# 电脑书城

中华读书报

■本版编辑:方文国 ■电话:010-67078075 ■E-mail:dushubaokf@163.com 2017年7月12日



传统风险不断,新的威胁一直出现。网络和数据安全的未来,无论是否基于区块链作为重要工具,都必须拥有整体安全理念。区块链虽然不是修复所有互联网问题的灵丹妙药,但他可以成为专家和工程师的强大工具,开发出变革性的安全应用,赋予互联网更丰富的价值和更美好的未来。

## 应用区块链重塑网络安全的未来

■徐云峰

为什么有人说互联网时代将要结束,区块链时代即将来临?因为互联网是分散而破碎的,导致信息私有化和信用成本高,如何让网民高效有效地证明“我就是我,你就是你”,是影响互联网普及发展的瓶颈问题。而区块链技术就保证了数据的真实可靠和公开透明,做到了不用到银行开财产证明,不用到警局开犯罪证明,不用到用人单位开在职证明就能完成各项工作,成为颠覆互联网应用的创新技术之一。

区块链技术是利用块链式数据结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问的安全、利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算范式。麦肯锡的研究表明,区块链技术,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。

区块链技术因为其解决了信息通信中的一个基础问题(拜占庭将军问题)而得到极大的关注和应用,将其对应到通信世界中,可有效解决分布式系统中进行信息交互时面临的难题,即在整个网络中的任意节点都无法信任与之通信的对方时,如何能够达成共识来进行安全的信息交互而无须担心数据被篡改。区块链的出现,让这个问题迎刃而解,当有一个公开、透明的账本存在的情况下,整个系统中的所有节点都能够在信任的环境下进行自动安全的数据交换。因而区块链技术具有重塑网络安全的潜质。

首先,区块链技术先天具有网络安全的基因。如以下一些区块链的关键技术都为解决某个网络安全问题而生,进而形成了区块链的支撑技术:

(1)Hashcash 是 1997 年提出的限制和禁止电子邮件垃圾邮件和拒绝服务攻击的系统。 Hashcash是一种需要牺牲处理能力作为安全机制的算法。这种工作证明创建了激励结构和网络验证,现在为加密货币提供支持。

(2)20 世纪 70 年代的 Merkle 树的密码学突破和20世纪90年代的分布式哈希表结合起来,为分布式系统创造自主性,容错性和可扩展性。

(3)1993 年 Nick Szabo 创造的智能合约算法是一种自执行代码。可以将合约写入到区块链中,无论何时,合约都能够可靠地监控合约中参与方的执行情况,参与方是无法进行欺骗的。

如今,网络攻击技术不断进步,互联网的中心化发展模式已成为黑客攻击的软肋。要想彻底解决这个问题,必须实现去中心化的网络。区块链技术可以为网络安全提供新的变革思路。透过目前的发展,区块链技术已在如下方面展示出优越性:

(1)数字身份认证

数字身份被广泛地定义为计算机系统用于表示某个实体(个人,组织,应用或设备)的任何一组信息。数字身份的常见形式是基于密码的访问凭据和用户档案,其可以包括用于验证实体被授权从事事务的各种身份凭证。

数字身份的三个基本方面:身份创建(创建有效的身份凭证),身份验证(这些凭据的验证)和授权(由这些凭证提供的权限的验证)。

目前的数字身份模型通常涉及具有不同提供商存储的单独身份凭证的用户。然而,区块链技术的分布式性质提供了关于数字身份的基本范式转变,其中身份凭证由个体用户而不是提供者来控制。美国非营利组织 Sovrin 基金会最近提出了一个“自主”身份的模式,用户管理和控制自己的身份证件。个人在由 Sovrin 管理的公共许可块上创建具有各种身份证件的数字身份。这些凭据随后由服务提供商根据需要被全球服务提供者访问和验证,但个人的个人信息仍然保留在个人控制之下。

(2)数据真实性保证

通常我们用数字签名来证明数据来源的真实性,然后我们需要费力地证明其对应的公钥的真实性,但这是个很难的事情。

区块链技术为我们提供了新的思路,用区块链存储文件签名信息,通过区块链节点的透明、分布式证明代替私钥的保密性,保证数据不被操控。

数据安全初创公司 Guardtime 的安全解决方案运行在私有链上,具有替代RSA数字签名的垂直解决方案:其KSI(无钥匙签名基础架构),其仅使用哈希函数加密来进行签名。KSI 在区块链上存储数据和文件原件的哈希值,通过哈希算法验证其他备份,并对比区块链存储的信息。任何数据修改痕迹可以很快被发现,因为原件的哈希值存储在几百万个节点上。

(3)消除单点故障

分布式拒绝服务攻击(DDoS)给我们的教训可谓深刻,黑客只需攻击域名服务(DNS)供应商,就可以切断 Twitter、Netflix、PayPal 等服务的登录入口,这也证明了中心化模式的脆弱性。

业内专家认为,用区块链技术构建DNS 系统可以有效改善安全形势,消除单点故障。Nebulis 是探索分布式DNS概念的项目, Nebulis采用以太坊区块链和IPFS替代中心化的HTTP,用来注册和解析域名。这样即使服务请求太多也不会导致网络崩溃。而且还可以省去与DNS解析等有关的费用。透明的分布式DNS将域名置于所有者控制之下,使得任何单个机构(包括政府)都无法操控。

(4)物联网访问控制

物联网正在飞速发展,随着连接设备的数量继续呈指数级增长,至关重要的是对这些设备的基础安全性的保证以及它们对互联网的安全性和稳定性造成的威胁的应对措施。

分布式IoT的概念是一种很有希望的方法。随着设备计算能力的提高,设备本身的智能也不断提高。利用这种边缘智能原理,用户对其生成的数据的粒度可以实施更多的控制。然而,由于这种方法的副作用,终端用户不应该成为使用安全机制的专家。一个简单的错误或错误配置可能会导致他们隐私的巨大破坏。因此,主要是在分散办法下的访问控制必须足够用于普通人。此外,分散式方案面临以下挑战:在设备方面实施当前的安全标准和访问控制解决方案更为复杂。它需要集中和计算能力,并不总是可用的,特别是在像传感器,执行器或RFID标签等设备上。而且,通过将这些功能外包给强大的功能,可以减轻处理大量访问控制相关信息的负担。实体防止端到端的安全性得到实现。此外,将授权逻辑委派给外部服务需要委托实体与设备之间的强信任关系。此外,它们之间的所有通信必须被保护和相互认证,以便被委托的实体安全级别至少与内部实施授权逻辑一样高。因此,我们认为,物联网需要一种适合其分布式性质的新的访问控制框架,用户可以控制自己的隐私,而不是由中央管理机构控制,同时也需要集中的实体处理授权功能难以约束IoT设备。利用块链技术解决上述集中式和分散式访问控制管理挑战的困境。

综上所述,区块链技术确实能够为我们提供一种全面的网络安全解决方案。实现端到端安全性,包括事务安全性,防范疏忽或恶意内部人员,通信基础设施安全和服务器故障等。

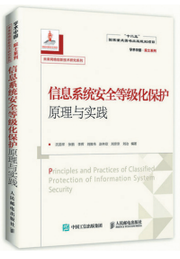
传统风险不断,新的威胁一直出现。网络和数据安全的未来,无论是否基于区块链作为重要工具,都必须拥有整体安全理念。区块链虽然不是修复所有互联网问题的灵丹妙药,但他可以成为专家和工程师的强大工具,开发出变革性的安全应用,赋予互联网更丰富的价值和更美好的未来。

(本文作者系中国指挥与控制学会认知与行为专委会副主任委员,中国计算机学会高级会员、中国计算机学会安全专委会常务委员;十一届、十二届全国青联委员,中国互联网协会特聘网络安全青年专家)

## 本版推荐

**《安全简史——从隐私保护到量子密码》,杨义先 著,电子工业出版社2017年06月,68.00元**

本书以优美、风趣的文字,对网络空间安全的关键技术进行了深入浅出的科普;把高深的安全理论和技术,演绎得生动、活泼,以至于普通大众都能在笑声中,毫无障碍地阅读全书。



**《信息系统安全等级化保护原理与实践》,沈昌祥、张鹏、李挥、刘敦伟、赵林欣、刘京京、刘冶 著,人民邮电出版社2017年05月,128.00元**

本书通过分析当今信息安全的严峻形势以及其重要特性,并结合我国信息系统等级化的管理历程,提出了适应我国国情的全新的等级化保护体系。首先明确了等级保护的体系构建,包括其整体结构以及各模块内容。

**《网络攻击与漏洞利用:安全攻防策略》,[美] 马修·蒙提 著,宴峰 译,清华大学出版社2017年04月,39.80元**

本书将讲解安全工具及其用法,简单介绍计算机操作的固有属性以及网络攻击和利用原理;并呈现多个实例,解释其工作方式、所用工具以及应用时需要的资源。

**《信息安全原理与技术(第3版)》,郭亚军、宋建华、李莉、董慧慧 著,清华大学出版社2017年03月,39.50元**

本书系统地介绍了信息安全的基本原理和基本技术。全书共11章,包括信息安全的数学基础,对称密码技术、公钥密码技术、消息认证与数字签名、身份认证与访问控制、网络安全协议、公钥基础设施、防火墙、入侵检测和恶意代码等内容。

**《Rootkit隐遁攻击技术及其防范》,张瑜 著,电子工业出版社2017年01月,58.00**

本书系统论述了Rootkit隐遁攻击的概念、原理、应用技术及检测取证。首先,简要回顾了Rootkit的由来、定义、原理、类型及其演化。其次,阐述了Rootkit技术的基础理论,包括硬件系统、软件系统,以及Windows内核驱动程序设计。

## IT风云播报 主持人 雪洋

**顺丰菜鸟之争:**6月1日凌晨,中国市值最大的快递物流企业顺丰和最大的物流及供应链平台菜鸟之间短兵相接“交战”。 随后,顺丰关闭了淘宝平台物流信息回传,菜鸟切断丰巢信息接口,双方矛盾进一步激化,甚至后来淘宝卖家指出其无法在物流端口上传顺丰单号。6 月 2 日晚,国家邮政局召集菜鸟网络和顺丰速运高层来京,就双方关闭互通数据接口问题进行协调。双方同意从6月3日12时起,全面恢复业务合作和数据传输。

**苹果公司发布iOS 11操作系统:**6月6日,苹果公司在WWDC2017大会发布了iOS11全新操作系统,针对中国用户推出特色功能,包括诈骗短信识别、扫描二维码、识别上海方言等。其中值得一提的是,苹果再度与腾讯公司携手解决骚扰诈骗难题,在已实现拦截骚扰诈骗电话、清理日历广告的基础上,带来了垃圾短信识别和欺诈网址识别功能,针对“接打电话、收发短信、浏览网页、查看日历”等四大可能经常出现骚扰问题的iPhone手机使用场景实现全覆盖。

**苹果强制打赏抽成30%:**6月11日,苹果公司在其开发者网站上更新《安全审核指南》,明确应用内向原创作者的“打赏”属于“应用内购买”,所有支付行为均需通过苹果公司提供的通道,并向苹果公司分成30%。此前,由于长久未能与苹果公司达成协商,iOS版微信已关闭了公众号内文章下的赞赏功能,而今日头条、知乎等则选择了妥协。

**摩拜单车获得超6亿美元融资 腾讯再次加持:**6月16日,摩拜单车宣布完成超过6亿美元的新一轮融资,这一数字创下共享单车行业诞生以来的单笔融资最高纪录。摩拜单车本轮融资由腾讯领投,新引入的战略和财务投资者包括交银国际、工银国际、Farallon Capital等重磅投资人;TPG、红杉资本中国基金、高瓴资本等多家现有股东继续增持跟投本轮。华兴资本在本轮融资中继续为摩拜单车提供独家财务顾问服务。

**京东618数据出炉:**京东618电商节从本月1日便声势浩大地展开了,不过,在这其中用户最疯狂的时段还要属6月18日零点开启的疯抢活动,在活动开启的第一个小时销售额便超过去年同期的250%,而到了该日凌晨2点11分的时候,京东618累计下单金额突破1000亿元。截至6月18日24时,京东平台自6月1日起所累计的下单金额达到了1199亿元。相对全国其他城市而言,北京、上海、广州、深圳、成都、武汉、西安、重庆、苏州、天津的参与量最为突出,收获了不少秒杀商品。

**中国移动完成千兆LTE外场下载测试:**近日,中国移动联合高通,基于TD-LTE 4G+网络,在浙江首次完成了商用终端的“千兆级速率外场测试”。测试数据显示,下行峰值速率达到700Mbps以上,平均速率680Mbps左右。此次外场测试的成功,表示中国移动已经具备将其4G+网络升级至全球最领先水平的能力,并且为即将到来的5G时代奠定坚实基础。

**腾讯:《王者荣耀》成全球最赚钱手游:**近日,根据第三方数据机构App Annie发布的5月全球手游指数榜单,由腾讯开发的《王者荣耀》成为了全球最赚钱的手机游戏,值得一提的,位居前三的手游都有中国公司参与其中。由网易、腾讯分别开发的《梦幻西游》《皇室战争(Clash Royale)》占据了第二第三的位置,名列第四的则是日本mixi旗下的《怪物弹珠》则是全球十大最赚钱手游中唯一一款没有中国公司背景的游戏。

**中国超级计算机成世界最强:**24年前,业内便开始评选世界最强的500台电脑。长期以来,美国都占据着该榜单的前三名。在最新发布的全球500强超级计算机榜单上,中国计算机排名超过了美国。根据最新的排名,两款中国超级计算机以及一台升级版的瑞士超级计算机占据了榜单前三名的位置,其中中国超级计算机神威太湖一号、天河二号分别获得了第一和第二的位置,美国的计算机名列第四至第六位。榜单中前十位的超级计算机美国霸占了5位,这一地位无人能够撼动的。此外,在全球500强超级计算机的名单中,美国上榜的超级电脑便有169台,数量居全球第一,而中国则以160的台数位居第二。

## “王者荣耀”:是游戏还是“毒药”?

■袁跃兴

据7月3日中国新闻网报道:最近,被戏称为“王者农药”的游戏《王者荣耀》似乎成了“毒药”。“13岁男孩因玩‘王者荣耀’被说跳下4楼,刚醒又想登录游戏”、“狂打手游‘王者荣耀’40小时,广州17岁少年患脑梗险丧命”、“小学生为玩王者荣耀‘偷’光家里积蓄”、“11岁少年玩‘王者荣耀’,三个月花光全家多年攒下的三万多”,这样的新闻近日频频出现在大众视野中,不仅网友们尤其是“受害者”家庭,对这款游戏表示极度不满,纷纷声讨,杭州的一位老师更是发文“怒怼”《王者荣耀》,批它“成了新时代‘黑网吧’”……

这位老师的文章叫《怼天怼地怼王者荣耀》:“我比很多家长都要痛恨看到孩子们沉迷手机的样子:那种专注、那种迷恋、那种爱慕、那种笑逐言开……我现在不能以丝毫的恶意来揣测我们的孩子。当孩子泪流满面的和我说,老师我控制不住自己,我不敢告诉父母,怎么办怎么办老师? 那一刻我感觉我的心也被扎了。手机是把双刃剑,对我们成年人来说,利大于弊,我们能自控,我们不会沉迷,我们不会打争霸赛直到凌晨3点,我们不会去买二手机只为能打游戏,我们不会花大把的钱去买游戏装备,我们不会时时刻刻感到手机里有人在呼唤自己的魂魄。但孩子呢?”文中有对孩子极端沉迷这款游戏的痛苦无奈,更有对这款风靡中国的手机游戏对于孩子们的时间、稚嫩的生命和单纯的心灵的侵占和伤害的痛斥……

从新闻看,不少孩子因为这款游戏玩到“虚脱”“失踪”、玩死玩伤,已引发社会关注,杭州这位老师的“怒怼”《王者荣耀》,更是对中国游戏业、游戏从业者的良知和责任的大声疾呼。

7月2日,腾讯通过其微信官方账号发布“《王者荣耀》将推最严防沉迷措施”的消息,7月4日以《王者荣耀》为试点,率先推出健康游戏防沉迷系统的“三板斧”,其中包括未成年人限制每天登陆时长、绑定硬件设备实现一键禁玩、强化实名认证体系等措施。但这样的技术手段,能否改变娱乐至死、沉迷病态的娱乐心理和游戏心理?

据公开资料显示,《王者荣耀》是全球第一大手游,其累计注册用户超过2亿,日活跃用户超8000余万,月流水30亿元,中国每7个人就有1个人玩。这款游戏的玩家,不仅包括大量的未成年的孩子,还有不少年轻人,甚至女性。因为《王者荣耀》玩家群体的庞大,以至有评论说,这款游戏已成“国民游戏”,甚至成为“一种社交需求”。

现代电子技术条件下娱乐经济中发展起来的游戏文化,其实是仍然难以脱离人类游戏文化产生的根源。游戏作为一种人类的活动,首先它是人们对待生活和生命的一种态度。这种游戏的态度,是单纯的,纯发乎自然怡情乐性的事情,游戏有一种超越利益的美,它有一种生命的自由感和精神世界的解放在内的,所以,游戏是没有什么利益可图的,而进入当代世界,随着消费经济时代的到来,把娱乐消遣活动作为经济,把游戏作为产业,游戏的文化本质精神正在被解构,游戏的超越利害关系的意义也被化解,游戏正在成为商业市场的附庸形式,按照市场的原则被纳入到当代整个娱乐文化工业中去。追求功利,追求商业化,追求价值利益,越来越成为游戏的直接目的,它们“发展的理由,除了利益,还是利益”。

2008年马云在电子商务专题汇报上表示“饿死也不做游戏”,“我们坚定地认为游戏不能改变中国,中国本来就是独生子女家庭,孩子们都玩游戏的话,国家将来怎么办?所以游戏我们一分钱也不投。人家投,我们鼓掌,但我们不做,这是我们的一个原则。”但商业总要往前走,当年不做游戏的阿里巴巴,也在5年后的2013年宣布进军游戏产业。

石悦,是2006年内蒙古地区理科高考状元,本科就读于清华大学建筑系,在校期间的成绩也非常突出,毕业论文被评定为优秀,研究生则是在北京大学深造,读研期间更是在北大拿到了含金量极高的国家奖学金,是一个名副其实的学霸。但毕业后她放弃建筑设计师的工作去从事游戏主播一职,目前在某网络直播平台拥有109万的关注,新浪微博90万粉丝。她已成为许多孩子、许多年轻人实现梦想的偶像。

游戏娱乐文化工业,商业利益目的是十分明确的,这就是它把大量的追求新奇事物的年轻人,当作是实现商业目的的猎物,当作时尚娱乐的主要市场。游戏娱乐文化所创造的一切时尚、流行、偶像、梦想、愿望、感官之乐,等等,几乎都是针对年轻人这个庞大群体的。于是我们看到了,许多年轻人的价值观念,精神状态,生活方式,人生梦想等,已经受到了当今这种时尚娱乐文化色彩的影响。

娱乐、游戏与社会实际生活的关系是怎样的? 当游戏娱乐从人的能量储备中借出的数目过大,因而在日常生活过程中无法偿付时,游戏娱乐对实际生活就成为一种危险。当这种情况达到危机顶点时,实际生活或“真实”的生活在情感上就破产了。这时,精神上出现了疾病,它的症状就是无止境地渴求游戏娱乐,并且完全丧失了对实际事务、对日常生计和社会义务都是必要的工作的兴趣和能力。这种精神疾病如果在一个人身上发展成为慢性病,他就会或多或少心安理得地相信,游戏娱乐是使人值得生活下去的唯一东西。如果在一个社会里这种疾病成了流行病,那么大部分人在大部分时间里就都会感染上这种病态的人生信念……

当娱乐工业文化开发游戏的直接目的是“除了利益,还是利益”,《王者荣耀》成了“国民游戏”、“一种新的社交方式”,游戏主播成为年轻人梦寐以求的新职业,不少孩子为《王者荣耀》抓狂……我们的文化、我们的娱乐、我们的游戏,是否已经出现了这种流行病? 我们是否该引起警醒?