摩石观察

密码是保障网络安全的核心技术和基础支撑，在维护国家安全、促进经济社会发展、保护人民群众利益中发挥着不可替代的重要作用。云物移大智的蓬勃发展，5G、智慧城市、互联网 + 政务服务的全力推进，离不开用密码技术来保障网络安全、保护数据安全、保证网上诚信，需要密码学与其它学科深入合作，需要密码产业与其它产业的深度融合，需要产学研管用的真诚协作，需要全社会共同传播密码知识与政策、研究密码应用技术、推进密码应用方案。

为激浊扬清，构建以密码技术为核心、多种技术相互融合的新网络安全体系，推进密码技术科学规范应用，长期深耕于信息安全一线的卫士通公司凝聚了一批国内顶尖的密码专家于 2016 年建立了摩石实验室。依托密码基础理论，探索密码创新实践，解决密码应用难题，培养密码专业人才，摩石实验室致力于让密码技术更好地服务于网络强国、数字中国和智慧社会。

本着共同的愿景，《信息安全与通信保密》杂志社与摩石实验室精诚合作，专门开辟《摩石观察》栏目。立足于密码本真，反思密码实践，《摩石观察》将以密码人的细致严谨叩问密码创新的真理之门，为广大读者了解、认识、掌握、使用密码技术提供准确规范的参考依据；同时我们期望以密码会友，与理想作伴，热忱邀请有志之士共同探索密码理论与应用的最佳实践，为推动金融等重要领域密码应用与创新发展而奋斗。

区块链技术的安全风险

王现方

1 背景介绍

2008 年，中本聪在一篇名为《比特币：一种点对点的电子现金系统》的论文中首次提出了比特币，随后在 2009 年比特币网络正式启动。经过几年的考验，比特币因其网络的稳定性及创新性而逐渐受到人们的广泛关注。随后，区块链这一概念被抽象出来，它可看作是比特币的底层技术。简单的理解，区块链是一种去中心化的分布式账本技术。

近两年，区块链逐渐成了热门话题，频繁出现在媒体及学术会议上，各类企业和研究机构也逐渐成立了区块链实验室，区块链这一新兴技术正在逐渐的发展。比特币可看作区块链的第一个应用，即区块链 1.0；区块链 2.0 也随

后出现，即以以太坊为代表的可编程的智能合约平台。时至当下，各种基于区块链技术的项目和相关的应用如雨后春笋般涌现，但区块链作为一门新的技术才刚刚起步，其本身还有许多不足和缺陷。本文从技术自身的角度探讨区块链面临的一些安全风险和挑战。

2 伪随机数生成器的陷门

区块链属于算法高度密集的工程，应用了大量的密码学算法，区块链达成的共识本质上是对密码算法所基于的数学难题的共识。区块链所用到的密码算法主要有数字签名算法和杂凑函数，随后也有很多密码算法和协议被引入应用到区块链中，如环签名，零知识证明，承诺协议，安全多方计算等。可以说，密码算法和协议的安全决定着区块链技术的安全。

在密码算法中，随机数是不可或缺的参数，安全的随机数生成机制是密码算法安全的重要支撑。由于真随机数的生成比较困难，一般在密码算法中都采用达到特定安全要求的伪随机数去替代真随机数。伪随机数一般采用伪随机数生成器生成，如果选取的伪随机数没有达到要求，算法就不安全，例如，比特币区块浏览器 blockchain.info 被曝随机数没有正确的生成，进而导致私钥暴露。另一方面，伪随机数生成器的设计有可能留有后门，即使是标准算法也不例外，例如，NSA 曾将带有后门的 Dual_EC_DRBG 写入 NIST 的确定性随机数生成器推荐标准，并收买 RSA 公司将该算法设置为 BSafe 中默认的随机数生成算法。值得一提的是，虽然比特币也选择了 ECC 来生成随机数，但选的是小众的曲线参数，有效地避开了这一问题。区块链中广泛需要生成随机数，如果选取的伪随机数生成器存在后门，造成的损失是不可想象和不可挽回的。一般构造的伪随机数生成器如图 1 所示。

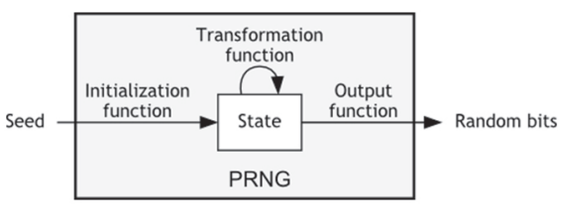

图 1 伪随机数生成器示意图

3 椭圆曲线的抗量子脆弱

基于椭圆曲线的密码算法，因其具有良好的安全性和运算效率而被广泛应用，椭圆曲线如图 2 所示。数字签名算法具有不可抵赖、防止冒充等特点，很多基于区块链技术的产品和项目中采用了基于椭圆曲线的数字签名算法，用于身份鉴别和对交易数据的确认。椭圆曲线数字签名算法的安全性依赖于椭圆曲线上离散对数的困难性，此类数学难题目前还没有被破解。随着时间的推移，一旦底层数学问题被破解，那么此类密码算法将不再安全。另外，虽然椭圆曲线上的离散对数问题在经典计算机上破解难度很大，但如果量子计算机出现，椭圆曲线数字签名算法将没有任何安全性可言。虽然目前真正实用的量子计算机还没有出现，但诸如 IBM，谷歌等这类公司正投入大量的人力财力研制量子计算机，一旦实用的量子计算机出现，目前绝大多数的区块链技术将彻底没有了安全保障。

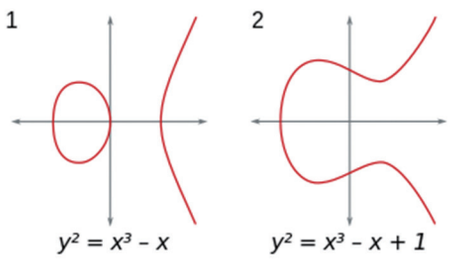

图 2 椭圆曲线示意图

4 杂凑函数的碰撞

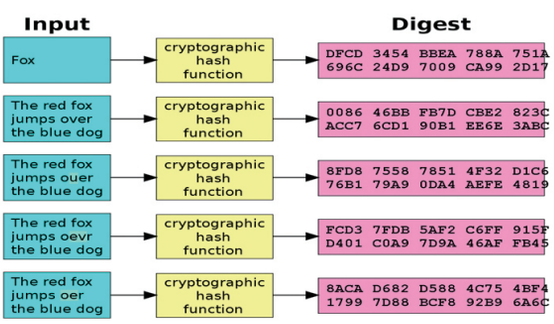

图 3 杂凑函数对输入消息的敏感性示例

密码杂凑函数将任意长度的输入生成固定长度的输出，一般用于产生消息摘要。杂凑函数示例如图 3。区块链中采用了各种不同的杂凑算法，例如，比特币中用到的杂凑算法是 SHA256，以太坊用的杂凑算法是 Ethash 算法等，杂凑算法的安全性决定着区块链技术的不可篡改性。同样的问题，如果杂凑算法的设计有缺陷或有后门，那么基于此算法的区块链技术将不再安全。即使杂凑算法设计的完美无缺，也并不表示该算法永远安全，杂凑算法从理论上一定会存在碰撞，只是发现碰撞的难度很大，概率很小。例如，我国王小云院士破解了 MD5 算法，谷歌构造出了 SHA-1 的碰撞。由此表明，即使目前安全的杂凑算法，其碰撞的发现也只是时间问题，到那时，基于该算法的区块链将不再可靠。

5 共识机制的欠缺

5.1 51% 攻击的可行性

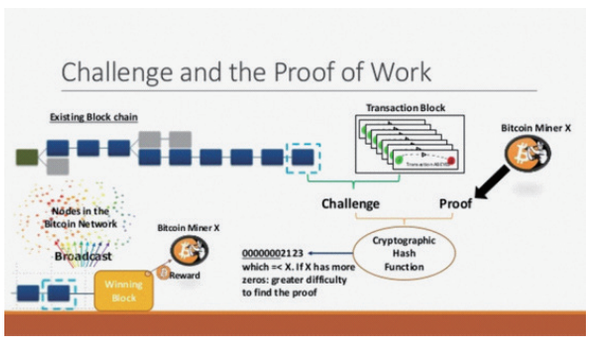

图 4 POW 的工作原理

区块链最大的创新在于能够达成无中心的信任共识，这是由其所采用的共识机制来决定的。目前常见的共识算法有工作量证明 (POW)，权益证明 (POS)，委托权益证明 (DPOS)。大多数区块链尤其是早期的各种数字货币均采用 POW 共识算法，例如，比特币采用的是 POW，以太坊采用的是 POW 和 POS 的混合机制，POW 的工作原理如图 4 所示。目前比特币网络很稳定，这与其强大的算力分不开，算力越高系统越稳定，单点进行算力攻击 (又称 51% 攻击，即掌握全网的 51% 算力之后，用这些算力来重新计算已经确认过的区块，对数据篡改和伪造并且获得利益的行为) 的可能性就越低。目前比特币全网的算力约为 25EH/s，但算力主要集中于各大矿池，根据目前的算力分布，前三大矿池的算力之和约为全网算力的 56%，即理论上前三大矿池联合起来可进行 51% 攻击。类似的，其

他采用 POW 的区块链应用项目，如果没有强大的算力支撑，就很容易受到单点的 51% 算力攻击，区块链本身不可篡改的属性将不再存在。例如，在 2016 年以太坊平台 Krypton 就遭受了 51% 攻击。

5.2 伪去中心与分叉

区块链的优势之一在于去中心化，这也保证了区块链数据的稳定性。但随着挖矿逐渐形成产业，以比特币为代表的区块链 1.0 产物的去中心特性逐渐弱化，形成了算力集中的矿池，一旦矿池出现问题就会影响全网，这也是 POW 共识机制所带来的风险之一。根据目前比特币的算力分布，全球约有 22 个矿池，这些矿池占有全网的 94% 的算力。

作为区块链最早的产物，比特币设计之初就考虑了如何防止单节点的恶意分叉，但却不能防止主动修改共识规则所导致的分叉。目前为止，比特币出现的分叉币有 BCH、BTG、BCD、SBTC、BCX、BTF 等，预计比特币的分叉币还会出现。如果区块链技术不能有效防止分叉的出现，就会降低社区的稳定性。因此，共识算法和共识规则随着时间的变化，都有可能导致软硬分叉的风险。

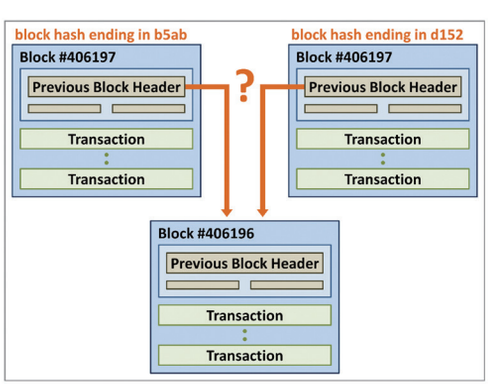

图 5 区块链分叉示意图

5.3 POS 的缺陷

与 POW 不同，权益证明 POS 消除了对硬件的要求，也不需要消耗庞大的电力，两者的对比见图 6。但 POS 本身也有一些缺点，例如，持币数量越多的人话语权就越大，另外，POS 本身并不能防止分叉的攻击，某些节点可能会尝试进行分叉，即使分叉最终没有被接受，该节点本身也没有任何损失。相反地其它节点看到分叉后，最好的策略就是同时在每条链上工作，因为节点不需要消耗资源，只需要用自己持有的币进行投票即可。因此，如果网络采用 POS 机制，还需要额外设置针对分叉的惩罚机制才能良好的运行。

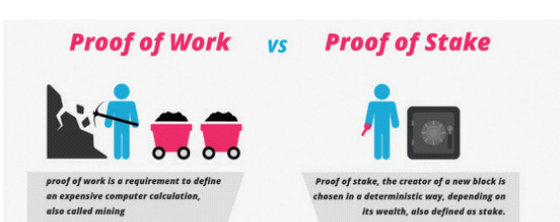

图 6 POW 与 POS 对比

6 智能合约的不完善

区块链 2.0 的创新与改进在于智能合约的出现，智能合约是一段可编程的代码，可部署到区块链上，一旦合约的条款触发某个条件，代码就会自动执行，即使有人想违约也很难。智能合约的原理如图 7 的示例。

智能合约在区块链中具有举足轻重的地位，但如果合约本身具有漏洞，则将会造成不可挽回的损失。例如，著名的以太坊智能合约应用 The DAO 因漏洞遭受黑客攻击，丢失数目庞大的数字货币，导致以太坊不得不采取硬分叉。另外，

智能合约的升级很难，出现漏洞只能进行类似以太坊硬分叉的方式处理。最后，智能合约本质上是一段代码，如果恶意的智能合约出现，类似计算机木马病毒，可能将会导致良好的智能合约感染，进而造成不可挽回的损失。

由于智能合约是不可逆的，部署到网络后无法升级修改，所以迫切需要智能合约的形式化验证，即判断程序是否按照预期运行。形式化验证是一种减少漏洞和防止攻击的有效手段，

但目前为止还没有找到一种形式化验证的解决方案。此外，目前的智能合约是根据预定义场景的响应规则，而如何能做到对未知场景的推演和响应也是智能合约面临的挑战之一。

虽然智能合约的出现是区块链技术进步发展的产物，但智能合约能否再进一步完善发展并带来巨大的效益还有待验证。

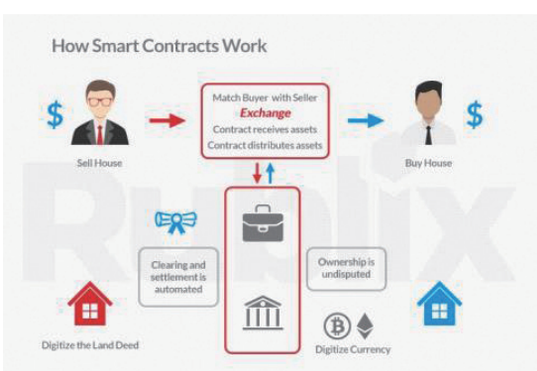

图 7 智能合约工作原理

7 隐私的泄露

时至当下，人们最为关心的就是个人隐私的保护，棱镜门事件暴露出了我们的隐私数据并不像我们想象的那么安全。区块链技术中采用一对公私钥来代表身份，并且交易数据都是公开透明的，任何人都可以查询。例如比特币不需要与真实身份进行绑定即可交易，但用公钥代替身份并不能做到匿名，只能算作假名，而且通过对每一笔交易的追踪和分析，也能判断出某些地址是否归属于同一人或机构，它的匿名性并不像起初人们想象的那样强。虽然目前已有很多数字货币的设计重点是针对隐私进行保护，但目前的方案都有各自的优缺点，能否设计出保密和效率折衷的区块链技术还需要进一步探讨。

8 密钥的丢失

密码算法的安全需要两点保证，其一是随机数的安全，其二是密钥的安全。区块链应用了大量的密码算法，除了保证密码算法的正确实施运行之外，还需要一套严谨合理的密钥管理方案。区块链数字资产的安全完全取决于用户自己掌握的私钥，与传统密码口令不同的是，私钥由每个用户自己生成和保管，没有第三方的参与，也没有私钥补发与管理机制，私钥一旦丢失或被盗，用户的资产将永远丢失。由于私钥是密码算法的关键参数，字符较长，用户难以记忆存储，如果存储在联网的电脑或者在线服务器或其它软件中，丢失的风险较高。目前已经发生了很多密钥丢失或被盗导致的大量财产损失的事件，比如自称是全球最大挖矿平台的 NiceHash 就因黑客攻击造成了超过 7000 万美元的比特币被盗走，这是私钥进行托管后被盗导致的。近期，著名的物联网区块链项目 IOTA 钱包种子生成网站被黑客入侵，损失 400 万美元，原因是用户生成钱包种子时为了回避繁琐的 81 个符号而委托相应网站代为创建。因此，设计

一种安全便利的密钥保护和管理机制是区块链长期发展的关键所在。

9 网络支撑的不稳定性

区块链的分布式技术使得全网的每一个节点都能参与进来，如果利用现有的区块链技术处理非常重要的数据，也会带来一定的风险。目前互联网所依赖的 DNS 根服务器一共 13 台，其中 10 台在美国，英国、瑞典、日本各 1 台。如果这些服务器遭受攻击导致域名不能解析，那么区块链将不能正常运转。例如，2002 年，根服务器遭受了有史以来最为严重的也是规模最为庞大的一次网络袭击，导致其中 9 台不能正常运转。区块链技术能否规避这些安全隐患也是值得研究和探讨的。

区块链受到人们广泛关注的同时也吸引大量的黑客对其进行攻击和破坏，这对区块链技术本身的发展和完善也是一个很大的挑战，目前大多数区块链数字资产的交易均在中心化的平台进行，平台的建设维护运营至关重要，因平台不稳定或有漏洞导致的财产损失案例数不胜数。例如，今年韩国最大的交易所 Bithumb 被黑客侵入数据库，盗走数字货币价值上百万美元；最近，日本最大交易所之一 Coincheck 被黑客入侵，资产损失 6 亿美元。各类区块链项目初始代币发行时，被黑客入侵修改钱包地址造成的巨大损失，也历历在目。交易平台的安全问题虽然不是区块链技术本身的问题，但却是区块链能否进一步发展的关键保障。

10 总结

区块链技术的出现，为我们打开了一个新的大门，以其无中心信任机制的特性，在金融领域已有了成功的应用案例。除此之外，在能源、医疗、公益、征信等领域都有着很大的应用潜力。作为一门新技术，区块链本身还不成熟，在应用中暴露出了各种不足，但这并不会限制区块链的应用，反而会促进区块链技术的创新、完善和发展。例如，实用的抗量子密码算法的研究成果越来越丰富，其国际的标准化也在逐渐推进，将新型的抗量子密码算法应用到区块链中，量子计算机的威胁将不复存在。

区块链已经被我国列入了十三五信息化规划中，相信随着时间的推移，区块链技术及其应用会发展的越来越完善，必将对社会和生活产生深远的影响。

参考文献

[1] 张滨，“区块链安全风险研究”，电信工程技术与标准化，2017，30 (11) :1–5.

[2] 王永涛，李斌，任望，刘孝男，“区块链广泛应用的潜在技术风险及其影响”，中国信息安全，2017 (7).

[3] 程显峰，“区块链技术的风险”，大众理财顾问，2017 (3) :66–68.

[4] 沈鑫，裴庆祺，刘雪峰，“区块链技术综述”，网络与信息安全学报，2016，2 (11).

作者简介

王现方，卫士通摩石实验室技术专家，主要研究方向为区块链技术和后量子密码。