

区块链的安全与防护

目前，区块链主要存在底层代码、密码算法、共识机制、智能合约、数字钱包等安全问题。

区块链面临的安全问题与应对措施

底层代码的安全性

区块链项目（尤其是公有链）的一个特点是开源。通过开放源代码，来提高项目的可信性，也使更多的人可以参与进来。但源代码的开放也使得攻击者对于区块链系统的攻击变得更加容易。2016年10月，国家互联网应急中心发布《开源软件源代码安全漏洞分析报告——区块链专题》，针对区块链领域的知名开源软件，结合漏洞扫描工具和人工审计的方式，在代码层面发现高危安全漏洞746个，中危漏洞3497个，数量较多的高危漏洞有不安全的随机数、不安全的JNI、空指针解引用等。2018年3月，慢雾安全团队披露了一起由于以太坊生态缺陷导致的亿级数字资产盗窃事件。攻击者利用以太坊节点Geth/Parity RPCAPI鉴权缺陷，恶意调用eth_sendTransaction盗取数字资产，持

续时间长达两年。

应对措施主要有两方面：一是使用专业的代码审计服务，二是了解安全编码规范，防患于未然。

密码算法的安全性

以比特币为例，每个区块都对应一个散列值，采用SHA256算法计算得到。在现阶段，该算法依旧满足散列函数的三个特性，单向性、弱无碰撞性和强无碰撞性，是安全的。由于SHA1和MD5已经被密码学者找到碰撞，所以，不应选取这两个算法作为区块链中的散列算法。

比特币中的交易采用了椭圆曲线数字签名算法ECDSA，确保了交易的完整性。比特币中的椭圆曲线采用的是Koblitz曲线(secp256k1)而非美国国家标准与技术研究院(NIST)推荐的secp256r1。虽然当前并无证据，但有分析认为secp256r1有可能是被NIST选取的带后门的椭圆曲线，而比特币在无形中避开了这一风险。

随着量子计算机的发展，越来越多的研究人员开始关注能够抵抗量子攻击的密码算法，如基于格的密码算法等。椭圆曲线密码并不能抵抗量子攻击，当对于密码的量子攻击在未来成为现实时，所有不能够抵抗量子攻击的密码算法都存在较大风险，需要被替换。不过，在比特币中，比特币地址是对公钥进行散列并使用base58编码后的结果，如果比特币资金存放在一个没有支出过的地址里，这意味着公钥尚未公开，则它们在量子计算机面前是安全的。

应对措施有：作为设计者，一是在设计时采用现阶段安全的密码算法，同时关注抗量子攻击的密码研究的进展，在其成熟后优先考虑使用；二是参考比特币对于公钥地址的处理方式，降低公钥泄露所带来的潜在的风险。作为用户，尤其是比特币用户，每次交易后的余额都采用新的地址进行存储，确保有比特币资金存储的地址的公钥不外泄。

共识机制的安全性

当前的共识机制有工作量证明(Proof of Work, PoW)、权益证明(Proof of Stake, PoS)、授权权益证明(Delegated Proof of Stake, DPoS)、实用拜占庭容错(Practical Byzantine Fault Tolerance, PBFT)等。PoW 面临 51% 攻击问题。由于 PoW 依赖于算力,当攻击者具备算力优势时,找到新的区块

的概率将会大于其他节点,这时其具备了撤销已经发生的交易的能力。需要说明的是,即便在这种情况下,攻击者也只能修改自己的交易而不能修改其他用户的交易(攻击者没有其他用户的私钥)。在 PoS 中,攻击者在持有超过 51% 的 Token 量时才能够攻击成功,这相对于 PoW 中的 51% 算力来说,更加困难。在 PBFT 中,恶意节点小于总节点的

1/3 时系统是安全的。

总的来说,任何共识机制都有其成立的条件,作为攻击者,还需要考虑的是,一旦攻击成功,将会造成该系统的价值归零,这时攻击者除了破坏之外,并没有得到其他有价值的回报。对于区块链项目的设计者而言,应该了解清楚各个共识机制的优劣,从而选择出合适的共识机制或者根据场景需要,设计新的共识机制。

智能合约的安全性

智能合约具备运行成本低、人为干预风险小等优势,但如果智能合约的设计存在问题,将有可能带来较大的损失。2016 年 6 月,以太坊最大众筹项目 The DAO 被攻击,黑客获得超过 350 万个以太币,后来导致以太坊分叉为 ETH 和 ETC。2017 年 11 月 7 日 Parity 多重签名合约漏洞导致 93 万个以太币永久丢失。

应对措施主要有两方面:一是对智能合约进行安全审计,二是遵

任何共识机制都有其成立的条件,作为攻击者,还需要考虑的是,一旦攻击成功,将会造成该系统的价值归零,这时攻击者除了破坏之外,并没有得到其他有价值的回报。对于区块链项目的设计者而言,应该了解清楚各个共识机制的优劣,从而选择出合适的共识机制或者根据场景需要,设计新的共识机制。



循智能合约安全开发原则。智能合约的安全开发原则有：对可能的错误有所准备，确保代码能够正确的处理出现的 bug 和漏洞；谨慎发布智能合约，做好功能测试与安全测试，充分考虑边界；保持智能合约的简洁；关注区块链威胁情报，并及时检查更新；清楚区块链的特性，如谨慎调用外部合约等。

数字钱包的安全性

数字钱包主要存在三方面的安全隐患：第一，设计缺陷。2014 年底，某签报因一个严重的随机数问题（R 值重复）造成用户丢失数百枚数字资产。第二，数字钱包中包含恶意代码。2017 年，有网友使用某投资微信群推荐的钱包软件，导致数字资产丢失。第三，电脑、手机丢失或损坏导致的丢失资产。

应对措施主要有四个方面：一是确保私钥的随机性；二是在软件安装前进行散列值校验，确保数字钱包软件没有被篡改过；三是使用冷钱包；四是对私钥进行备份。

区块链安全服务

针对目前区块链存在的底层代码、密码算法、共识机制、智能合约、数字钱包等安全问题，该领域也出现了一些提供安全服务的公司，它们主要通过技术手段、代码审计帮助客户解决各种区块链安全问题。

例如，成都链安科技有限公司对区块链智能合约进行形式化验证，开发了面向区块链智能合约安全性和功能正确性验证平台 VaaS。目前，

VaaS 平台已支持主流区块链平台（如以太坊、EOS 等）智能合约的形式化验证，并且已与国内 10 多家区块链行业的知名企业建立了合作关系。VaaS 形式化验证平台，采用了多种形式化验证方法，具有验证效率高、自动化程度高、人工参与度低、易于使用、支持多个合约开发语言、可支持大容量区块链底层平台的形式化验证等优点。VaaS 提供了针对智能合约的形式化验证工具，极大提高了智能合约的安全性与可靠性。产品通过对合约代码进行严格的安全验证，杜绝逻辑漏洞，确保合约安全，在满足实际应用效率需求的同时，达到有效控制漏洞风险的目的。

再如，厦门慢雾科技有限公司，专注区块链生态安全，已经为全球多家知名区块链公司做了安全审计与防御部署，作为第三方审计单位审计了 200 多份以太坊智能合约，累计发现数十个高危、中危安全问题。区块链生态风控产品——恶意钱包地址库，涵盖钓鱼、勒索、盗窃三大类型的恶意钱包地址，涵盖多种区块链数字资产，同时提供 Python、NodeJS、Go、Java 等主流语言的 SDK，可灵活接入产品风控体系。依托慢雾的墨子系统及蜜罐分析技术，以及能够近实时监控、分析社交媒体上钓鱼信息的语义识别模块，再辅以其安全团队专业的筛选、判断，保证了数据的准确有效。此外，通过其广大的生态合作伙伴，还可实现恶意钱包信息共享。“慢雾区”区块链安全社群已累计辐射人

数达 10 多万人，通过共享威胁情报、交流区块链安全技术，与众多的区块链从业人员一起共同努力为区块链生态安全添砖加瓦。

量子技术发展带来的安全挑战和应对

量子计算机就是建立在量子实体（如光子、电子、原子、离子）基础上运行量子比特的计算机，由于量子计算机具有基于量子比特的并行处理信息的能力，理论上其计算能力随量子比特位数的增加呈指数级增加，因此相比经典计算机具有超级强大的计算能力。国际上，Google、IBM、微软等公司都投入了巨资研发量子计算机的硬件及软件，2017 年 IBM 公司宣布研制出具有 50 个量子比特的量子计算原型机，2018 年 Google 公司发布了 72 个量子比特的量子芯片，微软公司主要针对拓扑量子计算进行研发，2018 年宣布取得重大进展。国内也有多个科研机构及阿里巴巴、腾讯、百度等互联网公司在量子计算领域进行前沿研究。

量子计算机将会给现在使用的密码体系带来重大的安全威胁。区块链主要依赖椭圆曲线公钥加密算法生成数字签名来安全地交易，目前最常用的 ECDSA、RSA、DSA 等在理论上都不能承受量子攻击。根据理论预测，对于一定长度的基于非对称椭圆曲线加密算法 ECC 密钥，用目前超级计算机需要几十年才能破解的密码如果采用具有数

量子计算机将会给现在使用的密码体系带来重大的安全威胁。区块链主要依赖椭圆曲线公钥加密算法生成数字签名来安全地交易，目前最常用的 ECDSA、RSA、DSA 等在理论上都不能承受量子攻击。一些量子算法将对目前区块链所采用的公钥密码体系产生严重的威胁，必须提出应对量子计算的安全策略。

千个量子比特的量子计算机及 Shor 算法预计数十分钟就可以破解。可见，一些量子算法将对目前区块链所采用的公钥密码体系产生严重的威胁，必须提出应对量子计算的安全策略。

为了应对量子计算机给密码带来的安全威胁，目前主要可以采用基于抗量子计算密码和量子密钥的方法。抗量子计算密码的优势在于，将抗量子计算密码应用于互联网中不需要添加额外的硬件设备，特别是昂贵的量子硬件系统，有利于快速大规模普及应用。量子密钥的优势在于其具有更高的基于物理上的安全性，而目前主要的缺点在于需要基于相对昂贵的量子硬件系统，将来量子硬件设备会进一步集成化和降低成本，这将有利于量子密钥的广泛应用。在今后的实际应对策略中，可以根据具体应用的安全需求，将两种策略组合使用。

应对策略 1：采用抗量子计算密码

量子计算机对一些特定数学问题可以极大地加速计算，但是目前看并没有对所有数学问题都具有加速作用，因此可以利用量子计算机


不擅长的数学问题来进行抗量子计算加密算法的研发。国际上早在 2006 年就举行了抗量子计算密码研讨会，目前有多个被认为是抗量子计算的加密体制：基于 Hash 的密码、基于纠错码的密码、基于格的密码、基于多变量公钥密码等，这些加密方法被认为在足够长的密钥下可以抵抗经典与量子计算攻击。

目前，国外已经有区块链采用了抗量子计算密码加密算法，英国的抗量子账本 (Quantum Resistant Ledger, www.theqrl.org) 采用了能够抵抗量子计算攻击的加密算法。而抗量子计算密码如果要广泛应用还需要相关国际通用标准的制定，因为新算法必须要既能抵抗量子计算机的攻击又能抵抗传统经典计算机的攻击，需要进行深入研究。

抗量子计算密码本质上仍然是基于数学的安全，未来量子计算进一步发展也有可能突破某些数学难题，让部分抗量子计算密码不再安全。如果纯粹从安全性上考虑也存在一定风险，因此人们也在关注基于物理安全的量子密钥加密方式。

应对策略 2：采用量子密钥

量子密钥分发 (Quantum Key

Distribution, QKD) 是利用光子的量子性质而分配密钥的一种方式，通过这种方式产生的密钥可以不断地给用户新的随机密钥，而且这是来自于物理层的随机性。在量子密钥分发的过程中，并不直接将密钥通过信道传给对方，而是双方经过进一步协商后产生密钥，如果中间有人试图窃听，那么就会增加系统的误码率而被发现，通信双方就可以舍弃这一段不安全的密钥而协商新的随机密钥。相比基于数学算法的密钥，量子密钥是基于物理上的安全，因此即使运算能力强大的量子计算机也无法对其进行计算破解。1984 年 IBM 的科学家 Charles Bennett 及其合作者提出了首个量子密钥分发协议 BB84 协议，之后又发展出了 E91、B92、MDI-QKD 等协议。中国在这个领域后来居上，目前处于世界最领先的水平。2017 年，俄罗斯科学家将量子密钥分发技术应用于区块链的加密，并在实验上进行了成功的演示。

(本文摘编自工信部信息中心等单位编写的《2018 年中国区块链产业白皮书》)