DIGITAL GOLD

The Untold Story of Bitcoin

数字黄金

比特币鲜为人知的故事

[美]纳撒尼尔·波普尔◎著
(Nathaniel Popper)

艾博◎译

中国人民大学出版社

中国人民大学出版社
·北　京·

图书在版编目（CIP）数据

数字黄金 /（美）纳撒尼尔·波普尔（Nathaniel Popper）著；艾博译. —北京：中国人民大学出版社，2017.4
书名原文：Digital Gold: The Untold Story of Bitcoin
ISBN 978-7-300-24011-4

Ⅰ.①数… Ⅱ.①纳… ②艾… Ⅲ.①电子货币—研究 Ⅳ.①F830.46

中国版本图书馆CIP数据核字（2017）第013854号

数字黄金
比特币鲜为人知的故事
［美］纳撒尼尔·波普尔（Nathaniel Popper） 著
艾博 译
Shuzi Huangjin

出版发行	中国人民大学出版社		
社　　址	北京中关村大街 31 号	**邮政编码**	100080
电　　话	010-62511242（总编室）		010-62511770（质管部）
	010-82501766（邮购部）		010-62514148（门市部）
	010-62515195（发行公司）		010-62515275（盗版举报）
网　　址	http://www.crup.com.cn		
	http://www.ttrnet.com（人大教研网）		
经　　销	新华书店		
印　　刷	北京联兴盛业印刷股份有限公司		
规　　格	148 mm×210 mm 32 开本	**版　　次**	2017 年 4 月第 1 版
印　　张	8.5 插页 2	**印　　次**	2017 年 4 月第 1 次印刷
字　　数	227 000	**定　　价**	56.00 元

CONTENTS

目 录

引子

午夜已过，大多数赌客都已回房睡觉，酒杯里残留着琥珀色的名贵威士忌。专门从当地赌场请来的分牌小姐，已提前半小时回去了。还没回房的赌客们让她把牌桌和牌留下，他们想继续玩。这帮人继续趴在赌桌上赌着。堆得老高的筹码，在这个挑高有三层楼那么高的木制弧形天花板下，显得那么的渺小。距离赌桌远端墙上有个超大的窗户。窗外是塔霍湖，有长长的码头，湖面上泛着闪闪的亮光。

赌桌远端背对着窗户的，是艾力克·伍希斯，才29岁。很难想象，三年前的他还处于失业状态，信用卡里欠着许多钱。他四处打着零工，艰难地维持着新罕布什尔州一间公寓的月供。可是今晚，艾力克穿着小山羊皮鞋，定制的牛仔裤，和身边那位对冲基金经理有说有笑。艾力克的发际线已经有些后移，但是他的脸看上去依然年轻，还带着独特气质，脸上的酒窝让他看上去更年少。他自嘲说自己昨天晚上在牌桌上的表现太差，但那是他所布下的“赌局战线”的一部分。

“我那是为今晚打基础呐，”他一边笑着，露出满口白牙，一边把一堆筹码推倒在赌桌中间。

艾力克输得起。他最近卖了一个赌博网站——一个由比特币这种神秘的数字货币和支付网络建造起来的神秘世界。2012年，他花225美元买下那个网站，换了个名字，叫作“中本聪之骰”。一年之后，他以1 100万美元出手。他还持有大量比特币。几年前他刚开始买进这种货

币的时候，每个才值几美元。如今，每个比特币值500美元，他的身家也飙升到数百万美元。起初比特币刚出来的时候，投资者和那些古板的商人还嗤之以鼻。如今，许多重磅人物对艾力克抛绣球。这次，他来到塔霍湖就是应身边这位对冲基金经理丹·莫瑞德的邀请。不少人已经在比特币里挖到了金山，丹·莫瑞德也想从这些人身上学一两手。

与莫瑞德家中的许多人一样，对艾力克而言，朝比特币里挖金子的冲动，跟想要赚钱可以说完全有关系，也可以说完全没有关系。他第一次在脸书上了解到有关比特币技术的事情后，他就预言，比特币的价值会飙升到天文数字。他也一直坚信，这种发展将是多层次比特电脑密码对当前世界某些主流权力结构（包括华尔街银行和政府部门）进行重新洗牌。它对金钱产生的影响，就像互联网对传统邮政和媒体产生的影响。艾力克认为，比特币的发展不仅能让他变得富有，还会让世界更加公正与和平，因为政府无法再提供战争所需的经费，个人也能控制自己的钱财和命运。

自从在新罕布什尔州失业以来，像艾力克这样雄心勃勃的人日子过得挺不顺的，这一点也不奇怪。他搬到纽约之后，说服了文克莱沃斯双胞胎——泰勒和卡梅伦——这两位脸书大侠，让他们注资近100万美元到自己创建的公司比特因斯坦（BitInstant）。然而这个合作的结局是以死相拼两败俱伤，最终艾力克辞职，带着女朋友搬到了巴拿马。

最近，艾力克老在巴拿马的办公室里待着，跟美国财政监管最高机构——美国证券交易委员会——的人打交道。他们要查艾力克出售公司股份来换取比特币的事情。这些股票给他的投资者带来了巨额回报。据艾力克观察，这些来调查的人根本不懂比特币的技术。不过，他们也搞对了情况，艾力克没有把他的股票登记备案。这样的调查，比艾力克在比特因斯坦公司的一位前合作伙伴的遭遇好多了。那人在两个月前，即2014年1月，因涉嫌洗钱被逮捕。

如今，艾力克不会轻易地被吓到。他跟许多人不同，他很有幽默感，能自嘲，还能调侃自己的境遇，这对他帮助很大。

“我经常提醒自己，比特币可能会垮掉，”他说，“虽然我现在看好比特币，但我经常自我检讨，告诉我自己，新技术通常都会失败的。”

但他还是坚持做，不仅是为了他在银行里越来越多的存款，还为他本人以及在塔霍湖的那些人一起创造出来的钱——一种新的货币，他认为可以改变整个世界的新货币。

5年前，艾力克第一次听说比特币的时候，情况可不是这么的高大上。他从不知名的订阅电子邮件里，收到一个叫中本聪的神秘人物发来的介绍。

中本聪一开始就把比特币和黄金进行了比较：**比特币将会是一种全球性的货币，人人可以拥有，可以使用。比特币也跟黄金一样，其价值由想购买的人确定——当时是一文不值。不过，当初的设计是把这种货币当作跟黄金一样的稀缺物资，总共只能创造出2 100万个比特币，而且很难仿造。比特币跟黄金还有共同之处：需要进行“挖矿”的工作，才能制造出比特币。**

比特币还有比黄金更优越的特性，如储存。若要把比特币从伦敦发往纽约，不需要跨洋运输，只要有一个密钥，鼠标轻轻一点就可以完成。就其安全性而言，中本聪依靠的是一种不可破解的数学公式，而不需要荷枪实弹的警卫。

把比特币和黄金相提并论，只是吸引了一些人的眼球。金条还是金条，实实在在地存在着。而比特币必须存在于设计精巧、去中心化的网络之中，正如各网页只能存活在互联网去中心化的网络之中一样。比特币的网络和互联网很像，不靠中心化的权威机构来运行。登录某个网站就能够制造出来货币，全世界任何人都能够制造。通过互联网，所有人根据一套软件指令——即互联网协议——来运作。这些协议管理网上信息的流向。比特币有自己的软件协议——用来管理系统如何运作的规则。

这套系统是如何运作的，要解释起来复杂得不得了——需要具备高等数学和拓扑学的知识。但是，早期的时候，一群忠实的比特币迷就知

道了比特币的基本特征。简言之，**它是一种全新的创造、持有以及发送货币的方法**。比特币和美元欧元都不一样，不是由某国的央行发行的，也不是由大型金融机构转账来的。比特币是由用户自己创造并管理的货币，新货币被维护这个货币网络的人慢慢制造出来。

因为创造比特币的出发点就是要向那些最强有力的金融机构发起挑战，比特币的网络从最开始就被一群忠实的比特币迷描述成一个乌托邦。互联网从大型媒体手中夺得了权力，并把权力赋予那些博客的博主和异见分子，比特币也声称要从银行和政府手里夺取权力，并把权力赋予使用这种货币的人们。

这些高大上的思想，被不少人冷嘲热讽，因为大多数人都认为比特币的结局可能跟虚拟宠物和庞氏骗局一样，以前听过太多，看过太多了。

但是，比特币降临世界，犹如末世出现了明灯。世界性经济危机刚刚发生，暴露了金融界和政治界太多的弊端，人们向往出现一个新的制度。茶党、“占领华尔街”运动、维基解密，以及其他的运动，目的各不相同，但核心都是要把权力从少数的精英阶层那里夺回，再分发给个人。比特币为这些人的愿望提供了一个很明确的技术上的解决方案。比特币对世人吸引力之大，以至于很多人放弃一切来追随比特币，艾力克·伍希斯以及他的许多朋友们就是如此。如果比特币做成了，不少人就会腰缠万贯。就像艾力克常常说的：“这是第一种既可以赚到大钱又可以改变世界的东西。”既然比特币能赚钱，那它吸引的就不只是愤世嫉俗的革命者了。招待艾力克的人——丹·莫瑞德，就是其中的一位。他毕业于普林斯顿大学，在高曼基金干过，然后自创了对冲基金。他成了比特币圈子里的风云人物。近期，他在比特币上斥巨资，希望获得巨额的回报。在硅谷，投资者和企业家们争相开发使用比特币的方法，以改善现有的支付方法，如在线支付平台贝宝（PayPal）、西联，以期抢夺华尔街的生意。

即使那些对华尔街或什么茶党一点也不关心的人都可以理解，要是能有一个全球性的货币，好处会很多——到别的国家不要换外汇；通过数字

支付，不需要每次都出示身份证明；即使穷人把这种货币存在自己的账户里，也不需要支付昂贵的管理费，还不需要处处用现金。另外，这种支付方式非常方便，不需要像现在的信用卡那样需要收20～30美分的费用。

但是到最后，许多更关注比特币实际应用的人还是用了比较革命化的语言来说明比特币的技术：通过破坏现存的状态来赢得挣钱的机会。在莫瑞德家的赌局开赌之前的餐会上，他开玩笑说，全世界所有的比特币加在一起，其价值等于牛仔衣裤、宿舍装饰品公司“城市衣着”的资产总额，即50亿美元。

“这太疯狂了，对吧？”莫瑞德说，“我想，几百年后，当后人像电影《猿人争霸战》那样，探录我们现在的社会的时候，他们会发现比特币对我们的世界的影响力要比‘城市衣着’大一些。”

许多银行家、经济学家和政府要员都对比特币嗤之以鼻，说那是狂热分子的推销手段，与400年前荷兰郁金香热的情况相同。有好几次，批评人士都对比特币发出警告，说朝着没有中央权威机构控制的更数字化的世界前进，危险众多。在莫瑞德家赌局进行之前的几周，全世界最大的比特币公司——Mt. Gox交易公司——发表声明，因为公司损失了客户近4亿美元价值的比特币，宣布破产。这是关于比特币的最新的丑闻。

但这么多的负面消息都没有摧毁比特币狂热分子的热情，支持者的人数还在不断增加。在莫瑞德家聚会之时，在各类网站上，网民们已经开设了500多万个比特币钱包，而且大多数是在美国境外。在莫瑞德家里赌钱的那帮人，形形色色，什么人都有：刚从中国飞回来的沃尔玛前高管；斯洛文尼亚刚毕业不久的大学生；来自英国的银行家；还有来自佐治亚技术学院兄弟会的两位弟兄。有些人是因为对政府的做法深表怀疑，有些人是因为对银行的做法恨之入骨，有些人是因为更深的个人原因而来的。比如说，那位在中国沃尔玛的高管，他祖父母逃离中国时，就是带着黄金逃的。在如今这个不明朗的世道里，比特币似乎是更容易转移的资产。

所有这些人各不相同，各自心怀鬼胎，他们参与了比特币的创建过

程，而且还将继续参与；他们也是比特币的使用者。比特币的创始人中本聪，于2011年突然消失得无影无踪，留下开源的软件，让比特币的使用者可以更新并改进。据估计，经过5年的修改，没有改动的中本聪源代码只剩15%。除此之外，比特币作为一种货币，它也像钱一样，只有有人使用它才值钱，才有力量。多一个人使用，它生存的可能性就更大一些。

这样一来，比特币就不只是一个普通的创业公司，也不是宅男幻想改变世界的同时还赚大钱的故事了。这已经是一个团体的创造发明，涉及我们生活中的方方面面：大家对政府和华尔街的愤怒；硅谷与金融行业之间的争夺战；我们对技术能挽救人类的脆弱的期待；以及我们对技术能带来的力量的担忧。本书中描写的每个人，他们因为各自不同的原因拥护比特币；他们的人生也都被野心、贪婪、理想以及人性的脆弱所改变；同时，也将比特币从模糊不清的学术文章变成数亿美元的产业。

某些人获得了财富，正如莫瑞德的豪宅所表现出来的财富一样；他家入门处的石头上镌刻着他的个人花饰图纹。某些人身败名裂，甚至锒铛入狱。比特币也多次几乎全军覆没。即使比特币垮了，它也会是一个极佳的案例，证明货币如何运作，谁可以获利，如何改进等。比特币不可能会在5年内取代美元，但它也给我们提了个醒——如果政府不再印那些带有已故总统头像的昂贵纸张，我们应该怎么应对。

在莫瑞德家豪赌之后，客人们纷纷打道回府。伍希斯来到莫瑞德家码头的尽头，因为今年冬天下雪不多，此时的水位很低。昨晚在赌桌上的兴奋，此时已荡然无存。他一脸懊恼，他说他最近辞去了在巴拿马的比特币公司CEO的职位。因为他的职位，他不方便说关于比特币革命性的潜力，这样的话语会对公司不利。

“我的兴趣不在经营公司，我要创建比特币王国。”他说。

再说了，他女朋友已经厌倦了巴拿马的生活，他也开始想念在美国的家人了。他打算几周后搬回科罗拉多州，那是他成长的地方。因为比特币，他这次回去，将是衣锦还乡。和他共创比特币王国的人，对此羡慕不已。

第一部
挖到数字黄金

在这个宏伟计划中，参加了比特币社区的人，就集银行和铸币厂于一身，集拥有者和使用者于一身。

第一章

2009年1月10日

这天是星期六。儿子的生日。圣芭芭拉的天气好极了。他小姨子也从法国过来这里玩。但是哈尔·芬利却需要在他的电脑前坐着干活儿。这是他数个月，甚至数十年来，期待已久的一天。

哈尔都懒得跟他老婆解释他在捣鼓着什么。他老婆是理疗师，对电脑一窍不通。哈尔现在搞的东西，他都不知从何跟她解释起。难道要跟她说：亲爱的，我要做一种新钱。

这确实是他现在做的事情。早上，他跑了很大一圈，然后回到自己的办公室。说是办公室，其实是客厅的一角，一张分区工作的办公桌，上面有四个屏幕，大小品牌各不相同。因为工作以及私人的用途，电脑各自连着不同的主机。剩下的空间，被左一堆右一堆的纸张、笔记本还有破旧的电脑操作手册占据着，凌乱不堪。但是，哈尔坐在那里，他可以看到客厅另一侧外边的前廊，如今是1月中旬，加州的阳光竟然还照得到。在他的左边，地毯上躺着忠实的阿奇，那是罗得西亚背脊犬，是根据牧夫星座里一颗星星的名字取名的。在这样的环境里，哈尔感觉轻松自在；在这里，他完成了最具创造力的编程工作。

他启动了笨重的IBM ThinkCentre电脑，调整好身子，在网上输入一

个网址：www.bitcoin.org。这是昨天他收到的邮件里提供的网址。

他在网上订阅了许多东西，几个月前，他第一次了解到比特币。通常他只跟认识多年的编程界的老相识们往来交流，但是，这次的电子邮件来自一个叫中本聪的陌生人，他介绍了一个电子货币的概念，还起了一个很响亮的名字——“比特币”。哈尔多年来一直在研究电子货币，他很怀疑这样的钱是否能用。但是这封电子邮件有亮点。中本聪许诺，他要发明一种货币，不受银行或任何第三方的管控。这种钱只存在于网络上电脑运算的记忆里。哈尔被中本聪的另一个说法吸引住了：拥有和使用比特币，无须向任何中央权威机构提交任何身份证明。哈尔干了大半辈子的编程工作，就是想努力帮助客户摆脱政府虎视眈眈的眼睛。

哈尔读完那份类似学术文章的9页纸的介绍，兴奋地给那个圈子写了回信：“当维基解密出现之时，我根本不觉得它能成事，但现在它已经是一个巨大的成功。”

鉴于圈子里有人持怀疑态度，哈尔敦促中本聪照着他所设想的系统，开始编写程序。几个月后，就是今天，1月中旬的星期六的上午，哈尔从比特币网站下载了中本聪编写的源代码。这是一个简单的.exe 文档，它在哈尔的电脑屏幕上自动打开，弹出一个清爽的窗口，开始安装比特币的程序。

第一次开启这个程序的时候，它会自动生成一个比特币地址清单，这就是哈尔的系统账户号码；还会生成一个密码，也叫“密钥”。用这些密钥就可以进入那些系统账户。除此之外，这个程序功能有限。其中一个重要功能是“发送比特币”。这个功能在哈尔看来没什么作用，因为他现在没有比特币。不过，他还没怎么用这个程序，它就宕掉了。

哈尔没有气馁。他检查了电脑的分析记录，然后立刻给中本聪写电邮，说他刚才想和网络上的其他电脑联机，然后发生了什么状况。分析记录显示，除了哈尔，还有两台电脑在网络上联着机，因为是同一个加州电信供应商的IP地址，所以哈尔认定，那是中本聪自己的电脑。

不到一小时，中本聪就回信了。他说试验不成功，他也很懊恼。他

说他以前测试过很多次，都没有出现过任何问题。不过，他对哈尔说，他把程序改小了，这样更容易下载，不过也可能就是因为这个原因才出现问题的。

“我想那是我的失策，”中本聪懊恼不已。

中本聪对哈尔表示感谢，然后又发给哈尔一个新版本，把删掉的东西放回去了。不过，这个版本也宕掉了。哈尔还是没有气馁。他不用微软视窗的操作系统，改用别的系统，这次他成功了。程序安装好之后，哈尔用鼠标点击下拉式屏幕，那个音效让他激动不已，他按下“生成比特币”的按钮。接着，他听到电脑的处理器滴答一响，开始高速运行。

一切正常运作了，哈尔稍稍休息了一下，做了点家务事，预定了离家不远的一家中餐馆的晚餐，还给他儿子安排了生日晚会。中本聪寄来的软件说明书上写着：“根据电脑速度的快慢，以及网络上电脑的竞争，生成比特币的时间，可能是几天甚至几个月。”

哈尔给中本聪发了一封短短的电邮，说一切正常：“我有事出去一下。电脑开着，程序开着，让它飞一飞。”

哈尔已经查询了很多资料，对自己的电脑现在正在干些什么及其基本原理，他已经了解了。比特币程序启动之后，它就会上网，通过网上的专属聊天渠道，找寻其他使用同样程序的电脑。目前，网络中只有中本聪的电脑。系统会发送50个比特币为单位的一组比特币，所有电脑都要去抢夺。比特币的发送是针对所有联机的电脑，但这些电脑必须进行一个运算比赛。赢得比赛的电脑将获得那一组比特币。当某台电脑获胜，领取了比特币，网上联机的电脑都会更新那台电脑的比特币记录。接着，系统电脑又开始发送下一组比特币，所有电脑又开始下一个运算比赛。

哈尔晚上回家时，他立刻看到他已经获得了50个比特币，在他的一个比特币地址上有了一笔记录，在“公众账目”上也有了一笔记录。这个公众账目上记录的是所有已经生成的比特币的情况。全世界最早生成的4 000个比特币中，目前已经有78组（3 900个）比特币生成了。那个时候，这些比特币分文不值，但是，这丝毫没有打击哈尔的斗志。他给

中本聪写了一封祝贺信，并抄送圈内的所有人，他让自己好好地过了一把成功者的瘾。

“试想，如果比特币某天成功了，并且成为世上主导的支付形式，”他写道，“那么，比特币的总值，将是全世界财富的总值。”

根据他自己的计算，每一个比特币的价值将达到1 000万美元。

祝贺信的结尾，他这样写道：“要比特币获得这样的成功，其概率很低，但是概率会是1 000万比1吗？大家好好想想吧。”

到了这个阶段，哈尔觉得，未来将是完全不一样的一个世界。

哈尔的父亲是个石油工程师，循规蹈矩的，除哈尔之外还有三个孩子。哈尔从小就看遍了经典的科幻小说，不过，他也拿微积分的书看着玩。最终，他考取了加州理工学院。对于能够挑战智力的事情，他总是迎头而上。还在上大一的时候，他就报读了研究生的课程——“引力场原理”。

不过，他不是书呆子。他人高马大，喜欢体育，喜欢在加州的高山上滑雪。他绝对不是加州理工学生中常见的那种社交菜鸟。他的这种积极精神，也充分表现在他的学术研究中。当他在宿舍里读到拉里·耐文的小说，里面提到把人体通过低温冷冻，以便在未来进行解冻的可能性，他就积极行动，找到了一个组织。这个组织要把这个可能性付诸行动。他还向阿科尔生命延续基金申请获取他们的杂志。最后的结果是，他和家人都交了钱，要把他们的身体冷冻起来，保存在洛杉矶附近阿科尔基金会的一个冷冻库里。

互联网的出现，让哈尔的世界无限扩展，他可以和世界上任何一个角落的人取得联系，和他们讨论看似晦涩却很激进的问题。在第一个浏览器出现之前，哈尔就加入了一些网上的组织，如“网络庞克”和“外星乌托邦”，在里面辩论，说新技术将改变他们造梦世界的轨迹。

这些网上组织最感兴趣的问题，就是技术如何改变企业、政府和个人之间的力量平衡。技术确实给个人提供了很多前所未有的新力量。还