yibite.com

壹比特 03

数字货币的崎岖进化

李钧 孔华威 编著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

壹比特 03

数字货币的崎岖进化

李钧 孔华威 编著

電子工業出版社
Publishing House of Electronics Industry
北京•BEIJING

图书在版编目（CIP）数据

数字货币的崎岖进化 / 李钧，孔华威编著. —北京：电子工业出版社，2014.4
（壹比特；3）
ISBN 978-7-121-22688-5

Ⅰ. ①数… Ⅱ. ①李… ②孔… Ⅲ. ①电子货币—通俗读物
Ⅳ. ①F830.46-49

中国版本图书馆 CIP 数据核字（2014）第 055250 号

书　　名：**数字货币的崎岖进化**

作　　者：李　钧　孔华威
策划编辑：刘声峰（itsbest@phei.com.cn）
责任编辑：刘声峰
特约编辑：任雨橦
印　　刷：三河市鑫金马印装有限公司
装　　订：三河市鑫金马印装有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编：100036
开　　本：720×1 000　1/16　印张：16.5　字数：171 千字
印　　次：2014 年 4 月第 1 次印刷
定　　价：40.00 元

本书内容仅代表作者个人观点，投资有风险，需谨慎！

前　言

货币的尺度和技术的进击

缺什么别缺钱。我们天天谈钱，嬉笑怒骂谈的那些个皱巴巴的满是细菌的钱。

我们偶尔也会谈“货币”，但会变得严肃，似乎“货币”是高大上的事儿，相关的都是专家、官员们在谈论的货币政策啊、汇率啊、贬值升值啊，等等。

百度百科说：货币是国家定义的、唯一的“用作交易媒介、储藏价值和记账单位的一种工具，是专门在物资与

服务交换中充当等价物的特殊商品”。再学术的定义，也逃脱不了货币就是钱，就是一种商品的事实，同样有使用价值和交换价值，与萝卜芹菜啥的一样，只是比较特别，因为它“同时”，同时作为价值尺度和流通手段。

货币这个东西似乎天生有两个特点：一是国家，二是尺度。

我们熟悉的米和秒就是长度和时间的尺度。尺度是个很严肃的事情。比如英国人要从中国进口两尺丝绸，交易双方对“尺”都要有共同的认识，否则就会乱套。

所以，在尺度方面要慎重其事。1889 年一个叫“国际度量衡局”的组织用铂铱合金（90%的铂和 10%的铱）制造了米原器，并规定在冰的熔点温度时所测量到的国际米原器上两道刻度之间的距离为 1 米。后来人们觉得这个有点太不够现代，1960 年定义氪—86 原子能级间跃迁辐射在真空中的波长的 1 650 763.73 倍为标准米。再后来又因为氪很难搞到，1983 年至今，一米被定义为“光在真空中于 1/299 792 458 秒内行进的距离”。对于人而言，除非你是电脑，这个精确值很难记得住。对秒的定义也很费周章，很拗口。1967 年对秒的定义是铯原子基态的两个超精细能阶间跃迁对应辐射的 9 192 631 770 个周期的持续时间。

这就是人类对尺度应该有的严谨态度。

这个时候，国家概念变得附属——不管你是什么超级

大国，还是“屌丝”小国——尽管英国喜欢用英寸英尺，美国喜欢用码，中国人有时还用市尺和寸，但是不管你用何种单位，都应锚定上面那个标准，不能浮动。

比较而言，我们对货币这个价值尺度，或者叫财富的尺度，似乎没有那么认真严肃。

一听可乐的使用价值是一样的，但是用各国（或地区）自己的货币去度量，会出现五花八门、令人无所适从的状态：英国 1.98 英镑，法国 2.1 欧元，日本 188 日元，美国 2.17 美元，新加坡 2.2 新元，德国 1.59 欧元，中国香港 9.8 港币，俄罗斯 65 卢比，中国上海是 5.9 元人民币。如果觉得日元和英镑只是英寸和米之间的习惯差别的话，我们还可以按照所谓的“汇率”来统一折合到美元，按说应该一样，但是不然，哪怕同样以欧元为单位，德国要 1.59 欧元，法国却要 2.1 欧元。

测量的对象没变，那因为是尺子出了问题。而反过来说，在你是不是很有钱这个事情上，不是你自己说了算，是尺子说了算。恰如杨贵妃到了今天可能不敢上大街——这个事情是值得拜金的同胞们思考的。

再进一步推理，所谓国家财富之间的竞争，实际上是尺度标准的竞争。所谓的财富是你的所有资产在我的账本上，用我的单位来衡量出来的一个数字而已——如此说来，货币这个事情，似乎没有啥“高大上”，反而很“吊诡”，非常有阴谋论嫌疑，难怪《货币战争》极度畅销。

货币这件事，看来需要来点改变。而信息技术和互联网可能是一个改变的入口。至少在信息技术的推动下，胶卷、磁带被数字化以后，为我们打开了一个数码相机、数字音乐和高清 3D“阿凡达”的全新世界，重新定义了我们的视觉和听觉。看来互联网也该动动“货币”这个奶酪了。

说实话，在刷各种卡的时候，纸币的实物概念已经动摇。当你用支付宝网购的时候，感觉钱只是数字，即使是密码，也只是数字而已——这个时候，也许密码就是钱，密码就是货币。而最近大热的比特币，就是由于其采用密码技术来控制货币的生产和转移，被认为是一种加密电子货币。

数字货币，也许是一个革命的方向。《壹比特丛书》的本意就是让我们在“价值衡量”这件大事上严肃起来，不掺杂细菌，中立地、技术范儿地讨论这件事——原则就是“开辟园地，欢迎来稿，长短不论，稿费从优”。

孔华威

中科院上海计算所所长

壹比特数字科技公司顾问

《壹比特丛书》联合主编

目　录

“屌丝”真身中本聪
把比特币送上太空
FBI 的比特币怎么办?
比特币挖矿环保吗?
“80 后”理科男的创业史

第一章

热点聚焦

01

“屌丝”真身中本聪

神秘的中本聪疑似现身了？2014 年 3 月 14 日《新闻周刊》称找到了中本聪，他是一个 64 岁的日裔美国人，而且他的名字真的是叫中本聪。和天才谢尔顿一样，他也喜欢收集火车模型。另外他曾经为美国军方做过信息安全相关的保密工作。

当天晚上接到运营部门的电话，听到这个消息我第一个反应就是“哇，这不会是假的吧？”照片里的中本聪头发蓬乱，穿着一身运动服，戴着眼镜，按照现在流行的观点，这是一个典型的“屌丝”，谁也不会把他和“比特币之父”以及十几亿美元的财富联系起来。毕竟全世界这几年都在找中本聪，而大家又怀疑中本聪是假名字，如果有谁真的叫中本聪，早被人找出来了。但接下来我们在连夜翻译《新闻周刊》的原文过程中，发现这个“中本聪”好像就是那个“中本聪”。

这个“中本聪”

根据《新闻周刊》的描述，中本聪是跟随他母亲从日本移民美国的。中本聪的弟弟对自己哥哥评价：“他是一个才华横溢的人，而我只是一个卑微的工程师。他非常专注，他的思维方式不拘一格。聪明、机智。数学、工程、计算机，只要你说得出来，他都能做到。”

这个中本聪名叫 Dorian Nakamoto，人如其名，从小聪明过人，对理科有特殊天赋，但性格有点古怪。青年中本聪先后在几家大型电子公司担任工程师，并参与过有关国防的保密项目。这可能是他开发比特币所需密码学知识的来源。2001 年后，中本聪结束了涉密部门的工作，之后十年他做了什么没人清楚，包括他的家人。

中本聪有过两次婚姻，留下了六个子女。其中他的第二任妻子为他生下五个子女。在20世纪90年代，他曾因失业而无法偿还贷款，房屋被银行收回。他的女儿表示，他可能就是因此改变了对银行和政府的态度。

中本聪现在在美国隐居，和90岁的老母亲一起过着世外桃源般的生活。当记者来到他家采访时，他竟然报警。当警察看到这个“屌丝”样的老头时也惊奇：“什么？这个家伙就是创造比特币的那个人？看起来他好像过着寒碜的生活呀。”

中本聪拒绝回答有关比特币的问题，但没有否认他就是比特币的创始人。“我已经不再参与，我不能回答任何问题，”他说道，拍着左手，回绝任何进一步的询问。“项目已经移交给了其他人。他们在负责它，我已不再有任何关联。”

那个“中本聪”

他说的项目已移交给别人，指的是比特币基金会接手了他的工作。根据比特币基金会首席科学家安德烈森的说法，他所接触的“中本聪”确实是一个独立开发者。中本聪的代码不是很整洁，没有经过优化和精简，而且使用了一些旧式的写法（指20世纪的写法）。看起来不像是一个团队合作的产物。

“大家看了比特币的代码后已经几乎认定了它是一个人开发的了，”安德烈森说。自比特币基金会成立以来，基金会已经重写了大约 70%的代码。“原版写得不是很好，它就像一个大毛球，但这是令人难以置信的。”安德烈森评价道。

另外一个支持这点的证据是，安德烈森作为中本聪指定的接班人，应该与中本聪进行过深入交流。在媒体曝光中本聪后，安德烈森说：“对于《新闻周刊》打扰中本聪的家人，我感到非常失望，我后悔曾经和 Leah（本次采访中的记者）交谈。”

随后，在那个“中本聪”曾经发表创世论文的网站 p2pfoundation 上，三年没发言的疑似中本聪的账号“Satoshi Nakamoto”突然发言，称自己不是《新闻周刊》里的那个“中本聪”。

“I am not Dorian Nakamoto．”

这次否认再次引起了网上的激烈争论。毕竟《新闻周刊》里提到的这个“中本聪”是最接近“比特币之父”的那个“中本聪”了。虽然要想证明自己是“中本聪”很容易，只要用创世区块签个名就可以证明，但要证明自己不是“中本聪”就困难了，更何况他真的就叫“中本聪”。因此虽然网上的“中本聪”不承认，但我们可以认为，这个“屌丝”样的老头，就是“比特币之父”中本聪。