新闻热线：010—58884062
E-mail：adaxuqian@126.com
■责编 许 茜
科技日报
2020年1月15日 星期三

直面量子计算威胁 数字货币在对抗中成长

陈 曦

“这与‘矛’和‘盾’一样，只要有盾，就一定有矛……”日前，华为公司创始人、首席执行官任正非在谈及信息安全时如是说。

任正非口中的“矛”和“盾”，分别指的是基于区块链加密技术的数字货币和基于量子计算机的破译密码技术。

那么，到底是“矛”更尖锐，还是“盾”更坚固呢？当两者相遇，又会发生什么？

对此，中国科学技术大学中国科学院量子信息重点实验室教授韩正甫近日对科技日报记者表示，区块链主要是用非对称加密算法来保护数字货币安全，而量子计算机以其无可比拟的计算能力，对上述加密算法形成威胁，使之可能被破解。

“通俗来说，为抵抗量子计算，加密算法需编制得更‘坚固’；为破解加密算法，量子计算机的性能需要更强劲。未来，构造数字货币的加密算法将与量子计算展开博弈，两者间或有一战。”韩正甫说。

强大算力对加密算法构成威胁

“到目前为止，业界对数字货币的定义尚未形成一个统一的标准。”从事区块链平台开发、建设与运营工作的微观（天津）科技发展有限公司首席运营官石卓对科技日报记者说，从广义上来讲，数字货币泛指一切以电子形式存在的货币，而狭义的数字货币一般特指以区块链加密技术为基础的密码货币，即区块链货币。如今，在“币圈”比较流行的比特币、以太币、瑞波币、莱特币等，指的都是区块链货币。

“可以说，比特币是数字货币的鼻祖，目前市场上的数字货币种类不少，但通常都是基于区块链技术，只是在技术细节上存在些许不同。”石卓介绍说，区块链因具有去中心化、不可篡改的特性而被广泛接受，它奠定了公众对数字资产的信任。而量子计算技术，可能会威胁作为区块链安全支柱的非对称加密算法的完整性，业界对此颇为忧虑。

这种威胁，主要来自量子计算机强大的计算能力。韩正甫介绍说，当前的密码科学其本质就是数学，多数密码其实就是由复杂模型转化成的数学难题。比如，RSA密码利用的就是简单乘法。“举例来说，127×733=93091，这是个简单的乘法等式，如果有人能很快推算出93091是127和733的乘积，那这个密码就被破解了。若乘积是一个100位的数字，那从这个乘积去倒推它是哪两个数的乘积，就是一个非常复杂的问题。”韩正甫说。

“区块链加密技术，主要采用的是非对称加密算法。在非对称密码中，加密和解密用的‘钥匙’是不同的，通常一个是公开的，被称为公钥；另一个是保密的，被称为私钥。公钥与私钥是一对，它们都是用算法生成的，如果用公钥对数据进行加密，那么只有用对应的私钥才能解密。如果给出私钥，很容易就能推导出其对应的公钥，但私钥一般都是保密的，用公钥反向推导私钥则十分困难，计算过程会特别复杂，这就是比特币安全的原因。”韩正甫说。

韩正甫介绍道，以前设计的密码都是抗电子计算机破解的，传统电子计算机需要一步步去求解，这种计算方式叫串行计算。有时为求解一个数值，电子计算机可能要算上万年，这样就在一定程度上保证了密码的安全性。

然而，这道计算难题，似乎能被量子计算机破解。量子计算机采用的是并行计算机制，即多步骤同时进行，这样计算速度就比电子计算机的串行计算机制快很多，特别是在处理复杂问题上。

“借助量子计算机，从公钥反向推导私钥，计算难度有望被大大降低。以前，用传统电子计算机需要经过上万年才能破解的密码，可能量子计算机3天就能将其破解，从理论上说，量子计算机是非对称加密算法当前遇到的最大‘敌人’。”韩正甫说。

量子计算软件尚难攻破“币门”

“想要破解密码，光有量子计算机这个硬件不行，还需要软件，即解密算法，需‘软硬兼施’，两者缺一不可。目前一般认为，肖尔算法和格罗弗算法，这两种解密算法，是公认的量子计算算法。”韩正甫说。

为比特币提供安全保障的，主要是两类密码：一个是在“挖币”过程中使用的哈希算法密码，另一个是在区块链上提供数字签名的算法密码。在“挖币”时，哈希算法会为每个区块计算出一个随机数，这个过程所得到的结果极易被验证，但很难被破解者找到。

“从理论上来说，量子计算机可破解目前正在使用的一些传统密码，但具体怎么破解，目前还没有成功的案例。不过，肖尔算法是最早被证明可在量子计算机上破解非对称加密算法的解密算法。”韩正甫介绍道，早在1995年，肖尔算法的研制者——数学家彼得·肖尔就宣布，如果有量子计算机，他就可破解当时普遍使用的非对称密码——RSA密码。

不过，目前肖尔算法还难以“对抗”哈希算法，格罗弗算法也尚难对基于区块链技术的密码构成太大的威胁。可是，因为肖尔算法和格罗弗算法是公开的，所以数字货币的研发者，在设计时就会有意避开它们。“截至目前，虽然没有人能破解哈希算法，但也不能说哈希算法是量子计算机不能破解的。”韩正甫补充道。

“除了哈希算法和签名算法，未来数字货币还可能会应用其他的密码技术。如果数字货币设计得不好，不用量子计算机，传统计算机也能将其瓦解。”韩正甫说，随着计算方法和技术的进步，目前未被破解的密码难题，未来也可能会被数学家攻克。

双方处于博弈状态 互推彼此进步

数学家们在积极寻找破译密码的“钥匙”时，密码学专家也在积极寻找对抗量子计算机的“武器”。

“目前，已有一些有望对抗量子计算的候选密码。”韩正甫说，比如格密码，它虽然已有几十年的历史，但是由于其在数学计算方面的难度较大，因此一直未被当作密码进行开发、利用。不过，由于量子计算机实在强大，它对密码的攻击是釜底抽薪式的，各种密码在它面前都很容易露出破绽。在这种情况下，格密码又重新被科学家“挖掘”出来，目前正在被重新设计，希望用它来抵御量子计算机的威胁。

石卓表示，还有人认为，应用多种密码联合机制，是可以抵抗量子计算机攻击的。例如，基于哈希算法的密码、基于纠错码的密码、基于格的密码、多变量二次方程组密码等，可将它们联合起来进行使用。但这种方法，因其秘钥长度过长、签名信息十分冗长以及运算时间过长，并不适用于数字货币。但未来可通过技术迭代，补足这些技术短板，用多种密码联合机制研发可抵御量子计算机攻击的数字货币。

除了运用技术手段，任正非表示，数字货币的安全，最终还要依靠法律来保障。“为什么假币不能流通？是因为一发现假币，警察就要去抓你，抓住你就找到了源头，处在源头的人就可能要被判刑。在法律的威慑下，假币不可能流通，货币安全就能够得到保障。因此，信息安全首先是个技术问题，但最终解决还是要靠法律。”任正非说。

“截至目前，量子计算机还未被真正研制出来，这些抗量子计算的密码研究也都处在起步阶段。”韩正甫说。

石卓也表示，量子计算机距离真正成熟还需要一段较长的时间，在此期间，区块链的加密算法也会不断迭代、升级，双方都处在博弈状态中，共同推动彼此技术的进步和发展。

行业观察

微软停止支持Windows 10 Mobile系统

PC时代的荣光照不亮移动时代的路

陈永伟

前不久，微软公司正式结束了对Windows 10 Mobile的技术支持。尽管早在2018年12月，微软就已宣布要放弃Windows 10 Mobile，但却一直保持着对其的技术支持。从这个意义上讲，Windows 10 Mobile仍是个“活着”的系统。而从近日开始，这款操作系统将不会再得到任何安全更新、非安全维护、漏洞修复等技术支持。

随着微软对Windows 10 Mobile支持的停止，采用该系统的应用软件也开始陆续离场，其他第三方应用提供商也逐渐放弃了这一系统。所有这一切，都为Windows 10 Mobile敲响了丧钟，它彻底退出历史舞台只是时间问题。

起个大早却赶个晚集

曾几何时，微软几乎是操作系统的代名词。在PC时代，微软的Windows操作系统所占有的市场份额，一度超过90%。然而，随着PC时代的远去和移动互联网时代的到来，微软在操作系统领域的霸权逐渐走向衰落。

说微软不重视移动端的操作系统，是不公道的，但纵观其在该领域的发展历程，可以用“起个大早赶个晚集”来概括。

早在2000年，微软就推出了一款专门针对平板电脑的操作系统。在较长一段时间内，这款操作系统曾在移动操作系统市场上占据主导地位。然而，它虽名为移动操作系统，但其在设计理念上和PC端的操作系统非常相像，并未根据移动端的特征进行具有针对性的调整。这一疏忽，为微软后来在移动端操作系统市场的溃败埋下了祸根。

2002年，诺基亚推出了基于塞班操作系统的手机。这款手机允许用户根据自己的需要来安装软件、扩展功能，并且针对移动端的特征进行了很多独特性的设计，这让人们首次见识了智能手机的强大。与此同时，塞班系统也开始在移动端操作系统市场上冲击Windows的统治地位。

为了回应塞班系统的挑战，微软推出了供手机使用的Windows Mobile系统。然而，Windows Mobile系统对硬件配置要求较高，不能和塞班系统一样，在小内存环境下流畅运行。更为重要的是，它并未太多考虑手机用户的使用习惯，操作十分复杂。因此，Windows Mobile推出之后并没有取得足够的反响，也没有在市场上普及开来。

此后，微软又陆续推出了很多新版本的Windows Mobile，试图以此赢得移动端操作系统市场主导权。然而，这些尝试都没有取得成功。做惯了PC端操作系统的微软，总习惯于用做PC端操作系统的思维来考虑移动端，在研制系统时，不仅对硬件配置要求很高，操作上也设计得十分复杂，因而在竞争中举步维艰。

如果说在2007年之前，微软还可凭借其“老本”在移动端市场上占据一席之地，但在2007年之后，它的状况只能用溃败来形容了。2007年1月，苹果公司发布了iPhone。这款手机一经推出，就大受追捧。由于iPhone用的是自家的iOS系统，因此微软在移动操作系统市场上的地位遭受了较大的打击。

不过，更大的打击还在后面。

2007年11月，谷歌公司联合84家硬件制造商、软件开发商、电信运营商一起组建开放手机联盟，共同推出了改良后的安卓系统。作为一款开源产品，安卓系统的安装和使用都是免费的。这一特征让手机制造商欣喜若狂，纷纷选用安卓系统来装备自家手机。到了2011年，安卓系统的市场占有率已超过塞班系统。不久后，安卓系统又迅速将市场份额扩张到80%，而Windows Mobile的份额却在节节败退，最糟时甚至退到1%。

为力挽狂澜，微软于2015年推出了Windows 10 Mobile操作系统。这时，微软终于踩上了移动互联网时代的步点，开始在系统设计上更多考虑移动端的特点，因此客观来说，Windows 10 Mobile确实有可圈可点之处。首先，它一改此前对硬件高要求的特征，在中等配置的手机中便可运行得十分流畅。其次，它能很好地支持Office组件，这极大满足了用户利用移动端办公的需要。

不过，遗憾的是，所有的这些努力，都未能帮微软赢得用户的心。到了最后，这款优质的操作系统还是没得到市场的承认。

在失败的泥潭中越陷越深

那么，这个在PC时代具有统治地位的公司，为何在移动操作系统市场上输得一败涂地？笔者认为，其根本原因在于，微软一直是在用做PC端操作系统的逻辑来做移动端操作系统。

相比PC，移动设备有两个鲜明的特征。首先，它的性能要远低于PC，因此在PC上能运行流畅的程序，在移动端很可能“跑”不起来。其次，相比PC端，移动端设备的显示面积要小得多，操作局限却大得多。这就要求移动端的操作系统必须简化操作，不能像PC端的操作系统那么复杂。一个移动操作系统想要成功，就必须根据这两个特点来优化设计。唯有如此，才能给用户带来良好的使用体验。然而，如前所述，微软由于固守PC端的逻辑，所以在初始的竞争中就被压制了下来。

虽然后来微软也意识到了问题所在，试图进行补救，但为时已晚。操作系统是具有很强网络外部性的产品，它的使用人数越多，对于新用户的吸引力就越大，因此安卓、iOS等操作系统在初期的成功很快就为它们的下一个成功铺就了道路。反观微软呢，只能在失败的泥潭中越陷越深。

当然，微软放弃Windows 10 Mobile、退出在移动设备操作系统市场的竞争，也未必完全是件坏事。事实上，在微软公司现任首席执行官萨蒂亚·纳德拉上任后，微软的重心已从操作系统转向了云计算。微软放弃了对移动设备操作系统的争夺，就意味着它将更多的资源转移到云业务上。所谓塞翁失马焉知非福，没准儿，放弃这个一直赔钱的业务，对微软而言是桩好事。

（作者系《比较》杂志研究部主管）

APP图标频“撞脸”，是否侵权要看两点

本报记者 张 蕴

在日前举办的2020年国际消费类电子产品展览会上，三星公司在对外播放的PPT中，其展示的面部识别图标，“神似”苹果公司的Face ID图标，三星由此被指涉嫌抄袭。

近来，在互联网圈此类事件频出。早前，社交应用绿洲APP图标被指与韩国著名平面设计工作室studio fnt 2015年给Ulju Mountain电影节设计的视觉形象高度相似。前不久，据媒体报道，脸书公司天秤币数字钱包的图标，与移动支付工具Current的图标十分相像。

为什么APP或其相关图标会频频“撞脸”？这些“撞脸”行为是否构成侵权？被“撞脸”的商家究竟该如何维权？我国又是如何界定此类侵权行为的？针对上述问题，科技日报记者采访了业内相关专家。

独创性内容成判定关键点

这些“撞脸”行为是否构成侵权？

青海辩理律师事务所律师哈成堂在接受科技日报记者采访时介绍道，在我国侵犯知识产权罪是指违反知识产权保护法规，未经知识产权所有人许可，非法利用其知识产权，侵犯国家对知识产权的管理秩序和知识产权所有人的合法权益，违法所得数额较大或情节严重的行为。

“根据《中华人民共和国著作权法》（以下简称《著作权法》）第3条规定，《著作权法》所称的作品包括计算机软件，即APP及其相关内容可被认定为是《著作权法》中的作品，应受到《著作权法》保护。APP作为网络商品，与其他商品一样，也有自己的商标，图标即可被视为商标，相关权利人享有商标权。根据《中华人民共和国商标法》（以下简称《商标法》）第57条的规定，未经商标注册人的许可，在同一种商品上使用与其注册商标相同、相似的商标，或在类似商品上使用相同或相似商标，容易导致混淆的，就应被认定为侵犯商标权。”哈成堂表示。

在中国社会科学院大学互联网法治研究中心执行主任刘晓春看来，判断APP“撞脸”是否构成侵权，要看两大要素。

“从著作权角度判断侵权，首先要看APP或其相关图标的设计是否属于常规设计，若属于常规设计，设计要素就会很接近，这未必构成侵权。其次，要看APP图标对于相关人群来说，相似程度多高。”刘晓春解释道，在判断是否侵权时，一般要从设计师角度来看，APP图标设计中是否含有独创性内容。这些意见对于判定侵权与否，至关重要。

及时申请商标可有效维权

在刘晓春看来，APP图标频频“撞脸”，是互联网行业浮躁的表现。“商家用非常接近的标识，我个人认为，这不是好现象。从业者应尊重原创，努力去创新，以增加自身的辨识度，而非通过投机取巧的方式去模仿别人。从长远来看，这是损害自身品牌和美誉度的行为。”刘晓春说。

那么，从商家角度来看，究竟该如何维权、避免被“撞脸”呢？

“可通过《商标法》进行维权。”哈成堂表示，在APP开发过程中，相关权利人可为APP图标申请商标，这是一种很好的选择。我国对商标权的保护，遵循的是申请在先原则，即谁先申请谁就享有商标权。同时，商标权的类别繁多，权利人在申请商标权时，一定要加以注意和区分，以免在申请操作环节上出现纰漏，不利于商标的保护。

那么，在国家层面，是否出台了相关文件或规范呢？有关部门又该如何进行有效监管呢？

国家市场监督管理总局局长张茅此前在接受媒体采访时表示，在我国知识产权虽属私权，但在众多领域，侵犯知识产权行为不仅损害权利人利益，还会危害公共利益。我国现行《商标法》明确规定，对侵犯注册商标专用权的行为，工商行政管理部门有权依法查处。

为有效查处侵犯知识产权行为，我国法律赋予行政执法部门行政检查、行政强制、行政处罚等权力。比如，我国《商标法》规定，行政执法部门可采取询问当事人、复制有关资料、实施现场检查、查封扣押相关物品等措施，并可实施责令立即停止侵权行为、没收销毁侵权商品和制造工具、罚款等行政处罚。对于5年内实施两次以上商标侵权行为或有其他严重情节的，还可以从重处罚，对于涉嫌犯罪的移送公安机关。这些处罚措施有利于迅速制止侵权行为，并在一定程度上消除了侵权者继续实施侵权行为的条件，可对侵犯知识产权行为形成威慑和预防。