可信区块链推进计划
TRUSTED BLOCKCHAIN INITIATIVES

区块链安全白皮书

（1.0版）

可信区块链推进计划

2018年12月

版权声明

牵头单位：中国信息通信研究院

支持单位（排名不分先后）：中国电子科技网络信息安全有限公司、成都链安科技有限公司、安比实验室、奇虎360、中国移动、北京丁牛科技有限公司、西安好码安全信息科技有限公司、慢雾科技。

编写组成员（排名不分先后）：

魏　凯、卿苏德、张　启、杨白雪、张奕卉、闫　树、白　健、杨　霞、郭　宇、蒋劭捷、鲍　帅、王　珂。

序　　言

进入2018年，区块链产业应用走向细分，从数字资产到税务存证、从供应链管理到公证确权，区块链技术与实体经济正在加速融合，各类资本和企业机构也在积极拥抱区块链技术。在区块链技术与应用快速发展的同时，我们也看到多数行业应用仍处于探索阶段，区块链技术成熟度不高，特别是在安全方面仍面临诸多挑战，由此引发的一系列区块链安全问题也愈发值得关注。

尽管区块链在底层技术上提供了可靠的安全保障，但攻击者仍能从区块链系统中找到漏洞并进行攻击。每年造成的损失十分严重，其损失额度从2017年开始呈现指数上升的趋势，截止2018年第四季度，已暴露的重大安全事件已造成34.1亿美元[1]的损失。

该报告第一章首先介绍了区块链的技术特征，从技术架构的角度分析区块链的安全性。第二章着重分析当前的安全现状、和区块链相关的安全服务业务以及安全领域的发展趋势。第三章至第八章围绕网络安全、密码安全、账本数据、共识机制、智能合约及应用生态六大部分，详细介绍了当前已知的攻击手段，并对其面临的安全风险进行了深入的剖析，最后提出相应的应对措施。第九章给出了相应的对策和建议。

本白皮书是可信区块链推进计划在区块链安全领域的第一个白皮书，由于编写时间仓促，文中存在一些不足的地方，欢迎业界专家多提宝贵意见。

1 数据来源BCSEC

目录
CONTENTS

第一章　区块链概述 …… 1

1.1　区块链技术特征 …… 1
1.2　区块链技术架构 …… 1
1.3　区块链安全性分析 …… 2

第二章　区块链安全态势 …… 3

2.1　区块链安全现状分析 …… 3
2.2　区块链安全服务业务分析 …… 5
2.3　区块链安全领域发展趋势 …… 6

第三章　网络安全 …… 7

3.1　网络模型及攻击方式分析 …… 7
3.2　网络安全风险分析 …… 8
3.3　应对策略 …… 9

第四章　密码安全 …… 10

4.1　攻击方式分析 …… 10
4.2　密码安全风险分析 …… 11
4.3　应对策略 …… 11

第五章　账本数据安全 …… 13

5.1　安全风险分析 …… 13

目录
CONTENTS

5.2 针对有害信息上链的应对策略建议 …… 13
5.3 针对隐私保护的应对策略建议 …… 14

第六章 共识机制安全 …… 15

6.1 攻击方式分析 …… 15
6.2 安全风险分析 …… 17
6.3 应对策略 …… 17

第七章 智能合约安全 …… 19

7.1 安全风险分析 …… 19
7.2 针对智能合约的应对策略建议 …… 20
7.3 针对虚拟机的应对策略建议 …… 21

第八章 应用生态安全 …… 22

8.1 安全风险分析 …… 22
8.2 应对策略 …… 23

第九章 区块链安全对策与建议 …… 24

9.1 加快制定区块链安全标准与规范 …… 24
9.2 鼓励区块链安全服务行业的发展 …… 24
9.3 推动技术研究和难点攻关 …… 24
9.4 强化区块链安全监管 …… 24

第一章　区块链概述

1.1　区块链技术特征

区块链被广泛认为是一种参与方共同维护的分布式账本。该账本使用密码学保证传输和访问安全，并能实现数据一致，难以篡改，以及数据可溯源等目的。在典型的区块链系统中，信息会按照各参与方的约定规则进行存储。为了防止信息被篡改，系统将以区块为单位，区块之间按时间顺序，并以加密的方式构成了链式结构。该链式结构中的任一个区块被篡改，则会影响到链上其他区块的正确性。当新的区块产生后，通过共识机制选出记录节点，由该节点决定最新区块的数据，其他节点共同参与最新区块数据的验证、存储和维护，数据一经确认，就难以删除和更改，只能进行授权查询操作。

区块链相较于传统数据库，体现了几个对比特征：从复式记账演进到分布式记账、从“增删改查”变为仅“增查”两个操作、从单方维护变成多方维护以及从外挂合约发展为内置合约等（详见中国信息通信研究院和可信区块链推进计划《区块链白皮书（2018）》）。

1.2　区块链技术架构

各类区块链虽然在具体实现上各有不同，其整体架构却存在共性，本白皮书中对于安全风险分类的分析，基于图1的一种架构组织方案。

来源：中国信息通信研究院等《区块链白皮书（2018）》

图1　区块链系统架构

该架构包含了9大模块，分别为：基础设施、基础组件、账本、共识、智能合约、接口、应用、操作运维以及系统管理。从整体架构来看，区块链的运行机制为：应用层生成交易记录，并对交易记录进行签名，通过SDK或RPC接口发送到区块链系统的节点并验签，在一定的时间周期，将交易进行打包成区块。打包后的区块通过共识机制，交给某一个节点加入到链上，并进行全网同步。下文的安全性分析也将围绕该架构分层的几个模块展开。

1.3 区块链安全性分析

由上文的整体架构的角度来看，我们将区块链安全分为三个维度：应用服务的安全性、系统设计的安全性（包含智能合约和共识机制）、基础组件的安全性（包含网络通信、数据安全和密码学）。下面将从这三个维度对区块链的安全性进行简要的阐释。

（1）应用服务的安全性

区块链的应用层为用户提供各类应用服务，其中包含了各种复杂的业务场景和业务逻辑，容易成为被攻击对象。突出的安全问题包括了：数字钱包安全、应用软件漏洞、被植入病毒程序风险、使用安全等；

（2）区块链系统设计的安全性

区块链系统本身已经提供了诸多安全机制，但设计方式的不合理仍会被人为利用并进行攻击。例如共识机制的设计不当，会造成分叉、双花攻击等问题；智能合约的实现逻辑出现漏洞，则会导致非法交易被合法化。

（3）基础组件的安全性

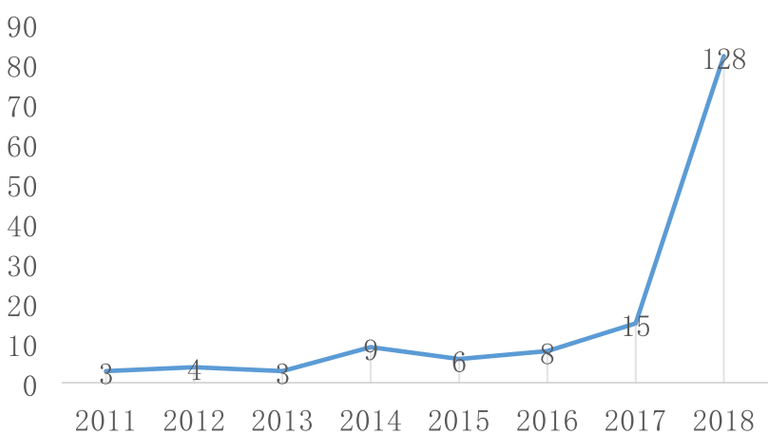
区块链系统提供了各种基础组件，以保证其安全性，如：芯片增强安全、硬件钱包、非对称加密算法、分布式账本等。最近一些公司也在积极提供可信的执行环境的解决方案，如Intel公司的SGX方案。针对基础组件的安全风险也分为：网络安全（信息传播）、密码学安全（验证加密）、数据存储安全（记录）。

第二章　区块链安全态势

2.1　区块链安全现状分析

（1）重大安全事件在全球范围内造成损失金额超过30亿美元

从2011年至2018年12月的重大安全事件[2]的统计来看，在2011年至2016间，区块链安全事件数量较少，从2017年以来，安全事件数量猛增，尤其是在2018年间呈现爆发态势。从侧面反映出来，随着区块链热度增加的同时，安全问题也日益突出。

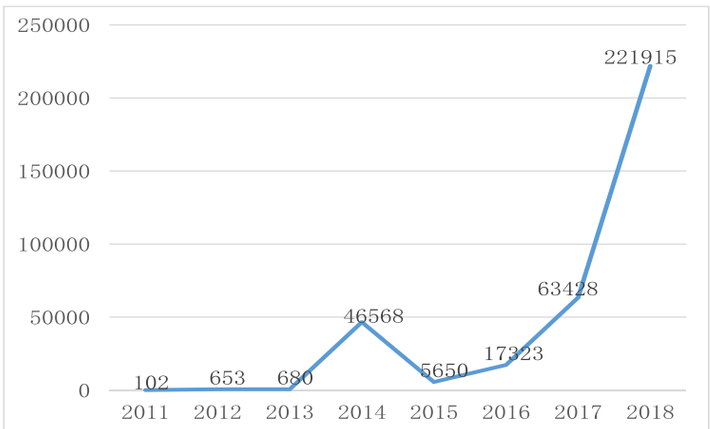


数据来源：BCSEC，截止2018年12月

图2　重大安全事件统计

从图3的统计可以看出，从2011年至2018年，历次的安全事件所造成的损失金额，和安全事件的数量一致，安全事件造成的损失也是逐年增多。区块链的主要价值体现在提供信任机制，如果安全风险得不到有效控制，那么区块链技术在垂直行业的广泛应用将无从谈起。

2 特指在业界造成重大影响或金额损失的安全事件

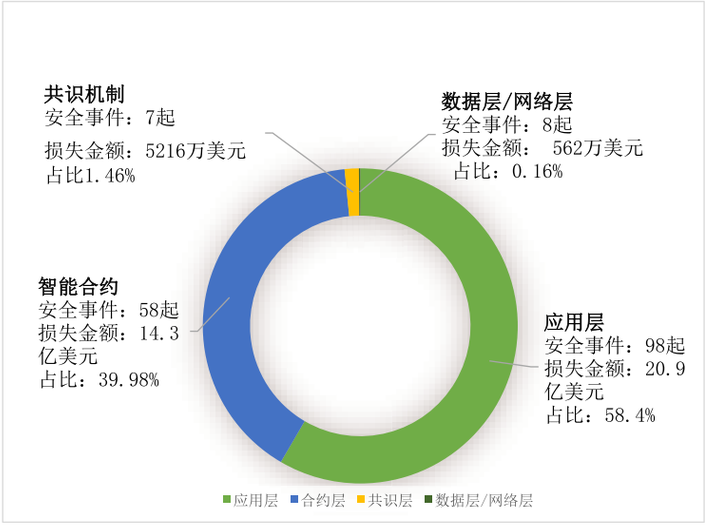


数据来源：BCSEC，截止2018年12月

图3　损失金额（万美元）统计

（2）重大安全事件集中在合约层和应用层

2011年至2018年12月，重大安全事件在系统的各个层级都有出现，但超过90%的安全事件集中在智能合约和业务应用，且造成了超过98%的损失。由于区块链技术独特的链式结构和共识机制，直接篡改链上数据几乎不可能，且区块链的P2P网络模式也增强了系统整体的容错性，同时有效避免了单点故障。对数据层、网络层和共识层的直接攻击成本过高。由于智能合约缺乏统一规范，且编写者的能力参差不齐，导致智能合约在实际应用中存在诸多漏洞。同时，使用者、第三方数字钱包或交易平台等业务应用由于采用了不安全的私钥管理方式，容易导致用户私钥泄漏，而造成重大金额损失。所以攻击者往往选择从成本相对较低的智能合约层和应用层作为攻击区块链系统的切入点。



数据来源：BCSEC，截止2018年12月

图4　2011~2018年安全事件分类

2.2 区块链安全服务业务分析

（1）区块链产业发展迅速，商业价值攀升

区块链产业近两年迅速发展，区块链技术已从最初的加密货币领域，逐步向着和各垂直行业融合的方向发展，根据中国信息通信研究院ICT产业数据统计，截止2018年6月份，区块链技术已广泛应于金融、贸易物流、电子商务、产权等领域。

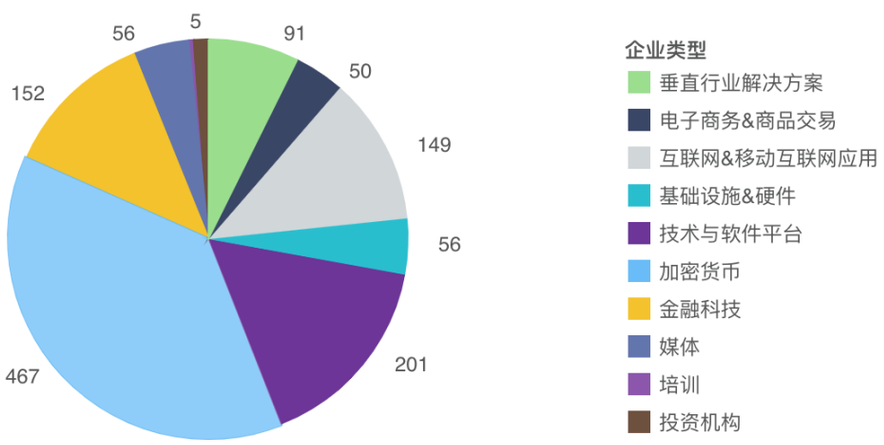


图5 区块链企业分布领域

（2）行业安全问题频发，催生安全服务需求

随着区块链带来的商业价值的增多，面临的安全问题也越来越严峻。由此催生了大量的区块链安全服务，诸多传统网络信息安全企业和区块链安全领域的创业公司，进入区块链安全领域，提供专业化的安全服务业务。综合对比各大安全服务机构所提供的业务板块，主要集中在以下几部分：

1）钱包安全审计业务，钱包通常用于用户的私钥或地址，私钥决定了数字资产的归属权，钱包安全审计尤为重要。钱包存在诸多安全风险，如：钱包客户端RPC API风险，私钥窃取，钱包软硬件漏洞攻击，在线钱包账号窃取等。

2）智能合约安全审计业务，目前各个区块链安全机构通过形式化验证或漏洞检测等方式提供智能合约安全审计服务，如：假充值漏洞审计，设计逻辑审计，条件竞争审计，权限控制审计。

3）安全评测服务，很多区块链初创公司缺少专门的安全部门，需要专业的安全团队

对整个产品做安全评测，并给出相应的安全加固建议。

4）威胁情报服务，同传统互联网的安全技术发展路线类似，区块链安全行业也引入了态势感知/威胁情报服务。通过对链上数据的监控和智能分析，在真正的安全事件出现之前，发出报警提醒对其进行防范。

2.3 区块链安全领域发展趋势

（1）隐私信息上链，催生多种隐私保护方案

区块链系统尤其是非许可类区块链，交易内容公开透明，2018年以来，出现了很多隐私保护的诉求，需要隐私保护机制来保证参与方的隐私权。目前主流的隐私保护策略有三种：1）基于事务隔离的策略，主要面向分片、多链、多通道等模式；2）基于隐私保护算法的策略，多种开源非许可链采用的模式；3）基于应用层权限控制的策略，许可类区块链采用的模式。

（2）智能合约成为安全风险“重灾区”，第三方安全审计服务兴起

从历次的安全事件中，可以看得出来，智能合约的漏洞不仅广泛存在，且造成的损失也十分巨大。当前区块链的智能合约的应用还处在初级阶段，合约编写的规范性和严谨性难以保证。近年来出现了以形式化验证为代表的安全审计策略，可以通过严格的数学证明的方式来确保合约代码所表达的逻辑符合意图。委托第三方专业机构进行安全审计将成为保证智能合约安全的发展趋势。

（3）单一的共识算法无法满足复杂业务场景的安全要求，共识机制向多种结合的方向发展

常见的共识机制包括PoW、PoS、DPoS、拜占庭容错等，根据适用场景的不同，也呈现出不同的优势和劣势。单一共识机制，各自有其缺陷，无法满足复杂业务场景的安全性，例如PoS依赖代币且安全性脆弱，PoW非终局且能耗较高。为提升效率，只能在安全性、可靠性、开放性等方面进行取舍。区块链正呈现出根据场景切换共识机制的趋势，并且将从单一的共识机制向多类混合的共识机制演进，运行过程中支持共识机制动态可配置，或系统根据当前需要自动选择相符的共识机制。

第三章　网络安全

3.1　网络模型及攻击方式分析

本部分将以比特币、以太坊、fabric三个的典型的区块链P2P网络架构入手，针对以上三种典型的P2P网络现存安全问题进行分析，包括设计层的女巫攻击、日食攻击等以及应用层的DDoS攻击（拒绝服务攻击）等。下面将重点讲解上述三种攻击方式的原理，以供相关机构参考，并在开发基于区块链网络的应用系统时采取措施加强防范。

表1　典型的区块链网络比较

网络模型	典型应用	是否有结构	是否有中心节点	网络攻击方式
全分布式非结构化	比特币	无	无	DDoS攻击、女巫攻击、日食攻击
全分布式结构化	以太坊	有	无	DDoS攻击、女巫攻击、日食攻击
半分布式网络	Fabric	有	有	DDoS攻击

（1）DDoS攻击

传统的DDoS攻击分为两步：第一步利用病毒、木马、缓冲区溢出等攻击手段入侵大量主机，形成僵尸网络；第二步通过僵尸网络发起DDoS攻击。不同于传统的中心化系统，针对区块链系统的DDoS攻击可以分为主动攻击和被动攻击。

主动攻击：通过主动向网络中发送大量的虚假消息，通过区块链的交易同步机制使反射节点瞬间收到大量的通知消息。攻击方可以通过假冒源地址避过IP检查，使得追踪定位攻击源更加困难。并且大量的流量流经网络，会导致网络的路由功能的下降。

被动攻击：被动攻击不同于主动，攻击节点等待来自其它节点的查询请求，再通过返回虚假响应来进行攻击。在真实环境中，攻击者常常部署多个攻击节点、在一个响应消息中多次包含目标主机、结合其它协实现漏洞。

（2）日食攻击

日食攻击是通过其他节点实施的网络层面攻击，这种攻击目的是阻止最新的区块信息进入到被攻击的节点，从而隔离节点。其攻击手段为：囤积和占用受害者的点对点连接时隙，将该节点保留在一个隔离的网络中，达到隔离节点的目的。目前的比特币网络和以太坊网络已经被证实均受日食攻击影响。

1）针对比特币网络的日食攻击，攻击者可以控制足够数量的IP地址来垄断所有受害节点之间的有效连接。然后攻击者可以征用受害者的挖掘能力，并用它来攻击区块链的一致性算法或用于“重复支付和私自挖矿”。

2）针对以太坊的日食攻击，攻击者可以垄断受害节点所有的输入和输出连接，从而将受害节点与网络中其他正常节点隔离开来。然后攻击者日食攻击可以诱骗受害者查看不正确的以太网交易细节，使卖家在交易还没有完成的情况下将物品交给给攻击者。

（3）女巫攻击

在P2P网络中，特别是公链网络，由于节点随时加入退出等原因，为了维持网络稳定，同一份数据通常需要备份到多个分布式节点上，被称为数据冗余机制。女巫攻击是攻击数据冗余机制的一种有效手段。

在区块链网络中，攻击者可以伪造自己的身份加入网络，在掌握了若干节点或节点身份之后，便会威胁到区块链网络，例如降低区块链网络节点的查找效率，在网络中传输非授权文件，破坏网络中文件共享安全，消耗节点间的连接资源等。

3.2 网络安全风险分析

（1）网络攻击手段简单化成本降低

DDoS攻击伴随着互联网的诞生，已发展了几十年。在这十几年的发展过程中，DDoS攻击越来越智能化和简单化，甚至在境外一些网站的网页上，使用者只需输入目标节点的ip地址，选择攻击时间，就可以发起一次DDoS攻击。随着近些年网络带宽费用的降低，攻击成本也更加低廉。

（2）网络攻击方式隐蔽不易被察觉

网络攻击者所用的计算机是攻击主机，可以是网络上的任何一台主机，甚至可以是一个活动的便携机。这些主机还分别控制大量的代理主机，代理端主机是攻击的执行者，负

责向受害者主机发送攻击。由于攻击者在幕后操纵，在攻击时不会受到监控系统的跟踪，身份不容易被发现。新型的DDoS攻击不需要建立僵尸网络即可发动大规模攻击，不仅成本低、威力巨大，而且还能确保攻击者的更加隐秘性。

（3）节点加入退出缺乏验证及监控

网络攻击的手段之一就是向区块链网络增加大量恶意节点，从而破坏分布式账本的真实性。在许可链中有严格的节点加入的准入机制和对节点的监控手段，可以有效避免恶意节点的出现。但在非许可链（公链）当中，节点的进出机制缺乏有效的验证，更容易受到因恶意节点的加入而带来的危害。

3.3 应对策略

（1）加强DDoS防御能力

应对DDoS攻击是一个系统工程，想仅仅依靠某种系统或产品防住DDoS是不现实的，目前完全杜绝DDoS攻击的难度较大，但通过适当的措施，比如安装专业抗DDoS防火墙，部署CDN等方式抵御90%的DDoS攻击是可以做到的，基于攻击和防御都有成本开销的缘故，若通过适当的办法增强了抵御DDoS的能力，也就意味着加大了攻击者的攻击成本，可做到有效的防御。

（2）加强节点准入机制

区块链网络用户应能通过标识建立唯一的、可验证的数字身份；合理设置对等网络节点的连接数目、连接时长、地址列表大小、更新频率、更新机制、连接选择机制、异常检测机制等。提供区块链服务的平台应具备基本的网络边界防护、网络入侵检测与病毒防御机制。

（3）加强转发验证机制

区块链网络应具备针对恶意节点检测和防御机制，能够及时检测出网络中的恶意节点（如，发起拒绝服务攻击的节点，不做转发验证的节点，转发错误路由信息的节点等），并进行针对性处理。例如针对这些节点可以采用限制接入、限制转发等策略，设置时间限制禁止建立持续通信连接等。针对恶意交易/区块：各节点应有合理的交易/区块转发验证机制，对不良的交易/区块不做转发。

第四章　密码安全

密码学是保证区块链上交易数据安全的关键屏障，密码学实现的安全往往是通过算法所依赖的数学问题来提供，而并非通过对算法的实现过程进行保密。一般分为对称加密和非对称加密。由于对称加密速度快，但相对容易破解，而非对称加密算法则相反。所以实际用中一般会将对称加密和非对称加密算法结合使用。表2是各类加密算法的对比。

表2　加密算法类型

加密类型	名称	计算方式	复杂度	速度	强度
非对称	RSA	基于可逆模幂运算	亚指数级	中	取决于因式分解难度
	ECC/SM2	基于椭圆曲线算法	指数级	快	ECDLP数学问题
对称	AES	RIJNDAEL算法		快	较高
	SM4	迭代和线性变换	32	快	较高
	DES	逻辑算法	48	慢（可硬件加速）	较高

4.1　攻击方式分析

（1）穷举攻击

此类攻击方式主要作用于散列函数中，且几乎所有散列函数或多或少都受此攻击方式影响，而且其影响程度与函数本身无关，而是与生成的hash长度有关，主要是一个概率论的问题，其中最典型的方式是基于生日悖论的“生日攻击”。

（2）碰撞攻击

此种攻击方式主要作用于散列函数中，比较典型的案例是“md5　摘要算法”和“sha1　摘要算法”。它的攻击原理是通过寻找算法的弱点，瓦解它的强抗碰撞性这一特性，使得散列函数原本要在相当长一段时间才能寻找到两个值不同hash相同的值的特性被弱化，攻击者能在较短的时间能寻找到值不同但hash相同的两个值。

（3）量子计算攻击

量子计算对于密码算法存在潜在威胁。Shor量子算法对于RSA的破解所需量子比特

数约为2n，目前使用的RSA算法一般达到2048位（相当于256位的ECC算法），也就是需要4096个量子比特的量子计算机，而目前量子计算机还未突破100位。因此量子计算机破解现有密码算法还需要很长的一段路需要走，而美国已经从2016年开始征集后量子密码算法标准，估计很快便会有新的抗量子计算的密码算法标准推出。

4.2 密码安全风险分析

（1）私钥管理方式存在安全风险

私钥管理的安全是区块链密码安全的前提，目前主流的方式是通过软硬件钱包的方式进行管理，或者由用户自行保管。一旦私钥丢失，用户不仅无法对数据进行任何操作，也无法使用和找回其所拥有的数字资产，造成无法挽回的损失。

（2）加密算法的工程实践中存在后门及漏洞

密码学发展到现在已经具有相当的成熟性了，ECC、RSA等加密算法本身已经被数学证明具有很高的安全性，但是由于其算法的复杂性，在工程实践中存在后门及漏洞。攻击者往往会利用这些漏洞，实现对私钥的窃取。

4.3 应对策略

（1）使用多种方式存储保障私钥安全

针对私钥安全的存储方式一般分为三种：硬件存储、软件存储和分割存储。选择合适的存储方式可以有效的加强私钥安全。

1、硬件存储，将私钥存储在硬件加密卡或者USBKey中，使用过程一般包括两种：a)将私钥存储在卡中，使用时将私钥导出在区块链客户端软件钱包中使用，使用完后在将外部私钥删除；b)私钥在硬件卡中直接进行签名运算，将打包好的交易输出，私钥在整个使用过程中不出硬件设备。

两种方式相比，a)的使用成本较低，一般用U盘即可完成相应功能，b)的安全性较高，使用成本较高，私钥执行环境在硬件中确保了整个运行环境的安全，私钥也不会被木马、病毒窃取。

2、软件存储，这是目前区块链系统中使用最多的一种方式，即通过设置口令，使用口令再将私钥加密存储在软件客户端中，使用方式非常简单，而且成本低廉，但安全性相

对于硬件是非常低的。

3、分割存储，这种方法是将原始私钥分成2到n份，将各个私钥部分分开存储在不同的区域或者用户身上，而在需要使用时，则通过一定的数学方法进行合成签名，从而避免整个私钥的泄露，而部分私钥的泄露也不会影响整个资产的安全性。这种方法安全性较高，但使用起来比较麻烦，最典型的方案便是门限签名方案，目前在区块链系统中一般应用到保护巨额资产交易。

（2）使用PKI数字证书管理及CA认证

PKI（Public Key Infrastructure）是一种遵循标准的利用公钥加密技术为电子商务的开展提供一套安全基础平台的技术和规范。通过第三方的可信任机构——认证中心CA(Certificate Authority)，把用户的公钥和用户的其他标识信息（如名称、e-mail、身份证号等）捆绑在一起，在Internet 网上验证用户的身份。眼下，通用的办法是采用基于PKI 结构结合数字证书，通过把要传输的数字信息进行加密，保证信息传输的保密性、完整性，签名保证身份的真实性和抗抵赖。

第五章　账本数据安全

区块链的数据结构可以分为三层来描述：首先是链、然后是区块，最后是交易。即在同一时间周期（如比特币的周期为10分钟）内的交易打包组成区块，按时间顺序将区块接起来组成了区块链。

由于区块之间用hash签名的方式相互关联，假设区块中的某一个交易发生了改变，则其hash值也会发生改变，最终使得该区块的ID发生改变，从而导致区块从区块链中断开，一个从区块链中断开的区块是不能获得区块链网络承认的，除非篡改该区块往后的所有区块的ID。因此，这种数据存储结构构成了区块链难以篡改的特性，同时也从客观上增加了有害信息上链的风险，以及对敏感数据上链后的隐私保护问题。

5.1　安全风险分析

（1）有害信息上链给信息管理提出挑战

区块链数据的难以篡改的特性使得区块链上的数据难以通过传统的方式进行修改和删除，增加了有害信息上链的监管难度，为信息管理提出新的挑战。

（2）隐私数据缺乏有效的保护措施

区块链的账本是具有分布式的特点，需要多个节点参与账本的存储与验证，而这容易导致人们对账本隐私的担忧。例如区块链的典型应用之一比特币，其每一笔交易都会公开记录在区块链账本上，任何人都可以查阅。只要通过分析每个地址发生过的交易，就可以发现很多的账号之间的关系。区块链的应用尤其是金融行业对隐私保护会更加注重。隐私问题成为区块链应用落地的主要障碍之一。

5.2　针对有害信息上链的应对策略建议

（1）探索上链信息审核机制，明确区块链服务主体

国内目前各行业都在积极探索区块链技术的应用落地，在应用落地的最初阶段积极探索上链信息的审核机制，并寻求与隐私保护之间的平衡，同时需要加强区块链主体服务节

点的监控，以便明确责任主体。

5.3 针对隐私保护的应对策略建议

（1）隐私数据链外存储

链外存储是将要保护的隐私数据存到链外，可以公开的部分数据放在分布式账本上，具体方式可以是将原文存到链外，对应的摘要信息存到分布式账本上。

（2）根据隐私要求的不同进行账本隔离

账本隔离是将具有不同隐私需求的账本，分别存放到不同的分布式账本上。一种是使用多通道（子链模式），隔离账本，例如fabric利用多通道(Channel)的机制，实现账本隔离保护隐私性。另一种是将业务数据仅传给参与人，非全网传播，业务数据只落在参与人的账本中。

（3）隐私数据需加密保护

加密保护是利用密码学算法，对账本数据进行加密，做到只有相关方才能够解密查看。

（4）对账本数据脱敏处理

部分明文是将分布式账本数据分为敏感部分与非敏感部分，对敏感部分进行隐私保护。

（5）使用群签名对身份匿名

身份混淆是将在区块链上交易用户的身份隐匿起来。fabric使用交易证书（TCerts）即每个交易的短期证书，满足一次一密、不可伪造、无关联性和可跟踪性。使得用户不仅以匿名方式参与到系统中，而且阻止了交易之间的关联性。还有使用群签名进行身份匿名。群签名是指一个群体中的任意一个成员可以以匿名的方式代表整个群体对消息进行签名。与其他数字签名一样，群签名是可以公开验证的，而且可以只用单个群公钥来验证。

第六章　共识机制安全

区块链作为一种去中心化的分布式系统，需要通过节点之间的底层共识协议来保证其账本的数据一致性。一般来讲，我们将区块链分为非许可链（公有链）和许可链，由于实际应用场景和系统架构的不同，不同种类的链所使用的共识算法也不同，所涉及到的安全性也有所区别。对分布式系统来讲，不同的共识模型在不同的环境下能够容忍的错误类型与节点错误数量不一样，由此我们可以由分布式系统共识的评判标准引申出对区块链的共识安全性界定。

表3　共识算法安全性比较

	PoW	PoS	DPoS	PBFT	类BFT	SCP
能耗	资源消耗巨大	资源消耗低	资源消耗低	能耗较低	能耗较低	能耗较低
出块时间	出块时间长，不能满足实际应用场景中的业务需求	出块时间较短	可以达到秒级的共识验证	出块速度较慢，不适用于大规模的节点共识	出块速度快，可以适应高频交易	出块速度快，可以适应高频交易
安全性	面临51%算力攻击	解决了51%算力攻击;中间步骤较多，易产生安全漏洞	解决了51%算力攻击;中间步骤较多，易产生安全漏洞	安全性较低，只能容忍少于1/3的作恶节点	安全性较低，只能容忍少于1/3的作恶节点	渐进式安全，参数可根据实际情况调整以抵御拥有强大算力的对手
一致性	易分叉，没有最终性	易分叉，没有最终性	没有最终性	具有最终性，不会分叉	具有最终性，不会分叉	具有最终性，不会分叉

下面我们将从几个典型的共识层安全事件入手，分析主流的共识算法存在的安全风险，以及这些共识算法适合的业务场景。

6.1　攻击方式分析

（1）双花攻击

简单来说，双花攻击就是指同一个货币被花费了多次。在区块链网络中，每个用户的

每一次交易都可以对应一个网络请求。而区块链整个系统会进行对此请求的验证。其中包括检查其资产的有效性、是否已经使用已花费的资产来进行交易。经过全网节点的检验后，广播这个成功验证的账本。由于区块链分布式系统的特性，其在交易的时候存在延时是不可避免的，所以交易并不是立刻执行。所以交易确认的时间要长很多，使得这种诈骗有可能实现，这就是比特币的double spending双重花费问题，简称“双花”。

（2）51%攻击

在PoW[3]共识算法中，系统同时允许存在多条分叉链，在PoW的设计理念中有一个最长有效原理：“不论在什么时候，最长的链会被认为是拥有最多工作的主链。”51%攻击是指在攻击者拥有超过整个网络一半算力的情况下，就有能力推翻原有确认过的交易，重新计算已经确认过的区块，使区块产生分叉，完成双花并获得利益。

攻击者实施51%算力攻击的动机一是可以完成对自己交易的双花，骗取交易接收方的利益；二是可以控制最长链的生成过程，从而获得区块奖励。

（3）自私挖矿

诚实挖矿的策略如下：其挖到区块链后就对其进行全网广播。而在自私挖矿的策略中，矿工挖到区块之后不发布，直到挖出第二块，从而控制最长链的产生。当攻击者的长链分叉信息率先传递到某个诚实矿工那里，这个诚实矿工会根据比特币的共识机制，认可该分叉内区块的合法性，并且选择在该长链尾部继续挖矿。这令攻击者处在更为有利的位置上。事实上，出现这种情况，恰恰是由于比特币网络信息传播存在时延所致。对于网络上的其他节点来说，这两个区块的高度是相同的，所以被其他节点承认的概率还有1/2，这样自私矿工就有了相对于其他人的优势。自私挖矿理论上支持33%和25%的算力发起攻击。

（4）确定性算法重放攻击

重放攻击(Replay Attacks)又称重播攻击、回放攻击，是指攻击者发送一个目的主机已接收过的数据包，来达到欺骗系统的目的。在区块链技术中，重放攻击是指“一条链上的交易在另一条链上也往往是合法的”。而这种攻击一旦发生，就会产生类似于双花攻击那样的效果：同一笔钱转给了同一个人两次，就会导致在不需要付款人参与的情况下多一次支付。

3 工作量证明算法

（5）权利压迫攻击

这种攻击方法简单来说，就是攻击者在获得记账权的时候利用手中的部分权利实施一些操作让系统的随机数产生偏移用以增加自己下一次获得记账权力的可能性。

（6）区块链贿赂攻击

恶意节点没有必要在Pow机制下为了使自己能做恶而恶意提升算力。反而，可以通过区块链协议之外的贿赂来收购数字货币或者挖矿算力，从而达到攻击原有区块链的目的。

6.2 安全风险分析

（1）单一的共识机制难以满足复杂业务的安全要求

发生在交易/区块上链前后的共识阶段。要求在共识过程中，保证交易数据不可篡改、真实有效。从共识攻击的角度，共识机制的设计应满足的安全要求有：防拜占庭攻击[4]、防双花、防女巫攻击、防预测[5]、防占用[6]、防欺诈/防贿赂等。目前来看，单一的共识机制很难应对所有的攻击方式，从安全方面角度出发，共识机制有向融合的方向发展。

6.3 应对策略

（1）合理界定共识算法的安全范围

共识算法的安全更多的是在确保安全和攻破安全防御所付出的代价之间找一个平衡点，判断共识算法是否安全应该立足于具体的应用场景以及该链所处的状态。比如，采用PoW共识算法的比特币系统，其有遭受51%算力攻击的可能。但是要构建一次超过全网一半算力的攻击需要付出很大的代价，该代价会远远大于收益，因此我们可以认为采用PoW共识算法的比特币系统是安全的。

（2）根据业务场景选择多种或可切换的共识算法

不同的共识算法有不同的侧重和工作效率，我们评价一个共识算法的整体性能一般采用四个维度：安全性、扩展性、性能效率、资源消耗。因此，面对不同的应用场景须选用

4 拜占庭攻击是指超过一定比例的节点合谋，针对共识算法漏洞的攻击，以达成非法共识的目的。
5 预测是指由于共识算法的漏洞而导致打包节点被预测到，进而被针对性的恶意攻击。
6 占用是指共识过程中被某些利益方持续占用，而影响共识的公正性。

不同的共识算法。为了保证安全性，也可以在全网采用多种共识算法，通过多级共识来确认交易。参考下表，可根据业务场景选择合适的共识算法。

表4　共识算法适用场景比较

	PoW	PoS	DPoS	PBFT/类BFT	Raft
场景	无信任环境	无信任环境	无信任环境	可信任环境	完全信任环境
应用	公有链	公有链	公有链	联盟链、私有链	私有链
去中心化	完全	完全	部分	低	低
吞吐量	低	低	高	高	高
出块时间	慢	慢	一般	高	高
节点规模	大	大	小	小	小
容错率	51%	51%	51%以上	33%	51%

第七章　智能合约安全

智能合约负责将业务逻辑以代码的形式实现、编译并部署，并按照既定的规则或者触发条件，自动执行。智能合约的操作对象大多为数字资产，这也决定了智能合约在具有高价值和高风险。本章将从智能合约程序漏洞、合约虚拟机漏洞两个方面分析漏洞的种类，并提出针对性的优化方案和解决措施。

7.1　安全风险分析

（1）智能合约设计与实现存在大量漏洞

由于智能合约本质上是部署和运行在区块链上的程序，在没有标准的合约模板或编写规范的情况下，我们很难要求程序员都能写出最佳实践的代码，一些逻辑不严谨的代码会造成智能合约的业务逻辑存在安全隐患。事实上，在历次的安全事件中，智能合约的漏洞引发的安全问题占了较多的比重。根据“区块链安全研究中心”2018年的智能合约检测结果，我们总结了主要的智能合约的安全漏洞类型统计如下：

表5　智能合约安全漏洞类型分布图

来源：区块链安全研究中心

类型	数量	占比
Call函数安全	41268	10.83%
条件竞争	13602	3.57%
重入攻击检测	2743	0.72%
权限控制	178925	46.97%
数值溢出	0	0.00%
事务顺序依赖	9488	2.49%
冻结账户绕过	1593	0.42%
逻辑设计缺陷	61798	16.22%
错误使用随机数	33809	10.38%

（2）虚拟机的安全漏洞少但影响范围大

目前大多数智能合约语言属于虚拟机语言，由其实现的智能合约需要运行在特定的语

言虚拟机，例如以太坊上的由Solidity语言编写的智能合约需要运行在EVM[7]上。虚拟机本身的安全性一方面可以保证智能合约运行结果的正确性，另一方面也可以防止运行其上的智能合约免受其他恶意合约的攻击。考虑到一个区块链系统的大量节点往往部署同样版本或类似实现的虚拟机，单个虚拟机漏洞的影响很可能影响到整个系统。

7.2 针对智能合约的应对策略建议

（1）智能合约的安全审计

智能合约往往被用来管理大量的用户资产和有价凭证，然而大多数区块链项目为了增加可信度和透明性，对其项目代码进行开源管理，这样使得项目更容易受到攻击。智能合约开发者在实现业务功能之外，额外学习大量的安全编码规范、已有漏洞问题、虚拟机安全版本等的成本过高。因此行业中细分出第三方智能合约审计机构，专门对智能合约安全进行深度的审计。接受专业审计机构的合约代码验证，也可以有效规避合约代码的潜在安全风险。

（2）智能合约的加密

智能合约不能被第三方明文读取，以此减少智能合约因逻辑上的安全漏洞而被攻击。此方法成本较低，但无法用于开源应用。

（3）智能合约的规范设计

根据应用的实际业务逻辑总结智能合约优秀模式，开发标准智能合约模板，以一定标准规范智能合约的编写可以提高智能合约质量和安全性。智能合约往往涉及各种的密码协议和算法实现。在实际应用中需要注意随机数来源是否可靠以及私钥存储安全。

（4）智能合约的升级和恢复

在尽量避免在智能合约实现漏洞的同时，我们也有必要在智能合约中引入发现漏洞时的应急方案。合约暂停恢复和合约升级是两种常见的应急方案。合约的恢复暂停使得合约的管理者可以在发现漏洞的情况下暂停合约的主要功能，并在合适的时间重新恢复合约的功能。合约升级使得合约的管理者可以将当前合约的使用者迁移到已修改漏洞的新合约上。无论采用什么样的应急机制，都需要保证该机制的实现本身没有漏洞，并且只能在受限的情况下被使用。

7 以太坊智能合约虚拟机

（5）智能合约的形式化验证

形式化验证的含义是根据某个或某些形式规范或属性，使用数学的方法证明其正确性或非正确性。形式化验证是一个系统性的过程，将使用数学推理来验证设计意图（用户功能需求）在实现(智能合约)中是否得以正确贯彻。

7.3 针对虚拟机的应对策略建议

在设计和实现智能合约语言虚拟机时，可以从以下五个方面考虑。

（1）目标语言和源语言的语义的一致性

开发者通常使用源语言（例如以太坊上的Solidity语言）开发智能合约，然后通过相应的编译器（例如以太坊上的Solidity编译器）将源语言程序编译成可以在虚拟机上运行的目标语言程序（例如以太坊上的EVM字节码)。目标语言和源语言语义的一致性保证了开发者的希望通过智能合约实现的意图，在虚拟机上能够得到正确完整的实现。

（2）防范拒绝服务攻击

由于区块链的去中心化特性，一个智能合约可能需要在多个节点上独立运行，以达成对该智能合约运行结果的共识。如果虚拟机中存在可以被智能合约触发的拒绝服务漏洞，攻击者就可以通过部署恶意合约瘫痪部分甚至整个区块链系统。因此，虚拟机的设计和实现中需要防范此类拒绝服务漏洞。同时，也需要结合区块链的机制设计防范拒绝服务攻击。

（3）防范虚拟机逃逸

虚拟机逃逸是指恶意智能合约可以利用虚拟机逃逸漏洞脱离虚拟机的控制，访问甚至控制虚拟机本身所处的运行环境，进而可以访问和控制其它合约在该虚拟机上的运行。攻击者如果通过虚拟机逃逸漏洞进一步控制区块链网络中的大多数节点，甚至可以发起51%攻击。因此，虚拟机设计和开发中需要尤其关注此类逃逸漏洞。

（4）多个智能合约运行环境的强隔离

无论采用什么样的虚拟机实现模型，虚拟机，特别是强调隐私保护的区块链系统上的虚拟机，需要保证在同时运行多个智能合约时，各个合约的运行环境的相互隔离。例如，不存在测信道使得一个合约可以探测另一个合约的敏感行为，不存在测信道使得一个合约可以影响另一个合约的运行。

第八章　应用生态安全

8.1　安全风险分析

（1）数字钱包安全

区块链的数字钱包指的是存储区块链资产的地址和私钥文件。区块链系统的提供方会发布全节点钱包，也有一些第三方公司为了进一步提高用户体验开发了钱包APP，钱包APP并不同步所有的区块数据，这两种数字钱包都属于热钱包。硬件钱包由于私钥不接触网络，相对安全性也较高。不过由于业务场景的快速迭代以及推广需求，无论热钱包还是冷钱包都会有一些的安全隐患会被忽视。

数字钱包安全隐患包含以下几方面：

a)用户操作被截屏/录屏，导致助记词、交易密码被黑客获取。

b)未检测系统运行环境，利用系统历史已知漏洞进行黑客攻击，远程操作APP。

c)APP伪造漏洞，利用APP未做防护或已知漏洞对软件包进行处理，对APP重打包植入恶意代码。

d)交易密码未检测弱口令，导致口令被攻击者恶意猜测，并用其进行交易。

e)核心代码未加固，导致APP执行逻辑被分析，本地加解密算法被逆向。

（2）业务平台安全

区块链系统的业务平台的安全依赖于应用开发者，主要取决于业务逻辑是否严谨，对每段业务代码是否进行大量的模糊测试与代码审计，系统是否存在安全漏洞和严重错误等，主要的安全问题主要体现在逻辑漏洞、木马攻击、DDoS攻击等方面。

（3）管理平台安全

部分区块链系统有着复杂的账户体系以及针对账户构建的权限管理体系。带来的潜在安全问题有：节点的认证与授权安全、账户和其权限的管理安全等。

8.2 应对策略

（1）推出完善的钱包安全检测方式

作为与数字资产安全息息相关的关键对象，加密数字钱包APP大多关系到高度敏感的用户数字资产交易，需利用专业的检测工具及方法对钱包进行全面检测，表6是常见的钱包安全的检测方式。

表6 数字钱包检测方式

安全检测类型	细分
运行环境安全检测	手机系统漏洞扫描 Root环境检测 APP完整性检测 网络代理检测 网络安全检测
协议环境安全检测	新用户注册安全 创建交易安全 交易签名安全 交易完毕确认 余额查询安全
数据存储安全检测	助记词创建安全 助记词存储安全 私钥生成安全 私钥储存安全 本地存储数据敏感性检测
功能设计安全检测	导入钱包功能安全 交易密码安全 用户输入安全 转账地址安全检测 https通信中的证书校验

（2）构建企业广泛参与的安全生态

区块链应用生态涉及如金融、存证、物联网等诸多垂直领域，需要相关垂直领域的企业广泛参与区块链应用安全的建设。在积极探索区块链解决方案的同时，共同推动区块链技术在数据存储的安全、加强隐私保护、节点认证安全等方面的发展和落地。同时政府层面应正确引导区块链技术发展和行业应用，在自可控的前提下鼓励企业在区块链的安全应用领域发挥积极的作用。

第九章　区块链安全对策与建议

现有的安全问题对认证机制、形式化验证、技术架构、数据保护和基础设施的全局发展提出了考验，我国在积极布局区块链的行业应用的同时，也应看到区块链应用的潜在安全风险，需要从加强技术研究，积极制定安全标准规范，加强监管等方面采取积极应对措施，正确引导区块链技术和产业应用的健康发展。

9.1　加快制定区块链安全标准与规范

区块链应用安全标准和规范的制定，有助于支撑各类应用的区块链技术平台的开发、运行、维护和管理，规范和引导区块链相关技术和相关软件的开发。加快制定具有我国独立知识产权的区块链相关安全规范和标准，提升区块链安全监控能力，以保障区块链产业健康发展和持续创新。

9.2　鼓励区块链安全服务行业的发展

区块链安全相对于传统网络安全，有共性的地方，也呈现出许多新的特征，鼓励传统网络安全企业进入区块链安全领域问题，推动相关的安全解决方案和安全服务的落地，如智能合约的审计、安全评测、区块链系统安全监测等，在区链应用大范围来临之际，提升区块链产品的抗攻击能力和安全性。

9.3　推动技术研究和难点攻关

加强技术研究和难点攻关投入，针对区块链技术性能瓶颈与系统安全性的平衡、隐私保护及数据检索安全等方面，积极开展研究工作，以满足区块链在各领域应用的安全要求。积极关注区块链技术的前沿方向，持续跟进安全解决方案的发展。

9.4　强化区块链安全监管

由于区块链的数据难以篡改、去中心化等特性，对监管层面提出了新的考验。需推动

监管模式的创新，明确区块链服务主体责任，积极探索在区块链系统中增加监管节点的可行性，推动建设跨部门监管的长效机制，加快制定区块链安全分级制度等。为生态应用的发展提供安全可靠的环境。

可信区块链推进计划

地址：北京市海淀区花园北路52号　邮政编码：100191

联系电话：010-62300249　传真：010-62304980

网址：www.trustedblockchain.cn