前　言

当今，全球信息领域的新一轮科技创新和产业变革持续深入，渗透范围越发广泛，作为研发投入最为集中、应用成效最大的信息技术，正是此次引领变革的主导力量和技术创新的竞争高地。

在此背景下，区块链作为一种分布式数据存储、点对点传输、共识机制、加密算法等技术的新型集成应用，发展势头迅猛，近年来已经成为世界各国研究讨论的焦点。其生态系统已延伸到物联网、云计算、大数据、人工智能等多个领域，应用场景也涵盖了金融、投资、监管等机构，引发了新一轮的技术创新和产业变革。

一直以来，安全问题都是信息产业的重大发展方向，随着科技技术的演变和复杂化，信息安全问题的需求日益迫切，同时也被赋予了新的内涵外延。而区块链作为一种新兴技术，安全性威胁是其迄今为止所面临的最重要的问题之一。

为全面了解和推动区块链技术和产业发展，解决区块链目前面临的安全问题，“白帽汇安全研究院”采用自主创新技术，根据区块链的数据层、网络层、共识层、扩展层和业务层的不同应用场景下的主流攻击事件进行探索，分析和总结，提出了安全加固、渗透测试、仿冒监测和合约审计四类安全解决方案，与国家安全机构、金融企业、信息安全部门、互联网巨头等建立深度合作关系，多项研究成果成功应用于漏洞预警和产品服务，最终整合编纂形成了《区块链产业安全分析报告》，并希望以此契机建立起安全可靠的区块链技术安全生态体系。

目录

一 区块链概述

1.1 定义

区块链[1]是一种分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式，是以比特币为代表的数字加密货币体系的核心支撑技术，且可以从两个方面来进行定义：从狭义的角度上来讲，区块链是一种以时间顺序排列的链式结构数据，并通过密码学的方式来保证数据的不可篡改、不可伪造。从广义的角度来讲，区块链技术是利用块链式数据结构来存储数据、利用链式数据的前后关系来验证数据、利用分布式节点来生成数据，利用共识算法来更新数据、利用密码学来保证数据的真实性、利用由程序代码组成的智能合约保证协议的不可违约性的一种同时具备高可用、高扩展、高安全等特性的全新数据系统。其核心优势是去中心化，能够通过运用数据加密、时间戳、分布式共识和经济激励等手段，在节点无需互相信任的分布式系统中实现基于去中心化信用的点对点交易、协调与协作，从而为解决中心化机构普遍存在的高成本、低效率和数据存储不安全等问题提供了解决方案。

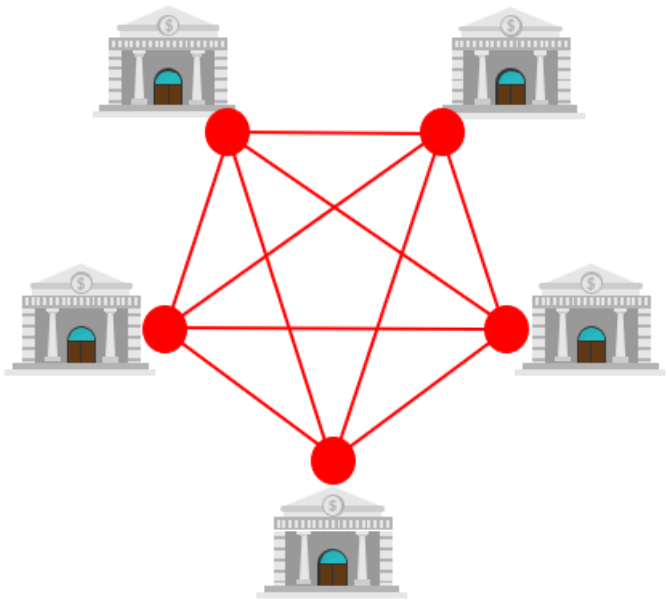
如下图所示，高亮的点是区块链系统中分布在全球各地的各个节点；而这些节点可以简单理解为一台服务器或服务器集群，并能够协同运转的数据库存储系统。区别于传统数据库运作——读写权限掌握在一个公司或者一个集权手上（中心化的特征），区块链认为，任何有能力架设服务器的个体都可以参与其中。来自全球各地的开发人员在当地部署了自己的服务器，并连接到区块链网络中，成为这个分布式数据库存储系统中的一个节点；一旦加入，该节点享有同其他所有节点完全一样的权利与义务（去中心化、分布式的特征）。与此同时，对于在区块链上开展服务的参与者，可以往这个系统中的任意节点进行读写操作，最后全世界所有节点会根据某种机制完成一次又一次的同步，从而实现在区块链网络中所有节点的数据完全一致。

1.2 特征

区块链技术是具有普适性的底层技术框架，可以为金融、经济、科技甚至政治等各领域带来深刻变革。在信息网络化的大背景下，当需要进行信息交换的时候，如何防止遭遇恶意欺诈，从而做出正确决策？具有去中心化、可追溯性等特征的区块链技术正好解决了此类难题，区块链的核心技术均围绕此进行展开。

1.2.1 去中心化

区块链使用分布式架构，在区块链网络中的节点同时扮演着“传播者”和“验证者”的角色，享受同等的权利、承受同等的义务，节点与节点之间可以自由通信，系统中的数据块由具有存储能力的节点共同存储。



1.2.2 开放性

区块链整体系统是开放的，除了节点的私钥以外，网络中的节点信息对所有人公开，区块链中的数据对所有人公开，区块链的源代码对所有人公开。

1.2.3 自治性

区块链采用基于预先设定好的规范或协议使得整个网络中的所有节点能够在自由、安全、无障碍的情况下的进行交互。

区块链技术将原本人与人之间”的信任转化为人对机器的信任，任何人为的行为都难以撼动机器计算的结果。

1.2.4 不可篡改性

在区块链系统中，由于使用了哈希函数以及非对称加密等先进的密码学技术，在信息经过验证后会被打包至区块中，由于区块链只做加法，所以区块链上的区块数据不可销毁。由于它是分布式的，所以单个节点对区块的修改对于整个区块链来说毫无影响，因此区块链的数据稳定性和可靠性都是极高的。

1.2.5 可追溯性

尽管区块链中的匿名性无法看到交易双方的身份信息，但区块+链的形式保存了从第一个区块开始的所有历史数据，连接的形式是后一个区块拥有前一个区块的 HASH 值，区块链上任意一条记录都可通过链式结构追溯本源，这样从另一个方面保障了信息的安全性。

1.3 分类

基于多种应用参与方式，区块链目前主要分为公有区块链、联盟区块链和私有区块链。

1.3.1 公有区块链

公有区块链是指：世界上任何个体或者团体都可以发送交易，且交易能够获得该区块链的有效确认，任何人都可以参与其共识过程。公有区块链是最早的区块链，也是目前应用最广泛的的区块链。是指像比特币区块链这样的完全去中心化的、不受任何机构控制的区块链。共识过程的参与者通过密码学技术以及内建的经济激励维护数据库的安全。

1.3.2 联盟区块链

联盟区块链是指：由某个群体内部指定多个预选的节点为记账人，每个块的

生成由所有的预选节点共同决定，其他接入节点可以参与交易，但不过问记账过程（本质上还是托管记账，只是变成分布式记账，预选节点的多少，如何决定每个块的记账者成为该区块链的主要风险点），其他任何人可以通过该区块链开放的 API 进行限定查询。

参与区块链的节点是事先选择好的，节点间很可能是有很好的网络连接。这样的区块链上可以采用非工作量证明的其他共识算法，比如有 100 家金融机构之间建立了某个区块链，规定必须 67 个以上的机构同意才算达成共识。

1.3.3 私有区块链

私有区块链是指存在一定的中心化控制的区块链。仅仅使用区块链的总账技术进行记账，可以是一个公司，也可以是个人，独享该区块链的写入权限，本链与其他的分布式存储方案没有太大区别。参与的节点只有用户自己，数据的访问和使用有严格的权限管理。联盟链由于存在一定的中心化控制，所以也可以认为是属于私有链范畴。

此三种定义的主要区别如下表所示，

公有链	联盟链	私有链
• 任何人都可加入网络及写入和访问数据； • 任何人在任何地理位置都能参与共识； • 每秒3-20次数据写入	• 授权公司和组织才能加入网络； • 参与共识、写入及查询数据都可通过授权控制，可实名参与过程，可满足监管AML/KYC； • 每秒1000次以上数据写入	• 使用范围控制于某个范围内； • 改善可审计性，不完全解决信任问题； • 每秒1000次以上数据写入

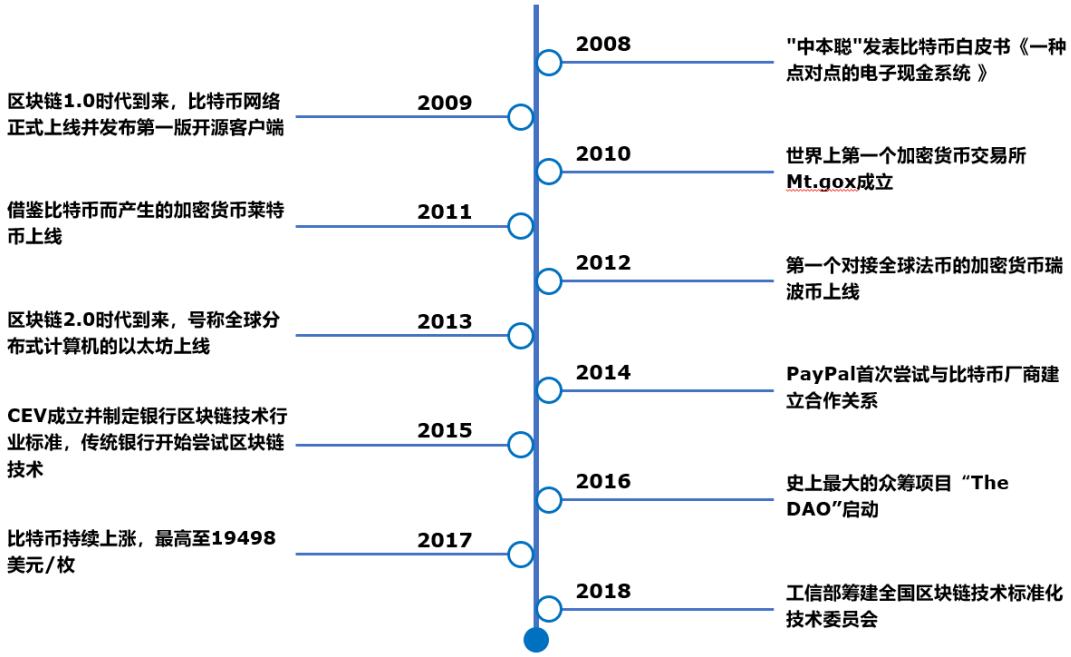
1.4 发展

早在 1976 年，Bailey W. Diffie、Martin E. Hellman 两位密码学的大师发表了论文《密码学的新方向》，论文覆盖了未来几十年密码学所有的新的进展领域，包括非对称加密、椭圆曲线算法、哈希等一些手段，奠定了迄今为止整个密码学的发展方向，也对区块链的技术和比特币的诞生起到决定性作用。

在 21 世纪到来之际，区块链相关的领域又有了几次重大进展：首先是点对

点分布式网络，1999 到 2001 的三年时间内，Napster、EDonkey 2000 和 BitTorrent 分别先后出现，奠定了 P2P 网络计算的基础。2001 年另一件重要的事情，就是 NSA 发布了 SHA-2 系列算法。

2008 年 11 月，“中本聪”发表论文《比特币：一种点对点的电子现金系统》，提出了区块链这种数据结构，区块链技术迎来了爆发式的增长和关注，技术迭代速度之快，超出任何人的想象，每隔一段时间就会有重量级事件发生，进一步助推了整个技术的发展。



二 区块链安全性

2.1 背景

安全问题一直是信息化社会的主旋律，随着区块链技术的广泛应用，随之而来的问题也越来越多，由于区块链去中心化，匿名性等一系列特点，目前在资本行业被大量使用，其中用于投资的情况也越来越多，正因为这一系列的特性与场景结合，随之而来的各类攻击也开始不断出现，从之前的区块链底层安全技术研究曝光，发展到后来越来越多的虚拟货币被盗，交易所被攻击等事件。而这些只是目前被暴露的一部分，随着区块链技术所产生的价值越来越高，所面临的攻击将持续增加。

区块链技术自身尚处于快速发展的初级阶段，面临的风险不仅来自外部实体的攻击，也有可能来自内部参与者的攻击，应对区块链技术的安全特点和缺陷，需要围绕物理、数据、应用系统、加密、风险控制等构建安全体系。与此同时，区块链技术的普及应用对保障数据存储，数据传输和数据应用等多个方面的安全和隐私保护提出了全新的要求。

随着目前所发生的一系列交易平台监守自盗、交易所遭受黑客攻击、用户账户被盗等安全事件，我们不得不承认一个事实，区块链的“安全神话”已然破灭。

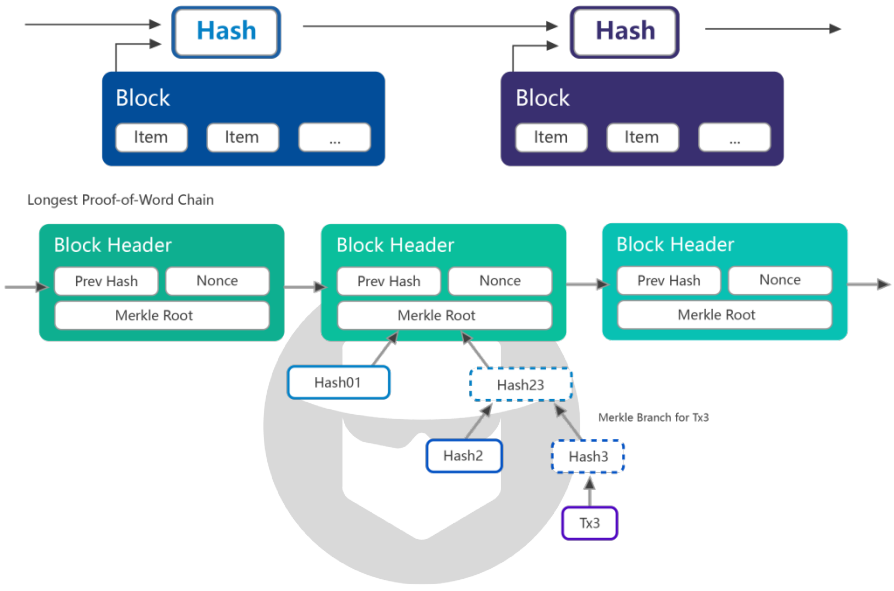
由于区块链目前异常活跃，不仅推动了虚拟货币的发展，而且还加强了现有的安全解决方案，对认证机制、数据保护和基础设施的全局发展提出了全新的要求。因此，急需建立一种或多种协同安全解决方案来提升区块链整体系统的安全性能。

2.2 底层原理

以链式结构保存基础数据，多个节点参与系统运行，以一定的算法对基础数据的操作达成一致性共识。

在“中本聪”的论文中，区块链是由若干个时间顺序、包含交易信息的区块从后向前有序链接起来的数据结构，每一个区块都包含了当前区块构成时间内所

有的信息，并由一个 Hash 值进行封装和指向上一个区块。数据结构可以被视为一个垂直的栈，可形象化地描述为每一个区块就像一个箱子，每一个新的区块都堆在上一个区块之上，形成了一摞箱子，于是“高度”就可以表示区块和首区块的距离；“顶端”就是指最新的区块；区块头就像是箱子的表面，封装了内部的交易信息，并标明父系区块链的位置。每一个区块头都可以找到其父系的区块，并最终回溯到创世区块上。



由于区块头要包含“父系区块 Hash”的字段，所以任何父系区块的修改，都会引发子区块的改变，而子区块的改变将引起孙区块的改变，这种变化会一直传导到最新的区块，并且这种改变是没有规律的，服从“雪崩效应”，这就意味着任何人想要更改之前区块的内容，将会耗费大量的算力来运算更长的链条，即实现“51%攻击”。这对于修改者来说，成本过于高昂。此外，即使实现了“51%攻击”，也只能抹除自己的交易信息，并不能修改整个程序和参数。

因此，区块链具有如下安全特性：（1）写入数据的安全性：对于写入区块链的数据而言，在共识机制的制约之下，当全网大部分的节点或者核心的节点认可这个记录时，这个数据的合法性和真实性才得以确保，记录才允许被永久写入区块链中。（2）读取数据的安全性：由于区块链中的数据是加密存储的，只有拥有用户私钥的节点才可以解密区块中的核心数据，进而获取区块内容。此外，区块

链的共识机制是复杂的，能否确保大部分的用户能够看到一个相同的账本。（3）分布式拒绝服务（DDOS）攻击抵抗：区块链的去中心化架构相比于传统的网络架构，其节点分散、无固定中心且具备冗余的特性，针对区块链的 DDOS 攻击将会更难展开。攻击者对某个节点攻击时，即便这个节点失效，也不会影响整个区块链系统。

2.3 安全分析

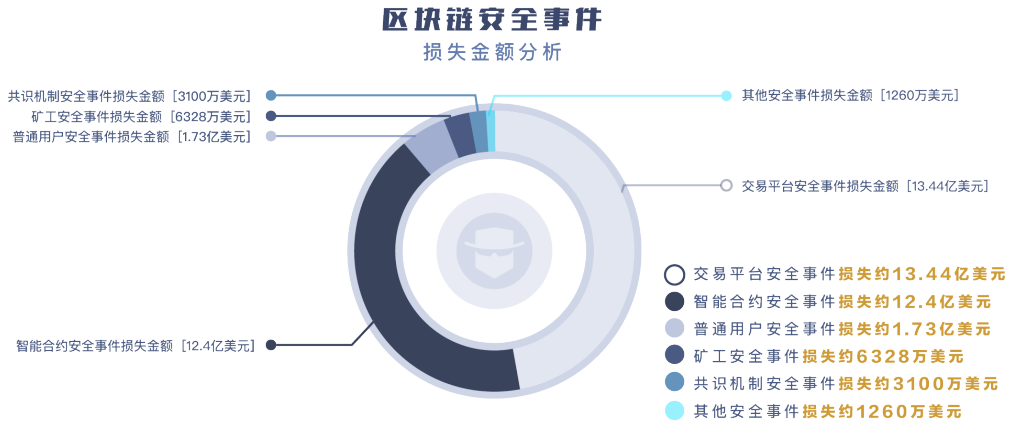
目前区块链面临了诸多方面的安全挑战，主要包含以下几个方面：（1）密码算法安全性：目前区块链基于的算法主要是公钥算法和哈希算法，其安全性来源于数学难度，相对是安全的。但是随着高性能计算和量子计算的发展和商业化，目前所有的加密算法均存在被破解的可能性，这也是区块链面临的一个威胁。（2）协议安全性：区块链中，如果一个节点能够掌控全网 51%的计算能力，就可以伪造或者篡改区块链的数据。在目前典型的电子货币的应用场景中，这是得不偿失。但是随着区块链应用范围的扩宽，攻击者为了达到某种目的，有可能实施这样的攻击。（3）使用安全性：区块链有着无法篡改，不可伪造，计算不可逆的特点，但是必须是在私钥安全的前提之下。但是目前针对密钥的攻击层出不穷，一旦用户使用不当，造成私钥丢失，就会给区块链系统带来危险。（4）系统安全性：在区块链的编码，以及运行的系统中，不可避免会存在很多的安全漏洞，针对这些漏洞展开的攻击日益增多，这对区块链的应用和推广带来极大的影响。

2.4 历史安全事件

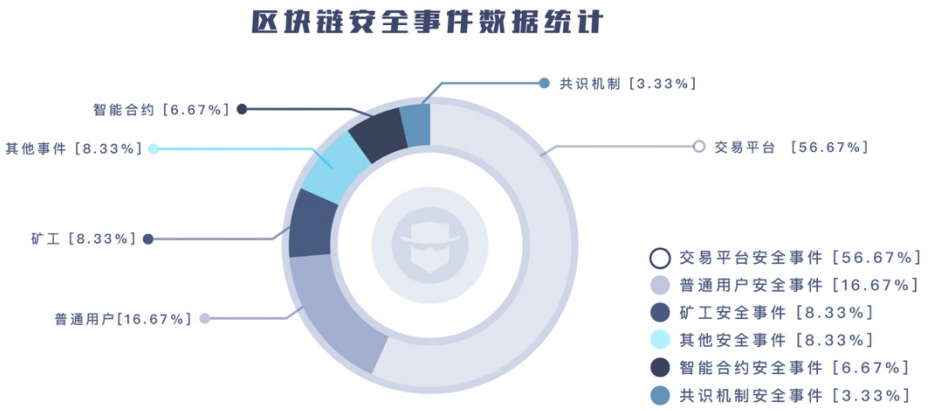
尽管区块链在最底层原理方面保障了其可靠性，但目前区块链安全机制并不十分健全，攻击者主要选择保护相对薄弱的数据层、网络层、共识层、扩展层和业务层进行攻击，每年因区块链安全漏洞造成的损失高达数十亿美元。

从分析结果来看，攻击事件大致可分为四类安全事件：共识机制、智能合约、交易平台和用户自身。

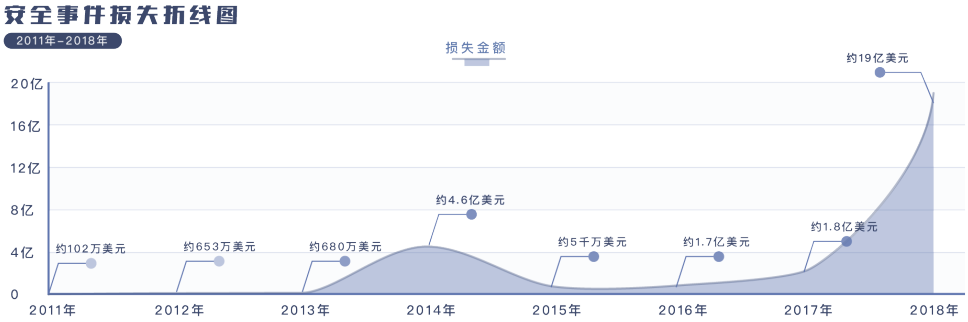
以下是 2011 年至 2018 年 4 月 30 日发生的各类安全事件所造成的损失：



及 2011 年至 2018 年发生的安全事件数量统计：



2011 年至 2018 年发生的安全事件所造成的损失折线图：



我们通过对历史的安全事件影响分析得知，目前近 80%的攻击损失都是基于业务层面的攻击所造成的，其损失额度从 2017 年开始呈现出指数上升的趋势，截止到 2018 年第一季度，所暴露的安全事件就已经造成了 8.1 亿美元的损失，按照历史的攻击趋势，相信以后此类攻击事件会越来越严重。

以下是 2011 年至 2018 年所发生安全事件的详细说明。

2.3.1 区块链自身安全事件

时间	事件	导致后果
2017 年 10 月	比特币网络遭遇垃圾交易攻击	10%以上的比特币节点下线
2016 年 8 月	基于以太坊的数字货币 Krypton 遭受来自一个名为“51% Crew”的组织的 51%攻击	攻击者利用双重支付盗取约 21,465 KR 的代币（约 3000 多美金）
2014 年 8 月	在线黑市 Silk Road 2 遭遇交易延展性攻击，比特币被盗	Silk Road 2 损失约 260 万美元

2.3.2 智能合约安全事件

时间	事件	导致后果
2018 年 4 月 25 日	SmartMesh 出现类似 BEC 的重大安全漏洞	导致约损失 1.4 亿美元

2018 年 4 月 22 日	BeautyChain 出现重大安全漏洞，价值几乎归零	BEC 凭空蒸发了 10 亿美元
2017 年 7 月 20 日	Parity 客户端附带的多重签名钱包智能合约被发现存在严重漏洞，攻击者可以立即接管钱包并吸收所有资金	攻击者从三个高安全的多重签名合约中窃取到超过 15 万 ETH（约 3000 万美金）
2016 年 6 月 17 日	运行在以太坊公有链上的 The DAO 智能合约遭遇攻击	该合约筹集的公众款项不断被一个函数的递归调用转向它的子合约，涉及总额三百多万以太币（约 6000 多万美金）

2.3.3 交易平台安全事件

时间	事件	导致后果
2018 年 4 月	印度比特币交易所 Coinsecure 公司钱包遭窃取	Coinsecure 被盗取 438 比特币，价值超过 300 万美元
2018 年 4 月	虚拟货币 Verge(XVG)，遭到攻击	黑客窃取了价值 100 万美元的 XVG 代币
2018 年 3 月	迪拜某加密货币交易所员工窃取 20 万美元的加密货币供个人使用	交易平台损失价值约 20 万美元的加密货币
2018 年 3 月	火币网遭到 DDOS 攻击	持续 3 小时系统无法交易
2018 年 3 月 7 日	币安交易所用户数据被盗	攻击者操纵币市，通过做空单获利约 1.1 亿美金
2018 年 2 月	交易所 BitGrail 被攻击，大量 XRB 被黑客窃取	平台损失约 1.7 亿美金
2018 年 1 月 26 日	日本最大的比特币交易所之一 Coincheck 遭黑客攻击	5.3 亿美金被盗。
2017 年 12 月	韩国数字货币交易所 Youbite 受到黑客入侵，造成的损失相当于平台内总	损失约为 4000 万美元

	资产的 17%	
2017 年 6 月	韩国最大交易所 Bithumb 三万用户信息被泄露	损失约 87 万美元
2017 年 4 月	韩国比特币交易所 Yapizon 被盗 3831 BTC，用户将平摊所有损失	损失约为 500 万美元，相当于该平台总资产的 37%
2016 年 8 月	Bitfinex 遭黑客攻击	约 12 万 BTC 被盗，损失达 7500 万美元
2016 年 5 月	香港数字货币交易所 Gatecoin 遭黑客攻击	损失约 200 万美元
2016 年 3 月	ShapeShift 丢失 23 万美元数字货币，“内鬼”将安全信息出售给黑客	数字货币交易所 ShapeShift 丢失了价值 23 万美元的数字货币
2016 年 3 月	比特币交易平台 BitQuick 服务器遭攻击	服务器下线
2016 年 1 月	交易所 Cryptsy 称其被攻击	1.3 万 BTC 以及 30 万 LTC 被盗，损失达 600 万美元，随后该交易所关闭
2015 年 2 月 14 日	国内山寨币交易平台比特儿遭到黑客攻击。	宣布被盗 7170 个 BTC，价值约 150 多万美金
2015 年 1 月	全球知名的数字货币交易所 Bitstamp 系统管理员被诱导执行恶意文件	导致该交易所损失约 500 万美金
2014 年 12 月	BitPay CEO 遭网络钓鱼，资金被骗	BitPay 损失约 180 万美元
2014 年 5 月	交易所 LocalBitcoins 遭受 DDOS 攻击	服务停止约 40 分钟左右
2014 年 4 月	BTC-E 比特币交易平台遭受强大的 DDOS 攻击	正常用户无法访问，给平台带来隐形损失
2014 年 3 月	美国数字货币交易所 Poloniex 被盗	损失 12.3%的比特币，暂未公布确切损失金额

2014 年 2 月	曾经世界第一的日本交易所 Mt.Gox，导致其最终被迫宣布破产	损失约 3.6 亿美金
2013 年 11 月	波兰比特币交易平台 Bidextreme.pl 遭受黑客攻击	4000 用户的钱包被盗，1.7 万个比特币遗失（在当时价值约 560 万美元）
2013 年 11 月 10 日	澳大利亚 Tradefortress 比特币银行被盗	丢失 4100 个比特币（约 120 万美元）
2012 年 9 月	Bitfloor 交易中心也被黑客入侵，Bitfloor 因此暂停运营	24,000 比特币（约相当于 25 万美元）被盗
2012 年 8 月下旬	Bitcoin Savings and Trust 被所有者关闭	留下据称约 560 万美金的债务。同时导致其被指控操作庞氏骗局。2012 年 9 月，美国证券交易委员会开始调查这一案件
2012 年 8 月上旬	2012 年，Bitcoinica 两度遭到黑客攻击	Bitcoinica 在旧金山法院被起诉要求赔偿约 46 万美金。被指控忽略客户资金的安全性以及伪造提款申请
2012 年	由于网站托管供应商 Linode 的服务器超级管理密码泄露，Bitcoinica 交易平台钱包内比特币被黑客窃取	价值 22 万美金的 46703 比特币失窃
2011 年 8 月上旬	作为常用比特币交易的处理中心之一的 MyBitcoin 宣布遭到黑客攻击，并导致关机。	涉及客户存款的 49%，超过 78000 比特币（当时约相当于 80 万美元）下落不明。
2011 年 7 月	世界第三大比特币交易中心部分 wallet.dat 访问权限丢失	损失约 17 多万个比特币（约 22 万美元）
2011 年 6 月 19 日	Mt.Gox（Magic: The Gathering Online Exchange）安全漏洞被黑，泄露大量数据	比特币交易中心的安全漏洞导致 1 比特币价格一度跌至 1 美分，具体损失金额未知

2.3.4 用户自身安全事件

时间	事件	导致后果
2018 年 3 月	印度女子与骗子共享证书，比特币被盗	受害者损失约 5.5 万美元的比特币
2018 年 2 月	有人在 twitter 上冒充知名人士如 Vitalik Buterin 诈骗数字货币	诈骗分子在短时间内诈骗到约 20000 美元的数字货币
2018 年 1 月	IOTA 社区大量用户钱包代币被窃取	给用户造成大量损失
2017 年 11 月	Bitcoin gold 遭钱包骗局，用户导入数百万美元比特币却不翼而飞	总共价值约 323 万美元的代币被窃取
2017 年 11 月	CryptoShuffler 木马从受害者的钱包中偷走了 160,000 美元的比特币	价值约 16 万美元的比特币被窃取
2017 年 10 月	交易所 OKEx 数位用户平台账号被窃取	被盗约 600 个 BTC，当时价值约 300 万美元
2016 年 12 月	黑客仅通过使用电话号码盗取用户大量比特币	某用户损失数百万美元
2015 年	比特币服务提供商 Purse 用户资金遭窃	公司部分用户的比特币资金遭窃（官方称 10.235 BTC），并导致网站在周日被迫下线数个小时，约 3000 美元
2015 年	利用 Google Adwords 污染搜索结果 Coinhoarder 钓鱼事件	攻击者从受害者手中盗取约 5000 万美元的数字货币

2.3.5 其他安全事件

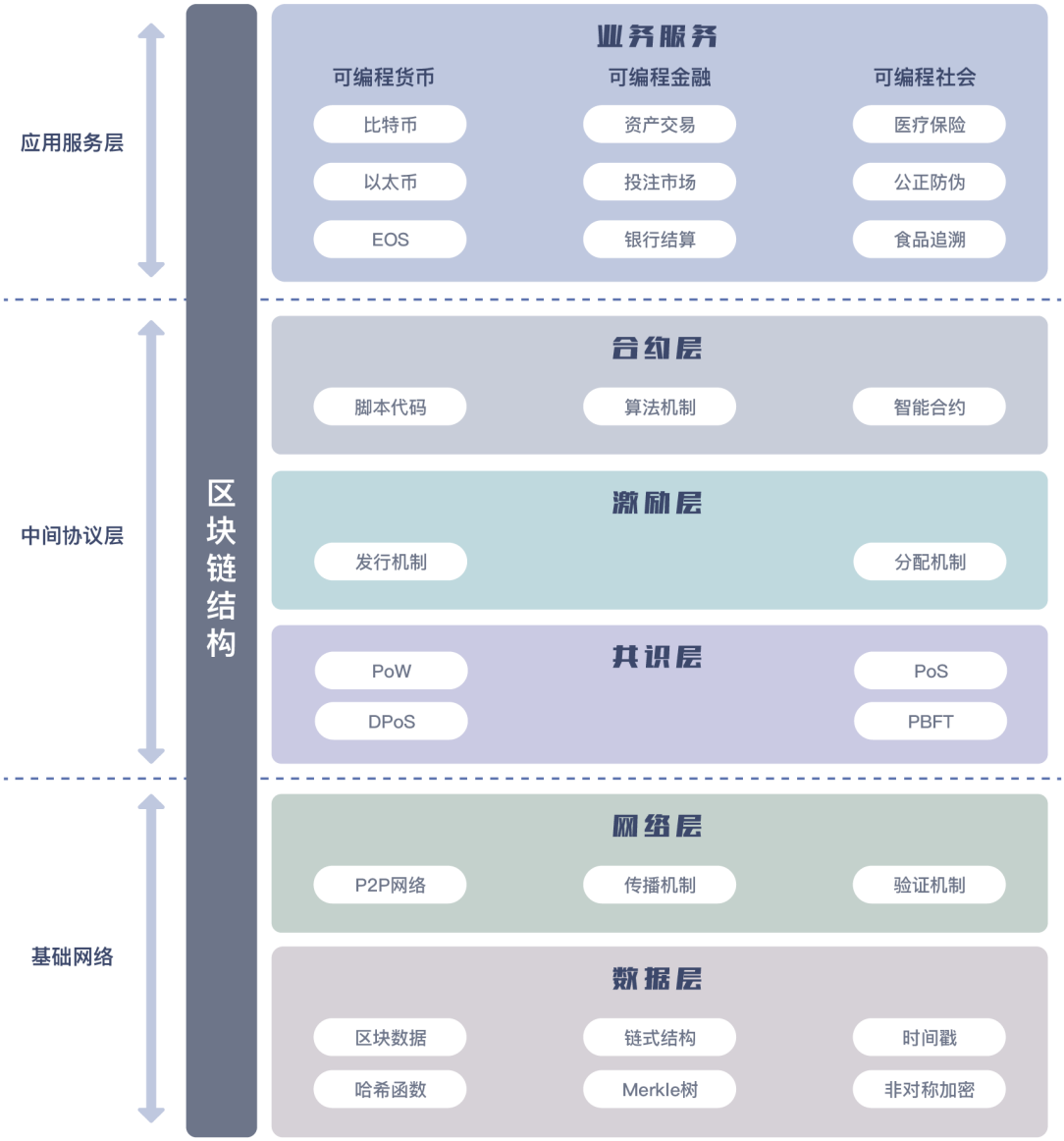
时间	事件	导致后果
2018 年 4 月	最受欢迎的以太坊钱 Myetherwallet 遭 DNS 劫持	总计约 524ETH 收已经被转入到两个黑客地址中。

2018 年 1 月	通过劫持在线钱包 BlackWallet 的 DNS 服务器，黑客窃取 40 万美金	BlackWallet 损失 40 万美金
2017 年 12 月	数字代币初创公司 Tether 宣布自己的系统遭遇黑客袭击	大约 3,100 万美元的代币从他们的虚拟财务部门被拿走并被发送到一个未知的比特币地址
2017 年 12 月	斯洛文尼亚加密挖矿网站 Nicehash 被盗	被盗约 4700 个比特币，价值约 6200 万美元。
2017 年 10 月	比特币黄金网站遭遇 DDOS 攻击	数小时内比特币黄金网站网站无法访问
2017 年 7 月	CoinDash 项目 ICO 众筹地址遭到黑客篡改	大约价值 1000 万美元的 eth 被发送到黑客钱包
2015 年 5 月	BitcoinTalk 论坛遭社会工程学攻击	用户数据疑似泄露，服务器下线
2015 年 3 月	AntPool，BW.com，NiceHash，CKPool 和 GHash.io 等矿池遭 DDOS 攻击	部分矿池服务中断，导致部分区块链项目全网算力下降
2014 年 8 月	黑客从比特币矿池中窃取 83,000 美元	至少有 51 个网络受到了 19 个不同 ISP 的损害，至少有一名劫机者能够利用这个漏洞将加密货币矿工的连接重定向到一个劫机者控制的采矿池，从而为自己收集了矿工的利润。
2014 年 6 月	Eligius 矿池遭受“块代扣攻击”	损失约 300 个 btc，价值约 120 万美元
2014 年 4 月	Blockchain.info 因被 DDoS 攻击服务临时下线	正常用户无法访问
2013 年 11 月	GHash.io 矿池对赌博网站 BetCoin Dice 进行多次付款欺诈，实施双重支出攻击	事件发生时，比特币社区内外一度对比特币的信誉机制、安全性产生怀疑，氛围一片恐慌

三 区块链攻击对象分析

基于目前世界各国对加密货币的态度不尽一致，在区块链货币领域黑客几乎可以为所欲为，尚处于无法监管的状态，所以思考已经发生或者可能发生的安全问题对于区块链应用来说是必不可少的。

就目前区块链的特征，我们进行了如下分层：应用服务层、中间协议层和基础网络。并基于以下层面出发，针对每层中各个“攻击面”去分析已发生或者可能发生的安全风险：



一般来说，区块链系统由数据层、网络层、共识层、激励层、合约层和业务服务层组成。其中，数据层封装了底层数据块区以及相关的数据加密和时间戳等技术；网络层则包括分布式组网机制、数据传播机制和数据验证机制等；共识层主要封装网络节点和各类共识算法；激励层将经济因素集成到区块链技术体系中来，主要包括经济激励的发行机制和分配机制等；合约层主要封装各类脚本、算法和智能合约，是区块链可编程特性的基础；业务层则封装了区块链的各种应用场景和案例。

该模型中，基于时间戳的链式块区结构、分布式节点的共识机制、基于共识算力的经济激励和灵活可编程的智能合约是区块链技术最具代表性的创新点。经过对区块链技术的各个层面进行纵向剖析，并针对上述层次的不同“角色”进行安全性分析后，我们发现目前攻击者通常从两个点出发：

1. 区块链中的中心化对象：交易平台、在线钱包等。
2. 区块链中的去中心化对象：智能合约、共识机制等。

我们根据攻击者主要采用的攻击方式、对象和等级，总结如下表所示：

名称	严重等级	攻击对象
恶意信息攻击	中危	区块数据
资源滥用攻击	高危	区块数据
穷举攻击	低危	加密方式
碰撞攻击	高危	加密方式
长度扩展攻击	高危	加密方式
后门攻击	高危	加密方式
量子攻击	严重	加密方式
渗透攻击	中危	P2P 网络
拒绝服务攻击	高危	P2P 网络
交易延展性攻击	低危	传播机制
日食攻击	中危	传播机制
验证绕过攻击	严重	验证机制

短距离攻击	中危	共识机制
长距离攻击	高危	共识机制
币龄累计攻击	中危	共识机制
预计算攻击	中危	共识机制
女巫攻击	中危	共识机制
逃逸漏洞	高危	合约虚拟机
逻辑漏洞	视具体情况而定	合约虚拟机
堆栈溢出漏洞	严重	合约虚拟机
资源滥用漏洞	高危	合约虚拟机
可重入攻击	高危	智能合约
调用深度攻击	中危	智能合约
交易顺序依赖攻击	中危	智能合约
时间戳依赖攻击	中危	智能合约
误操作异常攻击	视具体情况而定	智能合约
整数溢出攻击	视具体情况而定	智能合约
私钥窃取	高危	钱包
钱包软硬件漏洞攻击	高危	钱包
在线钱包账号窃取	高危	钱包
钓鱼攻击	高危	交易所账户
中间人劫持攻击	高危	交易所账户
木马劫持攻击	高危	交易所账户
关键 key&token 窃取	高危	交易所 API
挖矿傀儡	中危	挖矿节点
奖励接收地址篡改攻击	高危	挖矿节点
0day 攻击	严重	矿机系统
弱口令攻击	高危	矿机系统

扣块攻击	中危	矿池平台
中心化问题	中危	矿池问题
单点登陆漏洞	中危	交易平台
oAuth 协议漏洞	中危	交易平台
支付漏洞	高危	交易平台

3.1 数据层

3.1.1 区块数据

简要

基于区块链技术本身的特性，区块数据是分布在多个节点上的链式结构数据，节点与节点之间的“互动”将记录在区块中，然后在各个节点之间同步完整的区块数据，每个节点都有自己的一份区块数据，单一或少部分的节点的区块数据自行或被篡改，都无法影响整个区块链的运行，依赖这种去中心化的架构，可以很容易做到数据防篡改。

风险

针对区块数据的安全风险，我们分析总结了以下攻击方式：

恶意信息攻击

在区块链中写入恶意信息，例如病毒特征码、政治敏感话题等。借助区块链数据不可删除的特性，信息被写入区块链后很难删除。若区块链中出现恶意信息，将会遭到杀毒软件、政治敏感等多方面的问题。

资源滥用攻击

随着时间的推移，区块数据可能会爆炸式增长（节点之间恶意频繁交互），

也可能会呈线性增长，这主要取决于此区块链应用的设计，依赖现有的计算机存储技术，区块数据若发生爆炸式增长，可能导致节点无法容纳又或者使区块链运转缓慢，从而使稳定运行的节点越来越少，节点越少，则越趋于中心化，引发区块链危机。

不过目前主流的区块链应用譬如 BTC、ETH 等，都完好的解决了此问题，比特币的解决方法为固定区块大小为 1M，防止区块过度膨胀，区块链大小呈线性增长，即使到 2029 年区块数据也只有 1T 左右，但是此解决方案并不优雅，限制区块大小的同时也给比特币带来了交易时间长的诟病，目前比特币的一笔交易需要确认数小时。

攻击场景距离：若链中没有设计相应的操作限制，攻击者可以通过发送大量的垃圾信息来堵塞整个区块链，使区块链中真正的信息迟迟得不到处理，又或者使区块链中的存储节点超负荷运行。

案例

2017 年 2 月份，以太坊的 Ropsten 测试链就遭到了一次恶意攻击，攻击者发动了千万级别的垃圾交易信息，直接阻塞的网络的正常运行。

此案例虽然发生在测试网络上，并没有使以太坊网络受到实质性的影响，但也给我们敲响了警钟，区块链的应用目前还处于萌芽阶段，主流的应用不存在此问题理所当然，但不代表新的区块链应用不会存在这类问题，这都是区块链开发者需要注意的。

2017 年在 EuskalHack 安全会议上，有安全研究者提出了基于区块链模式的 botnet 网络，利用区块链网络进行 C&C 的恶意指令发布的并且提供了 POC[17]。

3.1.2 签名与加密方式

简要

密码学是保证区块链的安全性和不可篡改性的关键，而且区块链技术大量依

赖了密码学的研究成果，为区块链的信息完整性、认证性和不可抵赖性提供了关键保障。

风险

加密技术作为一个区块链整体的支柱，其安全性显得尤为重要，例如前些年所流行的 MD5 和 sha1 摘要算法，目前已经证明安全性不足，现在已经不能被商用。

所以，公认的高强度加密算法在经过长时间的各方面实践与论证后，已被大家所认可，但不代表其不存在漏洞，不可被破解。

如比特币目前大量使用的是 sha256 算法，到目前为止，此算法还是安全的，虽然有人依然持有质疑，但是并没有任何直接的公开证据表明此算法存在漏洞。然而，比特币所使用的算法也并不是毫无瑕疵，至少目前引发了以下问题：

1. sha256 算法对应的 ASIC 矿机以及矿池的出现，打破了中本聪最初设计“一 CPU 一票”的理念，淘汰了普通 GPU 挖矿，全网的节点逐渐减少，逐渐趋于中心化。
2. 假名制，通过公共账本你可以查看任意账户的所有交易信息，这显然是和隐私保护背道而驰的，而且在日常的互联网生活中很难不在互联网中留下痕迹，例如：在论坛中发布交易信息，钱包地址就与论坛账户产生了对应关系。门罗币在此方面则优于比特币。

所以，在设计区块链应用的时候，务必要对加密方式慎重选择。对于目前主流的签名方式[11]有如下：

签名机制	原理	安全性	性能
聚合签名	基于 co-GDH 和双线性映射	在约束条件下，即仅在不同消息上的签名进行聚合行为才有效，聚合签名具有抵御攻击者伪造签名的能力	聚合签名的认证时间和签名数成线性关系，在特殊情 况下，当所有 n 个签名由同一个公钥 k 发布时，聚合验 证速度更快
群签名	基于不可否认签名	可靠性和完备性；不可伪造性；匿名性；可追溯性；	公钥长度、签名长度与群成员数成线性关系，但是新增成员需要重启整个系

		无关联性；无框架；不可伪造的追踪验证；抗联合攻击性	统，故性能相对较低
环签名	群签名的变形，拥有基于 RSA 和基于拉宾版本的两种环签名	攻击者即使拥有所有成员的私钥也无法找到谁是具体签名者，因为确定真正签名者的概率为 1/n(n 为整个环成员数)，A 无法从各种不可忽略的概率中产生消息 m 的环签名	签名过程需要一个模幂运算，对于每个非签名者加上一个或两个模乘运算，而验证过程需要每个环成员一个或两个模乘运算。由于其生成或验证环签名的开销,与常规签名加上为每个非签名者加上一或两次额外的乘法开销是相同的，故即使当环包含数百个成员时，该机制依然高效可行
盲签名	基于 RSA 或 DSA 算法	若签名者不是消息的发送方，则盲签名可以通过盲化将消息 m 隐藏起来，签名者无法得知消息的内容，从而保护消息的隐私	取决于密钥长度、签名长度和签名和验证时间，尽管其基于的算法理论存在差异，但总体上与 RSA 签名或 DSA 签名机制的开销量类似
代理签名	基于离散对数问题	由于离散对数问题存在的固有问题，使得代理人可以伪造原始签名进行安全攻击，以及发生替换公钥等安全问题	由于离散对数的运算问题，所以该机制在计算复杂度和通信开销等方面，均劣于基于椭圆曲线问题的签名机制
不可否认的交互式数字签名(IIS)	基于双线性映射群系统的椭圆曲线对	可以保障所有者的不可伪造性和交易者的不可否认性	利用线性群的指数次数和元素长度计算复杂度和通信/存储成本两方面说明方案性能
盲的可验证加密签名(BVES)	基于盲签名和可验证签名	通过设置安全定义的三个方面，分别验证满足假设，其具有抵御欺诈的能力，	分别从区块产生时间和通过公平合同签署协议的通信花费来评估签名和协议的性能

		以此证明方案的安全性	
类似 ETSI 下长期签名的新签名方案	基于 ETSI 长期签名方案	当签名方案发生妥协现象时，此方案可以避免密钥对的改变和 hard-fork	开销方面，在改变哈希算法时，区块大小的开销取决于新散列函数的输出长度和块中交易数(交易的哈希值之间的相互引用数量)
在区块链交易环境下基于聚合签名所提出的新签名方案	基于椭圆曲线离散对数问题和双线性映射	根据安全分析，攻击者的潜在伪造能力无法实现，安全性能和聚合签名基本相同	通过聚合签名时间、聚合验证时间和签名空间大小来进行评估

针对加密方式的安全风险，我们分析总结了以下攻击方式：

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，其中最典型的的方式是基于生日悖论的“生日攻击”。

生日悖论：如果一个房间里有 23 个或 23 个以上的人，那么至少有两个人的生日相同的概率要大于 50%。这就意味着在一个典型的标准小学班级(30 人)中，存在两人生日相同的可能性更高。对于 60 或者更多的人，这种概率要大于 99%。

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。

长度扩展攻击

此种攻击方式主要作用于散列函数中，准确的说是基于 Merkle－Damgård 构造的摘要算法。其原理是通过算法弱点，在已知密文 hash 和密文长度的情况下，推导出密文与另一消息拼接后计算出来的 hash。

后门攻击

此种攻击方式作用于所有开源加密算法库中，RSA 算法是区块链中身份验证的基石，RSA 算法本身是没问题的，但是在实际情况中，人们可能更多的是选择别人已经写好的“轮子”直接拿来用，而不是自己再去实现一套加密函数。

这就带来了一个问题，在别人已经写好的“轮子”中，可能被安插后门，比较典型的案例是:NSA 在 RSA 算法中安插后门，使得攻击者能直接通过公钥算出私钥。

量子攻击[3]

此种攻击方式作用于大部分密码学算法。目前所有的加密算法以及摘要算法，其安全强度取决于它被穷举的时间复杂度，这使得依赖现有的计算机的计算能力，针对比较强的加密算法要对它进行暴力破解是非常难的，但是量子计算机拥有传统计算机无可比拟的算力，使得时间复杂度大大降低，于是，其安全强度便可能被瓦解，此问题是比特币社区中一直在讨论的问题。

案例

目前暂无实际攻击曝光，但在某些层面可能存在致命安全隐患

3.2 网络层

3.2.1 P2P 网络

简要

区块链的信息传播主要依赖于其点对点传输的特性，采用 P2P[4]式的网络架构，寻找适宜的节点进行信息传播，当建立一个或多个连接后，节点将一条包含自身 IP 地址消息发送给其相邻节点。相邻节点再将此消息依次转发给它们各自的相邻节点，从而保证节点信息被多个节点所接收、保证连接更稳定。

风险

P2P 网络依赖附近的节点来进行信息传输必须要互相暴露对方的 IP，若网络中存在一个攻击者，就很容易给其他节点带来安全威胁，中心化的网络不会太过担心此问题的原因是组织的网络中心的安全性都是极高的，即使暴露也不会有太大问题。

而去中心化的公链网络节点可能是普通家庭 PC，可能是云服务器等等，其安全性必然是参差不齐的，其中必有安全性较差的节点，对其进行攻击将直接威胁节点的安全。

针对 P2P 网络的安全风险，我们分析总结了以下攻击方式：

日食攻击

日食攻击[5]是其他节点实施的网络层面攻击，其攻击手段是囤积和霸占受害者的点对点连接间隙，将该节点保留在一个隔离的网络中。这种类型的攻击旨在阻止最新的区块链信息进入到日食节点，从而隔离节点。

窃听攻击

攻击者可以使用这种攻击来让区块链中的用户标识与 ip 关联起来，在某些情

况下甚至可以追溯到用户的家庭地址。

以比特币为例，当你在比特币网络上执行交易时，你的比特币客户端通常通过连接到一组八台服务器来加入网络，这个初始连接集合就是你的入口节点，每个用户都会获得一组唯一的入口节点。

当你的钱包发送比特币完成购买时，入口节点将交易转交给比特币网络的其余部分，研究人员发现，识别一组一口节点意味着识别一个特定的比特币客户端，以此来推导出某个用户。

那么，攻击者要做的是与比特币服务器建立多个连接，连接后，攻击者必须听取客户端与服务端的初始连接，这会泄露客户端的 ip 地址。

随着交易流经网络，它们将会与客户端的入口节点相关联，如果匹配，那么攻击者就知道这是来自一个特定客户端的交易。

BGP 劫持攻击

边界网关协议(BGP)是因特网的关键组成部分，用于确定路由路径。BGP 劫持，即利用 BGP 操纵因特网路由路径，最近几年中已经变得越来越频繁。 无论是网络犯罪分子还是政府,都可以利用这种技术来达到自己的目的，如误导和拦截流量等，目前在区块链网络中节点的流量一但被接管又能对整个网络造成巨大的影响，如破坏共识机制，交易等各种信息。而对于 BGP 劫持攻击中，目前有安全研究者已经证明该攻击的概念可行性，从 2015 年 11 月 5 日至 2016 年 11 月 15 日通过对节点网络的分析统计目前大多数比特币节点都托管在少数特定的几个互联网服务提供商(ISPs)，而 60%的比特币连接都是在这几个 ISP。所以这几个 ISP 可以看到 60%的比特币流量，所以也能够做到对目前比特币网络的流量控制权，研究者通过劫持的场景验证了至少如下两个攻击概念是可行的，同时给出了验证的代码[8]。

分割攻击

攻击者可以利用 BGP 劫持来讲区块链网络划分成两个或多个不相交的网络，此时的区块链会分叉为两条或多条并行链。攻击停止后，区块链会重新统一为一条链，以最长的链为主链，其他的链将被废弃，其上的交易、奖励等全部无效。

攻击场景举例：

1) 首先，攻击者发动 BGP 劫持，将网络分割为两部分，一个大网络、一个小网络。
2) 在小网络中，攻击者发布交易卖出自己全部的加密货币，并兑换为法币。
3) 经过小网络的“全网确认”，这笔交易生效，攻击者获得等值的法币。
4) 攻击者释放 BGP 劫持，大网络与小网络互通，小网络上的一切交易被大网络否定，攻击者的加密货币全部回归到账户，而交易得来的法币，依然还在攻击者手中，完成获利。

延迟攻击

攻击者可以利用 BGP 劫持来延迟目标的区块更新，而且不被发现。因为它是基于中间人修改目标请求区块的数据来做到的：在目标请求获取最新区块的时候，将它的这一请求修改为获取旧区块的请求，使得目标获得较旧的块。

攻击场景举例：

1) 攻击者修改矿工获取最新块请求
2) 矿工无法获取到新区块
3) 矿工损失算力以及奖励机会

节点客户端漏洞

攻击者在内网或者外网利用各种手段譬如漏洞扫描，0day 漏洞利用等技术，对节点客户端进行攻击，此类攻击主要针对客户端自身软件可能存在安全漏洞进行利用，获取节点的控制权限。

拒绝服务攻击

通过大流量，或者漏洞的方式攻击 P2P 网络中的节点，使网络中部分节点网络瘫痪，节点瘫痪意味着链中总算力受损，使得其更容易遭受 51%攻击，而目前进行拒绝服务攻击成本也较低，大量的攻击工具平台能轻易在黑市购买用于攻击。

案例

2018 年 3 月 22 日，闪电网络[10]节点遭受 DDOS 攻击，导致大约 200 个节点离线，从大约 1,050 个节点降到了 870 个。

3.2.2 广播机制

简要

在区块链中，节点是与节点互相连接的。当某节点接入到区块链网络后，单个节点会与其他节点建立连接。此时该节点就具备了广播信息的资格，在将信息传播给其他节点后，其他节点会验证此信息是否为有效的信息，确认无误后再继续向其他节点广播。

风险

针对广播机制的安全风险，我们分析总结了以下攻击方式：

双重支出攻击

又称双花问题[9]，指的是一个代币花费在多笔交易中的攻击，它的实现方法主要有以下几种。

1. 种族攻击：在面对 0 确认的交易便立刻进行付款的商家可能会遭遇此攻击。欺诈者直接向商家发送支付给商家的交易，并发送冲突的交易，将代币投入自己到网络的其余部分。第二个冲突的交易很可能会被开采出来，并被区块链节点认为是真的，于是付款交易作废。

2. 芬尼攻击：当接受 0 确认的付款时可能会遭遇此攻击。假设攻击者偶尔产生数据块。在他生成的每个区块中，他包括从他控制的地址 A 到地址 B 的转移。为了欺骗你，当他生成一个块时，他不会广播它。相反，他打开您的商店网页，并使用地址 A 向您的地址 C 付款。您可能会花费几

秒钟的时间寻找双重花费，然后转让商品。接着他广播他之前的区块，他的交易将优先于你的交易，于是付款交易作废。

3. Vector76 攻击：也被称为单一确认攻击，是种族攻击和芬尼攻击的组合，因此即使有一次确认的交易仍然可以逆转。对于种族攻击，相同的保护措施显然降低了发生这种情况的风险。 值得注意的是，成功的攻击会使攻击者花费一个块，他们需要通过不传播它来“牺牲”一个块，而是仅将其转让给被攻击的节点。

4. 替代历史攻击：即使商家等待一些确认，这种攻击也有机会成功，但风险较高。攻击者向商家提交支付的交易，同时私下挖掘其中包含欺诈性双重支出交易的分支。等待 n 次确认后，商家发送产品。如果攻击者此时碰巧找到 n 个以上的区块，他就会释放他的分支并重新获得他的硬币。

5. 51%攻击：如果攻击者控制全网算力的一半以上，则前面提到的替代历史攻击有 100％的概率成功。由于攻击者可以比网络的其他部分更快地生成块，所以他可以坚持自己的私有分支，直到它比诚实节点网络建立的分支更长，它将代替主链。

交易延展性攻击

延展性攻击者侦听 P2P 网络中的交易，利用交易签名算法的特征修改原交易中的 input 签名，生成拥有一样 input 和 output 的新交易，然后广播到网络中形成双花，这样原来的交易就可能有一定的概率不能被确认，在虚拟货币交易的情况下，它可以被用来进行二次存款或双重提现。

案例

1. 2014 年 8 月，在线黑市 Silk Road 2 遭遇交易延展性攻击，部分比特币被盗，损失约 260 万美元
2. 2013 年 11 月，GHash.io 矿池对赌博网站 BetCoin Dice 进行多次付款

欺诈，实施双重支出攻击

3.2.3 验证机制

简要

区块链的运行为了维持其数据的有效性与真实性，必须要有相应的验证机制来限制节点必须将真实信息写入区块中。

风险

针对验证机制的安全风险，我们分析总结了以下攻击方式：

验证绕过

验证机制的代码是区块链应用的核心之一，一旦出现问题将直接导致区块链的数据混乱，而且核心代码的修改与升级都涉及到区块链分叉的问题，所以验证机制的严谨性就显得尤为重要。

必须要结合验证机制代码的语言特性来进行大量的白盒审计或是模糊测试，来保证验证机制的不可绕过。

案例

比特币无限造币漏洞：2010 年 8 月 15 日，有人在比特币区块链的第 74638 块上发现了一条让人惊愕的交易，这笔交易里竟然出现了 184,467,440,737.09551616 个比特币，其中各有 922 亿个比特币被发送到两个比特币地址。

这次攻击的根本原因则是比特币的验证机制中存在大整数溢出漏洞，由于大整数溢出为负数，网络各个节点对黑客的交易均验证通过，导致了比特币区块链中凭空出现了大量比特币。

3.3 激励层

简要

激励层目的是提供一定的激励措施鼓励节点参与区块链的安全验证工作。区块链的安全性依赖于众多节点的参与。例如比特币区块链的安全性是基于众多节点参与工作量证明带来的巨大的计算量，使得攻击者无法提供更高的计算量。节点的验证过程通常需要耗费的计算资源和电能。为了鼓励节点参与，区块链通常会采用虚拟货币的形式奖励参与者，目前比特币、莱特币、以太币都是这种机制的产物。以比特币为例，奖励机制包括了两种，第一种是新区快产生后系统生成的比特币，第二种是每笔交易会扣除万分之一比特币作为手续费。在前期，每一个区块的创建者都会获得一定数量的比特币，创世区块提供 50 个比特币，之后随着系统中比特币数量的持续增加，这种模式提供的比特币数量会持续减半。当比特币总量达到 2100 万时，新产生的区块将不再生成比特币。这时主要依靠第二种手续费作为奖励机制。

风险

奖励不符合市场预期

区块链项目需要顺应市场自动适当调整奖励，而不是一味降低。若在区块链项目奖励机制中，当节点们的工作成本小于和接近于收益的时候，他们往往会选择不再为这个区块链工作，从而很容易导致中心化问题。

攻击场景：

1. 比特币区块链上的被全部开采完毕
2. 矿工奖励骤降，大量矿工下链
3. 攻击者以较低成本发动 51%攻击

案例

目前暂无实际攻击曝光，但在某些层面可能存在致命安全隐患

3.4 共识层

3.4.1 共识机制

简要

共识机制赋予了区块链技术灵魂，使它与其他的 P2P 技术差异化。

目前常用的共识机制有 PoW（工作量证明机制）、PoS（权益证明机制）、DPoS（股份授权证明机制），然而他们都不是完美的，都有各自的优点与缺点。对于各种共识机制的对比[11]我们列出如下列表进行说明：

名称	技术优势	技术不足
PoW	算法简单，易于实现 节点间无需交换额外的信息即可达成共识 破坏系统需要投入极大的成本	算力的消耗与浪费 区块确认时间难以缩短 新的区块链须找到一种不同的散列算法，否则会面临比特币的算力攻击 容易产生分叉，需要等待多个确认
PoS	对节点性能要求低 达成共识时间短(可实现毫秒级)	同 PoW 一样仍需要挖矿 PoS 会使得“富者更富” 没有最终一致性
DPoS	不需要挖矿产生区块 大幅缩小参与验证和记账节点的数量，属于弱中心化，效率提高 可达到秒级共识验证	整个共识机制依赖于代币，而很多商业应用不需要代币 牺牲了去中心化的概念，不适合公有链

投注共识	引入惩罚机制 有效抵御“51%”攻击 理论上，该共识模型中的出块时间甚至可比网络传播时间还要块	由于该共识过程是在某个高度上对区块状态的决策是独立于其他所有高度的，这将会导致一定程度的低效
PoI	提供了一种分布更为均匀的挖矿方法 解决比特币生态资源浪费与挖矿设备竞争 看重交易量、活跃度，以及和谁做交易	仅适用于 NEM 用户 对于 NEM 用户的重要性：取决于他拥有多少数量的货币和他的钱包交互数量
瑞波共识	保证任何时候都不会产生硬分叉 交易能被实时的验证	新加入节点要取得与其他节点的共识所需时间较长
PBFT	系统运转可以脱离币的存在，安全性与稳定性由业务相关方保证 共识的时延大约在 2~5 秒钟，基本达到商用实时处理的要求 共识效率高，可满足高频交易量的需求	当系统仅剩 33%节点运行时，系统会停止运行 当有 1/3 或以上记账人联合作恶，且其他所有的记账人被恰好分割为两个网络孤岛时，恶意记账人可以使系统出现分叉，但是会留下密码学证据
DBFT	专业化的记账人 可容忍任何类型错误 记账由多人协同完成 每一个区块都有最终性，不会分叉 算法的可靠性有严格的数字	PBFT 机制的缺陷依然存在

	证明	
Paxos 算法	性能高，资源消耗低 所有节点一般有线下准入机制	不允许有作恶节点 不具备容错性
Pool 验证池	不需要代币也可工作。 在成熟分布式一致性算法(Paxos、Raft)基础上，实现秒级共识	去中心化程度不如比特币，适合多方参与的多中心商业模式

风险

针对共识机制的安全风险，我们分析总结了以下攻击方式以及适用范围：

攻击方法	PoW	PoS	DPoS
短距离攻击（如贿赂攻击）	–	+	–
长距离攻击	–	+	+
币龄累计攻击	–	+	+
预计算攻击	–	+	–
女巫攻击	+	+	+

短距离攻击

此类攻击比较典型的是“贿赂攻击”，此攻击主要影响 PoS 共识机制，贿赂攻击流程如下：

1) 攻击者购买某个商品或服务。
2) 商户开始等待网络确认这笔交易。
3) 此时，攻击者开始在网络中首次宣称，对目前相对最长的不包含这次交

易的主链进行奖励。

4) 当主链足够长时，攻击者开始放出更大的奖励，奖励那些在包含此次交易的链条中挖矿的矿工。
5) 六次确认达成后，放弃奖励。
6) 货物到手，同时放弃攻击者选中的链条。

因此，只要此次贿赂攻击的成本小于货物或者服务费用，此次攻击就是成功的。相比之下，PoW 机制中贿赂攻击就需要贿赂大多数矿工，因此成本极高，难以实现。

长距离攻击

此类攻击比较典型的是“51%”攻击。在 PoS 中，产生每个 Block 的速度相对 PoW 快了很多。因此，少数不怀好意的节点会想着把整个区块链共识账本全部重写。这在 PoW 中是经典的 51% 问题，即：当某一个节点控制了 51% 及以上算力，就有能力篡改账本，但达到 51% 算力是件极其困难的事情。而在 PoS 中缺乏对算力的约束，那么就存在潜在可能篡改账本。

币龄累计攻击

在最早的 Peercoin 版本中，挖矿难度不仅与当前账户余额有关，也与每个币的持币时间挂钩。这就导致，部分节点在等待足够长时间后，就有能力利用 Age 的增加来控制整个网络，产生非常显著的影响。

预计算攻击

当 PoS 中的某一节点占有了一定量的算力后，PoS 中占有特定算力的节点，就有能力通过控制 Hprev 来使自己所在算力范围有能力去计算 Hnext。

女巫攻击

又称 Sybil 攻击，在 Sybil 攻击中，攻击者通过创建大量的假名标识来破坏对等网络的信誉系统，使用它们获得不成比例的大的影响。对等网络上的实体是能够访问本地资源的一块软件。实体通过呈现身份在网络上通告自身。 多于一个标识可以对应于单个实体。

换句话说，身份到实体的映射是多对一的。对等网络中的实体为了冗余，资源共享，可靠性和完整性而使用多个标识。

在对等网络中，身份用作抽象，使得远程实体可以知道身份而不必知道身份与本地实体的对应关系。

默认情况下，通常假定每个不同的标识对应于不同的本地实体。实际上，许多身份可以对应于相同的本地实体。

对手可以向对等网络呈现多个身份，以便出现并充当多个不同的节点。因此，对手可能能够获得对网络的不成比例的控制水平，例如通过影响投票结果。

案例

1. 2016年8月份，基于以太坊的数字货币Krypton遭受来自一个名为“51% Crew”的组织通过租用Nicehash的算力，进行51%攻击，导致该区块链损失约21,465 KR的代币。

3.5 合约层

3.5.1 合约虚拟机

简要

随着区块链技术的不断升级，区块链已经具备在链上繁衍出多种应用的功能，而实现这种功能的基础就是合约虚拟机（用于运行各种智能合约的平台），此技术的出现极大的提高了区块链的可扩展性，是区块链2.0的重要标志。

合约虚拟机的出现为合约代码提供了沙盒式的执行环境。

风险

合约虚拟机运行在区块链的各个节点上，接受并部署来自节点的智能合约代码，若虚拟机存在漏洞或相关限制机制不完善，很可能运行来自攻击者的恶意的

智能合约。

针对合约虚拟机的安全风险，我们分析总结了以下攻击方式：

逃逸漏洞

虚拟机在运行字节码的时候会提供一个沙盒环境，一般用户只能在沙盒的限制中执行相应的代码，此类型漏洞会使得攻击者退出沙盒环境，执行其他本不能执行的代码。

逻辑漏洞

虚拟机在发现数据或代码不符合规范时，可能会对数据做一些“容错处理”，这就导致可能会出现一些逻辑问题，最典型的是“以太坊短地址攻击”。

堆栈溢出漏洞

攻击者可通过编写恶意代码让虚拟机去解析执行，最终导致栈的深度超过虚拟机允许的最大深度，或不断占用系统内存导致内存溢出。

此种攻击可引发多种威胁，最严重的是造成命令执行漏洞。

资源滥用漏洞

攻击者可以在虚拟机上部署一份恶意代码，消耗系统的网络资源、存储资源、计算资源、内存资源。

所以在虚拟机中必须要有相应的限制机制来防止系统的资源被滥用。

在以太坊中采用的是 gas 机制，攻击者想要在以太坊虚拟机上做更多操作，需要付出经济代价。

案例

以太坊短地址漏洞：由于 EVM 并没有严格校验地址的位数，并且还擅自自动补充消失的位数，使得合约多发送很多代币出来。

3.5.2 智能合约

简要

智能合约是一种旨在以信息化方式传播、验证或执行合同的计算机协议。智能合约允许在没有第三方的情况下进行可信交易。这些交易可追踪且不可逆转。

风险

智能合约本质上是一份代码程序，难免会有因为考虑不周的导致出现漏洞的情况，所以在发布一份智能合约之前，进行大量的模糊测试与白盒审计是必不可少的。

在将大量资金放入合约之前，合约应当进行大量的长时间的测试。

至少应该：

- 拥有 100%测试覆盖率的完整测试套件（或接近它）
- 在自己的 testnet 上部署
- 在公共测试网上部署大量测试和错误奖励
- 彻底的测试应该允许各种玩家与合约进行大规模互动
- 在主网上部署 beta 版以限制风险总额

针对智能合约的安全风险，我们分析总结了以下攻击方式：

可重入攻击

当智能合约 A 调用智能合约 B 时,智能合约 B 可以在被调用的函数中写入“使智能合约 A 调用智能合约 B”的代码，这样就造成了可重入攻击。

比较典型的一个案例：

1. 智能合约 A 向智能合约 B 发起提现请求
2. 智能合约 B 向智能合约 A 转账，并调用智能合约 A 的回调函数

3. 智能合约 A 的回调函数中被写入的操作是“智能合约 A 向智能合约 B 发起提现请求”。
4. 又回到了步骤 1，一直循环步骤 1234 直到不满足循环条件。
5. 提现结束

调用深度攻击

在合约虚拟机中，会对智能合约的互相调用的深度定一个阈值，超过这个深度调用就会失败，例如在以太坊 EVM 中，调用深度被限制为 1024。

调用深度攻击可以让合约调用失败，即使这个调用在逻辑上不存在任何问题，但是在虚拟机层面以及不被允许了，因为调用深度达到了虚拟机中的阈值，超过阈值不再往下执行。

攻击者可以通过控制调用深度，来使某些关键操作无法执行，例如：转账、余额清零等。

交易顺序依赖攻击

智能合约的执行会随着当前交易处理顺序的不同而产生不同的结果。

场景：攻击者发布一个解题合约，在合约中写给出丰厚的解题奖励。等有人提交了正确答案后，此时的答案还需要经过其他节点的确认，合约才会执行奖励操作。此时攻击者可以提交一个将奖励额度调低的交易，这笔交易肯定是在奖励操作的后面，理论上不会造成给答题人带来损失。

但是，在区块链项目中，交易顺序并不是一成不变的，例如在以太坊中，交易顺序就会随着交易发布者的 gas（交易费）的高低来决定先确认哪笔交易。

此时若攻击者更改奖励额度的交易给的交易费比较高，验证节点会先执行这笔交易，最终会导致答题人最后得到的奖励额度是调低的额度。而攻击者以一个较低的成本就买到了正确答案。

时间戳依赖攻击

如果智能合约在敏感操作中依赖时间戳，可能会导致执行结果被预测。

场景：若发布一个抽奖合约，抽奖结果由当前区块的时间戳和其他因素组合

计算而来，攻击者可以通过提前尝试不同的时间戳来计算这个抽奖结果，从而导致结果被预测。

误操作异常攻击

当合约 A 调用另外一个合约 B 的操作的时候，合约 B 操作的执行可能会因为种种原因导致执行失败，从而退回到未执行前的状态，此时合约 A 若不检查合约 B 执行的结果继续往下执行，会导致很多问题。

场景：合约 A 调用合约 B 的提现操作后并在合约 A 的余额中增加与提现额度一样的数值。此时若没检查合约 B 的执行提现操作的返回值，就可能会导致合约 B 中的余额并没减少，而合约 A 中的余额却已经增加了。

整数溢出攻击

在常见的程序语言中，对整数类型的变量一般都会有最大值和最小值。智能合约本质上也是一份程序代码，合约中的整数也会有相应的最大值和最小值。一旦变量所存储的值超过了最大值就会发生整数上溢错误，导致变量最后存储的值为 0，反之则是整数下溢错误，变量最后存储的值为变量最大值。当然，溢出的情况并不限于以上整数上溢或者整数下溢，还可能会在计算、转换等过程中发生溢出。

场景：假设某个智能合约中的余额为无符号整数类型，此类型的范围为 0~65535，当攻击者通过某种方法使余额小于 0 时，它在智能合约中的余额将下溢为 65535。使余额大于 65535 时，它在智能合约中的余额将上溢为 0。

基于以太坊的多个 ERC20 智能合约就遭受过整形溢出漏洞的影响，如图：该漏洞就是一个典型的整形溢出导致，绕过业务逻辑，能够刷出大量的 token。

```
function batchTransfer(address[] _receivers, uint256 _value) public whenNotPaused returns (bool) {
    uint cnt = _receivers.length;
    uint256 amount = uint256(cnt) * _value;
    require(cnt > 0 && cnt <= 20);
    require(_value > 0 && balances[msg.sender] >= amount);

    balances[msg.sender] = balances[msg.sender].sub(amount);
    for (uint i = 0; i < cnt; i++) {
        balances[_receivers[i]] = balances[_receivers[i]].add(_value);
        Transfer(msg.sender, _receivers[i], _value);
    }
    return true;
  }
}
```

ERC20 相关的智能合约中就曾曝出过 batchTransfer（CVE-2018–10299），SmartMesh 合约中 transferProxy 函数，proxyTransfer 函数（CVE-2018-10376），UET 合约的 transferFrom 函数(CVE-2018-10468)，都出现过整形溢出的问题。

案例

1. 2016 年 6 月发生了一起史上最大的智能合约事件，它就是著名的 The DAO 攻击事件。导致价值 6000 万美元的以太币被盗，迫使以太币被硬分叉为 ETH 和 ETC。
2. 2017 年 7 月，以太坊发生了 Parity 多重签名钱包被盗事件，黑客从从三个高安全的多重签名合约中窃取到超过 15 万 ETH（约 3000 万美元）。
3. 2018 年 4 月，BeautyChain（BEC）智能合约中出现了一个灾难性的漏洞（整形溢出漏洞），导致损失约 10 亿美元
4. 2018 年 4 月， SMT 的智能合约漏洞（整形溢出）。

3.6 业务层

3.6.1 交易平台

3.6.1.1 网络带宽

简要

目前在网络中有许多以区块链作为底层技术的加密货币的交易平台，用户在通过交易平台来购买和出售加密货币，对于主流的交易平台，每天都有大量的用户在平台上进行交易，其网络带宽对于交易平台来说至关重要。

风险

针对交易平台的安全风险主要为拒绝服务攻击：

拒绝服务攻击

由于交易平台对于网络带宽的存在高需求，所以一旦发生 DDoS 攻击，对于平台和整个行业来说是非常严重的。若交易平台被 DDoS 攻击，不但交易平台蒙受损失，区块链货币的交易量也将大大减少，间接影响区块链货币的涨跌，在我们统计的安全事件中，以及调查的相关案例显示目前只要是交易平台上线都遭受到 DDOS 攻击过。

场景：攻击者首先通过 DDOS 使平台无法访问，此时通常一定会有相关的新闻资讯报道这次事件。然而普通大众并分不清拒绝访问攻击与入侵的区别，在自己所使用的交易平台被“攻击”后，为了自己的资金安全通常会选择转向别的平台，导致此平台资金、用户流失。

案例

1. 2017 年 5 月 12 日，Poloniex 交易平台遭受了严重的 DDoS 攻击，BTC/USDT 的交易价格一度困于 1761 美元，绝大多数用户都无法执行订单或是提取资金。
2. 2017 年 12 月 12 日，比特币交易平台 Bitfinex 遭受严重 DDoS 攻击，API 瘫痪。消息传出后，比特币下跌 1.1%，报 16968 美元。

3.6.1.2 账户体系

简要

账户是交易平台必须具备的基础配置，账户是开户的凭证，包含账号和密码，意味着你成为他们的用户，平台必须根据相关条约对你账号的隐私、安全负责。

风险

交易平台为保证用户的资金安全需要建立高强度的账户安全体系。具体需要做到如下几点：

1. 防撞库，人机识别
2. 进行敏感操作的时候启用多因素认证

3. 逻辑缜密，务必要杜绝“密码找回漏洞”、“登陆绕过”、“越权访问/调用”等漏洞
4. 防暴力破解，对登陆频率进行限制
5. 防 cookie 泄露，开启 httponly，杜绝 XSS 漏洞
6. 防跨站请求伪造，提交动作尽量使用 POST 并且增加 token，杜绝 CSRF 漏洞
7. 若使用 SSO、oauth 等登陆方式，务必严格遵循协议标准实现
8. 账号风控

针对交易平台账户体系的安全风险，我们分析总结了以下攻击方式：

撞库攻击

由于目前的网民普遍安全意识不足，经常会使用通用的用户名和密码，在不同的网站上使用同样的账号和口令登陆。

导致攻击者通过手机互联网上已公开或还未公开的用户名、邮箱、密码等信息来在要攻击的网站上通过程序批量尝试。

场景：攻击者通过网络钓鱼或者收集网络上已公开的与区块链相关网站的用户数据（包括用户名、密码等）在目标交易平台上使用程序自动化逐个尝试，导致账户安全受到极大威胁。

穷举攻击

若网站不对登陆接口做请求限制或者风控，会导致攻击者可以无限发送请求逐个测试可能的值来暴力破解某些关键信息。

场景：

1. 在短信验证中，若不对短信验证码的有效期做限制或者验证接口做限制，很容易短信验证码被破解。
2. 若登陆接口未做请求限制，攻击者可以通过大量的密码字典来暴力破解某个账户的密码。又或者说，攻击者可以通过大量的用户名字典来暴力破解密码为某个值的用户，比如密码为 123456 的用户。

单点登陆漏洞

在账户体系中此类漏洞比较隐蔽，攻击者可以通过 CSRF、XSS 等手段来窃取用户登陆的 ticket，从而导致用户账号被窃取。

主要有以下攻击面：

- 未使用 HTTPS 导致中间人劫持
- Jsonp 接口泄露 ticket
- CSRF 漏洞窃取 ticket
- XSS 漏洞窃取 ticket

oAuth 协议漏洞

oAuth 协议到 2.0 实际上已经足够安全，但是只是协议安全，并不代表它的最终实现就没有问题，在安全意识不足的情况下很容易导致出现一些潜在威胁，导致攻击者可以通过 CSRF 等手段来越权登陆他人账号。

主要有以下攻击面：

- 利用 CSRF 漏洞绑定劫持
- 利用 redirect_uri 授权劫持
- 利用 scope 权限控制不当越权访问

案例

2017 年 10 月 2 日，OKCoin 旗下交易所出现大量账户被盗情况，不完全统计损失金额在一千余万人民币左右，用户怀疑平台已被攻击，或有已被关闭平台的交易所员工向黑客泄漏了平台用户的账户信息，黑客通过用户信息破解账户密码登录平台，然后在平台上完成数字资产转移。

3.6.1.3 支付体系

简要

交易平台内充值、提现都涉及到了支付，所以完整的支付体系也是交易平台必备的基础配置。

风险

针对交易平台支付体系的安全风险，我们分析总结了以下攻击方式：

支付漏洞

凡是涉及到支付，则就有可能出现支付漏洞，且支付漏洞直接涉及到资金的安全问题，无论对平台或是用户来说都是高风险，必须要谨慎对待。以下总结了支付体系中常见的问题：

1. 修改支付价格问题：在支付时未对支付价格做后端验证，导致可以将价格调低甚至设为负数来通过交易获得收入。
2. 修改购买数量问题：在支付的过程中，数量也同时决定着价格，比如：1 个数量商品对应的是 100，2 个数据就是 200，那么当你修改这个值数量值为负数时，那么其金额也会变为负数，最后就会导致支付问题的产生。
3. 最大值支付问题：通过购买大量商品使得最后的支付数额非常大，后端可能存在大整数溢出漏洞，当数值超过了某个阈值后，得到的结果会为 0 或者负数。
4. 越权支付问题：后端缺少验证，导致可通过改包修改当前用户 ID 使用他人余额进行支付。

案例

目前暂无实际攻击曝光，但在某些层面可能存在致命安全隐患

3.6.1.4 业务逻辑

简要

业务逻辑即交易平台的业务流程或用户操作流程，还包含交易平台的交易策略和规范。

风险

针对交易平台业务逻辑的安全风险，我们分析总结了以下攻击方式：

逻辑漏洞

业务逻辑必须严谨，必须要对每段业务逻辑代码进行大量的模糊测试与代码审计，因为此类漏洞很难用传统的方式发现，只能借助于人的逻辑思维去思考其中可能出现的问题。目前常见的业务逻辑漏洞有如下几种：

- 越权漏洞
- 验证码漏洞
- 条件竞争漏洞
- 认证漏洞

案例

目前暂无实际攻击曝光，但在某些层面可能存在致命安全隐患

3.6.2 首次代币发行（ICO）

简要

ICO 是类似于 IPO 的一种区块链项目融资方式，用于项目的起步资金，与 IPO 不同的是：ICO 是一种以币换币的融资行为，一般以比特币或以太坊换取该项目代币。

风险

针对目前 ICO 的业务形态，已经发生了各种针对 ICO 业务的特定攻击场景如下：

篡改攻击

ICO 在募集资金的时候，一般会在项目官网上挂出收款地址，然后投资人会陆续往此地址转账以换取相应代币。

攻击场景：黑客通过域名劫持、web 漏洞、或社会工程学等等之类的攻击手段来篡改项目官网上的收款地址，此之后项目募集到的资金便落到了黑客的手中。

钓鱼攻击

攻击者利用社会工程学等手段来冒充官方，使用户向攻击者的钱包地址中转账。

攻击场景：

1. 利用近似域名+高度仿冒网站欺骗投资者
2. 利用电子邮件散步虚假信息，如 ICO 项目的收款地址更改通知等
3. 在社交软件、媒体上散步钓鱼信息来欺诈投资者

案例

2017 年 7 月，CoinDash 项目 ICO 收款地址遭到黑客篡改，价值约 1000 万美元的 eth 流入黑客钱包。

3.6.3 矿工

3.6.3.1 矿机系统

简要

普通的家用 PC、服务器等，并不是挖矿最合适的设备。一些厂商为了减少挖矿成本以及提高挖矿效率，根据币种的算法专门研发出了相应的挖矿设备。并在上面搭建相应的访问来提供远程访问以及控制，这种专门用来进行挖矿的设备即被称为矿机。

风险

设备厂商们的安全防护意识是参差不齐的，而且由于其闭源的特性，其代码的安全性无法被大众检查，一旦出现安全问题，结果就是致命的。

而且设备厂商是否会在设备中穿插后门进行远程控制，亦或是偷偷窃取挖矿产出，这些都还有待商榷。

针对矿机系统的安全风险，我们分析总结了以下攻击方式：

0day 漏洞攻击

矿机系统大多都是属于通用系统，很少会定制开发。一般是厂家售卖矿机时自带的，多个厂商肯能会使用同一套系统，只是贴牌配置不一样的硬件。

没有绝对安全的系统，矿机也不例外，一旦某个矿机系统被发现存在 0day 漏洞[15]，那系统的安全壁垒将瞬间被打破，攻击者可以利用漏洞拿到修改权限后进行奖励接收地址篡改然后劫持用户的奖励。

所以有必要对矿机进行访问控制以及网络隔离，以及相应的防护来抵御 0day 漏洞攻击。

渗透攻击

目前已经有组织对矿机进行持续性的渗透攻击，利用漏洞组合拳，最终获取到系统的篡改控制权限威胁矿机的系统安全，该攻击方式不限制于某一特定漏洞，最终以拿到系统权限为目的。

弱口令攻击

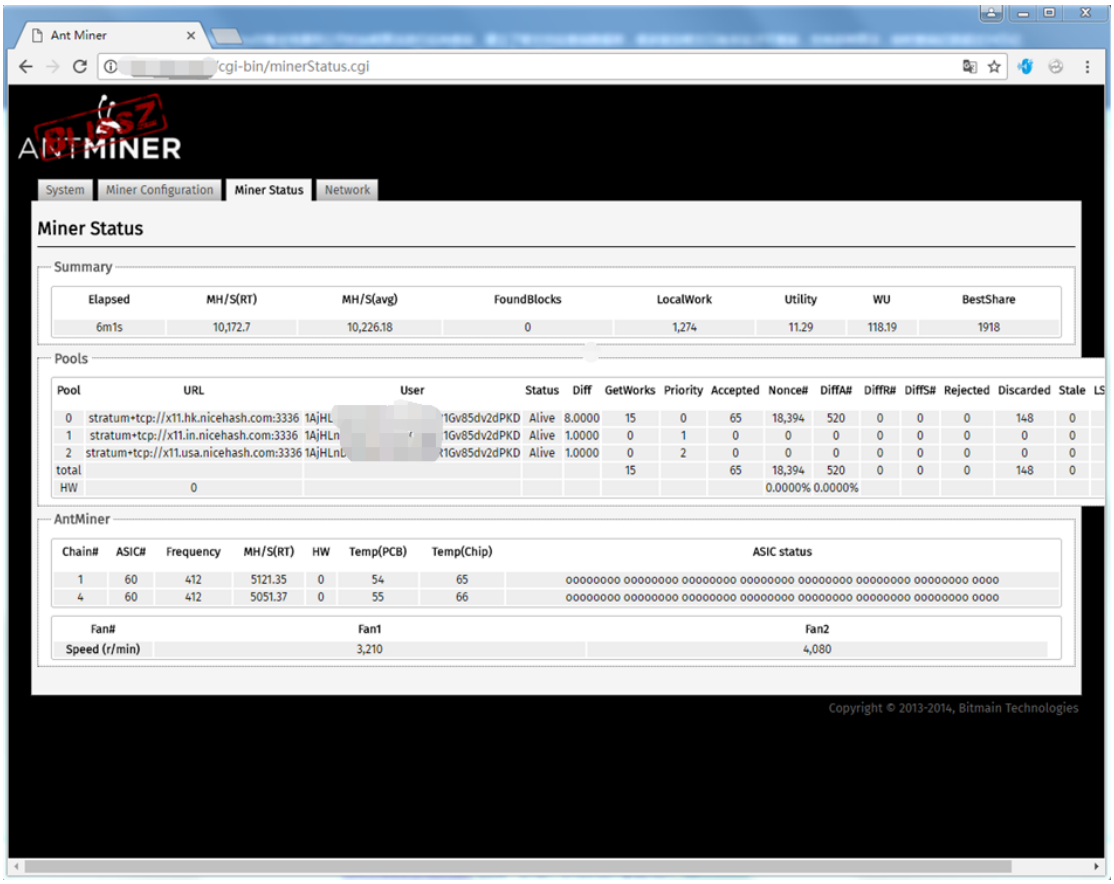
目前市面的矿机系统都是以 B/S 架构，在访问矿机系统一般是通过 web 或者是别的途径，若是在矿机上使用弱密码，则会极易遭到入侵。

奖励接收地址篡改

在挖矿主机系统被攻陷后，可能利用各种漏洞，最终黑客目的都是为了获取相关利益，而最直接的就是通过修改奖励的接受地址来使受害者的收获全部被黑客获取。

案例

1. 2017 年 4 月份，比特大陆旗下蚂蚁矿机被指存在后门，可导致矿机被远程关闭。若此攻击发生，将导致比特币区块链中损失大量算力。
2. 以下某挖矿系统存在弱口令，可导致比特币接受地址被篡改。



3.6.3.2 矿池

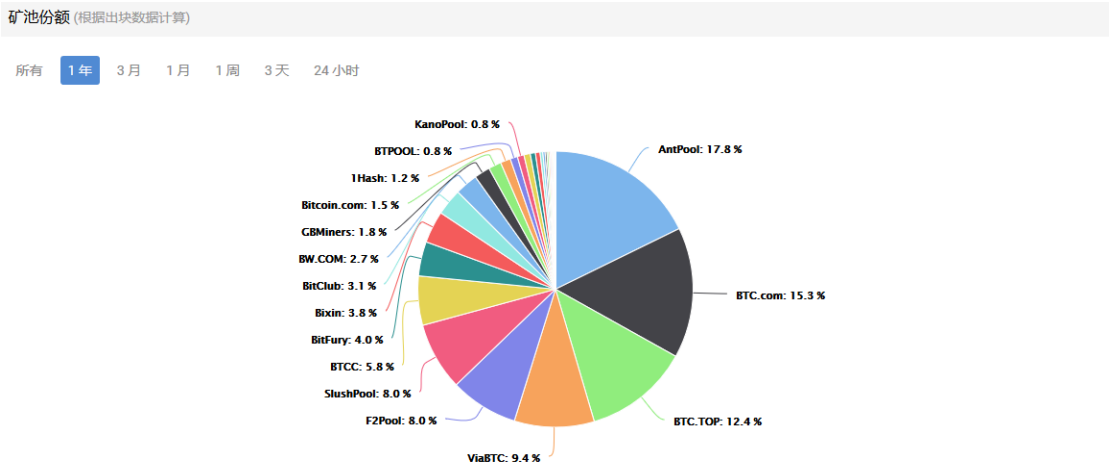
简要

由于比特币全网的运算水准在不断的呈指数级别上涨，单个设备或少量的算力都无法在比特币网络上获取到比特币网络提供的区块奖励。在全网算力提升到了一定程度后，过低的获取奖励的概率，促使一些“bitcointalk”(全球最大的比特币论坛)上的极客开发出一种可以将少量算力合并联合运作的方法，使用这种方式建立的网站便被称作“矿池”(Mining Pool)。

在此机制中，不论个人矿工所能使用的运算力多寡，只要是透过加入矿池来

参与挖矿活动，无论是否有成功挖掘出有效资料块，皆可经由对矿池的贡献来获得少量比特币奖励，亦即多人合作挖矿，获得的比特币奖励也由多人依照贡献度分享。

截止 2018 年 4 月，全球算力排名前五的比特币矿池有：AntPool、BTC.com 、BTC.TOP、ViaBTC、F2Pool，目前全球约 70%的算力在中国矿工手中。



（以上数据来至 https://btc.com/stats/pool）

风险

针对矿池平台的安全风险以及矿池本身在区块链网络的特殊角色，我们分析总结了以下影响区块链网络的攻击方式：

算力伪造攻击

矿池会通过某种特定的工作量证明检验算法来检验当前矿工的实际算力，但是在算法的实现上可能不一定完美无瑕，当算法的实现上存在某种漏洞可以虚报算力时，会给矿池平台带来很大的经济损失。

因为当前矿工实际上并没有给矿池贡献那么高的算力，却拿了与算力相当的奖励分配，对于矿池中的其他矿工来说极其不公平。

场景：黑客通过寻找矿池算力检验算法的漏洞来虚报算力，然后获取到与实际算力不想当的超额奖励。

扣块攻击

也叫做藏块攻击。在矿工参与矿池进行挖矿的过程中，只要有一个矿工解题成功，题解会上交给矿池，整个矿池所有的矿工便会共享这次的解题成果，并按照算力贡献大小来分配奖励。

但在实际情况中，矿池中的矿工可以不遵守规则，在得到题解后不回传给矿池，而是选择私吞，在这种情况下就会造成矿池利益的极大损失。

场景：矿池中的某节点在挖到区块之后并不上交给矿池，而是选择“私吞”，这样既能享受矿池所带来的福利，又能从挖矿中获得利益。

自私采矿攻击

自私采矿攻击(Selfish Mining Attack)[11]是针对区块链的一种典型攻击。由于挖取像比特币这样的加密货币，对于一个矿工(Miner)来说，需要高计算能力来解决密码难题(即工作量证明)，因此采矿变得十分困难。鉴于此，一组矿工(Mining pool，采矿池)通常会相互组合起来，并在成功解决密码难题之后，分享收到的奖励。这样有助于个体矿工在单独采矿时产生较连续恒定的收入而不是很少的收益。Eyal 和 Sirer 认为如果存在一群自私的矿工，采用自私的采矿战略，并获得成功，就可能会使诚实矿工的工作无效。这种自私采矿攻击表现为：一个恶意的采矿池决定不发布它发现的块，进而创建一个分叉，因此，网络中就存在由诚实矿工维护的公共链和恶意采矿池的私人分叉恶意采矿池在此私人分叉下继续进行挖掘，当私人分叉比公共链长的时候，恶意采矿池就发布该私人分叉，由于该分叉是当前网络中最长的链，因此会被诚实的矿工认定为合法链，所以原公共链及其包含的诚实数据将被丢弃。研究结果表明，一般情况下恶意采矿池采用自私采矿策略将获得更多的收益。

中心化问题（算力过于集中问题）

目前因为矿池的存在，违背了区块链去中心化的原则，当矿池做大，算力提高后，矿池变得过于集中，当算力达到全网的 51%后，从理伦上来说，如果能够控制整个网络达到或超过 51%以上的算力，将可以垄断开采权、记账权、分配权，将影响区块链的生态安全，这样加密货币的信用体系将不复存在，加密货币体系

也将彻底摧毁。

案例

1. 2014 年 5 月份，Eligius 矿池遭受扣块攻击，损失约 300 个比特币，在当时价值约 16 万美元

3.6.4 普通用户

3.6.4.1 系统资源

简要

在使用 PoW 共识机制的区块链中，存在一个非常重要的角色，那就是“矿工”，他们的主要作用是：

1. 解题：矿工需要通过计算来解决每过一段时间产生的“数学难题”，并通过“解题答案”来证明自己的工作结果，从而获取报酬。
2. 对账：对区块内的交易合法性以及其他矿工广播的“解题答案”进行核对，确认交易没有造假以及“解题答案”是正确的并盖章。
3. 记账：核对交易的合法性以及“解题答案”后，将这段时间的交易打包进新区块中。

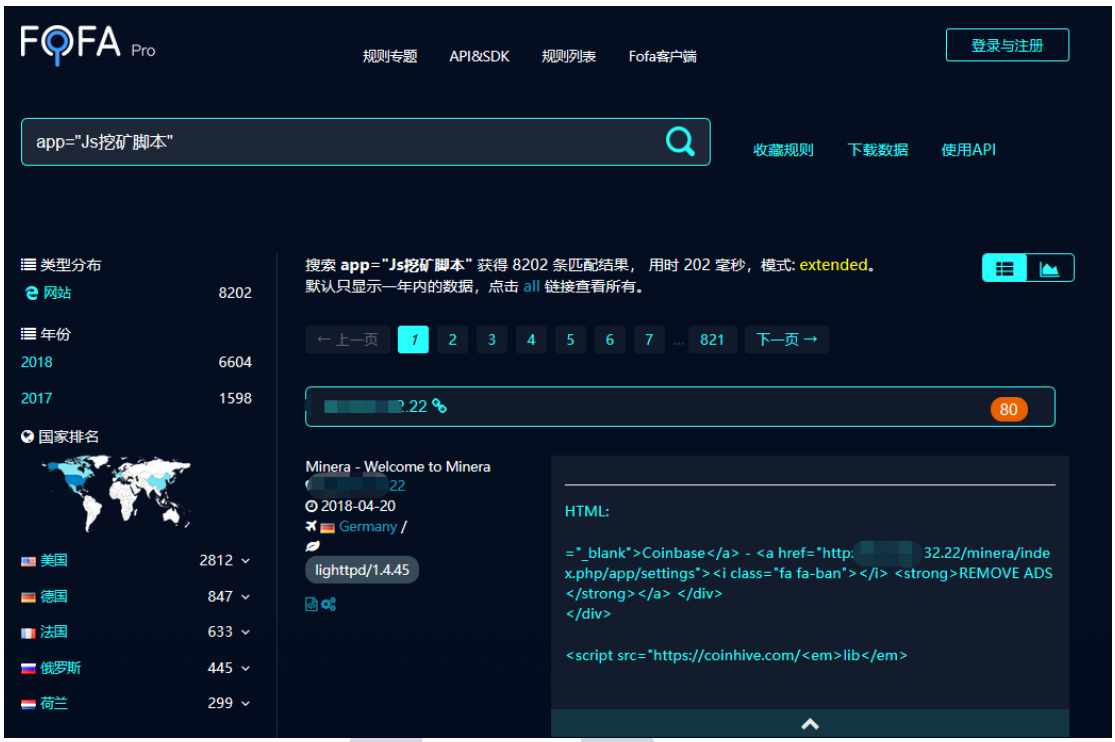
风险

针对目前用户的普通用户计算资源被滥用，用于挖矿的安全风险，我们分析总结了以下一些风险点：

挖矿傀儡

并不是人人都愿意当“矿工”。对于黑客而言，通过一些漏洞获得一些主机的权限或者网页端来挖矿是很容易的，黑客可以轻易地在被入侵主机上部署挖矿程序，消耗主机的系统资源与电力，以此来获取利益，目前市面上被黑客应用最多的就是门罗币(Monero)，因为植入部署方便，导致现在很大一部分黑产团体从原来的篡改网页，到现在直接植入挖矿脚本在网页里，如下我们通过网络空间测

绘系统检索目前互联网有大量网站被挂入恶意的挖矿链接：



案例

1. 2017 年下旬，有人发现很多网站首页中插入了 coinhive 平台的 JS 挖矿代码，使得大量访问网站的人系统变慢，疑似为黑客篡改首页权限导致。
2. 2018 年初，上百款《荒野行动》游戏辅助被植入挖矿木马，利用游戏主机的高性能来挖矿获取利益。
3. 2017 年至现在，很多攻击者利用“永恒之蓝”漏洞获取大量主机权限，然后在受害者的系统内长期潜伏挖矿。

3.6.4.2 钱包

简要

区块链的钱包指的是存储区块链资产的地址和私钥的文件。

目前主流的钱包分为冷钱包和热钱包。冷钱包是没有联网环境的，如市面上的硬件钱包就是冷钱包，由于其不联网的特性，使得它的安全性要在热钱包之上，但不方便交易。热钱包是在线的，例如电脑客户端钱包、手机 APP 钱包、网页

钱包等，都属于热钱包，它的交易是很方便的，但是安全性相对于冷钱包来说要低很多。

风险

针对钱包的安全风险，我们分析总结了以下攻击方式：

钱包客户端 RPC API 风险

区块链项目的客户端中目前通常都会有 RPC API 接口，给用户提供一个可程序化操作的接口，其中涉及到用户的一些敏感操作，例如：转账。

所以 API 的访问控制和鉴权至关重要，在没有鉴权和访问控制的情况下会造成如下攻击场景，以 eth 客户端 geth 为例。

场景：

1. 用户开启 RPC API，此时 API 只能做常规查询操作，并不能转账
2. 用户执行解锁钱包操作，此时 API 能执行转账操作并且无任何鉴权
3. 攻击者趁机在此 API 上执行转账操作
4. 代币窃取完毕

钓鱼攻击

在目前的互联网环境中，欺诈随处可见，这种攻击手段在区块链应用上也同样受用。攻击者可以伪造某个钱包客户端，无论从界面和操作上都可以做到和真钱包没有区别，可能他们只是在你转账的时候窃取你的私钥信息或者在转账地址上动手脚，就可以轻易地偷偷窃取你的资产。

所以，客户端一定要在官网下载，并验证官网发布的客户端文件 hash 是否与下载的客户端文件 hash 一致。

私钥窃取

因为私钥信息至关重要，所以很多人会选择将钱包私钥文件多点备份，而备份得多或者备份点不安全都有可能导致钱包私钥泄露。经调研，目前针对比特币的 wallet.dat 文件就出现在各个互联网中，例如：OSS 服务、网盘、GitHub、NAS 服务器、Web 服务等等互联网可接入的地方，都能看到密钥的存储，这是

极其危险的，甚至已经有攻击者开始针对密钥文件进行专门扫描，以及开发相关的木马病毒进窃取。

钱包软硬件漏洞攻击

钱包软件本身可能因为其本身或是开放的一些服务存在漏洞，影响用户的资金安全。

硬件厂商提供的钱包只是将钱包与线上网络隔离，并不能保证其本身的安全性就足够，由于其是封闭的，其代码质量对于大众是未知，且不良厂商在其中穿插后门也不是并无可能。

在线钱包账号窃取

由于在线钱包其方便、快捷等特性，使得很多人直接选择使用在线钱包。所以个人的资产安全与服务商的安全是一个强绑定的关系，个人的资产过分依赖于外部保障其实和中心化的应用比较类似，这与区块链根本理念相冲突，同时也给个人资产带来的很大风险。

案例

1 2013 年 11 月，比特币在线钱包服务商 Inputs.io 遭受黑客攻击，黑客透过电子邮件账号进行入侵，进而劫持代管账号，从中盗取了 4100 个比特币（在当时折算为 130 万美元）。

2 莱特币假钱包客户端盗币事件，攻击者通过修改开源钱包源代码，将显示的钱包地址固化为攻击者的钱包地址再重新编译，用户使用此地址接收转账的

时候很自然的就转账到了攻击者的账户中。

3 Ledger 硬件钱包漏洞，该漏洞让黑客可以在设备发货之前和发货之后窃取密码。

4 2015 年 2 月 23 日，比特币钱包运营商比特币存钱罐被盗，比特币存钱罐官方表示：黑客于 2014 年 6 月 30 日入侵了平台的 Linode 账号，并修改了 Linode 账号密码和服务器的 root 密码，从而入侵了服务器并且获得了服务器的控制和管理权限，导致比特币被盗。

5 在社区上，经常有用户表示自己的比特币余额被盗，而原因大多与钱包私钥泄露有关。

6 2018 年 3 月 25 日，币安发布公告表示部分社区 ERC20 钱包用户收到一封冒充 Binance 名义发送的“Binance 开启 ERC20 私钥绑定”诈骗邮件，邮件主要是为了盗取用户的 ERC20 钱包私钥。

7 2018 年 1 月份，名钱包开发商 Electrum 近期针对其比特币钱包的 JSONRPC 接口漏洞发布了安全补丁，这个漏洞能使攻击者通过 JSONPRNC 接口获取私人数据和加密货币。

3.6.4.3 交易所账户

简要

要在交易所中进行交易需要注册相应的账户，有了交易所账户就可以很方便的在交易所内进行买入卖出交易，相当于交易所账户掌握了你的数字货币的买卖权。

风险

在交易所中的账户安全需要在各个方面都有保障，只要有一个短板就会面临危险。

针对交易所账户的安全风险，从用户角度来说，我们分析总结了以下攻击方式：

钓鱼攻击

通过仿冒交易所网站的域名和页面来达到从视觉上欺骗受害者的手段，一般用来窃取用户的交易所登陆口令，攻击者拿到相关口令后开始进行转账操作。

中间人劫持攻击

攻击者可以在流量中转处截获流量，例如：路由器、网关等流量出口。不过好在目前多数的交易所一般都是采用 https，在此方面问题不算大，但是不排除在某些 API 接口的子域名未使用 https。

木马劫持攻击

木马通过按键记录，或是 hook 浏览器的方式来获取交易所账号的登陆口令或是直接劫持用户的资产，在历史安全事件就有攻击团体再各种相关虚拟货币网站，论坛社区发布带有木马的 APP 程序，来盗取劫持用户。

案例

1. 2018 年 3 月 8 日，币安网公布部分币安钓鱼网站案例

http://qbinance.com	http://registeronbinance.com
http://hbinance.com	http://binance-invite.com
http://reviewbinance.com	http://wwwwbinance.com
http://binance-cashback.com	http://bibinance.com
http://binance-referral-program.com	http://pbinance.com
http://thebinance.com	http://promo-binance.com
http://binance-promotions.com	http://rbinance.com
http://binance-register.xyz	http://tbinance.com
http://tradewithbinance.com	http://dbinance.com
http://wwbinance.com	http://httpbinance.com
http://binence.de	http://mbinance.com
http://isbinanceopen.co	http://register-binance.net
http://aivetorobinance.com	http://binance-sign-up.com
http://binance-exchange-register.com	http://binance-binance.com
http://registerbinance.com	http://wwwbinancecom.com
http://ebinance.com	http://wbinance.com
http://binance-japan.com	http://isbinanceopen.com
http://launchpadbinance.com	http://binance.com.hk
http://binances.today	http://binance.cx
http://inscription-binance.com	http://binancecoin.com
http://binance-coin.com	http://binance.hk
http://trybinance.net	http://binance.kr
http://trybinance.net	http://binance.my
http://binance-help.com	http://binance.sg
http://binance-exchange.uk	http://binance.pw
http://wwwlbinance.com	http://binance.ca
http://binance-referral-id.com	http://binance.mx
http://binance-review.com	http://binance.team
http://binance-com.top	http://binance-info.com

2. 2017 年 8 月份，一款名为 Trickbot 的木马就针对包括 Coinbase 在内的几家数字货币交易所增加了 web 注入攻击的功能，在受害者购买数字货币的时候和会将接受钱包重定向到攻击者的钱包，让用户误以为转账成功，其实最终转账操作都进了攻击者的钱包。

3.6.4.4 交易所 API

简要

各大交易所为了满足用户需要调用平台数据的需求，会开放一些 API 提供给用户使用。交易所 API 大致分为两类：

1. 公共 API 可以参考交易所的订单状况、公开的交易记录、交易版信息。
2. 私有 API 可以确认交易所的新订单及其取消、个人余额等信息，需要相应的 key 才可以使用。

风险

针对交易所 API 的安全风险，我们分析总结了以下攻击方式：

关键 Key&Token 窃取

私有 API 一般都涉及到用户的一些敏感操作，例如：买入、卖出等操作。所以，API key 一旦泄露，很可能会使自己的账户蒙受经济损失。而大部分人，甚至包括程序员都不一定有这种安全意识，存在 key 泄露的隐患，例如一些使用者，开发者可能有意或者无意就把相关的代码配置信息同步在 GitHub、公开网盘等互联网公共区域，互联网任意用户都能轻易的通过一些检索把这些敏感信息找出来。

案例

2018 年 3 月 8 日，币安网大量用户 API key 泄露，通过泄露的 key 直接操作用户买卖，导致一万余枚的比特币被用于购买其他币种，造成币市动荡。而某些交易所的 API key 到目前截稿为止在 GitHub 还能搜到。

Watch 1 Star 0 Fork 0

Code Issues 0 Pull requests 0 Projects 0 Wiki Insights

Tree: f2a2ba28ff Find file Copy path

o add binance f2a2ba2 on 8 Jan

1 contributor

21 lines (12 sloc) 557 Bytes Raw Blame History

```java
package com.binance.api.client;

import com.binance.api.client.impl.BinanceApiRestClientImpl;

import lombok.extern.slf4j.Slf4j;

@Slf4j
public class BinanceApiRestTest {
        public static String apikey = "BkC6YVJ5wMj[redacted]/cYVuGf3ROObbLBtBbm1msrzjv";

        public static String secret = "BkC6YVJ5w[redacted]YVuGf3ROObbLBtBbm1msrzjv";

        public static void main(String[] args) {

                BinanceApiRestClientImpl bclient = new BinanceApiRestClientImpl(apikey, secret);
                bclient.getServerTime();

        }

}
```

Code Issues 0 Pull requests 0 Projects 0 Wiki Insights

Tree: a26ae317ed Find file Copy path

Add files via upload a26ae31 on 8 Oct 2017

1 contributor

32 lines (23 sloc) 1.37 KB Raw Blame History

```php
<?php
        //SET KEYS
        $apiKey = "vmPUZE6mv[redacted]zvsw0MuIgwCIPy6utIco14y7Ju91duEh8A"; // Set your API Key
        $secretKey = "NhqP[redacted]5YNiP1e3UZjInC1VN65XAbvqqM6A7H5fATj0j"; // Set your Secret Key

        $symbol = "BNBBTC"; // Set which pair you want to get orders for
        $orderID = 6338879; // Set Order ID
        $serverTimestamp = time()*1000; // Take current UNIX timestamp and convert to miliseconds

        $params = "symbol=$symbol&orderId=$orderID&timestamp=$serverTimestamp";  // Set required paramaters
        $signiture = hash_hmac("sha256", $params, $secretKey); // Take the parameters, and sign them with the Secret Key

        $ch = curl_init(); // Initialise cURL
        curl_setopt($ch, CURLOPT_URL, "https://www.binance.com/api/v3/order?$params&signature=$signiture"); // Set URL + Parameters + Signi
        curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1); // Return values
        curl_setopt($ch, CURLOPT_CUSTOMREQUEST, "DELETE"); // Set HTTP Method to "DELETE"

        $headers = array(); // Set up our Headers
        $headers[] = "X-Mbx-Apikey: $apiKey"; // Put the API Key in HTTP Header
        curl_setopt($ch, CURLOPT_HTTPHEADER, $headers); // Enable Headers

        $result = curl_exec($ch); // Execute cURL command
        if (curl_errno($ch)) { // Check if any errors
                echo 'Error: ' . curl_error($ch); // Display Errors
        }
        curl_close ($ch); // Close cURL
        print_r($result); // Print Results


        ?>
```

四 区块链安全解决方案

基于上述区块链产业历史的攻击案例，结合区块链技术安全特点和安全威胁，白帽汇安全研究院建议从多个维度去进行综合防护，同时对于产业生态的安全需要区块链产业与区块链安全企业来共同提高区块链产业的安全性。

区块链产业安全主要围绕交易平台安全、矿池与矿机安全、用户安全、区块链底层安全、区块链业务安全。从基础安全建设、安全测试、安全审计、安全监测、应急响应，同时建立并完善区块链安全的规范、提高区块链产业人员安全意识多个方面来进行。最终提高区块链产业生态安全性。

4.1 区块链底层安全

区块链作为底层技术基础，支撑着整个系统。如底层出现安全问题，必将导致依托于此的上层均受到影响。其区块链底层的安全研究与防范变得极为重要。

在系统设计之初就应加入安全性设计，整个系统的安全防范、安全的处理在最初就应考虑。

区块链底层安全主要由区块链项目的建立者与区块链安全企业进行配合，来对其区块链整个系统进行安全方面的提高。

4.1.1 数据层

数据是区块链技术的最基本内容，为了防止上述针对数据的的攻击，主要从数据存储与加密算法两个方面来进行安全改进。

信息存储方面，建议对用户输入的数据（如备注信息）等内容进行过滤检查机制，防止被恶意利用或滥用。另外一方面，加密算法和签名机制出于安全上的考虑，不要轻易自写加密算法，建议使用成熟且可靠的加密算法。防止遭遇到算法漏洞的攻击和安全风险。

4.1.2 网络层

区块链与互联网是密不可分的,针对网络层的安全防御主要从 P2P 网络安全、网络验证机制两个方面来提升安全性。

可通过如下几点来进行防范：

- 在网络的传输过程中，使用可靠的加密算法进行传输，防止恶意攻击者对节点网络进行流量窃取或劫持。如开启 Jsonrpc 的节点强制使用 https 传输，而不是 HTTP 协议进行传输。
- 加强网络数据中传输的有效性、合理性、安全性进行验证，防止出现整型溢出等情况导致出现的数据错误。
- 节点网络安全性加强。重要操作和信息客户端节点做必要的验证。

4.2 区块链业务安全

区块链 2.0 以后，出现智能合约等新的理念，使得区块链的拓展性、便捷性极大增强。随之而来的安全漏洞也会越来越多。如上述提到的经典 The Dao 攻击事件。目前对于业务层面的安全主要通过安全审计来进行解决。

对于业务层的安全，主要依靠区块链安全企业开发相应安全产品或进行安全技术支撑，与区块链发起者建立合作等，从而避免或减少业务层上的攻击事件发生。

4.2.1 安全审计

针对历史案例以及可能存在的业务层安全问题，在正式发布之前进行安全审计工作尤为必要。

开发业务层代码安全问题，白帽汇安全研究院有如下几点安全建议和注意事项提示：

- 尽量避免外部调用
- 仔细权衡再发生重要操作时的代码逻辑，避免逻辑陷阱

- 处理外部调用错误
- 不要假设你知道外部调用的控制流程
- 标记不受信任的业务内容
- 正确的使用断言
- 小心整数除法的四舍五入
- 不要假设业务创建时余额为零
- 记住链上的数据是公开的
- 在双方或多方参与的业务应用中，参与者可能会“脱机离线”后不再返回
- 明确标明函数和状态变量的可见性
- 将程序锁定到特定的编译器版本
- 小心分母为零
- 区分函数和事件
- 避免死循环
- 升级有问题的业务层代码

4.3 交易平台安全

交易平台主要提供在线交易，形式主要为网站和 App 的形式。针对交易平台的安全性主要更加偏传统的安全防护。对于交易平台的安全性提高则主要由交易平台和安全企业或交易平台自建的网络安全部门。

白帽汇安全研究院针对区块链交易平台给出如下安全解决方案与建议：

- 再建设之初就设计网络安全架构。并随着发展不断调整
- 网络安全隔离策略，仅对需要对外开放服务的端口进行开放
- 选择使用具备高防护能力的 IDC 厂商，提高攻击者发起 DDOS 攻击的成本
- 线上业务系统需经过严格的安全测试，安全审计
- 对交易平台的所有资产进行实时的监控，对漏洞进行安全管理
- 建立安全预警机制，加强先于黑客发现安全威胁的能力

- 安全应急响应机制，出现安全问题第一时间进行处理
- 定期的安全测试、安全检查
- 对交易平台企业内部的安全管理
- 数据加密存储，防止数据被窃取后被滥用或使用户钱包或隐私信息被泄露而遭受损失情况
- 建立安全制度管理
- 提高交易平台企业内部人员的安全意识。建议定期对员工进行安全培训
- 与安全企业建立合作关系或建立 SRC（安全应急响应中心）
- 给交易平台用户进行安全引导

4.4 矿池与矿机安全

4.4.1 矿池平台安全

目前矿池平台聚集了大量的矿工，矿池平台出现安全问题，影响也将巨大。目前矿池平台也主要提供服务为主。白帽汇安全研究院针对矿池平台给出如下安全解决方案与建议：

- 在建设之初就设计网络安全架构，并随着发展不断调整
- 网络安全隔离策略，仅对需要对外开放服务的端口进行开放
- 选择使用具备高防护能力的 IDC 厂商，提高攻击者发起 DDOS 攻击的成本
- 建立安全预警机制，加强先于黑客发现安全威胁的能力
- 安全应急响应机制，出现安全问题第一时间进行处理
- 定期的安全测试、安全检查
- 对矿池平台企业内部的安全管理
- 数据加密存储，防止数据被窃取后被滥用或使用户钱包或隐私信息被泄露而遭受损失情况
- 建立安全制度管理
- 提高交易平台企业内部人员的安全意识。建议定期对员工进行安全培训

- 与安全企业建立合作关系或建立 SRC（安全应急响应中心）

4.4.2 矿机安全

矿机系统的安全主要对象为矿机生产商和矿工。矿机生产商应与安全企业进行合作，提高矿机系统的安全性。矿工则应该保护自己的矿机不被入侵。

白帽汇安全研究院建议：

- 矿机生产商应对矿机系统经过模糊测试和代码审计，确保系统安全性
- 矿机生产商生产的系统要求矿工必须修改默认账户，提高安全性
- 矿工应选择没有漏洞的矿机系统，避免自己使用的矿机被入侵，以免被攻击者恶意利用
- 矿工应设置安全复杂的密码

4.5 用户安全

白帽汇安全研究院对用户（交易平台用户、加密货币用户）的建议如下：

- 备份好自己的钱包文件
- 给自己的钱包文件设置密码
- 使用官方的钱包客户端，防止钱包文件存在后门或漏洞带来的钱包丢失
- 交易平台账户的加密货币账户建议转到自己的离线钱包里，防止交易所监守自盗或交易所被黑的情况下导致的加密货币丢失
- 安全杀毒软件，做好防护，及时更新系统补丁
- 对于重要的信息使用复杂的密码，并且不要多处使用同一个密码

4.6 安全企业责任

网络安全企业可以贯穿区块链生态产业，从区块链底层到业务层，再到交易平台，以及矿池、矿工。目前，安全还处再初级发展阶段，安全企业则应该主动发现更多的安全问题，帮助区块链厂商、交易平台、矿池平台、矿工系统提高

安全。为区块链产业生态安全做出巨大贡献。

除此之外，还应该建立区块链威胁情报，及时发现安全问题，及时做出响应。

五 总结与展望

区块链技术的底层机制、算法是区块链最核心的地方,是保障区块链稳定运行的根本，也是区块链开发者最关心的地方。目前，开发者将大量精力投入到了比较底层的算法安全上，使得区块链技术看上去难以撼动。

然而，通过近段时间的安全事件不难发现，安全问题越来越趋向于用户、平台层面，区块链的安全问题已经延伸到了传统的网络安全、基础设施、移动信息安全等问题。所以在谈及区块链安全的时候，不应该仅仅局限于区块链本身，它的使用者以及衍生的东西都需要我们的重点关注。

目前基于国家层面的管控措施也是未来值得研究的一个方向，虽然世界各国对加密货币，以及基于区块链相关的 ICO 的态度不尽一致，但是目前仍有大量的资金投入在虚拟货币市场，一个安全问题将可能导致数百亿的资金损失，甚至影响国家安定，出于避免巨额资金损失导致社会不稳定等因素的考虑，未来基于国家层面对于资金的保护、风险监控和预警，都是值得讨论的话题，虽然区块链本身是去中心化的技术，但是可以预见到，随着区块链技术的落地，其必将被应用到目前一些传统基础设施的技术中去，所以，对于区块链的安全研究是更加值得重视与跟踪的。

总体来说，区块链技术和其安全性问题仍会持续很长一段时间，主要原因：其一，全新的解决方案会进一步加快区块链的安全重建，创新技术和服务得到认可，进一步增强产业活力，提升技术价值；其二：随着生产生活逐渐向数字化，网联化和智能化转型，许多全新的变革性技术（如区块链）所打造的安全生态体系和技术将成为大势所趋；其三，由新技术衍生的产品安全技术服务范畴更加宽泛，将会催生更加繁荣的安全服务市场。

最终，区块链新兴技术和产业的有机融合，必将在未来产生不可估量的价值。

六 关于我们

白帽汇安全研究院隶属于北京华顺信安科技有限公司。研究院拥有一支从事网络安全研究的资深技术团队，致力于网络信息安全领域的深入探究，研究方向为网络空间测绘、安全大数据、威胁情报、态势感知、区块链安全等前沿安全领域。

七 参考来源

[1] Block chain https://en.wikipedia.org/wiki/Blockchain

[2] Luu, L., Chu, D.H., Olickel, H., Saxena, P., Hobor, A.: Making smart contracts smarter. In: ACM CCS (2016).

[3] Quantum attacks on Bitcoin, and how to protect against them

[4] P2P https://en.wikipedia.org/wiki/P2P

[5] Eclipse Attacks on Bitcoin's Peer-to-Peer Network

[6] Hijacking Bitcoin:Routing Attacks on Cryptocurrencies

[7] BGP hijacking https://en.wikipedia.org/wiki/BGP_hijacking

[8] Hijack-btc test code https://github.com/nsg-ethz/hijack-btc

[9] 双重支付 https://baike.baidu.com/item/双重支付

[10] 《The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments》

[11] 房卫东等.信息安全学术报《区块链的网络安全威胁与对策》

[12] C. Lin and T. C. Liao, "A survey of blockchain security issues and challenges," Int. J. Netw. Secur., vol. 19, no. 5, pp. 653–659, 2017.

[13] Atzei, N., Bartoletti, M., Cimoli, T.: A survey of attacks on Ethereum smart contracts.Cryptology ePrint Archive (2016).

[14] Hacking Blockchain https://www.rsaconference.com/writable/presentations/file_upload/fon4-t11_hacking_blockchain.pdf

[15] 0day 漏洞 https://baike.baidu.com/item/0DAY%E6%BC%8F%E6%B4%9E

[16] Ethereum Smart Contract Security Best Practices

[17] A PoC of a Blockchain-based C&C https://github.com/i3visio/blockchain_c2c

[18] Smart Contract Best Practices, https://github.com/ConsenSys/smart-contract-best-practices