



区块链技术: 金融科技的新蓝图

■本报记者 赵广立

它被认为是继蒸汽机、电力、信息和互联网科技之后,目前最有潜力触发第五轮颠覆性革命浪潮的核心技术;《华尔街日报》将其誉为“500年以来金融领域最重要的创新”;华尔街清算和结算所——美国证券托管清算公司(DTCC)CEO兼主席 Michael Bodson评价它是“一个可以将交易后环境进行现代化的千载难逢的机会”。

它就是区块链技术。仿佛一夜之间,“区块链技术”成了科技界和金融圈里最时髦的名词。放眼国内外,无论金融人士还是科学家,都对它青睐有加。云象区块链创始人兼首席架构师黄步添认为区块链不仅是当前金融科技领域的核心技术之一,更有望成为未来第四次工业革命的一项核心技术。

作为比特币的底层技术,区块链不仅不像比特币那样饱受争议,还正在更大程度上被接受着、被扩展着。诚如中组部“千人计划”学者、北京航空航天大学计算机学院教授蔡维德所言,面对区块链这样一项新兴技术,科技界、法学界以及金融界“各界人士都对其报以热情与兴趣”。

创造信任的机器

区块链起源于中本聪的“比特币”开源密码协议,目前最成功的区块链也是比特币的区块链。而区块链之所以让人遐想无限,正是因为它拥有了透明度高、不可更改、无需中间人的这些特性。

蔡维德告诉《中国科学报》记者,比特币技术旨在开发不受任何金融机构控制的“数字货币”。由于其本身具有特殊的非中心化主义倾向,因此作为匿名者的中本聪其后不久也销声匿迹,但从那时起,对数字货币底层的区块链技术的讨论却从未停止。

“目前区块链技术主要指通过特殊的算法、加密手段保证网络中数据库的一致性、安全性及可维护性。当前互联网中的所有节点都可以公平自由地跟其它任意节点通信,但是这个技术只解决了通信问题,没有解决信用问题,区块链技术的应用恰好解决了信用问题。”蔡维德说。

区块链如何解决信用问题?“区块链简单的理解就是,去中心化、不可篡改的分布式账本。”黄步添解释说,传统的账本记账错误的时候,不会整个都涂掉,可能会画一条线并做一个备注;现代的账务系统是建立在数据库系统之上,篡改数据成本很低。而区块链网络上的每个“节点”都保存一个完整的账本,那么篡改数据的成本会很高,这便是区块链得以解决信用问题的基础。

《经济学家》对区块链做了一个形象的比喻:简单地说,它是“一台创造信任的机器”。区块链让人们在互不信任并没有中立中央机构的情况下,能够做到互相协作。

如果将区块链仅仅视为一个公开透明、可信赖的账务系统,那就大错特错了。开源框



区块链技术是最有潜力触发第五轮颠覆性革命浪潮的核心技术。 图片来源:百度图片

架 knot.js 的作者“Alex Zhao”(网名)认为,区块链远远不止是一个账务系统那么简单,这项技术将使得“去中心化自动组织公司”(DAC)成为可能。

“DAC是一种能够从根本上颠覆人类社会组织模式的东西。我相信它对社会的影响,会超过工业革命,成为互联网给世界带来的最为深刻的变革。”Alex Zhao说:“它(区块链技术)的意义之重大、用途之广泛,一旦你意识到,你一定会像我一样激动万分的。”

“据谷歌搜索算法统计,2015年10月以来以区块链技术为关键词的检索持续高居榜首。”蔡维德也指出,自2015年以来,区块链持续得到世界各国金融领域的高度关注,显示了区块链技术广阔的应用前景。

高级玩家已进场

实际上,在过去的一年中,区块链已成为全球创新领域最受关注的技术,受到风险投资基金的热烈追捧。仅2015年,全球范围内的风投融资规模就达到了约4.8亿美元,2016年第一季度已达到了1.6亿美元。

除了投资布局,全球各领先的金融机构在具体推动区块链技术应用方面也有很多大动作。包括花旗银行、西班牙对外银行、摩根大通、摩根士丹利、瑞银等在内的40余家领先金融机构共同建立了R3CEV联盟,旨在推动制定适合金融机构使用的区块链标准,推动技术落地。近日,来自中国的平安集团已经加入R3联盟。

麦肯锡5月发布的一份研究报告认为,区块链安全、透明及不可篡改的特性,将使未

来金融体系间的信任模式不再依赖中介者,许多银行业务都将“去中心化”,实现实时数字化的交易。因此,在虚拟货币、跨境支付与结算、票据与供应链金融、证券发行与交易及客户征信与反欺诈等五大金融场景中,区块链将产生最直接和最有效的应用。

目前,区块链技术被应用最成功的场景,便是以比特币为代表的虚拟货币。现在,建立在数字货币区块链软件之上的应用程序已多达数百种之多。在国外,一些基于区块链技术支持的数字资产正在被研发、创造和试验。比如纳斯达克的智能股票,不需要交易所、结算公司,甚至不需要经纪公司,目前有6家公司在上面试验自动交易、自动结算。瑞银集团试验的智能债券,不需要现有庞大体系去促成交易,点对点依靠计算机设置的智能合约即可完成。

“从理论上说,围绕区块链这套开源体系能够创造非常丰富的服务和产品,比特币只是区块链巨大应用空间的冰山一角。”蔡维德说。

对区块链趋之若鹜的还有政府和央行。蔡维德介绍说,今年1月,英国首席科学家代表英国政府把区块链列为英国的国家战略,“这是一件非常惊人、非常重大的事情。一般而言,那些能够带来巨大经济活力、大大提高生产力的事业才能上升到国家战略,英国政府选中区块链,正是因为其认为区块链技术可以带动各行各业合作,从上到下都可以做。他们认为‘这件事情已被科学所证明’。”

英国政府和央行对区块链的态度是坚定的。6月16日,英国央行行长马克·卡尼(Mark Carney)在一次演讲中宣布,英国央行将开放合作,开始使用区块链技术,探索其在

清算、结算中的应用。此外,英国央行还考虑成立一个加速器,发展大量研究人员发掘区块链技术的潜力。

“英央行此举是金融领域一个巨大的变化。区块链技术的落地将带来全新的、全盘的监管技术,重新创造一个数字社会。”蔡维德说,与此同时,新型的法律——计算法学也将及时出现。

“在最近一次麦肯锡对全球金融机构的高管的调研访谈中,50%的高管都认为最快8个月,最近3年内区块链技术最后会有实质性的突破。对于商业银行而言,如何在短时间内掌握这些新的技术并加以应用尤为关键。”麦肯锡全球副董事合伙人韩峰表示。

仍存进一步挑战

然而,正当区块链以破竹之势“占领”金融领域服务时,6月17日虚拟货币以太坊遭遇攻击,全球最大众筹项目The DAO价值6千万美元的以太币被转移,引起了业界对区块链技术的巨大讨论。

蔡维德分析说,本次攻击是The DAO的协议漏洞,而非区块链技术本身存在安全问题,更不意味着区块链的革命性技术进步被终结。

“The DAO使用的是公有区块链而非私有区块链,意味着全世界任何人都可读取,任何人都能发送交易且交易能获得有效确认,任何人都能参与其中共识过程的区块链。这是第一忌。此外,The DAO使用了‘智能合约’,在我看来,‘智能合约’既不智能,亦非合约。”

蔡维德指出,The DAO事件将成为区块链技术应用的一个分水岭,高吞吐量、有隐私权、可靠性强而且是即时系统的私有区块链将成为各类应用开发的重点——英国央行采取的即是私有区块链。

此外,“区块链必须是第三代开始才能被金融机构所使用,必须是非常高速,而且必须要支持监管的各方面。”蔡维德提醒说。

DTCC首席技术架构师Rob Platnick也指出,尽管区块链技术的潜能和机遇让人兴奋,但还是存在一定限制,短期内区块链技术还不会被广泛采用。

“区块链技术仍不成熟,还缺乏证明。它们本质上具有规模限制,也缺乏无缝地整合到现有金融市场的底层基础设施。”Rob Platnick说,大型银行和服务供应商之间的区块链狂热最终会变成现实,一系列的技术开发热潮会创造“区块链孤立的迷宮”。

因此Platnick呼吁全行业广泛合作,进行金融业的现有核心流程的开发和重新架构,用区块链替代它们。

澳大利亚标准协会也支持为区块链发展建立一个全球标准,它呼吁国际标准化组织(ISO)建立区块链技术的全球标准。一旦标准出台,金融区块链技术的发展或将坐上通往未来的快车。

前沿点击

本报讯(记者李惠钰)日前,一项对肌萎缩侧索硬化症(ALS)病人进行的II期临床试验表明,将人类干细胞移植到病人的脊髓中已经具备安全性,但是疗效还不确切,需要进一步扩大临床试验样本量验证干细胞治疗ALS的效果。该研究已经发表在6月29日的《神经学》杂志上。

ALS是脑和脊髓运动神经元退化导致的一种神经紊乱疾病,也被称为“渐冻症”。据官方统计,每年约有5000名美国人被诊断为ALS,没有人知道ALS的起因,但是,它涉及了大脑和脊髓中控制全身肌肉神经细胞的崩溃。该病患者会逐渐失去肌肉控制能力,包括呼吸和吞咽,最终导致死亡。目前仍然没有有效方法阻止这种疾病。

参与该研究的15名ALS患者来自三所大学附属医院,所有病人都在研究之前的两年时间内首次出现ALS症状。研究人员将参与者分为五个治疗组,每名患者都向脊髓内注射了10到40次干细胞,细胞数目从200万到1600万不等。该研究为开放试验,也就意味着病人都知道他们将接受干细胞治疗。

所有参与者都接受了C3和C5区域之间颈部脊髓双侧干细胞注射,剂量最高的治疗组不仅在颈部脊髓部位进行了注射,还在腰部部位进行了双侧注射,不同剂量治疗组注射的干细胞数量在200万到1600万之间。随后研究人员对病人进行了9个月跟踪观察,搜集了有关副作用的信息,还利用ALS功能评定量表评估了疾病进展情况。

研究人员发现,多数患者对脊髓注射大剂量的干细胞有耐受性,但其中有一人出现了与治疗有关的严重并发症,两人出现脊髓肿胀引起疼痛,感觉缺失和部分麻痹,还有一人出现中枢性疼痛综合征。研究人员表示,多数副作用都与手术导致的短暂性疼痛以及免疫系统抑制药物有关。

研究人员将接受治疗的病人的功能与对照病人进行了对比,发现两组病人在疾病进展速度上没有出现差异,但是研究人员提醒到,目前还不应根据这样一个小样本本研究对干细胞疗法的有效性作出结论。

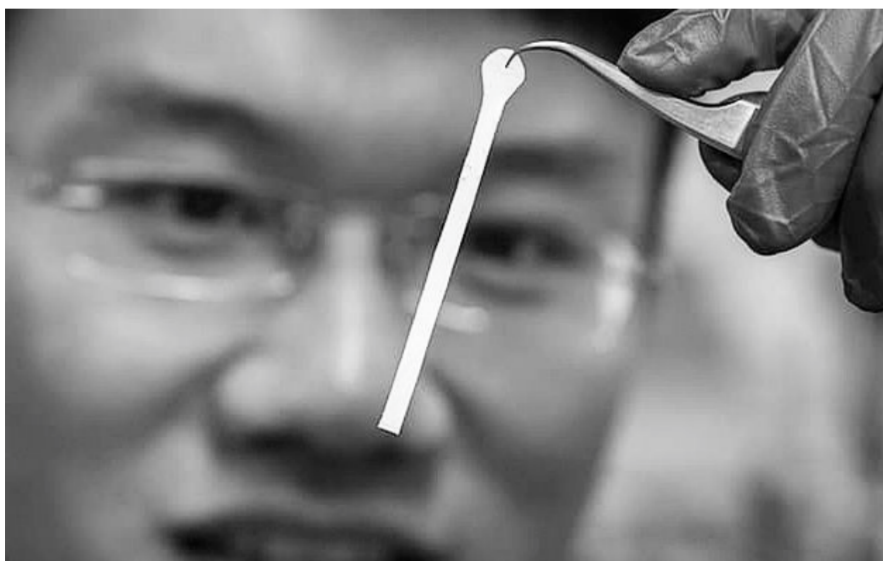
美国埃默里大学的Jonathan Glass博士主持了这一研究,他表示:“这只是开始的一小步。我们可以说这种疗法在ALS患者身上是可行的,现在我们要继续测试这个疗法的有效性。”Ericka Simpson博士是一名神经病学家和ALS的研究人员,她虽然没有参与这项研究,但她表示这个发现为人们提供了重要的希望。

休斯顿理工大学的临床神经学副教授Ericka Simpson博士称,向已经受损的ALS患者的脊柱内注射大剂量干细胞是安全的,这个发现是开创性的。但是,她强调,还有重要的问题没有解决,包括这个疗法长期的安全性怎么样?干细胞是可以分化成成熟细胞的原生细胞,干细胞还有失控生长的可能性。理论上来说,这些干细胞可能会最终导致癌性肿瘤。

研究人员表示,该研究的目的并非确定干细胞疗法对延缓或阻止ALS进展的有效性,并且该研究的参与人数较少,样本量不够大,不足以说明干细胞疗法的效果。该研究最重要的意义在于根据这项研究的结果可以设计更大型的临床试验来检验将人类干细胞移植到脊髓是否是治疗ALS的一个有效方法。

临床试验表明干细胞疗法治疗『渐冻症』具备安全性

酷技术



一种新材料遇到液体时会自动卷曲成吸管的管子。 图片来源:材料人网

材料也有“含羞草”

技术的进步帮助人类发现了众多功能神奇的新材料,今天要介绍的这个有点特殊,因为它有点内向,害羞时还会把自己卷起来。

说到危险液体,当然是科学家离它们越远,操控得越恰当越好。澳大利亚国立大学的科学家也是这么想的,最近他们就开发了一种新材料,其独特之处在于,遇到液体时它会自动卷曲成吸管状,可使液体在管内流动。

该项目负责人William Wong称:“如果在一端滴一滴水,材料就会卷曲成管子,液体能在管内流动15厘米(5.9英寸),利用这一特性,能快速自动成复杂造型,如弯曲或分离通道,从而把微流体系统分离开。”

材料由两层夹在一起的纳米纤维构成,上数第一层是超亲水性聚丙内酯,超亲水性即对水有很大的亲和能力,并在遇到液体时自行卷曲。第二层则由超疏水性(对水排斥)的聚氯乙烯(PVC)构成,当水在管内流动时,它可起到承接水的作用,因此管内衬里是防水的,因此这种材料制造成本低廉,并可批量化生产。

这种材料可能应用于包括生物传感器和微型机器人系统在内的多种领域。应用于上述两领域时,还要在材料边缘加上微型手臂,材料卷起来的时候手臂向内收,这有点像一碰就缩回的含羞草。要是再加上乙醇,管子就会重新打开。(盛夏整理)

科技解码

量子技术可以应用在量子模拟机、量子计算机、量子通信、量子密码、量子传感等多个领域。

量子信息技术: 人类发展的重要一环

■郭光灿

量子力学诞生了一百多年,这是人类最成功的理论。因为有量子力学的诞生,我们才可能有激光、有半导体以及更多先进技术。实际上,量子力学已经在人类生活中发挥着重要作用。

但是,以前由量子原理产生的器件,包括激光、半导体都是经典器件,而量子信息技术是直接利用量子的性质研制出的量子器件,而不是经典器件。这个量子器件的功能要远远超越经典器件的物理极限,这就是量子信息技术带来的新时代的新技术。

实现量子计算机与量子通信为时尚早

量子力学的基本性质主要包含了三个方面:首先,量子力学是叠加状态,所以从信息本身开始就是量子的;其次,量子具有非局域性,而体现了非局域性的纠缠态是量子信息里非常重要的应用;最后,量子具有不可克隆性。

量子计算机性能与电子计算机性能的对比,犹如电子计算机与算盘计算能力的对比。由于量子概率不确定性的特点,使计算机有望突破0即1的二元限制,使计算机存储、计算能力等扩展,从而使IT、通信领域软件、硬件获得革命性进展。

量子计算机实际上跟电子计算机一样,都是要解函数,不同的是量子计算机的处理操作是量子芯片。电子计算机用电子芯片去串行运算,用量子芯片替代它就会并行运算,所以量子计算机的速度就是在量子性,即叠加性导致的并行运算能力,相应的软件、编程也都做出相应的变化。

对于量子计算机,国际和中国科技界做了不懈努力。2002年国际上就开始研究,现在已经成了一个芯片的两个量子比特。虽然中国量子技术研究起步较晚,但近几年发展却非常迅速,在

国际上有一定地位,目前中国已经做到了三个量子比特,四个比特也正在做。

与此同时,中国的量子存储器各种性能,如保真度,还有存储模式等,很多指标上都在国际上处于领先地位。“十三五”期间,量子通信也被划定为未来5年国家重点战略项目。

量子通信从学术上说是通过量子网络把量子信息传递过去。如果有两个量子网络,我们就可构成联网,把所有的网络全连起来,就实现了一个量子云计算,这种功能将会比我们现在电子计算机为基础的计算机网络功能要强得多。

不过由于量子计算机、量子通信在技术突破以及产业化上有着相当大的难度,因此这两项技术还需要长时间的探索与研究,难以在短时期内得以实现。

率先发力信息安全和传感器领域

量子信息技术可能会成为对人类带来最大冲击的新技术。量子技术可以应用在量子模拟机、量子计算机、量子通信、量子密码、量子传感等多个领域。相对于其他领域来说,量子技术将会率先在信息安全以及传感器领域得到应用。

量子信息出来以后,对现在的保密系统产生很大的挑战。首先,现在的保密系统是利用数学的复杂度来确保保密信息的安全性,一个数学的问题要被解了,它的安全也就被破解。

在安全方面,量子计算机还比较遥远,但是量子密码是现在就可以用的。量子密码即量子保密通信。量子保密通信的安全性不靠数学计算的难度,而是靠物理定律,靠量子力学的确定性、不可克隆的基本原理,因而理论上没法破解,从而比现行安全技术更

为可靠。

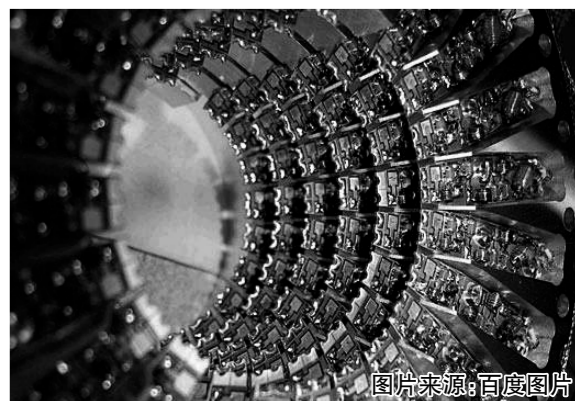
目前,量子密码稳定性等基本问题都已经解决。在某些领域,我国已经进行量子安全的产业化实验,技术已经接近于成熟。不过,由于缺乏量子中继技术,量子安全还只能在一个城市的城域网使用。两个城市之间还不能应用。目前各地正在大力推进智慧城市,量子密码在单个城市应用实现突破,已经开启了一个很大的市场。

另外,传感器利用量子信息,还可以很容易传感各种物理量,这个比现在的传感器不管是灵敏度、精度都有大幅度提高,而这也是在未来几年中将会面临的量子技术的应用。

现在在温度传感器、压力传感器、磁场传感器,我们现在正在做一个纳米级的显微镜,这些都是当前量子传感器领域的研究热点。

总之,量子信息技术将会是人类发展的重要一环。

(作者系量子信息领域专家、中国科学院院士,本报记者李惠钰根据其在第八届中国云计算大会上的发言整理)



图片来源:百度图片