基于区块链技术的安全性分析

齐 岳

北京电子科技学院，北京 100070

摘要：区块链是一个去中心化的公共数据库，是采用公钥密码算法、哈希函数、共识机制等技术搭建起的去中心化非认证系统，可作为底层应用部署在电子货币、智能合约、DAPP 等不同场景中，保证用户信息安全。本文主要从自身的安全机制和应用环境两个方面探讨区块链的安全性问题。

关键词：区块链安全机制；比特币；安全性

中图分类号：TG315.4；TP391.9 文献标识码：A 文章编号：1671-5586（2017）30-0093-01

引言

区块链技术起源于比特币这种新型数字加密货币，但由于其架构出色的易用性、安全性和稳定性一经问世就得到了广泛的关注和迅猛的发展，在智能合约、资产交易、银行结算等领域都有长足的应用。本文首先对区块链技术进行简要介绍，随后重点对其安全性进行分析。作为支撑电子货币系统的底层架构，区块链可以以不同的形式部署在不同的应用场景中。因此，本文主要从区块链自身的安全机制和应用环境两个方面对其安全性进行探讨。

1 区块链技术简介

区块链技术是由公钥密码算法、共识机制（分布式一致性协议）、P2P 网络通信技术、智能合约编程语言等技术组合，以去信任的方式共同维护一个公共账本，具有去中心化、可靠、匿名等特征，有效克服了传统中心化货币体系普遍存在的高风险低安全性等问题。区块链作为去中心化的非认证系统，旨在通过强密码算法无需建立信任关系即可集体验证维护分布式的可靠数据库，进而实现点对点交易，目前区块链最成熟的应用比特币即是这样的一种数字货币支付系统。此外，区块链还可以搭载智能合约、DAPP 等扩展性功能，支撑一个去中心化的市场。

2 区块链自身机制安全分析

（1）部分中心化。在以比特币为首的基于区块链的电子货币系统中，每个交易是一个支付用户数字签名的数据结构，包含收款方的公钥地址和哈希指针，这个指针必须指向一个已经被链上的某个区块所认可的交易才能保证有效。当产生一个新的区块时，诚实的节点会把币转移到收款方的地址，而攻击者的节点会同时把币放进另一个由其自己控制的地址当中，称为双重支付攻击。攻击的关键在于哪笔交易会被纳入矿池中的长期共识链中，在比特币的运行机制中节点会承认先发布在网络中的区块并在其之上延展。此时如果攻击者拥有全网 50%以上的计算能力就可以创建长度超过原主分支的区块，掌握全网的货币资产。然而随着全网算力的飞速增长，越来越多的虚拟货币被挖掘出来，这种部分中心化的攻击几乎不可能实现，但这种攻击可以抽象成多名矿工合作挖矿时利用双花漏洞有可能获得超出自己劳动所得的比特币数量，始终是货币体系中资金分化和去中心化的巨大威胁。（2）扣块攻击。双重支付是区块链系统最大的威胁之一，扣块攻击的其中一种形式—Finney 攻击就是双重支付攻击基于零验证交易的一种变型。攻击者生成一个有效的区块但并不向矿池广播而是广播由其所支付的交易，如果收款方采用零验证交易的方式确认交易，则攻击者可以在交易完成之后马上广播此有效块和与前者冲突的另一笔交易，下一个诚实的节点很大程度上可能将此交易纳入长期共识链，而包含真实交易的区块会被矿池所遗忘成为一个孤块，收款方利益将受损。除了对节点用户进行攻击之外，还可以使用扣块攻击对整个矿池的资源造成消耗。即矿工在找到区块后保留经过验证的哈希但不向外广播，矿工的损失仅仅在于原本可分摊的区块奖励，但整个矿池的收益就会逐渐减少。（3）地址保护机制。区块链系统通过公钥经双哈希运算生成摘要结果作为比特币地址的主体，再通过一系列编码和前缀、校验码生成比特币字符地址，用户在交易过程中仅需公开地址而非真实身份。这样的地址保护机制表面上可以隐藏用户信息，保障账户安全性，但这样的保护是很弱的，通过观察和跟踪区块链的信息，通过地址 ID、IP 信息等还是可以追查到帐户和交易的关联性，通过其他网络攻击技术手段窃取用户私钥。

3 区块链应用环境安全分析

（1）P2P 网络。P2P 网络技术是比特币系统稳定运行的保障，同时也契合区块链去中心化、隐私性强的特点。比特币的现实应用中遵循 P2P 网络的小世界模型原理设计和运行，以保证节点在加入退出改变等动态变化过程中比特币网络仍然保持稳定，从而增强整个网络的健壮性。但 P2P 网络的开放自由和匿名性等特点使得恶意节点有了可乘之机，Sybil 攻击就是威胁比特币网络的一大安全隐患。Sybil 攻击又称女巫攻击，是指在 P2P 网络中引入大量新的恶意节点误导节点路由表、消耗连接资源、传输非法文件等破坏网络通信安全的行为。比特币系统的开放性导致参与成本少、门槛低，攻击者可以利用这一漏洞制造虚假节点，发布虚假信息，降低网络可信任度。（2）交易平台。区块链作为底层的互联网协议，其本身的安全性可以通过高强度加密算法和梅克尔树的数据结构保证，但区块链技术应用平台的技术上的操作风险仍然存在，并且由于其去中心化的性质导致缺乏统一的监管制度体系，导致主观上的道德风险也很高。The DAO 是基于以太坊区块链平台的智能合约去中心化自治项目，2016 年 6 月 17 日由于其智能合约中存在的漏洞而被黑客攻击，损失达到 6000 万美元。The DAO 作为搭载在以太坊平台的去中心化应用，本次攻击是通过代码的递归调用利用合约既有漏洞实现的，虽然以太坊官方表述漏洞只存在于应用层，但本次事件仍是对于区块链去中心化信任机制的一次严峻挑战。虽然区块链技术在实际应用场景中仅仅是搭建了一个去中心化的应用平台，但平台本身也承担着用户与技术人员之间的中介关系，随着应用复杂度和技术难度逐渐增加，应用项目专业技术水平成为了实际应用过程中的安全性保障。且由于区块链所具有的不可篡改和不可逆的特性，发生攻击之后修正解决的成本都相当高昂。（3）高耗能低效率。区块链的数据结构采取哈希指针建立的二叉树，即梅克尔树，这个结构可以通过哈希指针追溯到任意数据，从而保证数据的完整性。但所参与的每一个参与的节点都需要实时更新存储整条链上的所有数据，这对节点的存储空间容量提出了很高的要求。另一方面，当发生数据更新时，区块链实质是整个数据链条串行写入数据，因此效率远远低于普通数据库，网络也会面临较高的负荷，在对大型数据的处理上缺乏可扩展性。随着区块链技术的进一步发展，数据存储量势必成指数级增长，因此在数据的同步处理和增删查改等方面的高能低效是未来区块链技术将要面临的安全性考验。

参考文献

[1]阿尔文德·纳拉亚南.区块链技术驱动金融[M].中信出版社，2016（08）7.