新民环球

本报国际新闻部主编 | 第456期 | 2014年3月13日 星期四 责编:卫 蔚

热点锁定

朝鲜11日公布最高人民会议代议员选举结果,当选者中包括金正恩的姑母、前“二号人物”张成泽的妻子金敬姬。

只在网上露网名 不见庐山真面目

谁是比特币之父“中本聪”

文 / 袁原

中本聪是个谜。他发明比特币,以网上发帖形式“露面”;只与少数极客电邮往来,内容仅限编码;3年前留言“我转做其他事”后彻底遁形……谁是中本聪?从天赋异禀的编程者,到无政府主义的数字朋克,乃至研究虚拟货币的学术团队,都曾是“嫌疑人”,却好像又不是。

美籍日本人中本聪否认自己创造比特币 本版图片 GJ

戴维·肖姆(左)以及奥马奥尼(中)都被列入嫌疑人名单,但谁是真正的中本聪仍然是谜

必备五才能

自从2008年11月提出比特币概念以来,中本聪只在网上出现过,没人听过他的声音,更没人见过他的庐山真面目,要从中还原出一个有血有肉的中本聪谈何容易。

然而,早年与中本聪有电子邮件往来的华裔数字朋克戴维认为,全世界够格当中本聪的人寥寥无几。戴维在20世纪90年代发明了一种名为b钱的电子货币,深知推出比特币的难度之大。

“发明比特币的人须具备如下才能:第一,深层次思考过货币问题;第二,掌握密码编写;第三,相信比特币可行;第四,有足够动力将这一理念付诸实现;第五,编程技艺精湛以确保其安全;最后,有能力组织一支开发并维护比特币的团队。”

“符合头三项条件的人已经非常少,比如我和尼克·绍博。”戴维说。

尼克·绍博曾是乔治·华盛顿大学的法学教授,也是一名出众的计算机科学家,是“中本聪真身”嫌疑人之一。他还是一位活跃的作家,涉猎之广、产量之高令人惊叹,博客撰文涉及诠释学、深海资源开发和密码安全等领域。

更重要的是,在1998年至2005年期间,绍博致力于虚拟货币研究,并开发了一个“比特金”体系,这被视作比特币的前身。他因此被高度怀疑是中本聪真身。

绍博本人在2011年5月发文否认这种猜测。然而,仍有好事者不依不饶,在去年12月比对中本聪留言和绍博博客,指出其中不少表达、行文习惯和拼写喜好高度一致。他们注意到,中本聪首次提出比特币半年前,绍博在网上征集合作者,参与其比特金项目。

戴维却认为,绍博不可能是中本聪,“我以自己和尼克举例,是指在中本聪出现以前,”他说,“我只想说,没几个人能符合所有条件。”他认为,中本聪应该更年轻、精力更充沛、更有理想。

“我发明b钱的时候还是个大学生,快要毕业的时候;尼克提出比特金的时候也差不多这个岁数,所以我认为中本聪应该是这个年龄的人,一个有足够精力和时间,不必操心发表署名论文的人。”戴维说。

依照如此逻辑,还能开释曾经在“嫌疑榜”名列前茅的道纳尔·奥马奥尼团队。奥马奥尼是都柏林三一学院的计算机科学家,1997年和两个同事合著一本关于电子支付体系的书,被视为比特币勾勒蓝图。

排除可疑者

鉴于比特币的政治敏感性,中本聪格外谨慎、低调,确实不像活跃在公众视线之内的学术界人士。在读博士生迈克尔·克利尔因此引起《纽约客》记者乔舒亚·戴维斯注意,一度成为中本聪头号嫌疑人。

戴维斯花了4个月分析网络留言后认定,中本聪只可能是英国或爱尔兰人。他2011年打入密码编写者年度会议,起初圈定9个嫌疑人,最后将目标锁定为23岁的克利尔。

克利尔就读于都柏林三一学院,精通C++编程语言(比特币的编程语言)。当同学们在网上晒照片、发评论、留下联系电话时,他的网上行踪却只有一个电子邮件。

进一步网络调查显示:2008年本科尚未毕业时,克利尔已是三一学院计算机系的尖子生;2009年,他受雇于爱尔兰联合银行改进其货币交易软件;他还合著发表了一篇关于点对点技术的学术论文,该技术是比特币的理论基石。

“你是中本聪吗?”戴维斯在简短交谈后问道。克利尔笑了起来,没有作答。一阵“尴尬的沉默”之后,他说:“如果你愿意的话,我可以给你讲讲比特币的设计原理,让你知道我是怎么想的。”

在电子邮件中,克利尔详尽分析了比特币的优缺点。他称,替爱尔兰联合银行工作不值一提,承认自己是个优秀的编程者、了解密码学并欣赏比特币,但否认是中本聪。“我不是中本聪,即使是也不会告诉你。”

这种暧昧的否认反而招致更多嫌疑。克利尔的照片也被挖了出来。甚至有人指出,他的眼镜镜框是名牌,作为一个在读学生怎么付得起?

克利尔终于招架不住,正式发表声明否认。他措辞谦卑地说:“我只是一个对密码学感兴趣的研究生,在任何方面都谈不上专家。”

他最近更明确表示,自己对比特币的欣赏仅限于技术层面,其中蕴含的无政府主义倾向令自己不安。他强调,自己的政治立场偏左。

其实,在克利尔被锁定为首要嫌疑人之前,即有分析人士指出,中本聪不会是二十出头的年轻人,因为其留言中不少表达和比喻只有上了年纪的人才懂。

此外,有编程常识的人都知道,每个人写代码有特定风格和特征,就好像每人各有文风。分析比特币的代码不难发现,虽然其设计理念完美,但并非毫无瑕疵,更像出自一个“母语”不是C++语言的编程者之手。根据这种逻辑,不仅克利尔不是中本聪,其他年轻且擅长C++编程语言的人也可排除嫌疑,例如有自由主义倾向的芬兰极客马尔蒂·马尔米和特立独行的比特币交易所Mt.Gox创始人杰德·麦凯雷博。

同名嫌疑人

精于编程、年长隐秘、有些厌恶银行,美国《新闻周刊》6日挖出一个符合上述条件的中本聪,定居加利福尼亚州的美籍日本人中本聪。

《新闻周刊》记者利娅·麦格拉斯·古德曼认为,如果比特币的发明者真想匿名行事,没必要取“中本聪”这种英语世界罕见的名字。

凭着这一直觉,她利用常驻人口数据口搜索,发现了10岁从日本移居美国的中本聪。调阅美国国家档案馆其他材料后,古德曼发现这个中本聪身上的“疑点”越来越多。

他生于1949年,从小天赋过人,曾就读加州州立工业大学物理系,精通数学、工程学和计算机。生活中,他是个沉默且情绪化的人,格外注重保护隐私。自从40年前从加利福尼亚州立工业大学毕业后,他再也没用过中本聪这个名字,而改用“多里安·S·中本”。

毕业后,中本聪曾供职多家公司,参与一些国防保密项目,也曾两度下岗。2002年以来似乎再没有过稳定工作。

他两次结婚,育有6个子女,但家人对他的工作却知之甚少。在女儿艾琳·米切尔印象中,父亲酷爱新技术,经常自己组装电脑。他在家里没日没夜地工作,却没人知道他在干什么。“他总是紧锁房门,如果我们胆敢碰他的电脑,麻烦就大了,”米切尔说。

然而,没有证据显示这个日本人与比特币之间的联系。古德曼为此前往加州天普市,拜访中本聪,后者却叫来了警察。他甚至不愿意与古德曼对视,只是低着头说:“我不再参与了,不能再讨论,已经将其交给其他人……我与此没关系了。”

这句话立即招来大批记者围堵中本聪。他不得不澄清,之前所言指自己不再是一名工程师,最后和愿意请他吃午饭的记者脱离重围。

相关链接

为可行性电子货币绘制第一幅蓝图 数字朋克教父:又一个嫌疑人

从中本聪近十万字的网络留言中,人们能为这个比特币发明者拼凑出一幅“网络肖像”,厌恶银行和小心谨慎是关键词。或许,要找到中本聪,还得回到发明比特币这种电子货币的初衷。这不得不提到数字朋克。

在20世纪90年代初期,一小撮数学和电脑的“骨灰级粉丝”意识到,网络的兴起暗藏威胁,可能引发前所未有的国家监控和商业入侵,严重侵犯网民权益。他们认为,密码学是抗衡这种威胁的最有效武器。于是,在这个政治、数学和技术交错的路口诞生了数字朋克,他们反对权威、迷信技术、强调隐私,成立了电子前哨基金会、维基揭秘等网站……比特币的设计理念中,依稀可见数字朋克主张。

实际上,数学家戴维·肖姆早在上世纪70年代末即开始研究数字化货币,提出匿名通信的可能,并因此获称“数字朋克教父”。他为此共申请了17项专利,还为可行性电子货币绘制了第一幅“蓝图”。

肖姆其实已计划发行这种名为e现金的电子货币。然而,受网络泡沫破灭影响,他位于荷兰的公司“数码现金”在1998年倒闭,未能实现发行电子货币的理想。

从此之后,肖姆淡出了密码学和电子货币讨论的视野,但无论中本聪还是其他极客,提到比特币时总会用到肖姆的理论。

不少数字朋克以为,生意失败之后,肖姆会出售技术专利,但熟悉他的人知道,他更在乎控制而非财富。他认为,网络社会已经走到一个性命攸关的十字路口,如果不加以显示,可能出现《1984》中的局面。

难怪,回顾电子货币和数字朋克历史后,《星期日泰晤士报杂志》记者安德鲁·史密斯认为,中本聪嫌疑人名单上,或许应该添上肖姆。

本刊主编 汪一新 卫 蔚