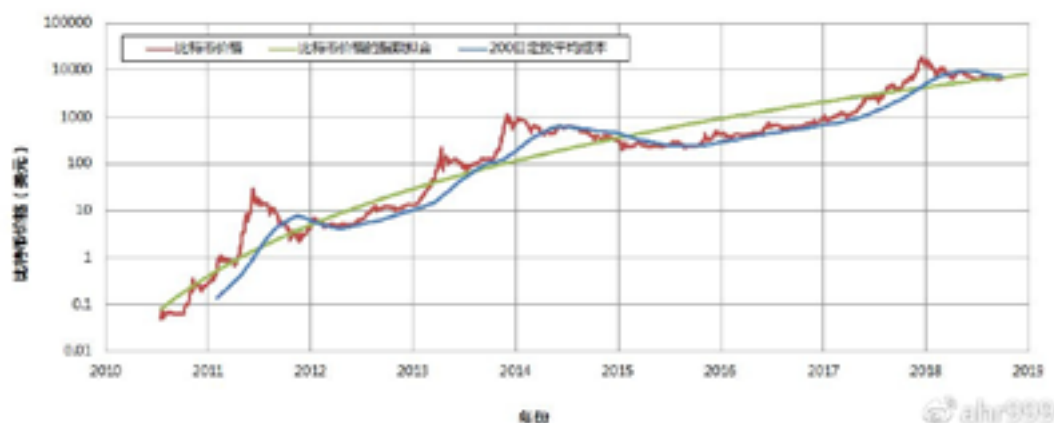


图 2. 比特币历史价格和 200 日定投平均成本

红色的线是比特币的价格，它符合指数增长模型，绿色的线是比特币价格的指数增长拟合线。理论上，只要你在币价（红色线）处于拟合线（绿色线）的下方购买比特币，都是划算的。

蓝色的线是 200 日定投成本，注意它与 200 日均价是有区别的。200 日均价是算数平均值，200 日定投成本是几何平均值。关于二者的区别请自行百度，几何平均值总是小于算数平均值的。

想象有这样一个入，他从 200 天以前开始定投比特币，每天固定投入 1 元。一直定投到今天，他的平均成本就是蓝色的线。

很多人推崇定投比特币，是非常有道理的。因为定投成本（蓝色线）在绝大部分时间里，都在币价（红色线）下方运行。也就是说，如果你坚持定投，你能跑赢绝大多数一次性买币的人。

那么，具体在什么区间内购买比特币最划算呢？同时满足两个条件：

比特币价格低于 200 日定投平均成本，意味着在这个时候买币，可以跑赢定投的人。

比特币价格低于指数增长模型的估值，意味着在这个时候，币价被低估了。

图 2 是指数坐标，看不清楚。我们现在定义两个比值，比特币价格 / 200 日定投成本，比特币价格 / 指数增长估值。在这两个比值同时小于 1 时候，就是比特币价格被低估，并且直接购买比特币比长期定投更划算的时候。

我们看看这两个比值的历史走势（图 3）。

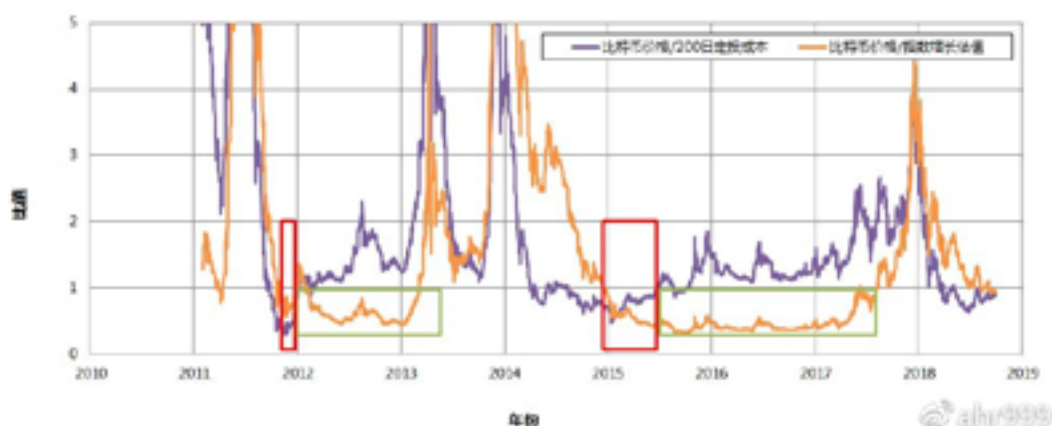


图 3. 比特币价格 /200 日定投成本和比特币价格 / 指数增长估值

历史上出现过两次，两个比值同时小于 1。一次出现在 2011 年底，时间持续 2 个月；另一次是 2015 年上半年。在图 3 中以红色方框表示。

在这两个时间段之后，都有很长的时间（超过 1 年），比特币价格 /200 日定投成本  $> 1$ ，但比特币价格 / 指数增长估值  $< 1$ ，这意味着币价仍然被低估，但直接买币稍逊于定投，但二者差别并不大。在图 3 中以绿色方框表示。

无论是红色方框，还是紧接着的绿色方框都是非常好的购买比特币时机。时间窗口其实很长，没有必要急于一时，深怕自己错过了什么。

那么，我们现在处于什么位置呢？今天，这两个比值都刚刚跨进小于 1 的区间，换句话说，我们可能正在迎来史上第三次最佳囤比特币的时机。

考虑到还有一年半比特币就要产量减半了，第三次最佳囤币时机的时

间窗口可能有一年左右。最终能囤积多少比特币，差不多就取决于我们过去的积蓄和未来一年时间内的场外赚钱能力了。

对比上一轮熊市，在这个区间内，仍然发生过比特币价格的腰斩。但无论如何，在这个区间内进行定投，成本不会比抄到最低点高多少了。

总结一下，长期来看，我们可以把矿工成本看做基本面。在大多数时间，定投都是极佳的策略。比特币价格同时低于 200 日定投成本和指数增长估值的时候，就是比特币价格被低估，并且直接购买比特币比长期定投更划算的时候。现在刚刚进入两个比值小于 1 的区间，我们可能正在迎来史上第三次最佳囤比特币的时机，时间窗口大约一年。

李笑来在《韭菜的自我修养》中说过：

梭哈是交易参与者的大忌，任何时候都要保留一定比例的现金。

我完全同意，也不推荐任何人梭哈比特币。如果你真的打算囤比特币，不建议资金量超过三成。关于这个问题，我们后面还会反复涉及到。从各种角度看，梭哈都是不值得的。

进阶：

囤比特币：  
唯有比特币

除了比特币，我不持有任何其它数字币。但是，我也不反对任何人持有任何币，哪怕是传销币。

8.20

看破一切，唯有比特币。

除了比特币，我不持有任何其它数字币。但我也不会黑任何币，因为从来没有哪个币可以通过黑别的币获得成功。

我相信，比特币只需要做好自己，根本不需要关心其它。但我也不认为所有其它币都没价值，相反很多都是有存在价值的，只是比特币更有价值而已。

比特币的分叉币，我全都卖掉了。有一些人宣扬所谓的 1:1 持仓，其实是没有自信，或者没有价值观的表现。分叉币的价值观与比特币在根本上存在冲突，一个对比特币有信心且知行合一的人，是不可能同时持有的。

但是，我也不反对任何人持有任何币，哪怕是传销币。

比特币是命最硬的

对于一个长期囤币的人来说，其实只关心一个问题：我国的币在 10-20 年以后能否存活？

其实，答案已经非常明显了，比特币存活的概率最大，因为比特币是最去中心化、网络最健壮、系统最安全、功能最简洁的。这不是说比特币就一定能活到 10-20 年之后，而是说如果连比特币都活不到 10-20 年之后，其它币更加没有机会。

有些人会推销 XX 币，把买 XX 币比喻成给比特币买个保险，这是完全错误的。如果比特币失败，XX 币只会死的更快。XX 币要存活，必须先祈祷比特币能存活。

换句话说，之所以今天大家还有机会发各种 XX 币，是因为各国还没有找到干掉比特币的办法。如果干不掉老大，就不值得干掉小罗罗，这就是小罗罗们还活着的原因。而一旦各国找到了攻击比特币的办法，你觉得你发的币还能活下去吗？私发货币一定是死罪。

既然是长期囤币，你就一定要选择命最硬的那个。

比特币是愿景最大的

市场上的数字币按照功能可以分为两大类，一类是以比特币为代表的货币类；一类是以以太坊为代表的應用类。事实上，货币也是应用，而且是最大的应用，没有之一。

这两类的愿景存在本质性区别，货币类的愿景远超应用类。

前面的文章，我已经多次讨论过，比特币的目标是成为人类储值的首选。而储值本身就是世界上最大的应用，是人人都有且与生俱来的需求，我们赚了钱就必然需要用某种方式存起来，储值是绝对的刚需。关于储值的总规模，我们也分析过，目前全球市值 134 万亿美元。

区块链应用的规模最终能做到多大呢？大部分区块链应用类的币，性质比较像股票。通俗的说，就是创始人要做一件事，需要融资，希望大家投钱。且不论这些项目是否值得投，就算做到比苹果和亚马逊还牛，也不过就是 1 万亿的规模。



所以，在愿景上，储值市场就比区块链应用要大至少 100 倍。

### 比特币会赢家通吃

接下来，我们来分析两类数字币的发展趋势。

在货币领域，比特币必然赢家通吃。对于货币而言，只存活一种货币是总体成本最低的，也是最高效的。货币是度量衡的一种，种类越多越混乱，因此，秦始皇统一六国之后，要统一度量衡。

如果我要求比特币付款，而你只接受莱特币，那么我们交易时就需要通过交易所兑换。这实际上，降低了效率。因此，货币的未来一定是赢家通吃的。

由于比特币在去中心化和安全性上，遥遥领先，吸引了大量优秀的开发者和坚定的储值用户。其它货币类数字币已经丧失了逆袭的可能。

但是，比特币要想完全挤掉其它币也不可能，因为很多币是有存在价值的。

一方面，它们可以为比特币开道。例如：比特币隔离见证之所以能够激活，就多亏了莱特币率先激活，证明隔离见证是安全的，击破了某些别有用心的人的长期谎言。

另一方面，它们也可以用于功能测试。一些高风险的功能，可以先在其它币上测试。但是，如果侧链出现，这种测试任务就会转移到侧链上。

所以，我预测未来会存活 3-5 种货币类数字币，但是，其它币的总和可能也只有比特币的零头。于是，持有比特币就足够了，因为你很难判断到底是哪几个其它币能存活。莱特币的位置也一样是危险的。

### 应用类会百花齐放

应用类就不一样了，它们大概率会出现百花齐放的局面。今天你提出一个 2.0，明天他整一个 3.0，后天肯定有人整 4.0 的，你放心。

最初提出做 2.0 应用是 BTS，请问现在它在哪里？做应用，要求又快又大，还要好玩，这种需求对技术的要求是无止境的。

为了便于大家理解，我打个可能不恰当的比方。苹果需要不断地更新换代，才能维持自己的领先地位，但黄金只需要维持稳定，就还是那个黄金。

货币的功能实际上是越少越好。我们可以想象一下，如果我们在纸币上还附加一个签合同的功能，还开辟一片空白区域供你留言和画画，或者还带着一款游戏供你消遣，你会觉得这是创新吗？显然不是。你一定会认为它华而不实，画蛇添足。人们终究还是会选择那个“干净”的货币，而比特币就是这么的干净。

既然如此，我们是不是就不能玩其它币呢？

当然不是。难道大家就只能投资黄金，不能投资某个公司的股票啦？某潜力原始股被你抓到了，也可以实现百倍千倍的收益。

我为什么不投任何其它币？

我被比特币的愿景深深吸引，它会赢家通吃，而且命最硬。那些乱七八糟的币在愿景上都无法打动我，而我又不会去做违心的事。我不会明明不喜欢中医，还去买中医股票，仅仅就为了赚钱。

而且，我也没有必要去投其它币。当只持有比特币就能实现财富自由的时候，也没有必要花时间去折腾其它币。投资最大的成本实际上是时间和精力投入。更何况大多数人玩来玩去，比特币却越玩越少了，连李笑来都不例外，真是费时费力还亏币，何必呢？

再次，大家可以想想，如果你选中的股票大涨，你会怎么办？很多人会选择套现，换成货币。那么币圈的基础货币是什么呢？毫无疑问是比特币。

所以，我根本不需要去炒乱七八糟的币，就可以坐享其成。因为无论别人炒亏了还是炒赚了，他们投入的真金白银，最终都会流到比特币上的。你赚钱越多，你的储值需求就越大。你亏钱越多，赚你钱的那个人的储值需求就越大。无论如何，我等着就好了。

我为什么不反对别人玩其它币？

我甚至不反对任何人发币，也不反对任何人玩传销币。因为，我是自由主义者，我坚持道德是用来约束自己的，而不是用来攻击别人的。

甚至你完全不看好比特币的话，我都支持你远离比特币，去买你自己看好的币。比特币的核心价值观不仅是尊重个人财富的自由，而且是尊重个人选择的自由。我跟它的价值观完全一致。

在一个完全自由的世界里，人人都应该为自己的行为负责。

一个姑娘非要跟渣男谈恋爱，通常你是劝不住的。如果用力过猛，她还会怀疑你对她有什么企图。唯有等她吃一次亏，她才有可能会长一智。

当然啦，还有可能出现另外一种结果——她患上了斯德哥尔摩综合征，深深地爱上了骗她的渣男。

无论哪种结果，你能做的都只有：祝她性福！

而且，你终会明白——给予一个人自由，哪怕她会走弯路，会受到伤害，也是你能够给予她的最大的尊重。

进阶：

囤比特币：  
不要跟着感觉走

囤比特币其实是反复决策的结果，别人觉得简单是因为只看到结果，而看不到决策的过程。

囤比特币其实是反复决策的结果，别人觉得简单是因为只看到结果，而看不到决策的过程。

人们常说：投资是反人性的。确实如此。

我们经常要做一些违背自己感觉的决定。比如：

放在长周期里，我如此地看好比特币，为什么又只投入三成资金？

放在短周期里，我认为比特币大概率会跌，甚至可能腰斩，为什么不先卖掉，等跌了再接回来？

既然其它币也可以百倍千倍，我又为什么连碰都不碰呢？

这些看起来都是反直觉，但这些都是经过深思熟虑的结果。能够用理性战胜感觉，是一个投资者必备的素质。

囤币囤到今天的人，实际上都不简单。因为，随着时间的推移，我们还会反复跟自己做斗争，在囤与卖之间纠缠着。

我一直告诉大家，要把私钥藏得深一些。因为只有这样，我们才不至于一时冲动做错事。但是，藏私钥只能拖延时间。

在冲动之后，如果我们不能把所有问题都考虑清楚，做出让自己信服的决策，我们迟早还是囤不住比特币的。

那么以上那些反直觉的决策，都是如何做出来的呢？关于如何做决策，这个话题实在太大了，市面上也有很多书籍在讨论。在这里，我仅分享

一个最简单的方法。

你仅仅需要懂一点概率论，并且理解预期收益率这个概念，并懂得如何计算它。

这个方法分为三步：

首先，把某个选项的各种可能性列出来；

然后，计算它的预期收益率；

最后，对比各个选项，看哪一个预期收益率最高。

让我们来看几个例子：

例一：愿景那么大，投入那么小。

事实上，投入的资金量是因人而异的。有的人心理承受能力强一点，可以五成；有的人心理承受能力弱一点，可以一成。总体来说，不推荐超过三成。

根据我们前面计算的结果，20年后，比特币会涨到1.6亿元。既然如此，为什么我们投入却不超过三成呢？

因为，比特币还是实验阶段，风险依然很大的。现在，我们假设比特币成功的概率是10%。实际上，这个概率值本身并不重要，重要的是，要牢记它不是百分之百一定成功的。

现在，我们计算一下，囤币和不囤币的预期收益率。输入条件如下：

10%的概率比特币成功，涨幅1000倍，即收益率100000%。

90% 的概率比特币失败，归零了，即收益率 -100%。

于是，

囤币的预期收益率： $10\% \times 100000\% - 90\% \times 100\% = 10000\% - 90\% = 9010\%$

不囤币的预期收益率：0%

显然，我们应该囤币。比特币成功的概率虽小，但是成功之后，那就是不得了的大事了。更何况，比特币成功概率绝对不止 10%，怎么着也有三成吧。我故意写得这么悲观，是想告诉大家，哪怕只有一成的把握，比特币依然值得拥有。

但是，我们能把全部资金都投进去吗？显然也不能，毕竟长期来看，很大概率是要归零的。尽快实现财富自由固然重要，保证现在的生活不受影响也很重要。

最优决策应该是，拿出部分资金囤币，推荐不超过三成，最多不能超过一半。后面我们还会从心理的角度继续讨论这个问题。

如果一切顺利，一轮牛市过后，你就会变成接近于满仓。因为，你投入的那三成资金，翻了几十倍。到那时，你再去体验满仓的感觉也不迟。

就算一切不顺利，比特币不幸归零了。你完全可以用剩下那七成资金，随便投点啥，很快就能把损失赚回来的。对你的生活根本不构成影响。

例二：看空不做空。

根据《囤比特币：寻找合适的够买时机》的分析，我们可能正在迎来史上第三次最佳囤比特币的时机。我们大概率会进入一个比特币的筑底过



程，先深跌到底，然后牛市开启。

其实，我认为短期后市，八成会跌，但是我的决策是不卖币。

很多人无法理解这个决策，认为我要么对自己的看法没信心，要么就是在忽悠别人。但是，八成会跌与不卖币其实是不矛盾的。

假设我对后市看法如下：

20% 的概率涨，涨幅 500%。这很正常，比特币这玩意的涨幅我们都见过，随便就是几倍。

80% 的概率跌，跌幅 50%。

于是，我们可以计算一下，持币和卖币的预期收益率。

持币的预期收益率： $20\% \times 500\% - 80\% \times 50\% = 100\% - 40\% = 60\%$

卖币的预期收益是：0%

虽然大概率会跌，但是持币的预期收益率仍然更高，所以我选择继续持币。

出现这种反直觉的结果，是因为比特币涨的概率虽小，但涨起来就是暴涨；跌的概率虽大，但最多不也就是腰斩吗？

你坐在开往未来的高速列车上，列车突然停了下来，有八成概率要倒车，1 个小时之后再启动，有两成概率突然发车，没赶上就再也上不来了。你会不会下车去玩 1 个小时，赌一把车不会突然发动？

建议不要赌，那 1 个小时玩不出花的，万一小概率事件发生了，后果可

就严重了。



对于比特币而言，这小概率事件就是我们常说的黑天鹅事件。一旦某个经济体爆发巨大危机，比特币列车突然启动，而你恰好下了车，那么你以后就只有看的份了。

黑天鹅之所以是黑天鹅，就是因为它没法预测。既然不能预测，我们就不能下车。

就算币价腰斩了，也没啥了不起的，也就是亏掉三成资金的一半，我们还有充裕的钞票可以用于抄底。偷着乐吧。

例三：XX 币收益可能更高，我也不碰。

我认为未来还有很多的币的涨幅可以超过比特币，但是，涨幅大我也不买，这其实也不矛盾。

如果你有一笔钱：

投比特币：20% 的概率涨，涨幅 500%；80% 的概率跌，跌幅 50%。

预期收益率是： $20\% \times 500\% - 80\% \times 50\% = 100\% - 40\% = 60\%$

投 XX 币：10% 的概率涨，涨幅 1000%；90% 的概率跌，跌幅 90%。

预期收益率是： $10\% \times 1000\% - 90\% \times 90\% = 100\% - 81\% = 19\%$

还是投入比特币的预期收益率更高。看起来，XX 币涨幅可能更高，但是，它暴跌的概率也更高。而且，平均 100 个币里面，能有 1 个币的涨幅超过比特币就不错了。

更何况，你可能会买很多种币，有些会涨，涨幅能超过比特币，但另外一些肯定会归零的。所以，在总体收益上，你想跑赢只囤比特币的人，极其困难。强如李笑来，站台发币无数，也没有能够办到。

以上三个例子，总结就是一句话，做决策不能跟着感觉走。

感觉会跌就去卖，感觉会涨就满仓买，是最不明智的。大多数早期玩家没囤住币的原因是，只要行情来了，就完全忘记了比特币的巨大愿景，只盯着眼前的一点点得失，从而忽略了踏空的巨大风险。

作为一个囤币者，并不是任何情况都绝对不能卖币的，急用钱的时候当然应该卖。但是，无论你选择继续囤，还是立刻卖，你的决策都必须是理性的，是经过深思熟虑的。

所幸的是，作为一个新人，相对于老人，在囤比特币的时候，是有巨大优势的。

通过《牛市起点的故事》，你应该也发现了，很多老人其实也没有多少比特币。如果你还有些经济积累的话，拿出一成资金，都比很多老人的比特币多。

币圈老人其实很不容易。因为面对的都是全新的局面，根本没有经验教训可以借鉴，全靠自己摸索，犯错的几率自然很高。而新人则可以充分借鉴和汲取前人的经验教训，做出合理的决策，尽可能地避免犯错。

很多老人在错误决策后，因为心理负担太重，就不会再回来囤比特币了，他们从此也就与人生最大的机会失之交臂了。而作为新人，大家是没有

这个负担的。

回想起来，我写《囤比特币》系列，实属偶然。哪怕在两个月前，我也不知道我会写这东西。所以，大家能够读到这些文章，冥冥之中，或有天意罢。

进阶：

囤比特币：  
币本位思维

比特币创造了一个全新的世界。在这个世界里，只有一个标准——比特币。

比特币创造了一个全新的世界。在这个世界里，只有一个标准——比特币。

当一个经济体用黄金背书时，我们可以说它在金本位下运行。同样的，当一个经济体用比特币背书时，我们就说它在币本位下运行。

现在还没有这样的经济体，但是我相信，未来会有的。我们还无法改变别人，但是，我们可以先改变自己，从我做起。

例如，如果以比特币为参考系，我们看到的美元走势是这样的（图 1）。

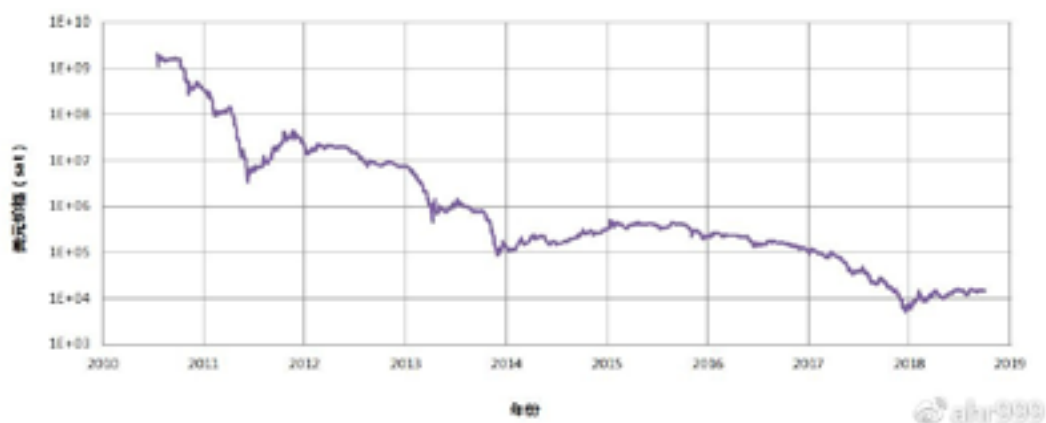


图 1. 美元相对比特币价格（单位：1 聪 = 0.00000001 比特币）

看得出来，美元是个归零币。美元从 2010 年的 20 亿聪已经跌到了现在的 1 万聪，未来还会继续跌，跌到 10 聪，甚至 1 聪也是有可能的。当然啦，以比特币本位看世界，绝大部分资产都是类似的走势，持续的贬值，持续的贬值。不仅如此，它们还剧烈波动。

这就像坐在火箭上看地面的感觉。所有东西都在摇晃，都在变小，持续的变小，持续的变小，直到消失。

你可能从来没有想过，简单的换一个参考系，能带来怎样的变化。但是，无论如何，作为先行者，你需要开始适应这些变化。

首先，很多概念就真的变了。

比如说，定投比特币就不能叫定投了，而应该叫作定存。囤比特币不再是投资，而是储蓄。

持有人民币，相当于持有外汇。我来自比特国，“移民”来到了中国，所以，我需要接受人民币支付工资，也会留下一些人民币，便于生活。我不会傻逼逼地要求商家接受我的本币（比特币）支付，而是主动换汇，使用人民币支付。

这个时候，你就能理解，那些要求比特币买咖啡的人有多么的傻逼。想买咖啡，你不会换成人民币支付啊？

如果做投资，只有赚了比特币，才是真的赚，否则，就是亏了。绝大部分人，肯定是亏的，不用怀疑。但我们肯定是赚的，也不用怀疑。

哦，对了，还有一件非常非常重要的事情。在我们的世界里，根本没有

通胀税这个概念，永远也不必再交了。

其次，消费会趋于理性。

从前，我的消费其实是有些过度的。比如，只要有点闲钱我就会去请人吃饭。不管我们是否愿意，贬值的货币一直在扭曲我们的消费观，毕竟持币就是亏。

后来，我进入币本位，一切就不一样了。那个时候，每顿饭局的花费都在 1 个比特币左右。要知道，这是比特币总量的两千一百万分之一啊，随随便便一顿饭就吃掉了，真心太可惜了。

于是，我开始故意接下很多工作，把自己整得特别忙，遇到饭局，不得不推掉。因为工作忙而推掉饭局，是不会有人介意的。

这个决定很明智。那段时间攒下的饭局钱购买的比特币，应该足够这辈子请客吃饭了罢。毕竟这几年物价跌得有点快，现在吃顿饭只需要 0.0X 个比特币了。

事实上，0.0X 个比特币也相当的贵，未来物价还要继续跌的。但是，这里面存在一个边际效应。如果相对于总持有量，0.0X 个比特币已经小到忽略不计了，那么消费了也就消费了，没啥感觉，即便是明知道这顿饭相当于吃掉了未来的几百顿饭。

那些想当然的认为比特币持续升值就会遏制消费的人，实际上从来就没有持有过比特币。当年还有人拿 1 万比特币买披萨呢。没有人会为了囤比特币，把自己活活饿死的。



消费只是变得更理性了。因为我们不得不在每次消费的时候，都仔细权衡一番，用未来的百倍千倍购买力去换现在的某个物品或服务是否真的值得。

再次，远离传销思维。

每一次牛市，比特币圈子里就会新出现一批伪比特粉。他们有个共同特征，见人就宣传比特币，任何话题都要扯上比特币，而且不遗余力的劝别人买比特币，用比特币。

他们会认为自己对比特币的贡献很大，他们会认为自己不是在搞传销，但是他们的所作所为与传销一模一样。他们可能还意识不到，比特币之所以名声不太好，跟他们有莫大的关系。

当然啦，这些人一般也坚持不了多久。币价一跌，好点的可能就离开了，销声匿迹。差点的甚至会从此走上黑比特币的不归路。所以，我称他们是伪比特粉。

一旦你使用比特币本位，你就再也不会努力“拉人头”了。因为，无论拉多少人进来，你的 1 比特币还是等于 1 比特币。

没有收益不说，你还需要注意“拉人头”给他人带来的风险。对方是否能承受的了火箭的颠簸？你以为你在帮他，其实你可能在害他，因为他可能身子骨很弱，坐在火箭上暴毙了。

越是努力“拉人头”，越暴露了你本质上对比特币缺乏自信，你骨子里还是信仰法币，因为“拉人头”只能赚取法币，赚不了比特币。

所以，请记住，比特币不需要拉人头，安心保管好自己的币才是正事。

你可能会说，既然比特币这么好，为什么我就不能告诉亲朋好友呢？如果是亲朋好友，你就直接帮他们买几个币吧。风险你来承担，收益归他们。如果做不到，说明你们的关系也不算多亲密吧。

最后，拥有富足心态。

有本书叫作《稀缺》，它的中心思想是，处于稀缺中的人们，其心智容量和认知能力会受到很大的限制，从而导致了其习惯于应付匮乏的行为模式。

通俗的说，贫穷实际上是一种心态，贫穷心态会让人变笨，当然也会变得更穷。

很多人深陷赌博，无法自拔。其实他自己知道赌博是错误的，却仍然越陷越深，就是因为长期的贫穷心态，渴望获胜却一直不可得，造成的智商变低。




梭哈也是一种典型的贫穷心态，梭哈之后你就会变笨。

接下来，我们再一次讨论三成资金囤币的问题。

如果法币本位，梭哈囤币和三成资金囤币，对于财富自由而言，差别是早一个周期（4年）。这很重要，毕竟财富自由快了不少。但是代价是，你会变笨。而笨人通常下车都早，我就没见过一个梭哈囤币的囤到了现在。

但是，如果换成比特币本位的视角，我们的感受会完全不一样。梭哈囤币和三成资金囤币，差别类似于 10 个币与 3 个币的区别，这就与时间无关了，10 亿聪永远是 10 亿聪，3 亿聪永远是 3 亿聪。

如果你已经有了 3 个亿，再增加 7 个亿并不能给你带来多少快乐。持有 1 个比特币，有多富有呢？你已经可以跻身全球 TOP 万分之一了。

Share:         

Bitcoin distribution

Balance	Addresses	% Addresses (Total)	Coins	\$USD	% Coins (Total)
0 - 0.001	11196634	49.44% (100%)	2,291 BTC	15,088,049 USD	0.01% (100%)
0.001 - 0.01	5046798	22.28% (50.56%)	20,641 BTC	135,935,517 USD	0.12% (99.99%)
0.01 - 0.1	3921809	17.32% (28.28%)	125,201 BTC	824,523,289 USD	0.72% (99.87%)
0.1 - 1	1755735	7.75% (10.97%)	568,962 BTC	3,747,085,484 USD	3.29% (99.14%)
1 - 10	580406	2.56% (3.22%)	1,513,323 BTC	9,966,137,680 USD	8.75% (95.86%)
10 - 100	131266	0.58% (0.65%)	4,356,003 BTC	28,686,884,915 USD	25.17% (87.11%)
100 - 1,000	14819	0.07% (0.07%)	3,721,140 BTC	24,505,931,751 USD	21.51% (61.94%)
1,000 - 10,000	1556	0.01% (0.01%)	3,421,828 BTC	22,534,783,076 USD	19.78% (40.43%)
10,000 - 100,000	122	0% (0%)	3,145,422 BTC	20,714,485,676 USD	18.18% (20.65%)
100,000 - 1,000,000	3	0% (0%)	428,462 BTC	2,821,676,411 USD	2.48% (2.40%)

图 2. 比特币地址余额分布（数据源：bitinfocharts.com）

图 2 显示，超过 1 个比特币的地址一共只有 70 多万个，全球 70 多亿人口，持有 1 个比特币就进入了全球 TOP 万分之一。持有 0.1 个比特币，也能进入全球 TOP 千分之一。（注：不用考虑交易所地址，把币存在交易所的人，根本就不曾拥有过比特币，即使不丢，也会卖掉的。）

我们需要尽早地培养自己的富足心态，把创造价值和实现自我放在首位，因为钱将来可能是不太缺的。而时间和精力才是自己最宝贵的资源。

拥有富足心态的你，肯定不会再去搭理那些你鄙视的人，也不会再与任何人争论，因为你只想关心你自己的成长。

总而言之，作为先行者，我们必须慢慢习惯以比特币来度量世界。从此，我们就像坐上了火箭，拥有了上帝视角，我们也将领略到从前无法领略的美景。

进阶：

囤比特币：心中无币

当理解上升到一定程度，我们不再需要关注任何比特币相关的信息。

当理解上升到一定程度，我们不再需要关注任何比特币相关的信息。

前段时间有人问我，为什么现在才提出囤比特币，比特币价格都几万元了，以前比特币价格低的时候，却没有提。

这真的是冤枉啊。整整 3 年前，比特币价格只有 1545 元的时候，我就在巴比特发表了囤比特币的文章，有图有真相，尽管当时的我对整个体系的思考没有现在这样系统。



图 1. 2015 年 10 月 6 日发表的文章截图

但是，在接下来的 3 年时间里，我确实极少提到囤比特币。这 3 年一共大概写了不到 10 篇文章，多是关于比特币扩容的，主要因为有些别有用心的人混淆视听。对比我最初在彩云比特的半年，翻译和写作 200 多篇文章，确实是太少了。

事实上，我把对比特币的注意力，几乎全部卸载了。

除了还保留了 1 个热钱包，其实也极少用，我把所有的比特币相关软件全都卸载了。我根本不看行情，不看新闻，也不看大 V 们的言论。

很多人让我推荐钱包，我真的无法推荐，我都卸载钱包好多年了。

为什么要这么做呢？

首先，99% 以上的信息对囤币者而言，毫无意义。因为无论别人怎么说，无论行情怎么走，无论 ETF 是否通过，囤币者都是只买不卖的。

时间和精力才是我们最宝贵的资源，如果花费大量时间和精力，就算能赚点币，也不一定就值得。更何况大多数人是亏币的。

其次，我们需要“空杯心态”。何谓“空杯心态”？如果想学到更多学问，先要把自己想象成“一个空着的杯子”，忘记以前学的其它内容，用全新的视角思考问题。

把注意力全部放在比特币上，你就没有心思学习其它内容了。长此以往，你会走火入魔。牢记，比特币并不是生活的全部。

再次，如果你确实囤过一段时间的比特币，你已经高出别人很多了。从入门阶段自己掌握私钥，到进阶阶段进入币本位思维，你对比特币的认识已经超过了 99% 的人，包括各种大 V。你没办法再去阅读低水平的内容，你会觉得侮辱智商。

财经大 V 们有个通病——讲的全是正确的废话。你读起来觉得全都正确，

但是，你真正想要操作的时候，却发现无从下手。

《囤比特币》系列，既告诉你为什么囤比特币，也告诉你应该如何囤，甚至连（四年后、八年后、十二年后的）结果都告诉你。而且，永远接受大家的检验。

大道至简的意思是，具备把复杂的问题简单化的能力，看问题抓主要矛盾。卖课程或者收群费的大 V 们会告诉你，没有大道至简，所有大道至简都是骗人的。这就是把简单问题复杂化，让你觉得很高深，有东西可以学，于是付钱买课程。

真正赚钱的人是不会开班开收群费的。一个炒币能赚钱的人，会在乎你交的那点群费吗？一个囤币就财富自由的人，会去开收费群吗？不多说了，说多了得罪人。

而且真正管用的信息往往是免费的。比如，关于囤币，包括我在内的很多人，早在 3 年前就免费告诉大家了。只是很多人不相信有这么容易的好事而已。

最后，卸载掉一切软件之后，卖币会变得很困难。因为，你需要重新下载并测试新版的软件，然后才能发送币，没有大半天时间是搞不定的。而只要一想到这么复杂，你通常就放弃了。

卸载一切是囤比特币进阶阶段的考核标准，因为囤比特币只需要私钥，连钱包都不需要，其它就更不需要了。

我知道，很多读者根本就没有去按照我文章写的内容去做。他们问了很



多问题，但我是不会去回答的。因为只要你囤过比特币，你就问不出这种问题。而如果你什么都还没有做，我也无意劝你去囤比特币。

甚至，我推荐大家在达到进阶标准（卸载一切）之后，把我也取关了。即使不取关我，等我写完《囤比特币》，我也基本不再刷微博了。四年后，咱们再见。

另外，卸载一切与三成资金囤币也是相关的。只有你投入量不大的时候，你才有可能做到卸载自己的全部注意力，否则，你根本办不到的。

于是，我们在这里系统的梳理一下三成资金囤币的问题：

比特币仍然是实验，风险很大。理性的决策不支持投入过高的资金。要保持富足心态，就不能投入过高资金，否则，贫穷心态导致智商变低，不利于长期囤币。

要做到卸载一切，也不能投入过高资金。

接下来，我们就真的没事可做了，但是，学习不应该停止。如果还想继续深刻理解比特币，还有些内容可以学习，推荐学习几个方面的内容：

批判性思维：这既是一种精神，也是一种技能。觉得免费的东西不值钱，就是因为你对信息缺乏鉴别能力。无论免费还是收费，我们对信息的质量要有自己的判断标准。

经济学原理：不要只读奥派，不要只读一家之言。读一读经济学导论、宏观经济学、微观经济学的相关内容，重点理解货币制度、通货膨胀、储蓄、投资和金融，等方面。

密码学原理：重点理解概率论、Shannon 理论、公钥密码学、椭圆曲线、Hash 函数、数字签名、伪随机数生成，等方面。

心理学：重点理解认知过程、情绪、压力、健康、行为和态度的相互影响，等方面。

希望大家能忘掉比特币，从更广的视角去学习这些内容。另外，囤币之后的学习可以非常轻松，因为你读书和学习，不是为了养家糊口，而是纯粹的丰富自己。毕竟你有比特币这个后盾，未来大概率是不缺钱的。

此外，请一定要维护好自己的人品，保护好自己的身体。

资本可以调配资源，放大我们的梦想。但是，资本在不同的人手里，对社会的贡献是不一样的。这既跟掌握资本的人的学识有关，也跟他的人品有关。

既然大家未来都可能非常的不缺钱，那么请从现在起，维护好自己的人品，不要骗人，也不要去做伤害他人的事情，而是多考虑造福他人。人品这东西，一旦败光了，花钱都买不来。

保护好身体，其实也不容易。很多人知道健身的益处，但是知道也做不到。就像很多人知道囤币的收益，同样知道也做不到。

最后，我想谈一谈价值观的问题。

什么是价值观呢？简单的说就是个人喜好。

比如说，某地计划建一个工厂，优点是拉动当地经济，缺点是消耗资源能源。

基于同样的事实，有的人支持建工厂，而另一些人会反对。为什么呢？因为前者认为拉动经济更重要，可以牺牲一点资源能源；而后者认为保护环境更重要，经济发展可以缓一缓。分歧的本质来源于价值观的差异。

价值观本身并没有对错之分，就像萝卜青菜各有所爱，你不能说喜欢萝卜的人就不对。于是以上问题问题，以及所有类似问题，往往会争论不休。

类似的，几乎所有关于比特币的问题，最终都可能是价值观的问题。例如：

PoW 维护了比特币价值网络，但消耗了巨量能源。是否值得？你认为值得就值得，你认为不值得就不值得。

比特币实现个人私产的自由，但是去中心化无法被监管也无人背书导致乱象丛生，是否值得？你认为值得就值得，你认为不值得就不值得。

比特币为了保证去中心化和安全性，适当放弃了主链的交易速度和容量，是否值得？你认为值得就值得，你认为不值得就不值得。

\ 类似的问题还有很多，我对上述问题的答案都是——非常值得。我坚持自己的价值观，也尊重别人的价值观，所以我不会就上述问题与他人争论。

我的价值观与比特币的价值观一致，如果你也是如此，那么相信我，比

特币就是属于你的，你也一定能囤得住比特币的。

进阶阶段就全部结束了。现在，你已经知道了比特币的价值来源，以及在什么时间购买比特币，懂得理性的决策，按照币本位在生活。你做到了！

手中有币，心中无币。

进阶：

囤比特币：  
打造强节点

成就最好的自己就是对比特币最大的贡献！

**成就最好的自己就是对比特币最大的贡献！**

如果我们认可比特币的价值观，我们一定会想要为它做点什么的，尤其是当比特币给我们带来巨大经济回报的时候。

于是，很多人会开始不遗余力地宣传比特币，这很正常，有好东西当然要分享。但是，正如我们前面所讨论的，切忌去“拉人头”。

首先，无论你拉多少人进来，都不会影响比特币的结局。换句话说，比特币成与不成，与你拉多少人进来，根本没有关系。拉进来除了影响短期价格，没有任何其它用处，而一个立志要囤 20 年的人不会在乎短期价格。

其次，如果你真正达到了心中无币的状态，你根本不会产生“拉人头”的想法。想象一下，你会天天把人民币挂在嘴边，没完没了地让别人持有人民币么？如果你这样做，你就是神经病。储蓄不是理所当然的事情么？需要天天挂在嘴边么？

再次，其实你也说服不了几个人。不是你的道理讲得不好，而是你自身不够强。马云放屁都是香的，而你说啥别人都当放屁。何必自讨没趣呢？

如果你真的那么看好比特币，你就自己默默地买，长期的持有。

以我在币圈的观察，那些努力“拉人头”的，通常都不持久。之所以热衷于“拉人头”，是因为害怕，害怕下跌，害怕崩盘，害怕归零。越是

害怕，就越希望多拉一点人进来，抱团取暖嘛。

实际上，坚持持币本身就是对比特币最大的贡献，这意味着我们对比特币储值的认可，也需要很大的勇气和智慧。所以，我们真的可以什么都不用做，只管囤币。

如果我们非要为比特币做点什么的话，那么就去——努力成就最好的自己。

这个逻辑非常简单，我们每个人都是一个比特币节点。我们越强大，比特币就越强大，整个比特币网络就越强健。

无论我们的职业是什么，继续把原本应该做的事情做好，做到极致，把自己培养成行业领军人物。人们一谈起某件事，首先想到的就是你。

这两个显而易见的好处。第一，我们很靠谱，我们的意见会受到重视；第二，我们的收入会快速增长，能调动更多社会资源。

我们越是牛逼，对比特币的帮助就越大。哪怕我们从来不提比特币，至少我们不会像很多人那样去诋毁它。仅巴菲特一个人对比特币就造成了几万点伤害。我们当然不应该寄希望于巴菲特改变思想支持比特币，我们应该通过自己的努力去超越巴菲特。

我最近发现一个有趣的现象。有很多其他领域的大V在关注我，看我的文章，但是既不点赞，也不评论。我其实很理解他们，他们不想让别人知道他们在关注比特币。

他们经历的，我都经历过。在生活中，我就是从来不提比特币，他们想必也跟我一样。不提没关系，努力做好自己，就足够了。

在我们不够牛逼的时候，有些道理不用跟人讲，讲了也没人相信。当我们足够牛逼的时候，我们不需要讲任何道理，也能扭转他人的错误认识。

我们越是富有，对比特币的需求就越大。如果每个支持比特币的人，场外赚钱能力都翻了10倍，币价自然要翻10倍的。我们应该用自己的身价给比特币增值，而不是反过来，希望比特币给自己的身价增值。

按照大多数人的逻辑，我现在这样继续增持比特币，没有意义。虽然通过几年的努力，我的收入大幅增长，但是币价却涨了几十倍。即使我拼命增持比特币，对总持有量而言，基本没影响。

但是，我仍然选择继续增持，因为我是币本位思维，谁会嫌自己存的钱已经够多了，以后不再存啦？换句话说，收入越是涨，我的储值需求就越大。

考虑到比特币的归零风险，我的行为其实是不理智的。但是，这就是我回馈比特币的方式啊——永不退出，让我的投入与比特币共存亡。说得更通俗点，这钱哥不要了，哥就想看看这个实验能不能做成。

我之所以敢这么做，最关键的因素是，我的收入涨了，我已经不在乎自己的投入啦，哪怕全部归零。所以说，我们越是宽裕，就越不害怕损失，持有比特币就会越坚定。

总而言之，与其把时间花在“拉人头”上，不如努力成就更好的自己。



与其拉入几个弱节点，不如把自己打造成强节点。把自己这个比特币脑残粉变得无比强大，就是对比特币最大的贡献。

此外，如果你以成就最好的自己为目标，那么你的家人就不会反对你持有比特币。我知道很多人因为比特币与家人闹矛盾。如果你以为家人是因为不懂比特币，才反对你持有比特币，那你就大错特错了。他们真正担心的是，你不学无术，不求上进，深陷赌博或者传销。

而如果你工作努力，生活积极，你的家人就会特别信赖你。在这种情况下，你拿出一点闲钱囤比特币，即使被他们知道了，他们也不会反对。因为你从来都是靠谱的，而你居然选择囤比特币，所以唯一的解释就是，比特币也是靠谱的。

只有你足够靠谱时，你才能够给比特币做信誉担保。我的家人支持我，我也根本没有费过口舌去解释什么。

所以，努力吧。终有一天，你会发现，即使没有比特币，你也一样是个成功的人，一个上进的人，一个高级趣味的人，一个不差钱的人。

而拥有了比特币，你如虎添翼。比特币将放大你的梦想，当你发现自己掌握了大量财富，很多你以前想都不敢想的事情，就会变得越来越容易实现。

到了那个时候，你可以选择利用手中的财富，去实现更大的梦想，去推动社会，去造福人类。

如果你是这样的人，而比特币又掌握在你手中，那真是它莫大的幸运。

贡献：

囤比特币：  
运行全节点

成就最好的自己就是对比特币最大的贡献！

私钥决定比特币所有权，全节点捍卫比特币规则。

如果我们一定要回馈比特币，除了把自己打造成强节点，我们还有第二件事情可以做——运行全节点。

比特币的目标是成为最好的储值手段，其中一个最重要的特性是，总量有限。持有比特币，永远不必再交通胀税。

但是，你可能会问，我们又如何保证比特币的规则不被改变呢？会不会有人能够修改比特币的总量呢？

这个时候就得靠全节点了。

全节点负责验证比特币网络上的交易和区块，任何不符合规则的交易和区块都会被全节点抛弃。由于比特币总量是区块奖励和减半规则共同控制的，如果全节点不同意，比特币总量就不可能被修改。

事实上，比特币所有规则的修改都得征得全节点的同意，而每个人都可以运行自己的比特币全节点，这意味着比特币的规则掌握在用户自己手中。

人人都是中本聪，我们自己定义自己心目中的比特币。

开发者可以发布带有新规则的客户端，但是他们需要说服全节点进行升级，否则新规则就无法执行。也就是说，全节点可以防止开发者擅自修改

规则。

如果我们担心比特币总量被修改，我们就应该自己运行全节点，表明态度。只要其它用户的想法跟我们一样，开发者就算改了规则，也无法被执行。如果有全节点要犯傻，它就会被分叉，等同于被大家开除了。无论如何，我们都仍然留在我们认可的区块链上。

这也是为什么开发者总是优先考虑向前兼容——软分叉升级，因为任何不向前兼容的升级，其本质都是扩大了比特币的运行规则，都极有可能被全节点拒绝，从而发生分叉。

矿工也可以尝试修改规则，例如，打包不合规的交易，或生产不合规的区块，但是，它们会被全节点抛弃并屏蔽，从而给自己带来经济损失。

因此，全节点是比特币赋予每位用户的最高权力，是每个比特币用户手中的剑。我们认可什么样的规则，就运行具有什么样规则的全节点，于是，我们的比特币就永远是那个我们认可的比特币。

而反过来，如果任何人想要更改比特币规则，他就必须说服全节点，否则，他的新规则就只有他自己认可，他把自己给分叉出去了。

某些矿工会忽悠大家，让大家放弃运行全节点的权力。但是，这是我所见过的最傻的事情，因为这种忽悠是个悖论，根本不可能奏效。

那些能够被忽悠的人，根本就不运行全节点。而运行全节点的人，都懒得去争论，只管自顾自地运行着全节点，你根本拿他没办法。

这就像保镖想要造反，但害怕人们手中的剑，于是想欺骗人们放下剑。那些能够被欺骗的人，一定是从来不用剑的，也不在乎剑有什么用。而那些用剑的人，当然懂得剑的威力，又怎么可能会放下？保镖无计可施，只能骂骂咧咧，试图激怒人们，但手中有剑的人拿好剑就行了，用不着理会他们。

私钥决定比特币所有权，全节点捍卫比特币规则。手握私钥有快感，手握全节点也有快感。

每当看到有人想作恶，写一些颠倒是非的垃圾文章，我都会去默默地查看一下自己的全节点状态，并产生一种“你能奈我何”的快感。我很清楚，他们叫得越凶，越说明他们拿我没有办法。

哪怕我们从来不运行全节点，我们也应该拥有运行全节点的权力。手上有剑不用和手上没剑是有本质区别的。如果当年没有勒紧裤带发展原子弹和氢弹，能够换来随后几十年的高速和平发展吗？

从个人的角度看，即使不运行全节点也不会有什么太大的影响。但是要记住，这个时候，我们需要信任，我们选择信任其他比特币用户，他们运行着全节点。

选择信任别人是我们的自由，但是我们同样需要保留不信任任何人的权力，否则我们也会失去选择的自由。

目前运行全节点的成本已经很高了，每年租服务器大约也要花费几千元。在家里电脑上运行的 Core 钱包，通常不是合格的全节点，尽管它也是有益的。

但是，如果我们把巨额财富储存在比特币上，同时还想回馈比特币，我们就应该运行全节点，对整个比特币网络的安全作出自己的贡献。

一方面，我们的全节点可以帮助其它节点同步区块数据；另一方面，更多的全节点等于更强健的比特币网络，使得攻击者，哪怕是国家级攻击者，也难以下手。

比特币的目标很宏大，未来遭受任何规模的打击都是正常的。买咖啡这么小的事情，从来都不是比特币的目标。

所以，拿起手中的剑，捍卫自己的财富，为比特币保驾护航。

成就最好的自己，把自己变成比特币的最强节点，同时维护一个真正的比特币节点，这就是我们能为比特币作出的最大贡献。

我们是比特币贡献者。当其他比特币用户需要信任时，我们是他们坚实的后盾，提供他们需要的信任。当其他比特币用户不需要信任时，我们坚决维护他们自行验证的权力。

正是千千万万的比特币贡献者，成就了今天的比特币。那些看不懂比特币价值的人，根本不知道比特币背后都站着什么样的人，以及这些人有多么宏大的目标。

**Don' t trust. Verify.**

终章：

不忘初心

## *To Da Moon !*

写到这里就真的全部结束了。能够把这件事情完成，我非常高兴。

写作的过程令人愉悦。得到了很多人的赞赏和鼓励，我非常感谢。

在比特币的圈子里，我是个异类，很不合群。

我是极少数，从来没有踏过任何坑的人。

我是极少数，只囤比特币的人。

我是极少数，从来没丢过币的人。

我是极少数，把曾经加过的群全部退干净的人。

我是极少数，避免与币圈产生利益瓜葛的人。

当然啦，我也不在乎是否合群，反正我也不在圈里混。

从一开始，我就为比特币感到兴奋，今天仍然如此。

从一开始，我就期待参与这场实验，今天仍然如此。

从一开始，我就坚定地囤积比特币，今天仍然如此。

我没有忘记初心，我愿意坚持原则。我也懂得感恩。

如果你还有些心理学基础，你一定知道，行为是可以改变思维的。长期囤比特币这个行为，也一样改变了我的思维。

我自认为是个非常勤奋的人。小时候，父母告诉我，勤劳致富，我深信不疑。比特币改变了我的财富观——致富不一定要靠勤劳。目前，我获



得的所有工作收入，全部加起来，都没有傻囤比特币带来的财富增长多。

但是，我并没有因此而变得懒惰。人生是一段路途，财富可以让这段旅途更精彩，这是毋庸置疑的。勤奋也可以让这段旅途更精彩，这是很多人没有意识到的。

囤比特币的本质是储蓄，说得通俗点就是存钱。我们把今天剩余的财富留到明天发挥更重要的作用，这其实是一种美德，是我们中国人的传统美德。

还记得，上小学的时候，妈妈把我带到银行，开了个帐户，让我每个月定存零花钱。她想培养我储蓄的习惯，出身于穷苦的农民家庭，她总是精打细算，未雨绸缪。

那是我储蓄的开始，但我并没有坚持多久。存通胀币真的没意义。反而是，借得越多，赚得越多。父母辛劳一辈子，也没有能够看透事情的本质，依然生活节俭，努力存钱。我真的不忍心告诉他们真相。

是比特币教会我储蓄，让我理解定存，并且带给我回报，不仅仅是经济上的。

我从来没打算动用比特币，有它没它，对我的生活都没有影响。但它对我的心态却有很大的正面作用，它是我坚实的后盾。我可以放手去做那些有风险没收益，但有价值的事情。

换句话说，无论是否有收益，无论是否会失败，我只考虑某件事是否真的值得我去做。如果没有比特币，我不确定自己是否依然能够这样。

这不正是储蓄的意义么？解决后顾之忧，才能冲锋陷阵。

写《囤比特币》显然有风险。我预测了比特币价格的未来走势，存在犯错的可能性。但我还是要写出来，因为怎么想就怎么写。

写《囤比特币》显然没收益，我的比特币不会因此而增加。它也不会对比特币的发展有什么帮助，无论我写还是不写，比特币该怎么发展还是怎么发展。

至于做这件事情的价值嘛，毕竟价值是主观的，写作和分享的过程让我很愉悦，所以我个人认为有价值。至于它是否能带来更大的价值，就交给大家去评判，交给时间去检验。

无论如何，所有以上的改变，我都得感谢比特币！它可能是处于这个时代的人，能够遇到的最大的机遇。

囤比特币，是运气，是缘分，是福分。写《囤比特币》，也是运气，也是缘分，也是福分。

非常感谢所有居然能坚持看到这里的人！

我会永远跟你们在一起，见证比特币的伟大。



Buy and Sell