《比特币》

图书基本信息

书名：《比特币》

13位ISBN编号：9787508643007

10位ISBN编号：7508643003

出版时间：2014-1-1

出版社：中信出版社

作者：李钧,长铗

页数：272

《比特币》

内容概要

2009年，比特币诞生。比特币是一种通过密码编码，在复杂算法的大量计算下产生的电子货币。虽然是虚拟货币，比特币却引起了前所未有的全球关注热潮。
这一串凝结着加密算法与运算能力的数字不仅可以安全流通、换取实物，1比特币价值甚至曾高达8000元人民币。有研究者认为比特币具备打破几千年来全球货币由国家垄断发行的可能性。在不经意间，比特币引起的金融新浪潮已悄然成型。
虚拟货币并不是新鲜事物，为什么只有比特币受到如此追捧？它激烈变动的价格行情更让投资者们担心：比特币的合理价格到底是多少？其价格的支撑体系又在哪里？如此剧烈的上下波动是不是预示着它的不稳定直至最终崩盘？
作为国内首批参与并研究比特币的开拓者，《比特币：一个虚幻而真实的金融世界》作者们对这些问题都有着深刻的理解。本书从介绍比特币的概念出发，全面、系统地阐述了比特币的起源、发展、技术原理、生态圈等关键问题，还大胆畅想了比特币的现实应用、未来前景。
《比特币：一个虚幻而真实的金融世界》坦然面对比特币引发的种种争议，针对政府、货币体系等问题，以开放的态度、翔实的资料与读者交流，深入探讨比特币改变全球现行货币体系，朝货币发行非国家化的方向前进的可能性，揭示了比特币对现实金融业，甚至对未来世界的影响。
《比特币：一个虚幻而真实的金融世界》讲述的是一场伟大的货币实验，及一个虚幻而真实的金融世界。如何认识与思考这一实验，有助于理解互联网时代金融世界的逻辑。

《比特币》

作者简介

李钧，壹比特数字科技首席执行官。
长铗，著名科幻作家，巴比特社区创始人。

《比特币》

书籍目录

《比特币》

《比特币》

精彩短评

1、没讲清原理。但是有部分有趣的内容，提到了如零知识证明的内容。
2、缺乏营养
3、较全面介绍了这种去中心化的基于数学密码学的货币及其经济体系，向提出货币非国家化的伟大的哈耶克致敬！
4、关于比特币原理和系统的介绍好不错，但是比特币金融部分的内容完全是为了唱多而唱多，逻辑混乱
5、自我扫盲。全书多人供稿，章节逻辑不清；几乎没有经济方面内容，大部分讲技术，哈希算法、通信、加密什么的，看完依旧满眼黑；安利成分很足，可是并不太可信。总结：比特币系统相当于一个公开匿名电子账簿，由全球云承载，全网同步，对算力投入有特定奖励机制，存在51%攻击风险。PS：BTC的通缩属性怎么办？持有BTC就尼玛能抢劫所有人，真是轻松愉快哈。
6、写的不够好，好几个地方重复出现。作者功力一般，不过值得一看。
7、介绍比特币的普及读物，还算客观。然而在现在的环境下比特币也只能是一场泡沫，并没有什么卵用。
8、纯粹的涨知识
9、作者虽然设想了比特币现实存在和可能存在的BUG，而且也认为绝大多数BUG是可以解决的，但是想象跟未来往往不会重合
10、书一般吧。很一般。科普性的吧，可以挑几个章节看看
11、还算值得推荐作为入门材料。虽然很多重复内容，但中国出版业大概也就这水平吧，各种网文抄一遍——之所以给3星，是因为太“安利”了。
12、作者肚子里边还是有蛮多干货的，基于比特币（区块链）的应用看得很有意思。斯诺登的那个想象的故事很有创意。
13、一本入门都算不上的密码学简述，给两颗星完全是看在对比特币的历史描绘上。比特币的根本问题不在于数学，而在于人，全篇的描述只是略略带过，不断强调密码学的可靠。
14、这本书对比特币作了详尽的介绍，让我对比特币有了全面的认识，观点深刻，让人醍醐灌顶
15、外行看下热闹，密码学基本看不懂
16、挺有意思的一个东西，原理上来说其实有很多可以借鉴的，是一个很好的实验。
17、真是天才的思想！
能让人绝对信任的只有数学了吧。
18、不如直接看论文https://bitcoin.org/bitcoin.pdf
19、新kindle开工，背光有点儿耗电啊。书后半部是货币发展史，减一星。
20、介绍了重要的点对点 去中心化思想
21、入门书，其中的技术理论看不懂。。如果能多一点对金融体系货币体系更深入更全面的东西更好了。
22、比特币的出现其本质是好的，而如今其前景仍不甚明朗。而本书最大好处就是对于其的科普。
23、看前面几篇足矣。
24、『去中心化有助于实现货币民主，保护私有财产，使交易高效、便捷，避免双重支付……已经足够有价值了。』
25、有点啰嗦 相对易读
26、很差，有空写书评
27、此时一般的难懂
28、大都算常识性内容，适合从来没有接触过比特币的人读。
29、讲得挺明白
30、还不如跟一个从业者聊俩小时有收获。
31、epub版。能开拓视野，学到新知的书~~其中作为比特币基础的密码学知识写得通俗易懂，还看到了对于哈希值的简明讲解，读之前完全没料到的~~可作为【素材资料】~~
32、了解了解，准备定投比特币
33、非常不错的科普

34、从头翻看了一遍，好吧，有些地方没有看明白。但是加上知乎比特币的介绍，已经对比特币有了一个粗略大框的了解，~
35、作为一个介绍性质的科技读物，已经写得很不错了，深入浅出，清晰全面。
36、A good introduction to the bitcoin and the big idea behind it. Further study and research needed for me to understand the maths part...
37、对于比特币思想价值解释的不错
38、虽然没有想象中的好，但开阔一些见识，作为普通读物还可以
39、读过这本书，写的还可以
40、还是不够深入浅出
41、货币天生是信息……但有种废话的感觉，老实说，没通过本书理解比特币到底是什么？
42、不是BTC的问题，是我的问题，配了好多...
43、了解太少，无法评价。
44、比特币热潮渐淡，区块链来势凶猛。回头再看这本写自2013年的书，仍然颇多启发。数字货币对传统金融领域目前来看依然影响甚微，涉及到主权、利益、监管其合法性和公众接受度依然遥不可及。不过分布式记账的区块链技术对智能合约和软件定义世界在经济领域的应用已经可以看到些许曙光，作为一名公钥算法领域的老人从中心化的PKI/CA领域到区块链应用，颇感兴奋。
45、基础知识详解
46、简单明了，有些安利吹嘘的口气，但作为普及读物还是不错的
47、没有看完的动力…
48、比特币的前世今生
49、前面理原理的部分科普得凑合；后半部分关于货币，金融的介绍对于我这种金融白痴来说还是不错的安利。

怎么现在出本科普类的书这么乱搞了吗？就是几篇论文的扩充和基本原理的填补
50、看完觉得比特币真牛

《比特币》

精彩书评

1、比特币实质是参与者互认的公开记账体系。交易者凭借程序计算争夺账本数据块（“挖矿”），获得新增货币。它象征着货币价值去实体化的虚拟时代的开始，体现着货币发行去中心化的构想。难道这是未来的大趋势？！那我们这些脑子不好使的人怎么办？
2、作为一本书，因为是类似“众筹”的集体创作，章节之间的逻辑关系和条理并不十分融洽，部分内容重复甚至意见相左，也从侧面表明即便在比特币圈内部大家的认识也并不完全一致。但是，并不能抹杀比特币作为一个社会实验的巨大价值。关于比特币本身，这本书已经说的很清楚了，如果你和我一样不是一个商业投机者，而对比特币技术及其背后的社会影响感兴趣，大概记住两句话也就够了：计算即权力；货币即信息。比特币本身能否成长为一个成熟的虚拟货币我并不十分关心，我也不赞同大家一窝蜂像抢小米一样去抢比特币，一项新技术的产生到成熟有一个十分漫长的过程，即便比特币这个实验会失败，但是在我看来未来类似或者优于比特币的虚拟货币将会重复出现。比特币（或者将来可能取代比特币的虚拟货币）的经济作用及其带来的一系列网络变革，将真正开启互联网经济的新时代，并将带动社会变革。以前我也有点不理解长铗不写科幻却一直到处卖比特币的安利，但是当你真正了解比特币的时候，大概每个极客都会感觉参与比特币的确在创造未来。（这些重要性书中都有，可能写的还不够。顺带一提，第一篇关于比特币的科幻发表在《新科幻》2013.11上，陈格《乾坤一掷》，作为小说仍有改进之处，但比较精准了描述了作者自己对比特币的认识，一种科幻的未来将在等着我们）当然支持比特币的人认为这是抛弃了肮脏的政治而将人类托付给纯净的数字，某种程度上是对的，某种程度上也过于乐观，即便不考虑技术自身的发展。
3、原地址 http://blog.sina.com.cn/s/blog_63045e190101d4ny.html一、货币的演化过程先简单回顾一下人类货币的演化过程，大概有以下阶段：a. 1.0版本：自然货币（贝壳、牲口、金银……）这个阶段，货币基于一般等价物的稀有性或者实用性，货币不可能出现人为操纵的超发。b. 2.0版本：早期纸币、银票到本位纸币当贸易量越来越大，实物货币太不方便了，而且大家发现其实并不在意货币本身有什么价值，在意的只是这么多的货币能不能交换到足够的物品，于是纸币这种信用货币逐步诞生，由钱庄、地方政府逐步到中央银行负责发行和规划。而纸币本身其实是没有任何价值的，这个阶段，货币信心是基于国家信用或者说国家暴力，我们相信货币价值是能够稳定的，虽然事实往往并不如此，但也不得不被迫接受。c. 2.5版本：刷卡时代这个阶段其实和纸币时代没有本质的差别，只是现金被数字化了，国家发行货币也越来越简单，只需要在人民银行的数据库中加几个零，然后转到各大银行的账户上就好了。d. 3.0版本：密码学货币可是当国家信用被刷爆，我们还可以相信什么？事实上，凡是依赖人参与决定的事情，必然无法杜绝黑幕和私心。其实真正可以相信的东西确实有一个，就是数学！可是，即使我们都认为数学足够可信，可是怎样依据数学创造出一种货币呢？在没有互联网的时代，这个问题依然无解。而现在，真正意义上的第三代货币确实已经诞生了，虽然还处于大多数人无法理解的概念阶段。二、比特币到底是什么a. 本质：基于密码学的公开记账系统百度百科是这样写的：比特币是一种由开源的P2P软件产生的电子货币，是一种网络虚拟货币。比特币不依靠特定货币机构发行，它通过特定算法的大量计算产生，比特币经济使用整个P2P网络中众多节点构成的分布式数据库来确认并记录所有的交易行为。P2P的去中心化特性与算法本身可以确保无法通过大量制造比特币来人为操控币值。一眼看去全是黑话，非专业人士大概很难读懂。简单来说，比特币系统的本质就是一个公开记账系统。每个帐号的每一笔数额流动都被记录在案。而且每个人手上都有一份完整的账本，可以统计出有史以来每个帐号的每一笔流动，当然，也就能算出特定账号当前余额是多少。这里最关键的一点在于：每人手上都有完整的账本，这个系统里没有任何人有唯一决定权。这意味着没有任何人可以决定向这个系统增加货币或者改变规则，因为个体的修改会被整个网络否决掉。除非有人可以修改50%以上人手上的账本，这就是比特币系统里所谓的51%攻击，显然这并不太可能出现，而且随着网络的增大难度也随之递增。b. 挖矿是在干什么伴随着比特币发行的关键词是挖矿。这实在是太让人费解了，挖矿是在干什么？比特币是从哪里挖出来的？这着实是很科幻的一件事！其实挖矿的本质是在争夺记账权。在比特币的世界里，每大约十分钟会向公开账本上记录一个数据块，这个数据块里包含了这十分钟内全球被验证的交易。但是由谁负责记提交这个记录，是需要抢的，怎么抢会在后面的数学部分解释。为什么要争夺记账权？因为抢到记账权的人被允许向自己的账户增加一笔金额，当前的数额是25比特币。c. 怎么限制发行数量前面说到，在比特币被创造的时候就在规则中限制大约每十分钟只发行50个给抢到记账权的人，而且这个数额每四年会减半，现在已经减到25个。用数学求极限

，可以算出到2140年，一共会发行2100万个，目前的发行量大概是1100万。要改变规则，依然需要51%攻击。当前发行量可以到这里查询：http://blockchain.info/charts/total-bitcoinsd. 矿池是什么随着整个网络计算能力越来越强大，普通电脑的计算力几乎没有机会抢到记账权了。那么大家就组队吧，组成一个矿池，如果矿池抢到了记账权，那么钱按照计算贡献来分配。三、比特币的数学基础a. 收款地址是什么刚接触比特币的人印象最深的大概是那一串乱码般的地址。那是什么东西？会和别人的重复吗？很多文章上说的私钥是什么？这里要引入第一个重要密码学概念：非对称加密算法。通常大家概念里的加密和解密是只有一个密码的，比如压缩一个文件时候加上密码，那么解压的时候输入同一个密码就可以解开了。事实上，一直到上世纪70年代，密码学都停留在这个层面上，学名叫做对称加密算法。直到70年代，两位出色的数学家出现，他们提出了一种新的密码学思想，就是加密和解密要用不一样的密码。通过数学办法，产生一对密钥A和B，当使用A加密一份数据，必须使用B来解密；而使用B来加密数据，必须用A才能解开；而且根据A可以很容易计算出B，反过来则不行。A就叫私钥，B叫做公钥。顾名思义，A是保密的，B是公开的。听起来好像也没有什么特别的不是么！仔细思考一下，就会发现这里解决了两个问题：1）任何人想发一个加密文件给我，只需要用我的公钥B加密后公开放到网络上，而且不用同时从某个隐秘渠道告诉我密码是什么，因为只有掌握了私钥A的我才可以解密。2）当我要证明一件事情确实是我发布的，只需要用私钥A加密，然后公布出去，大家发现用我的公钥B可以解密出来，就足以相信这确实是我公布的，因为私钥只有我拥有。这个过程也叫数字签名。没错，钱包地址就是那个公钥！因为公钥和私钥要需要使用特殊的算法成对生成，所以不能像普通密码一样人为设置，而且看起来也没有规律性。通常是安装了比特币客户端后由系统自动生成。而私钥就隐藏在钱包文件中。想详细了解比特币的非对称算法请戳：椭圆曲线算法（http://baike.baidu.com/view/531769.htm）。那么地址有多少？会不会和别人碰上？这么形容吧：如果每粒沙子里面都有一个地球，那么地址数大概等于地球上所有沙子里面的地球的沙子数总和。如果你生成了一个其他人有余额的地址，那恭喜你真的中奖了！如果愿意，这笔钱就归你了！b. 比特币怎么支付形象的比喻，比特币的支付方式其实就是在发微博，私钥就是微博密码，微博用户名就是公钥。当A要给B付款，只需要在自己的微博上说“我给@B付款1比特币”，然后挖矿的同学就会验证你是不是有足够的金额，如果验证通过，就把你这条微博和十分钟内的验证过的其他微博合到一起转发一次。当有足够的人转发（通常认为6个就足够了），就认为这一笔支付成功了。而如果你发微博说“@B支付给我1比特币”，这显然是非法的，没有人会帮你转发，因为只有拥有B的私钥才有权限说这句话。当然，这个转发行为是需要满足一定条件才允许的，以避免你可以自己弄6个号帮自己转发了，详细条件见下条。c. 如何争夺记账权争夺记账权的办法其实就是大家玩一个密码学游戏，这个游戏叫：哈希，再具体一点叫做：SHA-256。哈希的特点是：可以根据任意一段数据计算出一个很大的值，而且计算结果相当随机，无法预知大小。大家比的就是在十分钟内看谁找到一个数字和上一个数据块的哈希以及十分钟内验证过的微博连起来可以算出最小的哈希值。谁算出来的最小谁就抢到了记账权。同样至少要小于某个值才被允许有转发权，这个值越小对应的就是比特币网络的难度系数越高。由于计算结果的随机性，所以没有办法优化算法，只能从0开始一直往上算，这时候比的就是谁算的快谁就有机会先找到这个数字。如果这十分钟内没抢到记账权，就白算了，重新进入入下一轮。担心SHA-256被破解是嘛？事实上，担心这还不如担心宇宙毁灭来得靠谱些。四、比特币的特点a. 我的币在哪里这是很多人最困惑最不能理解的问题，我的地址里面有了一笔金额，可是它在哪里啊！？在我的电脑里吗？还是在钱包里？其实根本没有这么“一笔钱”存在！它无处不在实际上又根本不存在！它存在于所有人的账单上，大家只是知道你有这么一笔钱，而不用关心钱在哪里，实际上确实也并没有任何形式的存在。好比你在乎银行卡里的数额对应的现金放在哪吗？其实只要我的卡能刷就够了。而使用比特币时也并没有把某个币给对方，只是使用私钥发一个声明“微博”。b. 方便追踪因为每个人都维护着账单，所以可以轻易追踪到任意帐号上的资金流动。比如最近的芦山地震，壹基金接受比特币捐赠，可以戳这里(http://blockchain.info/fb/1dumifq)查询明细，每一笔的到账时间、数额和支出都可以清晰看到，亲，这相当于直接查询银行内部原始账单哦！c. 隐私保护虽然我们可以查询每个帐号的流水信息，但是并没有办法将账号和现实的人对应起来。只要愿意，每个人都可以有几乎无限个地址。这是在人类历史上，第一次从技术上保障了私人财产神圣不可侵犯、不可追踪、不可冻结。d. 纸钱包和脑钱包私钥我们通常藏在钱包文件里，事实上它同样只是一个字符串，只是比地址略长一些，我们完全可以把它抄写或者打印到一张纸上，然后郑重放到保险柜里。那一个字符串就承载了你全部的比特币财富哦！基于比特币更有意思的一个创造是脑钱包，这完全是超乎想象的神奇！在这个网

站（http://brainwallet.org/）可以通过一句话来生成一对公钥和私钥。只要能记住这句话，你就可以再次根据它生成私钥，在任何有网络连接的地方提取你的比特币。但是千万要选一句可以全球唯一的话，不然碰撞的机会就会大大增加了，当然，这也很容易，比如想一句：张小明和老婆赵小花的第三个儿子叫波波。大概是很难被碰撞到的。这意味着你可以把所有的财富存在大脑里，是不是觉得足以秒杀一切！e. 可证明和不可证明想像一下，当你使用的是脑钱包，这个世界上将没有任何证据可以证明你拥有这么一笔钱，除非失忆或者死亡，这笔钱才会丢失。同样，也可以轻易证明你拥有某个地址上的财富。只需要使用私钥加密一条信息发布出来就行了，大家就可以确认你对该账户的拥有权，而不必把私钥公开才能证明。比特币官方客户端自带这个功能。f. 丢失无法找回很多人想知道一件事，如果我的钱包文件丢了或者私钥忘记了，还能找回来这笔钱吗？对不起！神仙也帮不了你！这里可没有拿身份证找回这码事，那部分币就永远消失了。其他FAQ：a. 比特币和Q币的差别是什么？请把上面的文章重新读一遍。b. 比特币是一个骗局吗如果看完了还认为比特币和庞氏骗局有什么相似之处，那就当作是骗局好了。c. 比特币有哪些挑战需要面对？大的来说有4点:政府封杀、山寨币、黑客攻击、可能的自身缺陷。d. 如果网络出问题了，比特币不就不能用了吗如果网络出问题了，刷卡也会不能用的。e. 国家禁止怎么办？目前的情况下，国家还没有能力立法禁止一个人在电脑里拥有某个文件，或者禁止你记住某一句话。f. 为什么钱包地址的金额和blockchain上查询的不一致？这也是很多人困惑的地方，其实在钱包里是生成了一批地址，我们看到的只有一个，其它的是用于找零的地址，从钱包支付会自动从多个地址里面挑选最合适金额支付的。如果要用纸钱包或者脑钱包保存，全部转到纸/脑钱包账号上吧。找零具体细节请参考这里：https://en.bitcoin.it/wiki/Changeg. 比特币超越了现有法律是的，一切都该与时俱进，不是么h. 比特币意味着什么网络热炒的所谓升值都是次要的，真正意义在于网络和算法开始尝试接管人类在金融方面的职能，可能对未来的社会架构造成深远影响。建立在足够连接力和计算力上的自底向上力量足以重构社会！i. 比特币有什么缺点吗当然，不过网上谈缺点的文章很多了，用一个货币实验的视角去看待更适合。重要的是思想已经出现。本文摘取了网络上许多的有价值的观点，再加上作者的理解组成，无法一一列举，在此一并感谢！本文另有姊妹篇《为什么要重新发明货币》，欢迎参考。

4、不知道比特币什么时候火起来的，自己一直都没有注意到。当它真的火起来时，发现自己已经玩不起了。索性就不是很关注它了，加上各种负面消息以及不了解，所以不觉得比特币能有什么未来。看完这本书，对“比特币”有了一些了解。这个东西真的很神奇，才出现没有多少年，有谁能说清楚它的未来。而且追根究底这种东西也不是凭空冒出来的，也是在不断的演化着。现在“比特币”还有一些缺点，但是应该不会消失，可能会进化成其它东西。下面的一段内容来自这本书中，描述了比特币未来的形态，感觉很美好。互联网的一些重要资源——例如DNS（域名解析系统）根服务器和云服务器——分布过于集中，展现出中心化的弊端。如果服务器空间变成一种P2P去中心化的全球云，所有网站的内容都可以放在上面而不用担心网站会在一夜之间被关闭。域名系统在Tor里已经实现，而且Tor还采取P2P互联的方式让各个客户端之间相互帮忙传递流量，从而使得网络无法被封锁。Tor和电驴之类的P2P服务都有一个致命的缺陷，即它们对使用者的道德和自觉性要求极高，内建的激励机制并不强，所以大部分人都是用的时候开启客户端，用完就走人，特别是BitTorrent下载，每次充当“种子”的人都要呼吁希望大家留种。但是反观比特币的矿工，根本没有人要求他们购置硬件、消耗电力甚至忍受巨大的散热风扇的噪音，可他们依然踊跃地去做这些事情，就是因为有巨大的物质刺激。如果上面的服务结合比特币的思路，这些服务将会获得翻天覆地的变化：有人会长期挂Tor，因为可以赚Tor币；有人会专门买硬盘阵列来当作“种子”或者做电驴共享，因为可以赚驴币等。直接使用比特币的技术框架来实现这些功能最简单，流通性也最强。

5、2013错过了机遇，那就要把握好2014年，在亚马逊卓越图书http://sina.lt/joyo比特币这本书无旦期间做促销只要5元.....

6、源地址http://yilinhut.com/2013/10/20/4915.html许多人质疑比特币的焦点都在其所谓“通缩”特性：由于比特币总量有限，趋于升值，所以人们都倾向于囤积而不是花出，于是流动性很差，不能成为主流的通行货币。这里还有两个层面，一是时间的，二是空间的。首先，基于货币未来升值的考虑，我们对它的使用可能会尽可能保守，而更少进行投机、投资活动。在这一层面上来说，比特币将减弱所谓“流动性”是必然的，但这未必不是好事，我在之前的一系列文章（如比特币与环保）中都提过，比特币可能扼制资本的盲目扩张和过度投资。当然，人性还是贪婪的，人们仍然会进行投资，只不过会倾向于更节制、更慎重。但这一问题暂时搁在一边，许多人还从另一个层面出发质疑比特币的流动

性，那就是援引所谓劣币驱逐良币的格雷欣法则，认为当某人同时持有比特币和另一个更劣质的货币时，会更倾向于花出劣币，而比特币由于其各种优点，让人们不舍得花出，于是最终无法在市场上通行。这个论点由于援引了所谓格雷欣法则这一不明觉厉的原理而显得煞有其事，但实际是非常牵强的，事实上，格雷欣法则与比特币根本没有关系。所谓格雷欣法则产生于金属铸币时代，用以解释金银币的流通规律。这一法则通过以下两种原理起效：1、面值与市值之别：金银币有国家铸造，并规定了法定的“面值”，比如1块金币相当于15块银币之类。然而，金与银本身亦有市场价格，而市场的比价并不是定死的，而是浮动的，许多时候会与法定比值有系统性的偏差，例如，尽管1金币在面值上相当于15银币，但1金币所含黄金的价值可能相当于20银币所含白银的价值。也就是说，你需要20块银币才能在市场上买到1块黄金，但15块银币就能兑换1块金币。在这个时候，如果我手持金币，凭什么要把它当作法定的货币使用呢？如果我要把金币 用作货币去花销，那么按照法律，它只能相当于15块银币，而我把它化成黄金卖能卖出20块银币，那傻子才会拿金币当钱花呢。于是在这种情况下，金币作为流通货币的流通性就会降低，人们倾向于囤积而不再使用。2、成色优劣之差：另一种情况在只有一种法定铸币的情况也会发生，因为古代的铸币有成色之分，有些货币可能缺了个角，但仍然可以按照其面值计算，甚至许多人都在花出金币前故意切下一角保存。更典型的情况是，国家在鼎盛年间发行质地和成色最佳的钱币，而到后来，铸造的钱币逐渐掺入杂质，工艺也不再讲究，但面值仍然一样。总之，市场上流通的货币中有些是短斤缺两的，另一些是成色十足的，那么当我花钱时，自然就会选择尽快花出那些成色不佳的货币，而留下良币。我们看到，这两种原理归根结底就是说，钱币的“面值”与其“真实的”价值不符。当然，我们有可能对格雷欣法则加以推广，解释一些当代市场中的现象，例如老版1角钱含铝的价值可能高于1角钱，那么它一定会被新版1角钱取代。又例如政府强制绑定本币与外币的兑换比例，但这一比例与市场实情不符时人们可能会大量囤积外币。但如果完全脱离了该法则之所以起效的基本原理，那就不该再套用所谓格雷欣法则来说事了。而比特币与格雷欣法则的适用情形根本沾不上边，甚至比特币的特点恰恰从一开始就消除了格雷欣法则起效的可能性。首先，比特币不是法币，因此，它没有任何外加的“法定面值”；其次，它也没有任何基于质料的内在价值，没有成色问题。它的价值来且仅来自于市场中的自由交换行为。比特币摆脱了中央银行的发行体系，也不再依赖于政府或权威机构来颁行铸币标准。这在许多怀疑者看来是缺乏“政府背书”。但关键恰恰在这里，所谓政府背书究竟是背的什么书？政府从来不保证货币不贬值，从来不保证一块钱永远都能坐一趟公交，也不保证十块钱永远都能值一顿午饭，要保证这些事情，靠的是公交公司或餐馆老板，而不是靠政府背什么书。那么政府保证的是什么呢？要害就是：政府为劣币背书，因此保证了劣币驱逐良币的发生。当实际市场中一枚银币只值一枚金币的1/20时，由于政府的“背书”，一枚银币的面值仍然可以保持有一枚金币的1/10,。这意味着，如果商人偏爱金币，愿意以金币定价，那么他标价1金币的商品，也必须可以以10银币的代价支付。政府的背书保证了劣币的购买力，只收金币而拒收银币的商家将会遭到法律的制裁，因此如果说商人希望用商品换来1金币的价值，就不得不将其定价为2金币，也就是20枚银币。当然，顾客也会不愿意支付2个金币，而是拿出银币来交易。那么我们来考虑一下如果没有政府背书会发生什么：金币和银币之间的比价关系将缺乏一个权威确定的标准，它们的汇率将是根据市场浮动的，如果今天市场的牌价为1枚金币换20枚银币，那么1枚金币就能够换20枚银币，20枚银币也能够换1枚金币，因为市场牌价是由互相平等的交易者自由交易而产生的，它就是实际能够发生的兑换，而不是任何人独断的规定。在这种环境下，有些商家可能喜欢金币，有些商家则更爱好银币，但无论是以金币报价还是以银币报价，情况都差不多。当我报价1金币卖某件商品时，客户可以把他手头的20银币先在市场中兑换到1金币然后来支付，或者我也可以先收入20枚银币然后自己去市场兑换成金币。因为没有政府背书，劣币的概念将不复存在，金币与银币在市场上处于对等的地位。不过一些质疑者可能立即会指出比特币问题的特殊之处，与金币—银币的关系不同，比特币与法币的不对称性更加显著，关键在于，比特币总量恒定，是所谓通缩货币，而法币一般总会不断贬值。但这有关系吗？因为法币不断贬值而能够驱逐其它竞争货币？这听起来就有点荒谬。假设我手头有1个比特币和1万人民币，假设按照当前的市场汇率，它们大致相当——也就是说我可以随时到交易所用1个比特币换1万人民币，或者反之，无非是要支付非常少的利差和手续费而已。那么现在我要去市场买东西，我是更愿意花掉1个比特币呢还是更愿意花掉1万人民币呢？由于我更看好比特币，更愿意囤积比特币，所以答案似乎是显然的，我更愿意花掉1万人民币而把比特币留在手里。但问题在于，既然如此，我为什么不更早就把这些人民币换成比特币呢？如果我早就持有这些人民币，而我又更偏好比特币，那么我可能早就把它们换成比特币了，为什么一定要到今天才来抉择呢？而且由于

交易的便利性，我可以随时，哪怕是在柜台前，通过我的智能手机把人民币卖出换来比特币，因此我更愿意花出哪种货币并不取决于我对两种货币的未来预期，而只取决于当前的市场报价——例如说，商家开出的价格。如果说商家愿意给比特币支付提供哪怕些微的优惠，以抵消我随时把人民币换成比特币时所需额外支出的手续费，那么我就没有理由拒绝这一优惠。比如市场汇率是1比特币换1万元，但商家开出的标价是0.99币或1万元，那么我与其花出1万人民币，还不如把它们先兑成比特币，付款后还多赚回0.01币。那么商家可能给出这样的优惠吗？当然可能。事实上现在许多开通比特币支付的商家往往把汇率定在一个比市场偏高的位置而不是提供优惠，这是因为他们仍然偏爱法币，最终还要以法币结算。但试想如果情况倒过来，他们更偏爱比特币的话，当然可以为比特币支付提供更优惠的价格。在传统的劣币驱逐良币的模式中，商家们当然也是更愿意收入良币的，但在商家和顾客的博弈中，法律压制了商家的主张，令商家无法自由开价。但是现在，商家更容易表达自己的偏好。作为顾客来说，我随时在人民币与比特币之间互相兑换并没有什么关系，但商家的兑换却相对麻烦，例如，如果他收入的是纸币，那么在把这些纸币存入银行之前无法随时兑换成比特币；或者，如果他通过信用卡刷卡机或支付宝之类电子平台收入人民币，往往需要支付另一笔手续费。最终兑换成比特币时商家也得支付一笔手续费。那么如果顾客能够让喜爱囤积比特币的商家免除这些中间环节，那么商家当然乐得提供优惠。而如果在市场中，商家们普遍都偏爱比特币，而顾客们也都偏爱比特币，那么顾客们也就没有理由非得捏着人民币等到用来购物，而不是趁早兑换成比特币了事。到那个时候，人民币唯一优势可能是贷款消费，由于比特币的升值趋势和人民币的贬值趋势，人们可能很难借到比特币但容易借到人民币，因此顾客们可能更愿意选择信用卡透支消费而非使用比特币，哪怕后者有一定优惠而前者要支付额外的利息。但是，在比特币已趋于主流以至于能与法币分庭抗礼的情况下，法币现有的信贷体系势必遭受冲击。例如说，我如果借钱给你，最后得到的本利回馈超不过比特币的升值的话，他为什么要借钱给你而不是换成比特币呢？随着比特币的发展，一旦越来越多的投资者开始以比特币计价，不仅将导致使用比特币的透支变得困难，而是将使得一切投资都变得慎重，一切透支都变得困难。而且，即便是在透支消费中人民币仍占优势，但作为现金的流通方面比特币不会被驱逐。除非到哪一天人们都没现金了，每个人的账户里都是负数，都拿不出钱来买比特币，只能以政府指定的方式透支购买指定商品，那么劣币的驱逐力也许还能发挥一些作用。但这顶多是法币系统走向崩溃的回光返照罢了。总之，所谓劣币驱逐良币并不是市场自然发生的，而是“政府用劣币驱逐良币”的缩略而已，一旦能够摆脱政府的控制，这一劣币法则就会失效，而比特币恰恰是要让货币摆脱政府的控制，而让良币重回市场。若非注明，随轩的文章均为古雷原创。

7、《比特币》号称是关于比特币的第一本书。作者的确比较全面的介绍了比特币的很多方面，从起源到发展前景，以及对公众普遍提出的问题的回答。 这本书对于初识比特币的人来说是一本全面了解比特币的好书。关于比特币的一些特性，我基本上赞同作者的大部分观点。比如去中心化技术的广阔前景、数学比政府更可靠、路径依赖等等。不过对作者的关于51%攻击的观点有一点不太认同。作者提到，如果有一个人或组织（或政府）具有超过全网50%的计算力，那么他应该发现维持现有规则更符合自己的利益。我认为，如果政府组织花了很大力气达到了50%计算力，他很可能担心不久会失去这样的优势。为了长远利益，他更倾向于消灭比特币，以保证法币的地位，从而永久解决发行权的问题。当然，如果是非政府组织，就会如作者所言，宁愿用比特币获利，也不愿意消灭比特币。

8、比特币或许将是21世纪最优秀的发明之一，而在其向全球拓展的过程中，《比特币-一个虚幻而真实的金融世界》一书将成为不仅是中文社区，更是全球比特币社区的引路者。作为中国第一本比特币领域的著作，其作者囊括了中文比特币社区里的八名成员，内容覆盖了比特币的历史、发展及未来的九个关键领域。比特币不仅仅是一种货币，它更是一项开源的去中心化运动，引起了更为广泛的讨论，探讨货币本身所扮演的角色和其使命，以及社会与政府之间的互动。因此，对于个人来说，了解比特币的使命及其迄今为止的大事列表是至关重要的。本书覆盖范围广泛，囊括了比特币的各里程碑事件，包括币值的大幅升跌，海盗党创始人Rick Falkvinge所做的工作，2013年加州圣何塞举行的比特币大会，加州政府与比特币基金会之间的官司纠纷，MtGox交易所与美国政府间的沟通互动，比特币生态圈在德国的迅猛持续的成长，以及比特币在非洲通过Kipochi钱包实现与M-Pesa整合后的发展。而更深远的关注则落在了去中心化支付系统和交易所的未来上。比特币是当今最优秀的加密货币，而其他的支付和交易体系，如莱特币和瑞波币也已崭露头角。《比特币-一个虚幻而真实的金融世界》将目光投向了比特币和其他加密货币的未来，并同时将货币的历史和比特币的特有价值（这一价值远超其法币价格）纳入考量。《比特币-一个虚幻而真实的金融世界》一书将作为催化剂，围绕比特币这一主题

，发起更为深远的对话。比特币及对货币和社区的愿景，令万国万民无论背景，共同工作，相互分享见解。在一个小政府，自由市场以及如比特币生态圈这样的鼓吹自由的环境里，要成事得胜，需对不同性别、不同信仰、不同文化、甚至不同的社会经济形态一视同仁。比特币不仅仅是一种正在成长的电子货币，更是拥有巨大发展潜力的跨文化无国界货币，所有互联网用户都能使用。在全球各比特币群体正迅速成长的今天，我期待能看到中国比特币社区进一步发展壮大。中国比特币社区的潜力非常巨大。而身处全世界最多人口的国度，中国比特币社区将是比特币长期成功的催化剂！我认为《比特币-一个虚幻而真实的金融世界》一书，将进一步令中国及中国以外地区的人们更深入的了解和支持比特币。让我们继续推动其全球范围的成长，令这一了不起的去中心化数字货币为人类所用，使其不仅带来金融领域的进步，更推动言论自由，摆脱中央集权的操控。比特币：解放市场，解放世界
。Elizabeth T. Ploshay比特币基金会董事会成员比特币基金会教育委员会成员《比特币》杂志通讯主管
原文：http://www.8btc.com/elizabeth-bitcoin
9、如果在微博上掀起轩然大波的那篇《中国仍然是中国，比特币依然是比特币》是传销单的话，那么这本《比特币》或可称作传道书。前者逻辑混乱无人信，后者原理精深少人懂。前者谬论哗众吸引无数眼球，后者平和理性然而乏人问津。这样的冰火两重天或许正代表了比特币目前的困境之所在。不是每一位人民币使用者都要精通《货币银行学》，但是若想长期持有比特币却最好能够读透这本《比特币》。"比特币之于我们的吸引力，正如20世纪50年代实验室里的巨型机对麻省理工学子的冲击，70年代车库里的微型机对辍学大学生们所释放的魔力，这种毫无来由的沉迷有一个共同特点，那就是他们都奉行与计算机本身雅致的逻辑相一致的理念——开放、平等、协作、分享，以及不惜一切代价亲自动手改进机器并改善整个世界。"作为国内最早的一批"比特币教徒"，本书作者可谓是钻研最深、信念最坚的那一小撮"使徒"。然而，也正是因为由于对这种"未来货币"的革命性深信不疑，他们过于高估了比特币目前的群众基础。抛开错综复杂的技术性问题，货币的本质就是一种信任。尤其是，比特币这种"看不见、摸不着"的虚拟字符串，人们的信任就是它的生命线。比特币的实质是一种算法，一种基于去中心化、总量恒定的特点而自发产生的社会契约信任。有多少人理解并认可这种算法的精妙、可靠之处，愿意将身家押注其上，比特币的群众基础就有多大。如果说建立在国家信用之上的法币是"赢家全拿"，一次性的。那么，"比特币帝国"的扩张就必须是一个人一个人争取，渐进式地。以基督教为例，如果不是走上层路线，而是完全"去中心化、分布式"地发展，它不可能在两千年时间内占领地球。比特币去中心化的前提就是"人人都是发钞人"，而这种权力的分散要建立在对比特币原理的理解之上，但除了少数极客以外，没有多少人能理解哈希算法和非对称加密，更搞不清楚"矿机"究竟是个什么玩意儿。如果现在就要在法币和比特币之间做一个选择的话，相信算法还是相信政府？答案不言而喻。然而，今年以来比特币行情的"火山喷发"让包括本书作者在内的"信徒"们产生了一种"我们的兄弟遍天下"，"比特币的时代即将到来"的幻觉。"比特币就像是一只贸然闯入的黑天鹅，它不仅废除了被认为是金融智慧最高成就的中央银行制度，还让建立于信用货币基础之上的高度杠杆化的金融金字塔有了崩塌的危险
。"作者的勃勃野心在这段话中表露无遗，几乎要吹响向银行系统冲锋的"集结号"
。"笔者曾在一个比特币的QQ群里担任管理员，群里大部分是刚入门的比特币者，对于比特币的原理一知半解，连中本聪的论文译本都没完整读过。这些人却往往一出手就买上几十上百个比特币，即使按照当时的价格，也相当于人民币几万到几十万元。他们无一例外的对于比特币的未来充满了信心。"很难想像，这些出手阔绰的买家"信心"从何而来，除了"投机"或"洗钱"，我想不出来有什么别的答案。而比特币之所以成为今年最炙手可热的投机工具，除了全球通胀时代天然通缩"商品"的吸引力、媒体大惊小怪的推波助澜之外，更多的是钻了比特币天生特点的空子。市值小、流动性高、7＊24小时交易，使比特币成了"数字时代的郁金香"。而比特币的全球性、不可冻结、不可追踪性又使它成了毒品、枪支等地下交易的首选中介。央行铁腕的骤然收紧也只是为了打击投机和非法交易，而不是一些比特币分子一厢情愿理解的"受到威胁后的反击"。如果说法币能够找到维持币值稳定的"锚"，那么比特币目前还只能随着央行态度、媒体风向暴涨暴跌，除非比特币一统"现实、虚拟两道"，不再需要和法币、其他虚拟货币兑换，否则"锚在哪里"将一直成为它的"阿喀琉斯之踵"。比特币拥护者一直引以为豪的"铸币税"为零恐怕也站不住脚。根据中本聪的"天才"构想，“ 挖矿来获得比特币 ”的目的是通过这些计算来确保比特币的正常交易并

防止重复支付。挖矿的关键动作不是挖而是维护，产出比特币只是一个副产品而已，仅仅是为了奖励那些为维护比特币金融系统做出贡献的人。本书作者将挖矿工比作银行业中印钞工和保安，但问题在于比特币"印钞工"印出来的所有"钞票"都进了自己的口袋。而普通人只能够用产品来换取"钞票"，在人人都成为"挖矿工"早已不现实的情况下，这难道不是另一种"铸币税"吗？如果说法币系统是国家垄断之上的人人平等，那么比特币系统就是"按照进场先后收益递减"的人人不平等。作者曾经在书中比较了银行业和比特币系统的维护成本，在挖矿难度越来越高，矿机"军备竞赛"变本加厉的情况下，比特币系统的维护成本只会越来越高，2100万枚全部挖出来之后，"矿工"们依然需要穷兵赎武地挖矿，那时候这笔巨额成本就要分摊到每一笔交易之上。而在银行系统基础上升级改造的互联网金融成本则会越来越低。目前，每一笔比特币交易都需要等待6个数据块的完全确认，耗时一个小时，这使得它几乎不可能用于陌生人之间的小额交易。如果要解决这个问题，只有引入第三方进行"链外交易"，也就会因此产生中介费用。依此类推，随着比特币使用者的几何级数增加，各种金融中介也会越来越多。到最后，除了物理成本的节省，比特币系统的成本或许将与银行体系持平。而且，银行业也可以渐渐告别物理货币而转向电子货币，只要电子支付的便利性能够媲美目前的纸币系统。"轮子只能发明一次"，作者对于莱特币、狗狗币这样跟风而上的"山寨币"并不担心，它们目前的算法水平还都不能和比特币相提并论，也没有能够威胁到比特币的创新之处。即使这些"山寨"难成大器，但一拥而上把水搅浑之后，比特币的软肋将一览无遗地暴露在公众面前。他们难以区分不同算法之间的微妙差别，只会把它们一视同仁地视为"任何人都可以巧立名目制造的数字玩具"。不过，这样对比特币的发展未尝不是一件好事。当投机大军呼啸而去，盲目入市者自动或被迫离场，比特币泡沫慢慢消退，不用再承受超出其当前价值的关注，退回到它原来的地方，退回到一小撮理想主义者的金融实验。欢迎关注微信公众账号：财经评书，热门财经图书、畅销职场小说、经典经济著作，提取书里精华，用文字和声音将书中智慧一网打尽。让你在碎片时间也能“读完”一本本好书。

10、听了作者的细致阐述 大致了解了比特币的运行规则 但很多计算机网络技术方面的说法不是很懂 因为有些不懂 所以产生一些不信任 个人认为 它是一个超时代的产物 。 比特币本身有些电子化的金本位意识 只是本身不再具有价值属性 这种突破却看不出有何重大的意义 金本位的退出似乎最大的原因是囿于流通性能低下吧 所以现代货币体系就足以应付 。作者说它还能有效避免通货膨胀 我觉得说服力不够 纸币的滥发固然能导致通货膨胀 但比特币如果可以被无下限地分割成多个单元 跟纸币滥发的效果不是一样的嘛？ 作者一直强调比特币的最大优点是去中心化 可是一旦去中心化过后人们凭什么对他有足够的信心呢 何况你说的一些强大的算法支撑以及p2p技术绝大部分人是不懂的 。经济发展到一定阶段 金融势必会对货币翻云覆雨 而这一切如果完全去中心化 信马由缰 肆意发展 得不到一点点的监管或者控制 必然会为少数人控制 。作者口口声声说政府无力打击它更没有打击它的动机 可是对于银行这类金融机构呢 一旦他们的法币业务被比特币金融一口一口吃掉 他们还能坐得住吗 势必殊死一搏吧 而他们又轻易掌握政策性优势。 另外 全球商业还远没有成熟到全部交易都电子化吧 如果作为一种全球通用度量衡 又觉得没必要 。 比特币更像是一支充满噱头的概念股 貌似新颖 通过买卖决定价值 而非本身具有价值大家才去买卖。（ 本人不是学经济学的 不揣浅薄 望观者不吝赐教）

11、关于作者通货紧缩（deflation）部分解释，我不能赞同，我认为：一、无限分割，即使可以做到，也只是影响比特币的计价单位，如百元、元、角、分等，并不会改变一个单位比特币的购买力，所以也不会解决通货紧缩问题。二、预期电子产品会降价但依旧现在购买，与通货紧缩毫无关系。通货紧缩是指decrease in the general price level of goods and services，是general而不是某些产品。三、说作者说“稳定的通货紧缩只会发生在无弹性货币体系中，比如黄金、比特币，通货紧缩非但不会破坏经济，反而会促进经济发展。”，十分不认同。（或许我该补充不认同理由？关于通货紧缩，是不是可以这样理解：？首先，看比特币的设计（没读过原文。。），把解决通货紧缩寄希望于流通速度，似乎不大可能。。其次，寄希望于货币供应量，比特币总量是固定的，似乎也不太可能。（喂喂。。但是，只是比特币的总量固定，而不是货币的总量固定。鉴于比特币是开源的，可以诞生大类的“山寨币”。大量“山寨币”可以以一定的比例与比特币兑换，从而增大货币供给量，由此避免通货紧缩。最后，为什么要设置固定总量而不是，固定的增长率，比如5%之类的。这样就可以很容易的避免通货紧缩，也可以使大家形成很好的通胀预期。我认为，原因可能是，设置总量固定，可以为“山寨币”的生存

和生长提供空间，从而在各种货币之间可以形成竞争。这才是奥地利经济学观点？哈耶克的去中心化是建立在竞争机制的基础上的。比特币更多的被强调了它的技术以及去中心化，而被忽视了其开源以及总量固定带来的货币之间的竞争。竞争是一种很好的约束，“山寨币”之间，以及“山寨币”与比特币之间的竞争是必需的。欢迎反驳。
12、“很多人以为我疯了，但我的看法是，只有相信逻辑的力量，才能活在未来。”【《中国企业家》注】四川芦山县“4·20”7.0级强烈地震发生后，灾区收到了各种各样的捐赠物，其中最奇怪的是公益组织壹基金收到的230多枚比特币捐款。李笑来，原新东方托福名师，号称是中国拥有比特币最多的人。比特币在过去一个多月里吸引了足够多的眼球，从3月10日到4月10日短短一个月的时间里，它的汇率从1比特币兑换46美元暴涨至230美元，让投资者大呼刺激。4月11日凌晨，在比特币位于230美元高位时，李笑来警告大家：“这一轮疯涨有结束迹象……投机的见好就收，跑吧。”之后比特币一路狂泻，最低时跌至54美元，随后李笑来又不慌不忙标价60美元挂单抄底。他认为，“比特币汇率大幅波动是因为人们用几千年积累下来的货币经验对付这种年轻的货币。”比特币到底是“电子黄金”还是“疯子骗傻子”的游戏？点击进入下一页这个世界上最危险的东西，当然也是最有价值的东西，不是子弹、不是暴力，而是思想。人类历史无数次证明了这是一条真理，今天我们讨论的比特币其实就是一种思想。我先来说说比特币的历史。其实比特币的出现颇具神秘色彩。2008年，有一个域名bitcoin.org被静悄悄匿名注册成功。同年10月31日，有一篇名为《比特币：P2P电子货币系统》的论文被发表在某个网站上；10天之后，开源社区sourceforge.net上出现了一个叫bitcoin的项目，这就是比特币的起源。这个项目的创造者究竟是谁没有人知道。开发者只留下了一个中田聪（Satoshi Nakamoto）的名字，他在搭建完比特币体系后就从互联网上彻底消失了。此后项目由两个前Google工程师维护，但即便是他们俩也声称从未见过中田聪。有人说中田聪是从未来坐着时间机器来到现在写了这个程序的。比特币不单单是一种电子货币，它背后是P2P思想。P2P的意思就是点对点（peer to peer），它从诞生之日起就成为一种颠覆性的技术，过去当我们要下载一个文件，必须连接到一个中心服务器。但这一过程效率很低，因为整个网络上只有一个下载服务器。但是P2P技术让客户端变成服务器，边下载边上传，这一下就出现了无数服务器，于是下载速度瞬间就提升了，当今世界上96%的流量都是P2P流量。比特币代表的P2P思想是更加强大的。原因是它遵循一系列的协议。人与人之间遵循协议是很难的，往往是谁嗓门大、谁手里有枪就听谁的，但机器遵循协议却是一件非常简单的事情。从一开始，比特币就是真正的货币——只不过大多数人并不相信而已。可大多数人的疑虑重重在过去三年多的时间里并没有阻止比特币成为互联网上最有影响力的货币；而放眼将来，也无法阻止它最终成为地球上最有影响力货币之一。回想我第一次见到比特币时的心情只能用震惊来形容。2011年1月，比特币价格超过了1美元，我就是从那个时候开始知道比特币的。大概两个星期后，我在《连线》杂志上看到了一篇详细报道，当时我就震惊了——一个被人们称作游戏币的东西，竟然比世界上最主流的货币还贵。于是我开始做功课，我把中田聪那篇论文找来看了好多遍。这时候一个比特币价值已不是1美元而是6美元了。我决定卖掉一部分美股，购买2100个比特币，毫不犹豫。当时的想法很简单：因为根据协议比特币总发行量只能是2100万个，而我居然可以拥有这个经济规模的万分之一，这实在太酷了。买完后就不停地涨。后来涨到25-26美元的时候，我决定开始“挖矿”。“挖矿”就是用电脑生产比特币，需要用特殊显卡支撑强大计算能力。这么贵的显卡并不好找，我几乎跑遍了全国才搜罗到了我需要的显卡。当时很多人都觉得我疯了。我后来还去见了一些风险投资人，建议他们投资建立比特币交易所，可这些见多识广的投资人也觉得我疯了。实际上还有比我更疯狂的——瑞典海盗党创始人Rickard Falkvinge。此人早在2011年就宣布将自己所有的财产都换成了比特币，这还不够，他还借了很多钱大量囤积比特币——知道地球上也有这样真正的疯子存在，让我感觉舒服多了。2011年6月，在朋友帮助下，我在天津和北京交界处建了一个“矿场”：一共46张显卡，装成23台机器，放在一个定制集装箱里，需要两万瓦以上供电功率……当时的耗资相当于一辆奥迪Q5的价格。资金来自于我过去三个月里从比特币上的获利。原本的计划是在2012年11月，一半比特币发行完毕之前，通过“挖矿”获得更多的比特币。可是，这个当时可能是亚洲最大的矿场并没有给我带来多少收益，甚至是一场灾难。因为供电不稳定，断电之后，别说远程管理了，远程启动都不可能，动不动那些显卡就闲置两周甚至更久，然后修复后两天内又挂掉。几个月后，我不得不以1/5不到的价格处理掉了那些硬件。实在不甘心的我，只好不断买卖——当然，更多时候是在买入，买到买不动了为止。经过很多轮买卖，又恰逢大幅度跌荡，最终我获得了通过挖矿根本不可能获得的数量。在2011年底，比特币仅占我个人资产四分之一，现在已是我现实资产的30倍。历史一次又一次地证明，害怕新生事物是人类的习惯。当

我们的话题深入到一定阶段后，就不仅仅需要智商了，还需要勇气。其实目前关于比特币的任何信息都是公开的，因为它本身就是开源的，连每行代码都是公开的。但是仍然有很多人对它充满恐惧。由于比特币是个新生物，最广泛的说法就是比特币最适合用来洗钱，但是比特币汇率波动这么大，今天你有100万，明天就变成50万，洗钱你受得了吗？说匿名货币可以买毒品，买毒品要有地址的，卖毒品的爽了，不用承担责任，但买毒品的写假名字也收不到啊。而纸币本来就是匿名的，随意谱写钞票本来就是违法的，你兜里的钞票写名字吗？政府就是要求钞票匿名的；至于安全问题，美元安全吗？可能放地下挖不出来了，起火烧掉了，被洗衣机卷了……所以解决安全问题从来不是货币的任务。还有人问：“比特币真的有价值吗？”其实，一种货币是否有价值只取决于有没有人愿意使用它买卖。谁说“金本位”就是由黄金支持货币了？准确地讲，是公众相信政府用等价值的黄金在支持货币。注意，是“相信”而已——事实上，政府究竟有没有做到，谁都不知道——有人知道了也不告诉公众而已。而实际上，政府用黄金担保并不可靠，因为政府总是可以偷偷加印货币。而且所有纸币本身就是虚拟的——纸币本身没有价值，它“代表”一个价值数额。我们之所以姑且相信银行，是因为我们不得不相信。然而，比特币不一样，所有使用比特币的人自愿相信。我坚信“自愿的信任”远比“被迫的信任”更有价值。所以我相信比特币比我见过的任何纸币都更真实。最重要的是，当我反复研读中田聪的论文之后，我得出了一个结论，比特币最重要的革新是它是一种“通缩货币”——它只发行2100万个。通胀货币只能不断贬值，而通缩货币，只能不断增值。此外比特币通过P2P，用去中心化的方法解决了多重支付的问题。数字化货币不是比特币的创新，当银行存在的那一瞬间，货币就数字化了。但当银行可以转账时，就有多重支付的问题了。最明显的就是支票诈骗，无论法律多完善都预防不了，一个人可以拿着100万同时和十几家商户签合同，但是钱只能支付一次，这样一来很多人就受骗了，比特币就不存在这个问题。而现实生活中已经有大量的人愿意收取比特币作为报酬。又由于已经有很多人愿意用传统货币购买比特币，所以比特币已有相应的汇率存在，也早已有人提供买卖比特币的服务。这次芦山地震，我就组织了一次比特币捐款，一共募集了34.5461个比特币，按照募捐期间最高的汇率，167美元，并补上零头，共计33000元人民币。我没有将这笔钱交给任何组织，正在寻求一个方式，将钱直接交给某个受益方。比特币会不会消亡？我的看法是，很难。这东西一旦启动了，就关闭不了。当我们回顾历史会发现，P2P网络自从启用就没有被关掉过，有些网站可能会倒掉，但是种子文件存在于那里，早晚会被下载得到。我深知P2P的威力，一切P2P网络都如此：一旦启动，就无法阻止。所以P2P是一种时代潮流，是无法更改的。历史无数次证明，个体力量变得越来越强大，也将变得越来越独立。比特币最大的意义在于，这是人类史上第一次，从技术层面上彻底、纯粹地保证了“私人财产不可侵犯”。我想我之所以能坚持到现在，是因为我并没有把比特币当作钱，而是把它当作一个美丽的主意，一个伟大的社会实验，可以每天做思考，做验证，其乐无穷。我是一个自由主义者，也是一个未来主义者。我的看法是：只有相信逻辑的力量，才能活在未来。比特币（Bitcoin）是一种由开源的P2P软件产生的电子货币。比特币不依靠特定货币机构发行，它通过特定算法的大量计算产生，比特币经济使用整个P2P网络中众多节点构成的分布式数据库来确认并记录所有的交易行为。P2P的去中心化特性与算法本身可以确保无法通过大量制造比特币来人为操控币值。

13、本文比特人2013年度征文活动的参赛原创作品，首发于比特人论坛，因此没有在博客首发。本以为评奖没戏了，于是昨晚顺手在博客上发了，没想到还是得到了第二名的大奖，因为提前半天转载（到了巴比特），我已自愿扣除奖金10%作为惩罚，在此对比特人网站表示歉意和感谢。1.比特币浪费资源？比特币的工作量证明机制，也就是所谓的“挖矿”，经常被人诟病：那么多机器全力运转，耗费大量能源而什么都不产出，仅仅为了维持比特币网络的安全运行而已。这么多“白白浪费”掉的能源岂不是意味着比特币是很不环保的？许多人都认为这是一个大问题，例如Sunny King在比特币的基础上开发出的新币种PPC，就旨在解决比特币的耗能问题。诚然，在耗能方面，PPC的确比比特币更加节约，但也有另一些代价，PPC为了减少能耗而作出的某些改变未必是好事，但在这里我不想深入分析PPC和比特币的优劣得失，这已经是另一个层面的问题了。首先，我们要看看比特币的“能耗”究竟是否是一个致命的问题，在这个问题上，作为对比的首先应该是传统货币，而不是作为衍生的同门密码学货币。相比于传统的货币体系而言，比特币的能耗非但不是其致命伤，而且可以说是非常节约了。比特币的能耗看似巨大，但它维持了整个比特币网络的运行，货币的发行和交易都由这一网络支持。不需要印钞机造币厂，不需要中央银行和各级银行体系，也不需要复杂的国际汇兑系统。光是一家“中国印钞造币总公司”，就“下辖22个大中型企业和1个国家级技术中心，拥有员工近3万人，净资产总额300亿元。”这些大中型企业及其员工的每天要耗多少电？“中国人民银行”一年的支出就

在百亿级（而现在比特币的总币值都没那么多），光是三公经费中的公车开销就达到3亿。如果把全世界的印钞厂和央行都加起来，还不算各级地方银行和汇兑业务，维持传统货币的交易体系究竟要耗多少能源和资源？如果说比特币挖矿机空耗能源啥都不生产，那么央行又生产了什么呢？当然，比特币网络目前还处于新生阶段，直接与成熟的央行系统相比较也是不公平的。随着比特币的发展，其能耗恐怕还会提升几个量级，也会出现一些衍生机构造成额外的消耗。但无论如何，比起庞大而臃肿的传统货币体系，总是小巫见大巫了。比特币的新币产出每四年减半，用不到等百年后新币产尽，十几二十年后，新币在挖矿中的份额就将变得很小，挖矿的收入将主要由交易费构成，而每一笔交易费都是每一个交易者为了自己的交易更快得到验证而自愿支付给矿工的。于是，挖矿的能耗始终不是无限的，而是在市场自发平衡中得到限制的——挖矿的耗能不会长期超过挖矿的收入，否则矿工不会开动机器；挖矿的收入主要来自交易者额外支付的交易费，而这些交易费都是交易者觉得为了让这笔交易得到验证而值得付出的费用。交易者们认为为了验证交易值得付出多少额外消耗，矿工就会投入相应的能源去开采。总之，比特币网络的所有消耗最终将趋近于合理的市场价。但是在传统货币体系中，维持系统的代价并不是市场自发平衡的结果，相反，总是央行通过其垄断的权力试图用其货币政策去调节市场，央行总希望自己成为市场平衡的原因而非结果，央行的存在是一个超越市场的，天经地义的东西，市场无条件地供养着央行，它的消耗或浪费根本没有限制。2.环保不止是节能我们说比特币系统比传统的货币体系更节能，但这并不就意味着比特币更“环保”，究竟什么是“环保”，还有待追究，至少，环保不止是节能的问题。甚至“节约能源”也未必是更环保的。例如节约用水，一定更加环保吗？这还得看具体的情况。例如我从河里打三桶水回来洗个澡，你就用一桶水就能洗澡洗衣服拖地，那么你是比我节约，但最终水都还得流回河里去。我用完的这三桶水对河水造成的污染未必比你的一桶水更多，甚至我对环境的影响可能更加温和。除非我要去截取整条河流，而你只截流三分之一，那么或许你更环保一些。但人们之所以要截取整条河流，却也是出于某种节约的心态：河水滔滔逝去，大量的能源白白流逝，开发水电站把这些白白浪费的能源利用起来，岂不是更节约吗？这似乎也挺有道理，很多人都持有这样的看法：水电站是清洁能 源，有利环保，所以要多造水电站。但多造一处水电站，就一定会少建一座火电站吗？事实绝非如此，多造一座水电站的结果往往只是促使水电站周围多建几个矿场、化工厂而已。如果说比特币耗能是白白浪费，那么这些能源拿去炼钢就一定不是浪费了吗？因为这些钢材很有用？但它们将要用在哪里？用在了（比如说）大举的建设、开辟大量新城、新楼，新工业园区、新矿场、新电站、新炼钢厂……如此循环，不断扩张。但说到底这些建设活动又是不是浪费呢？你或许要说：这些建设满足了人们的需求，所以都是有用的。但人的许多需求本身也是在相应的技术、文化环境中被培育出来的，大量的建设和生产不会填补并减轻人们的需求，反而不断刺激着新需求的产生。而需求的更新一方面可以说是进步的标志，但另一方面，如果欲求陷入无节制的膨胀，就正是环境危机的根源。其实古老的生活方式经常是更加“浪费”的，而现代人以效率的逻辑衡量万物，把一切自然物看作有待利用的资源，榨干一切可以产生效益的东西而不留余地，每一项资源都必须产生效益，这种文化倾向本身恰是环境问题的根源之一。当然我也不是说只有现代人特别糟而古代人很环保，古代人同样也会造成环境破坏，许多文明都毁于生态灾难。但唯独到现代，环境问题变成了一个全球的、全局的问题，不再只是一些具体的，可以明确定位其前因后果的问题，也不再只是影响一时一地一部分人的问题。因此任何具体的举措，节约也好，治污也好，在某些局部问题上造成缓解的同时，也许在更大的层面上反而加剧了问题。3.专制和放任都无法解决问题既然环境问题是一个全局的问题，是否必须一个掌控全局的权力，比如世界政府，来协调控制，才能应对环境问题呢？显然不是这样的。当然，有些专制独裁政体，比如朝鲜，由于拖慢了工业化进程，或许真能减缓环境灾难的发生，但这一政体的存在本身就是一场灾难。更不用说有些专制政体，例如苏联和天朝，更是成为奔向环境灾难的急先锋。但是不是像许多乐观主义者所认为的那样，完全放任自由的市场经济，就可以避免环境灾难了呢？那也未必。自由市场对环境灾难的扼制方式主要有两条：一是产权明晰，二是市场竞争。如果说这座山这片河都是公家的，权责不明，大家都事不关己地尽情污染，出现问题时也互相扯皮，这样的确很糟糕，而如果这些土地和河流都是有具体的私人或企业所有的，那么他们就更愿意对其尽心照管，而其他利用或破坏这些私有资源的人也将有明确的谈判对象。这种明晰产权的做法被证明是利于环保活动的开展的，甚至中国也有些地方开始引入这种模式来治理污染了。但私产制也并不是万能的，我们很熟悉所谓“囚徒困境”、“公地危机”等寓言，也就是说在许多情形下，每一个私人都出于个体利益最大化的考虑而做出的决策，在整体看来可能是最糟的情况。另一方面，许多环境问题是全局性而非地方性的，且不说臭氧空洞和全球变暖这样的大问题，

光说一条河流，其上游、下游和支流等等都是互相牵扯的，上游的截流或排污将会直接影响下游的生态，更不用说许多难以精确测定的间接影响。自然环境之间互相牵扯影响的复杂性总是要高于个体和公司互相关联牵扯的复杂性，一些能够具体定位出破坏者和受害者的环境问题当然会在私产制下得到更好的化解，但更多难以定位出破坏者，甚至难以确定受害者的问题则仍然难以解决。再说市场竞争机制，比如能源短缺了，能源就会涨价，如果涨到一定程度，自然就会激励人们去开发和研究新的替代能源。现在替代能源成本还较高，所以难以推行，但依靠市场机制，等到传统能源真的濒临枯竭的时候，自然能够找出替代的办法。污染和环境破坏也会造成生活成本的提高，等到生活成本高到一定程度，自然会激励人们去治理……总之许多乐观者相信市场能够自发地调整好一切。比特币的拥趸们基本上不会支持专制制度，大多都是自由市场的支持者，包括我在内。但支持自由市场并不意味着迷信市场的力量，市场之手终究不是上帝之手。要害还是在于，环境问题是一个全局性的问题，而且许多环境破坏都是积累性的、不可逆的。环境灾难往往在无法预知的情况下，以无可转圜的方式发生，事到临头再自发调节也许太晚了。例如复活节岛的生态灾难是一个很好的例子，岛民们砍伐树木用作滚动装置来搬运石料和石像（相当于把滚木当作消耗的能源），等到岛上的树林被开采殆尽，石像的筑造工程当然要搁置了，但树林并不会很快恢复原样，相反，树林破坏造成水源流失、生物灭绝，最终整座岛变得无比贫瘠，岛民们自相残杀，最后文明失落复归野蛮——以至于西方人发现这座岛时还以为那些巨大的石像是外星人的杰作。要注意，森林破坏导致物种灭绝和环境灾难这一连串过程是缓慢的，在此过程中滚木的成本并不会显著地提高，岛民也没有足够的科技以预测危机，一旦发现危机，就已经到了无力逆转的境地了。事实上，类似这样的局部的生态灾难造成文明毁灭的情况在历史中经常发生，但不同的是，以前的生态危机都是局部的，一个岛的文明毁灭了，其它岛也许发展了起来，最后总有些文明幸存下来。但如果说复活节岛之于当时的岛民，就如同整个地球之于我们现代人，这个生存的环境如果遇到了全局性的、不可逆的生态灾难，我们可就无处可逃了。有人会说，那些古代文明之所以自取灭亡了，正是因为他们没有现代科技和市场经济等等，而现代西方文明终于找到了生存的诀窍，所以不再会面临这样的灾难了。我当然愿意相信这一点，但何以证明这一点呢？我们能看到的只是人类的力量日趋强大，发展速度日新月异。但力量越大、只能意味着一旦碰壁，遭到的打击也越大，速度越快，意味着在危机面前越难以刹车。何以保证我们一定能在致命的全局性危机发生之前总能够及时规避呢？我看到的一种最可笑的论证是：迄今为止的发展成就足以给与我们信心，但这就好比说“我从前没死过，这证明我将来不会死”，或者“前十八年年年都长高，于是我们可以预计将来也每年都会长高”。4.市场经济的文化背景总之，无论是专制还是放任，计划经济还是自由市场，都无法让我们在环境危机面前高枕无忧。但难道比特币就能解决问题了吗？当然，也不能，没有任何一劳永逸地规避危机的手段。但我相信，比特币能够有好的影响，而且这种影响是全局性的。比特币将首先影响经济环境和文化环境，而经济、文化环境的改变最终将影响人与自然环境的关系。无论是科技还是经济，它们也都不是完全独立的系统，市场环境总会与技术环境和文化环境相互影响。“理性经济人”的设定只是一个抽象的幻想，而从来没有真实存在。真实的市场参与者并不总是以趋利的效用逻辑来行事的，人们文化、信仰和思想的倾向也将决定市场的走向。每一个个体都有自己的主观好恶，个人的偏向聚集在一起时不会完全抵消，而是会呈现出某些特定的“时代精神”、“时尚”、“风气”之类的全局性偏向。这些文化偏向不能简单地视作市场经济系统中的噪音或干扰元素，而是应当视作市场经济之上的一个更大的时代背景。例如汽车市场中，有些车明明性价比更高，但因为中国普遍的反日文化，就可能滞销。转基因、有机食品等标签也会左右人们的选择，更不用说奢侈品、装饰品等“无用”的商品的价值完全取决于消费者的文化偏好。那么如果“环保”成为一种流行的文化偏好，环保的观念和风尚深入人心，那么我们完全可以想象，环保的逻辑可能在一定程度上超越效用逻辑，对经济系统产生某种全局性的影响——这种全局影响并不需要诉诸一个中心化的专制机构，而是借助于同样是自由开放的文化交流。那么如果比特币能够促进一种更环保的文化或生活习惯，那么它当然能促进整个经济环境朝向更环保的方向扭转。我们说决定市场关系的不仅仅是效用逻辑，也就是说人们在选择商品时不只是考虑“成本—收益率”，更会带入各种文化、时尚乃至信仰的衡量。而仅就“成本—收益”这一衡量方式而言，也并不是单纯、客观的。冷漠的人可以不理会反日或反任何什么的情绪，不被各种忽悠和渲染蒙蔽，只带着效益逻辑参与市场，但我们仍然要问：他以什么衡量效益？人们以金钱来衡量成本和收益。且不论这种拜金主义是否狭隘，我们先要问：哪种金钱？金钱从来不是脱离于时代和文化的某种外在标尺，金钱也是市场的一部分，本质上也是一种商品。而不同形式的金钱所蕴含的文化倾向也是不同的。例如，同样用效益逻辑来衡量：眼前的80块和五年

后的100块哪个更值？如果你说的是人民币或美元，我会更倾向于选择前者，如果你说的是津巴布韦元，我必须肯定选前者，而如果你说的是比特币，我就更可能选择后者。这样的倾向当然会直接影响我生产和消费方面的决策。我在“比特币：常识与教条”一文中已经讲过了，通胀货币鼓励提前消费，鼓励寅吃卯粮的生活方式，从普通人到一国政府，大家都以借新钱还旧债为日常状态。借贷如此容易的确能够大大促进创业者前期扩张圈地的速度，但同时也把扩张的逻辑固化为一种文化定势。就个人来说，就是只顾眼前，朝生暮死地享受当下，而缺乏长远眼光；就国家来说，就是刺激其侵略性、扩张性的方面，例如金本位的崩溃恰是第一次世界大战以及越南战争的后果（而根本不是因为许多经济学忽悠我们的所谓通缩之类的本质缺陷），现在战争预期也仍然与通胀预期直接关联（美国作势要打叙利亚时国际市场什么反应？）；而就全人类来说，通胀逻辑的后果就是面对自然界的扩张态度——先污染、后治理，先发展起来，能源问题生态问题到时候总会解决的。我们倾向于先透支环境，把治理的责任留给后世，这种风范与借新钱还旧债的通胀逻辑是完全一致的。当然，如果能始终像现在这样，经济不断加速发展，科技不断加速进步，而市场环境或自然环境不发生任何超出预料的剧烈变化，那么这种借新钱还旧债的循环就始终能够持续下去。但问题在于，越是持续下去，我们就越是不知道如何才能够停下，一旦发展遭遇瓶颈或阻滞，新仇旧债一并涌上来时，我们可能没有任何办法。如果问题只是局部的，比如塞浦路斯，那么也许好解决，专制者一声令下直接在银行账户中增添或抹掉几个零就缓解了。局部的生态灾难也可能通过移民、殖民、或者干脆靠死一批人来解决。但全局性的灾难呢？如果美元体系的货币生态发生了全局性的崩溃，我们或许还能指望推倒重来，比特币来拯救世界。但如果地球生态系统全面崩溃，难道整个人类文明都要推倒重来吗？而比特币带有的倾向，鼓励人们更慎重地持币——这并不会造成主流经济学家闻之色变的通缩危机，通缩这一概念本来就是通胀逻辑下的副产品，因为整个文化习惯了通胀，一时的停滞才成为一个严峻的问题。就好比吸毒者时而会遇到毒品不足的状态，而只有在这个状态下吸毒者才会感到不适，而在他所以为的“正常状态”，亦即毒品供应充足的状态下，他是完全舒适的，因此人们误以为问题出在毒品不足的状态，而不明白这一不适状态恰恰是被误认为正常的“舒适状态”的必然后果。吸毒者只会恐惧毒品不足，正如通胀文化只会恐惧通货不足。比特币并不会让人永远不把钱花出去，而是促使人们花钱和借钱都更为慎重，眼光更加长远。这当然可能在表面上减缓某些产业的扩张速度，例如神木的集资挖煤就不可能那么疯狂，鄂尔多斯的造城运动也不会那么迅速，但总体来说，庄重而长远的眼光不会是坏事，比特币不会真正阻碍发展，而是让发展以更稳定、更扎实、更环保的方式推进。5.自大与迷信——环境危机的根源在这里，比特币不仅是以间接的文化感染的方式促进环保，而且，更在某种意义上直指环境危机的根源：人类的自大与迷信。事实上“环保”这一概念本身就体现着人类的自大——我们要保护环境、保护大自然、保护地球……但地球难道是需要我们保护的吗？哪怕人类全死绝了，地球还是照转，新的生态系统早晚还会生机勃勃地繁衍起来。不是我们保护着环境，而是环境保护着我们。而现代人似乎取代了上帝的位置，自以为是地承担起了照管万物的职责了。人们自觉不自觉地相信：人类的科技，人类的力量，能够掌控一切。即便现在不能控制的部分，将来早晚都会有办法控制——这就是人们对待自然环境的态度，同时也是人们看待市场环境的态度。科学家和工程师们自以为他们在保护着自然环境，而经济学家和金融家们则自以为他们在保护着市场环境。美联储、各国央行为了维护市场的健康、稳定，需要不断地刺激、调整、计划、指引，精密地操控着一切。然而，市场真的需要人们控制和保护吗？人们又真的能够成功地维持市场稳定吗？是生态平衡保护着我们的生活而不是我们保护着生态平衡，是市场保障着我们的经济生活而不是我们在维系着市场平衡。无论是中苏的“计划经济”，还是欧美的“前瞻指引”，人们总相信科学的力量不仅能够掌握市场的走势，还能在任何变化下应对自如。但这是自大，而且是个迷信。人类的能力永远是有限的，当人的力量不断增强时，人的行动所激起的动荡和反应也就越大，当市场的领地拓宽时，其所面临的不可预知的边界事件也就越多。人永远总是活在“环境”之内，而不能活在环境之上去支配整个环境。比特币能“保护环境”吗？能控制环境的未来吗？不能。但它有助于消解人们的自大和迷信——它要消灭央行，打消人们”那些英明神武的经济学家能够保护市场、控制一切变数“的迷信。所谓“天有不测风云”，“自然”的本质就在于它总是某种外在于人类的自行其是的力量，人类的知识总有其边界，求知的事业与其说是为了消除知识的边界，不如说只是为了不断地拓宽它。人们在不断地拓宽自己的生存环境，但永远活不到环境外面。因此无论在什么环境下，”节制“、”未雨绸缪“的策略总是需要的，我们要发展，但也总要”留有余地“。在经济生活中，人们”留有存款“就是一种”留有余地“的自我节制。这并不能让我们预知并规避所有的”不测风云“，但至少能让我们不至于跑得太快而难以转身、在危机临

头时陷得太深、摔得太惨。若非注明，随轩的文章均为古雯原创。
14、基于个人对新事物好奇，总想着去了解一些。所以买了这本书，想要好好了解一下。刚开始的地方觉得写的还很不错，我也确实知道了比特币的起源、是什么、怎么用、未来的发展前景等基本概念。但是越往下翻下去，内容重复的越多。一个概念、一个理论作者很喜欢翻过来倒过去的苦口婆心的讲述。于是就在没耐心仔细看下去，而是简阅了而已。并且，先撇开这本书的内容怎样不谈，从读卷首开始，一个疑问一直伴随着我到写书评为止都挥之不去。“ 对于国家税收占财政收入95%的中国来说，这个比特币的腾空而出恐怕是一个噩梦吧！ ”如果说比特币的去中心化思想得以成功推行，那么消费者应该是雀跃声高涨不下，不用交税了，任何商品、任何服务。海淘也无需交关税了。更加省钱也便捷了。也不存在汇率风险了，任何国家之间的交易活动会变得异常的稳定。不知那时国家会将财政收入的结构作何调整以适应那样的社会。并且如果这样的一天的真的到来的话，恐怕我们国民的素质、整个社会的信用体系都会有令人惊讶的改善吧。那我就期待一下！正如相机胶卷的逐渐消退一样，并不意味着这个行业从此消失不再、破产了而已，更是一种时代变迁引起的强制性变革的体现。只有不断地变革、创新才会继续前进。这个道理不仅仅适用于企业、机构，更适用于国家、社会。更更是说给我自己的。

《比特币》

章节试读

1、《比特币》的笔记-第1页

我们的世界因哲学、政治、宗教、文化和语言之限而分隔，却因交易的愿望而合为一体。这愿望是终极的人类社会契约，赋予我们学习、合作及竞争的共同动力。
==========

他认为创业公司可以在虚拟钱包、汇兑和支付3个领域大展拳脚： 1.虚拟钱包。虚拟钱包服务帮助用户持有比特币，提供银行活期存款账户的一些功能。如Coinbase等。 2.汇兑。汇兑服务将美元兑换为比特币，或将比特币兑换为美元。如Mt.Gox等。 3.支付。支付服务帮助商户在交易中接受比特币支付。如专为比特币提供支付解决方案的Bitpay公司等。
==========

金属货币的世界靠天然的产量限制货币发行量，靠天然的化学属性进行防伪，靠天然的珍稀性保证购买力。 纸币的世界靠中央银行的领导和经济专家决定发行多少货币，靠不断提高制作工艺和更高级的验钞机进行货币防伪，靠国家力量来保证购买力。 而在比特币的世界，上面的规则通通失效。数字世界有自己的规则：通过数学，更确切地说是通过密码学保证比特币种种天方夜谭般不可思议的特性。
==========

去中心化的意思就是不由某个人或某个群体主导一切，而是大家集体参与、共同决定。在沟通方式低效的年代，这是一件非常奢侈的事情，但由于能够保障所有人的权利、及时纠正可能的错误，所以人类社会形态也遵从这个思想，从中心化不断迈向去中心化。
==========

比特币通过构建自己的生态圈展现了社会契约重构的一个鲜活案例。自由本位的货币（包括目前所有的法币）本质上是一纸契约，政府低成本印出的每张钞票代表着它与持有者签订的一份价值合同，这个合同名义上以政府的信用为担保，实质上以政府的强制力执行，因而是一种强制契约。个体既无选择的余地，亦无对抗的能力
==========

著名的路径依赖理论，即人类社会中的技术演进类似于物理学中的惯性，一旦进入某一路径就可能对这种路径产生依赖。
==========

2008年的金融危机让人们都熟悉了一句话：大而不倒。这是指一个金融系统越庞大，它就越有保障。因为越大越有价值，越有价值，倒闭的破坏力越大，使得连政府都不得不想方设法阻止它的倒闭
==========

。黄金派的观点是，货币就应该是商品货币，没有价值支撑的货币都不是好货币。信用派的观点是，货币只要有政府强权来支撑并强制使用就可以，它是用国家信用做担保的。比特派的观点是，比特币几乎符合货币理论里对货币的所有定义，同时还优于黄金和信用货币。
==========

货币的发展表现出3个典型特征：货币材质去实体化、货币价值虚拟化和货币职能符号化。
==========

价值存在于共识（信任）和交易本身。不是为什么值得信任，而是你是否选择信任。之前的社会信任

都是基于一定的实际效用和货物或者国家政体而产生的，而比特币是基于去中心化、总量恒定的特点而自发产生的社会契约信任。
==========

货币不像普通人所理解的那样，是一个价值存储工具、一个交易单位或者记账单位，而是一个技术上的具有集体记忆功能的工具。
==========

2、《比特币》的笔记-06-手续费、块链大小和转账速度

随着币值的升高，比特币的转账手续费会越来越贵；
是这样的吗？看图
每个比特币的交易费用=总交易费用/总交易量
2012.11.29至今，每天

3、《比特币》的笔记-第1183页

在正常情况下，私钥和比特币地址一样难记，而在http://brainwallet.org上，

4、《比特币》的笔记-概览——思维导图

思维导图
可放大的图片下载 http://www.kuaipan.cn/file/id_9808872080491006.htm?source=1

5、《比特币》的笔记-第2381页

货币发行上，政府也不是必要的参与者（但是不意味着不能参与，法币与私企、个人发行的货币也可以是竞争关系）。

6、《比特币》的笔记-挖矿

挖矿的关键动作不是挖而是维护，产出比特币只是一个副产品而已，仅仅是为了奖励那些为维护比特币金融系统做出贡献的人。所以，挖矿的意义并不是白白消耗电力和磨损硬件来做无意义的计算以获得比特币，而是通过大量计算防止作弊，维护整个比特币系统的安全。

7、《比特币》的笔记-第1769页

2004年，山东大学教授王小云公布了MD5的破解报告

8、《比特币》的笔记-02-无处不在的风险-期货矿机的期货风险

你按照当前的算力估算矿机到手后的收益，似乎前景很光明，但几个月后拿到矿机时，你的收益只有当前的几分之一，可能根本就无法收回成本。挖矿的边际收益，现在都-2000%以下了.180天数据恐怖的算力增长。180天数据期货矿机大观。图中唯一一个不是期货的，成本回收>1年

9、《比特币》的笔记-无处不在的风险

在比特币价格虚高时，黑客们借币做空，然后组织大规模分布式拒绝服务攻击使交易平台瘫痪，

引起恐慌，造成大规模抛盘，他们再在底部接单买入。

10、《比特币》的笔记-第1128页

挖矿就是将过去一段时间内发生的、尚未经过网络公认的交易信息收集、检验、确认，最后打包加密成为一个无法被篡改的交易记录块，从而成为这个比特币网络上公认的已经完成的交易记录，永久保存。

11、《比特币》的笔记-01-比特币能购买什么-支付的便利性

一般认为，随着比特币市值的增加，价格的稳定性应该也会逐渐呈现出来，那么比特币极有可能成为一种稳定性强、流通性好的天然国际货币
这句话根本不对。由于每天产生的比特币数量几乎差不多，一个近乎完美的线性增长。那么市值的变化直接可以近似为汇率的变化（已用数据验证过）。于是这句话就等于说，随着价格的增加，价格的稳定性也会逐渐呈现出来，这不是扯淡么？以2013年12月至今的数据为例。证明的是 市值与价格是一个东西，而不是要证明价格会逐渐稳定

12、《比特币》的笔记-第2548页

这种既能充分证明自己是某项权益的合法拥有者，又不把有关信息泄露出去的方法就叫零知识证明，即提供给外界的“知识”为“零”。

13、《比特币》的笔记-第1142页

如果矿池抢到了记账权，那么就按照计算贡献来分配这次获得的收益。

14、《比特币》的笔记-一次使用比特币交易的全过程

有一天，长人在网上闲逛的时候发现了一家网店，里面的商品新潮有趣，而最重要的是，它支持比特币支付。作为比特币的坚定信仰者，他与店主聊得非常投机，决定以10个比特币的价格购买一件商品。出于对店主的信任，长人与店主约定，由前者将10个比特币打到后者的地址上，而后者在收到比特币后再将商品发出。 店主打开自己的比特币钱包，创建了一个新的比特币地址，并告知长人。店主创建新地址的本质是生成了一个密钥对，这个密钥对由一个公钥和一个私钥组成，其中私钥只有店主自己知道，而公钥则是公开的，可以用来验证支付的真伪。 长人收到店主的地址信息后，打开了自己的比特币钱包客户端，并指示客户端将10个比特币发送到店主的收款地址。钱包客户端里储存着长人所有地址的私钥，为了简化问题，我们假设长人在其中一个地址里放了11个比特币，而本次支付只从该地址进行扣款。在发送比特币时，钱包客户端以该地址的私钥对本次交易进行签名，并向全网公布这次交易信息。 这个时候，网上所有的节点或者说每一个矿工都会验证这个交易是否有效。验证方法也很简单，拿出这个地址的公钥对照即可。在这个环节，名叫宋欢平和睡空空的两位矿工也接到了这个交易信息。在经过验证确认交易有效后，他们把这个交易放进内存里，等待进入数据块。过了一段时间，宋欢平的电脑算出了一个符合条件的随机值，系统宣布一个新的合格数据块诞生，并向整个网络公布了这一消息，其他节点（包括睡空空）收到后就开始在这个数据块之后开始新的挖矿工作。而长人和店主的交易信息就被打包放进了宋欢平挖出的数据块里，并且得到了初步确认。当下一个区块链接到这个区块时，交易就会得到进一步的确认。在连续得到6个区块的确认之后，长人和店主的这笔交易基本上就不可逆转地得到了确认。 店主发现10个比特币已经到达他的地址，经过一段时间的等待确认后，他把商品发给了长人，本次交易宣告完成。

15、《比特币》的笔记-第2255页

《比特币》

一种不受监管的数字货币，通常由其开发者发行和控制，为特定虚拟社区的成员使用和接受。

16、《比特币》的笔记-0

123*91=11193 193*11=2123 （91*11=1001）
比特币现阶段的大幅波动并非全然坏事。大量比特币交易者就是从投机开始，慢慢地接受并承认它。
挂钩的商品和服务越多，比特币就越稳定。

《比特币》

版权说明