让比特币更好花

企业家与学术界期待数字货币发展突破安全瓶颈

当电子货币比特币在 2009 年 1 月创建时，除了寥寥无几的若干个讨论电子货币的群体之外，这种货币并未引起其他人的注意。比特币的起源一直扑朔迷离：有说法称它是由一个别名叫作“中本聪”的人或组织于 2008 年创建的，但至今为止其创始人身份仍然是个谜。而其创建目的看起来也像是一种唐吉诃德式的狂想：作为一种设想的“电子货币”，比特币可以创新性地使用强大的加密算法以保证交易的安全性。用户的身份将会受到伪身份的保护，相关交易记录也会被完全分散。同时，该系统不需要任何人管理这些交易——不需要政府，不需要银行，甚至也不需要中本聪。

然而，现在电子货币在全球已经风靡，并且蒸蒸日上。今天，全球有约 1460 万比特币流通单位，这些叫作比特币的电子货币以小写字母“b”为符号，它们的全部市场价值在 34 亿美元左右。比特币使用量增长在部分程度上归结于一些不法分子利用匿名方式，进行毒品走私甚至更严重的犯罪活动。但该系统同样引起了诸如摩根大通私人银行等金融机构的兴趣，这些机构把电子货币看作是一种可以使其内部付款流程简单化、减少国际金融交易成本的交易方式。事实上，比特币已经引导产生了其他 700 多种电子货币。今年 9 月，随着 Ledger 期刊（学术界里只报道加密货币的期刊）的发行，比特币进入学术圈的时代正式开启。

> “如果比特币不总像现在这样“搬起石头砸自己的脚”，那么其账户链条可能是“21 世纪最重要的一项发明”。

图片来源：Chris Ryan

问题乍现

让学术界和企业界对该系统着迷的是比特币的核心，即相互衔接的链条，它可以作为每笔比特币交易的正式在线分类总账。尽管这个链条可以在使用比特币软件的整个电脑网络中复制，而且那些计算机的用户彼此之间并不认识或信任，但这种数据结构可以让交易记录及时得到更新，从而使其受黑客攻击或破坏的风险降到最低。

很多人把这种链条结构看作是大量其他应用的模板，如包括自我执行的雇用契约和进行网上投票以及众筹资金的安全系统等。这正是 Ethereum（由瑞典一家非营利组织 Ethereum 基金会在今年 7 月启动的一个基于上述链条结构的系统）的目标；同样，这也是电子货币和协议倡议（IC3）学术联盟的研究议程，该联盟由美国纽约伊萨卡康奈尔大学带领，同样于今年 7 月成立。

英国伦敦大学学院密码编码专家 Nicolas Courtois 认为，如果比特币不总像现在这样“搬起石头砸自己的脚”，那么其账户链条可能是“21 世纪最重要的一项发明”。在比特币链条执行过程中，存在着若干个显而易见的缺点，例如安全问题远不够完美。到目前为止，已经出现 40 多起偷盗及抢夺比特币的案例，其中若干起事件涉及的价值超过 100 万美元。

电子货币公司和研究人员正在利用博弈论和先进电子货币理论等手段解决这些问题。“电子货币和很多其他系统不同，它如果发生极其细微的数学错误，那么就会产生灾难性的后果。”IC3 共同执行人 Ari Juels 说，“我认为，当薄弱点出现的时候，就需要寻求学术界的帮助，因为那里有很多专家。”

价值狂飙

事实上，学术界对于电子货币及其先驱的兴趣至少可以追溯到 20 年前，当时密码学家 David Chaum 做了很多开创性工作。彼时，在荷兰阿姆斯特丹国家数学和计算机科学研究所工作期间，Chaum 就希望保护买家的隐私和交易安全。因此，1990 年，他创建了最早的数字货币 DigiCash，该货币可以让用户通过他设计的密码协议进行匿名交易。

然而，DigiCash 在 1998 年破产，部分原因是因为它像传统银行一样有一个集中的组织机构，然而却未能融于当时的金融行业和行规。但其理论在 10 年之后中本聪设计的比特币中却再次重现。这种设计结构包含了众包和点对点网络——两种方式都有助于避开集中管控。该系统对任何人开放：它所需要的仅仅是上网和利用比特币软件开放源。用户计算机会形成一个网络，其中每台机器都是总账户版本更新的资料夹。

中本聪在开放源领域存在的核心挑战是，需要确保没有人能够找到重写总账户的一种方式，通过这种方式两次花费同样多的比特币，否则就会造成比特币被盗。他的解决方式是把要添加到总账户中的新交易增加额变成一种竞争：这种做法也称为挖掘。

挖掘从比特币交易传入开始，然后会不断地向联网的每台电脑进行播送。这些信息会被“挖掘者”（即那些选择参与交易的团体或个人）收到，挖掘者会开始竞争交易通行权，并生成新的交易模块。赢家是首个播送交易“证据”的用户，成功交易模块会在比特币网络中传送，并被添加到总账户链中，目前，总账户链条的模块长度约有 40 万个。

从理论上讲，这种竞争会让模块链条保持安全，因为对于任何一名挖掘者每次的解码能力来说，要解开这个编码都非常难。这意味着，没有人能够获得总账户链条中的加密信息，因此也就不能够重写总账户。

挖掘还可以稳步增长比特币的供应量：赢得每个交易模块的挖掘者都会获得一次奖赏，目前的奖赏是 25 个新比特币，这个价值大抵相当于 6000 美元。中本聪的设计还可以控制比特币供应量的增长，即通过自动调整题目的难度，这样大约每十分钟会增加一个新模块。此外，每过 4 年，创建一个新模块的奖酬大致会减少一半，其目的是使总比特币的供应量控制在 2100 万美元左右。

前景看好

事实上，整个比特币网络系统并不能决定比特币相对标准货币、真实货物及服务的价值。其价值取决于市场力量，即当人们进行比特币交易时的网络兑换率。其中的现象之一是，当前的市场价格已经明显上升，尤其是在 2013 年，当时的要价已经从 1 月份的每比特币 13 美元狂飙到 12 月底的每比特币 1200 美元。这也让真实的产品可以用电子货币来支付，如两个棒约翰披萨店制作的披萨饼在 2010 年 5 月 22 日购买时是 10 万比特币，但现在它们的价值几乎达到 1200 万美元。

日益增强的比特币挖掘也导致个体挖掘者开始联合他们的计算机来源。去年，最大的挖掘联盟 GHash.IO 控制了整个比特币挖掘能力的 50%以上，这将会带来一系列问题，因为任何人如果控制了超过一半的挖掘能力，那么他们就可以在添加模块时击败其他人。这将会让他们获得交易账户的有效控制权，同时让他们一次次使用相同的比特币。这不止仅在理论上可行，事实上，成功控制 51%的挖掘能力已经使其击败了更小的电子货币，如 Terracoin 和 Coiled-coin，后两者被严重破坏以致停止流通。为了减少来自挖掘联盟的威胁，一些现有的电子货币，如 Litecoin，开始更加依赖计算机记忆能力而非处理能力的编码，这种转变将让挖掘联盟建立专门的计算机网络变得非常昂贵。

同时，其他的问题还包括在比特币挖掘过程中需要浪费许多电量，为了减少浪费，研究人员已经提出了一种叫作 Permacoin 的新货币，希望通过其节省用电量。尽管如此，无论比特币的未来如何，普林斯顿大学计算机专家 Arvind Narayanan 都强调称，该货币系统的研发者及学术界人士都是独一无二的。“这是一个非常活跃的知识体系，我相信在未来 20 年，我们会在计算机课堂上教授这项技术。这一点，我很确定。”（红枫）

尼泊尔纪行

废墟之上

震后尼泊尔教育在艰难中前行

■本报记者 冯丽妃

编者按　全球气候变化和自然灾害对地理环境复杂、经济不发达的地区影响尤其严重，应国际山地综合开发中心（ICIMOD）邀请，《中国科学报》记者近日赴尼泊尔进行了实地考察访问。“尼泊尔纪行”将陆续刊登该国震后重建及气候变化影响相关报道。

在晌午的阳光中，这间粉刷成绿色的教室十分明亮。一个扎着黑色长辫子的女孩正在埋头读书。“我长大后，梦想是做医生。”女孩抬起头说，圆圆的脸上露出两个酒窝。她的名字叫 Ainisha B.K，这个 15 岁的女孩是尼泊尔杜丽凯尔一所乡村学校——Shree Bhewani 初级中学 8 年级的学生。

今年 4 月 25 日，尼泊尔中部地区发生了一场震级 8.1 级的地震。随后一个月，震级超过 4 级的余震接连发生了近 300 次。目前，据统计，地震已导致 9000 多人死亡，超过 2.2 万人受伤。“它（那场地震）就像上帝和魔鬼之间的一场战争，最终魔鬼胜利了。”一名居住在杜丽凯尔一个山顶村庄的当地妇女在接受《中国科学报》记者采访时回忆说，当地距离震中约 220 公里。现在，地震已经过去了 3 个多月，从教育到住房、从农业到交通运输，震后的尼泊尔仍在挣扎中前行。

环顾这间教室，可以看到地震造成的累累“伤痕”：被掀掉的屋顶、墙上的裂缝、没有玻璃的窗户。现在，铁栅栏取代了通常的窗玻璃，四面墙上撑着一根根铁管。它们的作用是防止墙上的裂缝继续扩大，同时支撑起学生头顶的临时铝合金房顶。在这间教室中，Ainisha 和另外 3 名学生正在温习功课，他们中两人是 8 年级，两人是 7 年级。

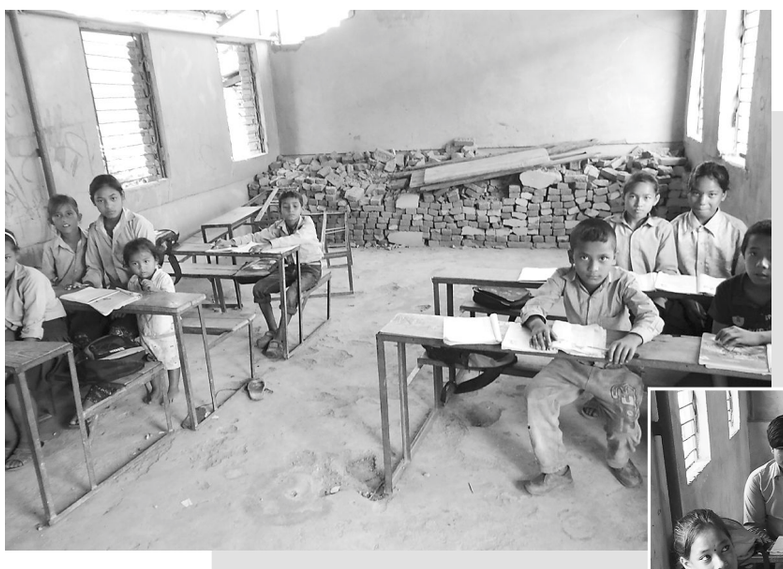
现在，这所学校从一年级到八年级共有 45 名学生，8 名老师。“地震前注册的学生人数比现在多，地震后很多学生辍学了。”Ainisha 的老师、负责教授七、八年级的 Rukmani Nepal 告诉《中国科学报》记者。尽管在尼泊尔从一年级到十年级的教育都是免费的，但是现实情况依然是年级越高，学生人数越少。“一些父母想让他们的孩子回家帮助做农活，一些父母担心学校教室不安全。”她说。政府工作人员曾来学校检查受损情况，但是到目前为止，除了在学校中心搭建的一个塑料帐篷作为临时教室以外，一切都没有改变。

对比来看，杜丽凯尔地区 Hanumah 中学的学生人数在震后并未明显减少。依靠政府发放的 15 万卢比（约 1000 元）救济款和当地村民捐助的 65 万卢比（约 4200 元），该校设法筹建了一个新实验室以及一个临时图书馆。现在，学校从一年级到十年级共有 350 名注册生和 17 名老师。该校校长 Dhakal Phasad Dhikal 在接受《中国科学报》记者采访时说：“地震后，我们对家长做了很多思想工作，让他们相信孩子来学校上学是安全的。”

然而，现在让 Dhakal 和其他教育工作者担心的是另一个问题：创伤后应激障碍（PTSD），即个体经历、目睹或遭遇到死亡威胁或严重创伤后，所导致的延迟出现并持续存在的精神障碍。“地震太可怕了！”Ainisha 说，“有时，一些汽车会在半夜从我家门前的马路上经过，我和爸爸妈妈以为是地震来了，就赶快爬起来跑到屋外。”

为了治疗学生们的创伤应激障碍，缓解他们的焦虑，Dhakal 表示，学校试图通过诸如唱歌、做游戏等方式让他们快乐起来。“但是孩子们受到的惊吓过大，可能要花费很长时间才能让他们恢复过来。”Dhakal 说，“现在，我们的问题是缺少这方面的心理专家。”

尽管如此，希望正在这片被地震摧毁的土地上萌芽。“未来，我想做一名老师，那样我就可以帮助更多人获得知识。”Kabina Shrestha 说，她在当地一个叫作 Dunnara Besi 的村子读初中 9 年级，她非常感谢父母可以让自己在地震之后继续上学，因为她的家里并不富裕，而且非常需要帮手做农活。而对于 Ainisha 来说，明年她将前往首都加德满都追逐梦想，并在未来成为一名医生，从而帮助那些受疾病困扰的人。



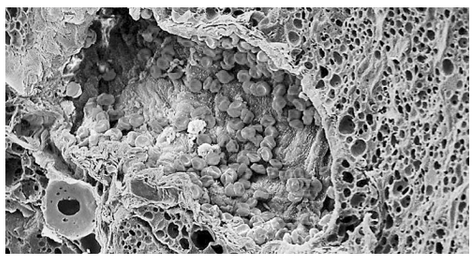
◀尼泊尔杜丽凯尔一所乡村学校的学生正在地震后受损的教室中学习。　冯丽妃摄

▶在尼泊尔杜丽凯尔一所乡村学校，Ainisha B.K（右一）和其他三名学生在温习功课。　冯丽妃摄

科学线人

全球科技政策新闻与解析

英国癌症研究中心发起“大挑战”竞赛



黑素瘤内的血管是肿瘤微环境的一部分，而这正是英国癌症研究中心“大挑战”瞄准的区域。

图片来源：K. Hodivala-Dilke & M. Stone

一个 2000 万英镑的资助项目，正在等待提交解决癌症 7 大挑战之一最佳方案的研究人员的到来。

这项由英国癌症研究中心日前宣布的新竞赛是为了促进研究协作，以便开发那些未经检验但有希望成功的想法。该中心是英国研究类慈善机构的巨头。顾问委员会成员、来自美国俄勒冈健康与科学大学的 Brian Druker 表示，“他们愿意承担一定风险并看到某些项目失败。”Druker 曾帮助研发了靶向癌症分子缺陷的药物模型——格列卫。

该慈善机构希望未来 5 年，通过一系列 5 年期资助，在该项目上花费 2 亿英镑。挑战题目由 Druker 和其他顾问在过去数月内提出。问题清单包括：绘制肿瘤内的细胞和分子“地图”或者微环境；设计靶向涉及多种癌症的基因——MYC 的药物；消除由爱泼斯坦－巴尔二氏病毒引发的癌症，这种病毒是东亚某些癌症的主要起因；研发预防非病毒类癌症的疫苗。

该慈善机构首席科学家 Nic Jones 表示，这些领域此前均被研究过，但并未获得足够资源，或者说科学研究还不够成熟。例如，关于肿瘤如何入侵免疫系统的最新研究促成了一些新药的产生，并且为研制从一开始便能预防肿瘤生长的疫苗提供了启发。“你可以想象此类研究会有多么强大。”团队成员可能来自学术界和业界，但必须包含英国研究人员。

这项英国的努力令人想起“抵抗癌症”（SU2C）。这是一项由美国好莱坞推动的筹款活动，自 2008 年起已将数百万美元投入大型的研究“梦之队”。它还同美国国家癌症研究所（NCI）的项目——“棘手的难题”保持一致。该项目由时任所长 Harold Varmus 于 2010 年发起，旨在确认癌症研究中被忽视的问题。不过，相较于 NCI 的资助，英国癌症研究中心的经费将高出一个数量级；而和 SU2C 资助的有望 3 年内进行临床试验的项目相比，它将解决更加基本的问题。（宗华）

漱口水中氯己定成分或能拯救大量新生儿

氯己定或能预防脐带残留物感染，并因此每年拯救近10万名新生儿。

图片来源：Colin Crowley, Save the Children

2012 年夏季的一个周五晚上，手里拿着一杯酒的 Pauline Williams 正在上网。此时，她突然有所顿悟。作为英国葛兰素史克制药公司（GSK）孕产妇和新生儿健康产品研发部门的主管，Williams 正在寻找 GSK 能在发展中国家作出更多改变的方法。在《柳叶刀》杂志上，她发现了 3 篇文章，而它们非常有说服力地证实了一种抗菌剂——氯己定如何能够预防新生儿残余脐带感染并避免死亡。Williams 来到盥洗室，再次确认了她的预感：洗必泰——GSK 制造的一种漱口水——将氯己定作为关键成分。

GSK 日前宣布，公司正在向欧洲药品管理局申请获得一种氯己定凝胶的批准。这种药品将专门用在发展中国家新生儿的脐带上。其含有的氯己定浓度比用于漱口水的高很多，同时耐热，而且能小袋包装，和用于快餐店的番茄酱包相似。研究证实，这种凝胶更容易被人们接受，并且比溶液中的氯己定更容易用于残余脐带。

“这看上去很令人激动。”美国斯坦福大学儿科医生 Gary Darmstadt 表示。他是最早发现氯己定有望用于预防残余脐带感染的团队成员之一。2006 年，这项在尼泊尔开展的研究发表于《柳叶刀》杂志。并未参与这种产品研发的 Darmstadt 是 GSK 和拯救儿童基金会之间一个合作项目的委员会成员。

对于新生儿，大多数发达国家采用的是被称为“干燥脐带护理”的方法。这意味着修剪的脐带残留物可在没有任何处理的情况下自然脱落。然而，在发展中国家，女性通常在家中很不清洁的条件下分娩。像金黄色葡萄球菌和大肠杆菌等介质很容易进入脐带残留物，并因此感染，有时甚至造成致命性的后果。与此同时，Williams 介绍说，在很多文化中，脐带残留物会习惯性地被裹上牛粪、蜥蜴粪便、灰烬或芥子油，以期加速其愈合，而这会进一步增加感染风险。她表示，氯己定是一种被广泛使用多年且安全的抗菌剂。（宗华）