Blockchain can be Blocked（比特币网络通讯底层漏洞详解）

微位科技weway / 2018-04-16 12:37:19 / 浏览数 1479 安全技术 漏洞分析 顶(0) 踩(0)

现在可见的几乎所有加密货币和区块链的讨论都源于中本聪的白皮书：《比特币：一种点对点的电子现金系统》Bitcoin: A Peer-to-Peer Electronic Cash System（Satoshi Nakamoto）。

2008 年11月1日，一个密码学邮件组收到了 satoshi@vistomail.com
邮箱发出的这份白皮书，2009年1月3日，中本聪的个人电脑里挖出了50个比特币，并在创世区块里留下一句永不可修改的话：“The Times 03/Jan/2009 Chancellor on brink of second bailout for banks（2009年1月3日，财政大臣正处于实施第二轮银行紧急援助的边缘）。”

当时正是英国的财政大臣达林被迫考虑第二次出手纾解银行危机的时刻，这句话是泰晤士报当天的头版文章标题。区块链的时间戳服务和存在证明，让第一个区块链产生的时

2009年10月5日出现了最早的交易所汇率：1美元 = 1309.03比特币。十年后比特币的价格已经超过8000美元，按照2017年峰值的最高价20000美元一枚计算，2100万枚比特

在币值飞涨的疯狂年代，已经很少人再去翻看中本聪的白皮书。仅有九页的白皮书只是一套技术方案，所有的篇幅都是为了探讨一个“币”的实现，超越软件技术本身，我们去

去中心化=大多数人正义

[白皮书摘要]：本文提出了一种完全通过点对点技术实现的电子现金系统，它使得在线支付能够直接由一方发起并支付给另外一方，中间不需要通过任何的金融机构。虽然数字signatures）部分解决了这个问题，但是如果仍然需要第三方的支持才能防止双重支付（double-spending）的话，那么这种系统也就失去了存在的价值。我们在此提出一种

细读比特币白皮书，你会发现中本聪的“去中心化”背后的潜台词是“大多数人正义”，共识机制是比特币的核心理念。

建立一套“去中心化的P2P支付系统”，没有中心（中介）的支付系统，要避免“双花”（双重支付double-spending）如何核对记账？答案是通过共识机制：用密码原理和工作

产生一条新的交易记录时永远有先后顺序，即便是双花也总有先后顺序，同一用户不可能同时创造两笔交易。比特币首先引入了基于时间戳的随机散列，让其形成前后相关的

要避免双花，我们只需要证明其中一条链有效即可，并且将其记录到交易链条上，其他的交易就是无效的了。要证明其中一条是有效又不允许中心化从存在，只有一个办法：

POW
共识算法正是为了解决谁是大多数的问题，“大多数”的决定表达为最长的链。新区块进行节点广播，一旦有节点收到了这个区块的广播，会按照“当且仅当包含在该区块中的所

验证通过后，这个节点就不会再接受别的节点的同样区块了。同时这个节点会终止自己正在进行的包含同样交易的区块计算，也就说不会在进行无用功了，节点在这个区块基

由于网络延迟，如果同时有几个节点互相收到交易区块，记录同样的链条（分叉），该僵局的打破要等到下一个工作量证明发现。通过一段时间运行，总有一条区块链时序最

共识机制替代中介信任，那么我们探讨一下极端情况下可能会出现什么问题？

假想的灾难

让我们一起头脑风暴一场假想的灾难：

2018年某一天下午15：30，中国的海底光纤突然出现故障，国际出口被阻断。整个比特币网络仍旧正常运转：国内的矿池、矿场币照样挖；国外的矿场、交易所继续正常挖

17：40，故障后2个小时，光纤故障排除，国际出口复通。

在故障期间，中国境内的算力形成一个链，境外的算力形成另外一条支链。按照共识机制，就看哪条链的长度更长，而长度较短的另一链会被淘汰，即这条被淘汰的支链上产

由于中国国内的算力占比高达70%，国外链毫无意外会被淘汰，这将为比特币带来灭顶之灾：在故障发生的两个多小时，境外矿场的算力成果被销毁了，海外所有的比特币交

大规模通讯中断会将比特币网络撕裂为算力悬殊的两个分支，那么最优的策略是故障发生那刻起，整个比特币网络立即停摆，直到故障修复。否则如果保持隔离状态继续运行

为防止支链带来的干扰造成损失，比特币一笔交易至少需要 6
个区块的确认，一个区块时间是10分钟，6个区块就是一小时。假如故障导致的网络隔断超过一小时，就会给交易带来冲击，隔断时间越长冲击越大。

人们对比特币容灾能力的讨论，更多地关注于分布式的多节点存储备份，忽略了共识机制本身造成的隔离和吞没效应。

这样的假想并非天方夜谭，就在 2018年3 月30日，非洲国家毛里塔尼亚由于海底电缆被切断，造成全国范围内彻底断网时间长达 2
天，该起事件还同时影响数个周边国家，断网噩梦首次在现实中上演，说明全球范围内的网络基础设施并非人们想象的安全。

实际上，全球大约 97% 以上的网络数据通过海底电缆传输，但各国出于军事目的而进行的海底电缆附近活动并不在少数。2013 年，有 3
名潜水员在埃及被捕，他们被指控为涉嫌切断海底电缆。

而在军事战略家的理论中，全面切断海底电缆，影响该国军事通信能力，对敌方造成经济损失和瘫痪性灾难，也不失为一种重要的备选打击手段。

并且，能让比特币陷入瘫痪的可能还不止天灾。

算力垄断≠51%攻击

目前对比特币的信仰建立在全网51%算力难以企及上，然而最近人们越来越多开始担忧，掌握大规模ASIC矿机的矿场事实上已经垄断了51%算力。

根据《麻省理工科技评论》在
2018年1月18日发布的最新研究表明，比特币和以太坊都属于开放区块链系统，即原则上任何人都可以成为矿工，但因为这样的架构特性，自然形成了相应的组织集中挖矿资

基于每周一次的统计，排名前四名的比特币挖掘活动就占整个系统挖掘活动的 53%；而以太坊挖掘活动的中心化程度甚至更加稳固，前 3
大矿机占整体系统每周平均挖掘活动高达 61%。算力垄断是否已经动摇了比特币“去中心化”的特性？

答案是否定的。51%攻击不会来自生态内。

这是因为矿场巨头们虽然集中控制了算力，但他们按照游戏规则，付出了大量硬件投资和电费消耗。如果发动51%攻击，整个系统的价值就会崩溃，那么攻击获得的比特币就

51%攻击必然来自于体系外。

从假想天灾我们可以得到一点启发，发动51%攻击不一定要靠控制算力，影响网络层可能是成本更低，更可实现的方式。下面发散列举一些可能性：

1. 大规模的黑客攻击行动，控制主干网络设备的路由策略，发动BGP攻击。
2. 网络设备商的后门权限。针对核心路由器0day漏洞的蠕虫病毒在传播过程中，有意或无意地封闭了国际出口。
3. 电信运营商的国际出口通讯故障。
4. 国家防火墙的限制和阻断。

以上类似天灾的场景中，发动者都可以是体系外的成员，并且不需要耗费大量硬件和电力资源投入，只需要控制网络层就可以轻松实现。这就暴露出比特币和所有加密货币最

被忽略的默认前提：信道安全

区块链的底层是P2P网络通信技术，区块链本质上是一个基于P2P的价值传输协议。

比特币采用了基于国际互联网（Internet）的P2P（peer-to-peer）网络架构。P2P是指位于同一网络中的每台计算机都彼此对等，各个节点共同提供网络服务，不存在任何

早期的国际互联网就是P2P网络架构的一个典型用例：IP网络中的各个节点完全平等。当今的互联网架构具有分层架构，但是IP协议仍然保留了扁平拓扑的结构。在比特币之

“比特币网络”是按照比特币P2P协议运行的一系列节点的集合。除了比特币P2P协议之外，比特币网络中也包含其他协议。例如Stratum协议就被应用于挖矿、以及轻量级或移
bitcoin network）”指代所有包含比特币P2P协议、矿池挖矿协议、Stratum协议以及其他连接比特币系统组件相关协议的整体网络结构。

运行比特币P2P协议的比特币主网络由大约7000-10000个运行着不同版本比特币核心客户端（Bitcoin
Core）的监听节点、以及几百个运行着各类比特币P2P协议的应用（例如BitcoinJ、Libbitcoin、btcd等）的节点组成。比特币P2P网络中的一小部分节点也是挖矿节点，它

比特节点通常采用TCP协议、使用8333端口（该端口号通常是比特币所使用的，除8333端口外也可以指定使用其他端口）与已知的对等节点建立连接。

P2P网络只是为所有节点提供了信息交换的方式，做事的还是共识算法和加密算法。但接收方必须信任，数据区块的传送过程中没有被任何中间方改变破坏。这实际上需要一

我们信任区块链软件，相信它在运行中不受破坏，而传输的是非伪造的数据。
我们信任运行区块链软件的运行系统，它在运行中不受破坏，而传输的是非伪造的数据；
我们信任为系统提供网络的中央处理机，相信它不受破坏，而传输的是非伪造的数据。

这种信任，基于“网络中立化”而产生。然而，互联网的传输和承载网建设，属于高度资本性投资。因此，所有的互联网基础建设，均来自通讯企业高额投资，而互联网服务，

这便带来了一个相对矛盾的问题：“去中心化”的分布式系统，承载于中心化的互联网服务之上，但却并未被广泛意识到，这种天然的高度中心化的底层传输网络，对“去中心化

从比特币的协议细节便可看出，其对传输层的攻击并未充分防范。比特币的传输协议报头都是明文，且规律恒定，其报文开头4个字节就是0xF9BEB4D9。相信中本聪在设计

但这种高度自信、过分依赖于信道安全性的协议，在网络底层发动的攻击中，便显得格外脆弱。愈合攻击便是一种足以瓦解比特币信仰的攻击手段。

愈合攻击Merge attack ：

有趣的是，“区块链”Blockchain一词本不是白皮书中的原生词汇，尽管原文中提及“区块”Block达67次，提及“链”Chain的有27次，但中本聪从未将Blockchain合并在一起。
can be blocked。

区块链的核心是共识机制，共识是分布式系统经过网络传输“投票”决策模式，干预和影响分布式系统的承载网络。我们发现，在特定场景下，恶意地利用共识机制，可以间接

愈合攻击，简而言之，是先通过“撕裂”，将区块链网络隔离成能超过“共识阈值”（比如POW的51%）的两个独立链条，然后间隔一定时间（超过交易确认时间）后，让两个链

愈合攻击实际上是分区攻击（Partition attack）+延迟攻击(Delay attack)的连续组合攻击手段，其破坏力远超DDos攻击和IP封堵。

针对节点、矿工的DDos、封堵ip地址等攻击方式，其影响力是短暂的。无论对任何IP地址发动DDos攻击，被攻击者都是有感知的，因为节点和矿工将立即意识到，自己无法
愈合攻击直接撕裂网络，形成两个大局域网。两个网内的节点均可以相互通信，并无断网感知，也就无从采取防范措施。它利用网络层，在愈合的一刻使“共识机制”崩溃：假
is
Law”，则必然出现分链被吞没；不遵守代码约定，则需人为分叉，进而颠覆信仰。更致命的是，愈合攻击可以高效率地反复进行，分治对冲，比特币网络就就会瘫痪。

愈合攻击并不仅针对比特币网络有效，对于以太坊等加密数字货币，同样有着致命威胁，尽管以太坊在通讯协议上进行了一定程度的加密，但这仅仅是为了保护智能合约的安

因此，无论是哪种数字货币，只要没有在通讯底层从数据和行为上抹去特征，便难逃愈合攻击的火力覆盖。近年来广受炒作的山寨币，包括莱特币、门罗币、比特币现金、量

进一步来看，所有的共识算法，包括POW、POS、DPOS，都需要保证传输无干扰。因为分布式系统的共识算法本质上都是在信道安全的前提下，解决一致性和正确性问题。

BGP劫持

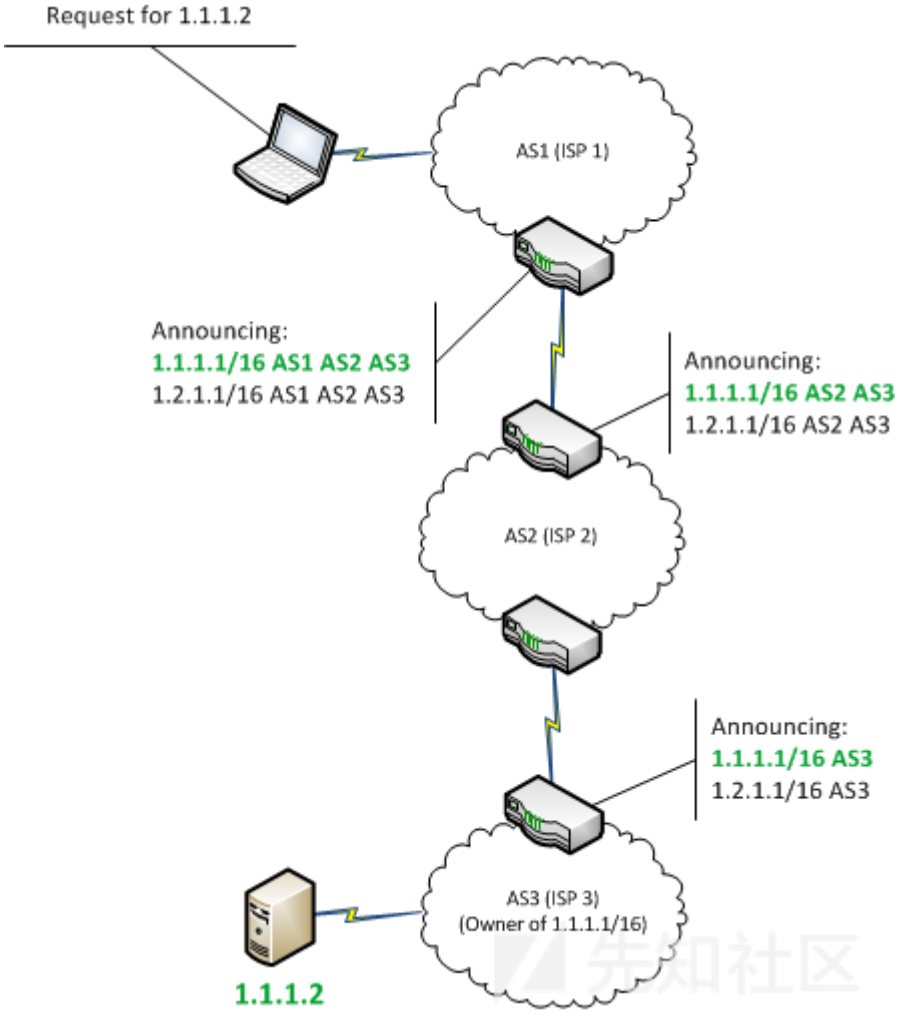
愈合攻击是瓦解区块链的技术手段，实施愈合攻击，最常用的是BGP劫持。什么是BGP劫持呢？

正常的矿机与矿池的通讯应该包括这几个步骤：
矿机 -> 网络运营商A -> 网络运营商B -> 网络运营商... -> 矿池

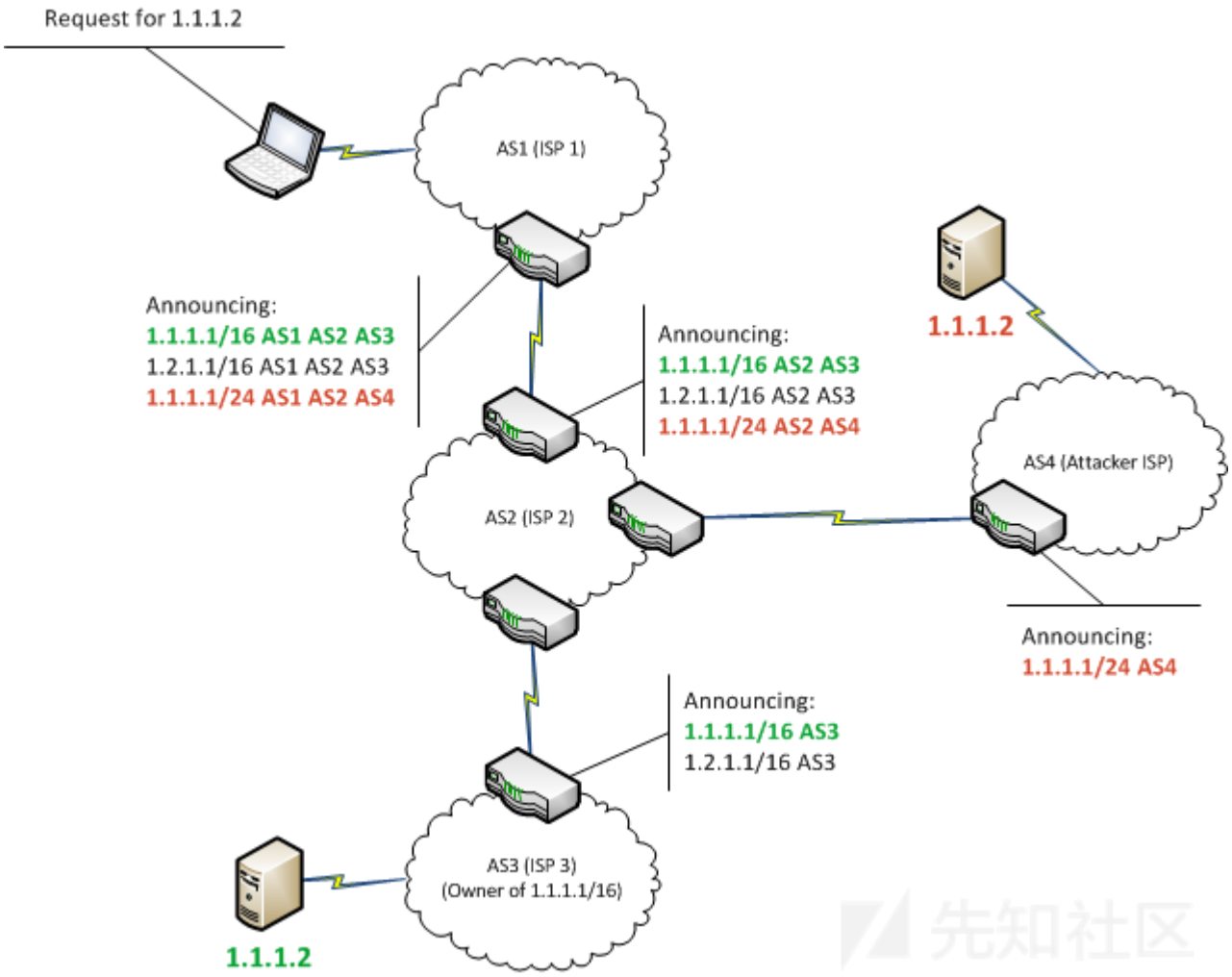
由于比特币矿池的跨地域性，在矿机和矿池之间的网络运营商（ISP）可能有数个作为跳转。这是极不安全的，任何一个环节的都有可能被黑客通过边界网关协议（BGP）劫

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。无论是网络犯罪分子还是国家防火墙,都可以利用这种技术来达

BGP是一种网络协议,用于交换因特网上各网络之间的路由信息。一般情况下,它用来确定在独立运营的网络或自治系统之间路由数据的最佳路径。
因此,它也常常用来寻找从ISP到ISP路由数据的路径。需要注意的是,BGP不是用来传输数据的,而是用来确定最高效的路由路径的。
实际的传输工作,是由其他协议来完成的,例如TCP/IP协议栈。



现在,假设我需要发送数据到世界的另一端。最终,这些数据肯定会离开我的ISP所控制的网络,因此,必然就会用到BGP。
当然,路由路径是无法通过单独一个自治系统来决定的,这需要其他的BGP对等端或邻居的参与才行。
这些对等端是些已经通过手工配置为共享路由信息的自治系统。当自治系统学习新路由的时候,这些信息就会进一步传播到其他对等端。
通过梳理从BGP对等端收集来的路由信息,处理这些数据的路由器就能够找出最佳路径。这些最佳路径是参考多种因素综合得出的,包括距离以及路由器管理员实现的配置设置
由于传播路由的对等端是手工配置的,因此有必要入侵一台边界路由器来广播外部BGP通告,从而实现因特网级别的BGP劫持。尽管这做起来非常困难,但是BGP劫持攻击确实已



因为BGP决定了数据从源端到目的地端的传输方式,所以,必须要关注该协议的安全性。通过操纵BGP,攻击者可以按照自己的意愿来修改数据的传输路线,从而达到拦截或者修改
为了劫持因特网级别的BGP,需要配置一个边界路由器,让它发送含有未分配给它的前缀的通告。如果恶意通告比合法通告还要具体,或者声称提供更短的路径,那么流量就可能被
攻击者经常利用弃用的前缀来进行劫持,以免引起合法属主的关注。通过广播含有虚假前缀的通告,受攻击的路由器可能会污染其他路由器的路由信息库。
在污染了其他路由器之后,恶意路由信息可能会进一步传播到别的路由器中,或自治系统,甚至主干因特网上。

最近几年来,已经有多起BGP劫持攻击被记录在案：

比较著名的就是13年巴基斯坦屏蔽Youtube的事件。由于巴基斯坦电信部门错误地把屏蔽youtube加到了BGP上，导致该协议上的所有AS都被屏蔽了。换句话说，全世界其

在Renesys记载的案例中,2013年BGP劫持技术曾经用来重新路由数据,使其在到达目的地之前,先经过任意指定的国家。
其中,一个攻击案例中的数据流量,在到达起目的地之前,竟然先绕道墨西哥至美国,然后转至白俄罗斯。通过散布虚假BGP广播,白俄罗斯的ISP成功将非法路由传播到了因特网上
在这个案例中,很可能是一种公司或国家间谍行为。不过,有迹象说明,即使非国家级别的对手,照样也能够发动BGP劫持攻击。

2014年Dell
SecureWorks分析的一个案例中,BGP劫持被用来拦截比特币矿机到采矿池服务器的链接。通过将流量重路由至攻击者控制的矿池,攻击者就能够窃取受害者的比特币。
这次攻击在两月内收集到了价值$83,000的比特币。

在2015年7月,监视软件供应商Hacking Team被黑,泄露的内部邮件表明,在2013年,意大利政府曾经与Hacking
Team有关合作,同时,意大利的一家ISP也购买过该公司的BGP劫持服务。 由于托管Hacking
Team指令控制服务器的IP被阻断之后,该服务器已经离线,因此该恶意软件与指令控制服务器的连接也一直保持不可达状态。通过公布托管该指令控制服务器的虚假IP前缀,Ha
Team竟然又恢复了对受害者机器的访问能力。 这是第一个记载在册的西方国家政府使用BGP劫持的案例。

致命伤： “拜占庭将军问题”&“两军问题”

比特币是分布式系统一次空前的社会实验，也被称为解决“拜占庭将军”问题的成功实例。在此强烈建议大家百度或者维基一下理论原型。

拜占庭将军问题是2013年图灵奖得主 Leslie Lamport 在 1980 年的论文 The Byzantine Generals Problem
中提出的分布式领域的容错问题，这是分布式领域最复杂、最严格的容错模型。Lamport是分布式系统的祖师爷级的大师，这个故事也广为流传：

拜占庭位于如今的土耳其的伊斯坦布尔，是东罗马帝国的首都。由于当时拜占庭罗马帝国国土辽阔，为了防御目的，因此每个军队都分隔很远，将军与将军之间只能靠信差传
在战争的时候，拜占庭军队内所有将军和副官必需达成一致的共识，决定是否有赢的机会才去攻打敌人的阵营。但是，在军队内有可能存有叛徒和敌军的间谍，左右将军们的

拜占庭将军问题不去考虑信差是否会被截获或无法传递信息等问题。Lamport已经证明，在存在消息丢失的不可靠信道上试图通过消息传递的方式达到一致性是不可能的。

另一个比“拜占庭将军问题”更基础，更广为人知的是“两军问题”Two Generals’ Problem：

两支军队，分别由两个将军领导，正在准备攻击一个坚固的城市。两支军队都驻扎在城市旁边的两个不同的山谷里。两军之间隔着第三个山谷，两个将军想要通讯的唯一方法

两军问题是阐述在一个不可靠的通信链路上试图通过通信以达成一致是存在缺陷的和困难的，这个问题经常出现在计算机网络入门课程中，用于阐释TCP协议不能保证通信两

对比两个故事，我们会发现两军问题和拜占庭将军问题有一定的相似性，但必须注意的是，信差得经过敌人的山谷，在这过程中他可能被捕，也就是说，两军问题中信道是不

两军问题是在计算机通信领域首个被证明无解的问题，由此也可推论出，信道不可靠条件下的"拜占庭将军问题"也同样无解。

这意味着我们传输信息时仍然可能出现丢失、监听或篡改的情况。也许只有未来的"量子通讯"可能解决加密通信的问题。

搁置各种加密货币共识算法的优劣争论，我们必须看到本质问题，是共识算法离不开信道安全前提。

比特币在理论上的缺陷，就是出在网络通讯层的安全上。人们过高的着迷于区块链这种技术在时间戳签名、哈希链等密码学上的贡献，而忽略了其作为分布式系统的网络层安

网络通讯混淆协议BSO

比特币的信仰建立在彻底去中心化的大前提下：整个体系公平、自治，不依赖也不需要现有的中心化机构介入，甚至也无法介入。因此，评价一个加密货币成功的标准必须在

比特币要实现彻底去中心化，承载价值网络之名，就必须运行于安全的网络上，成为加密到底层通讯协议的全加密货币。现实的网络世界，完全安全、透明、中立的网络通讯

以太坊和一些加密货币开始使用加密通讯协议，这是一个好的开始。然而这些协议仍留有很多痕迹。在2018年初，移动互联网系统与应用安全国家实验室举办的一场通讯加

我们认为需要重新设计一种更优的区块链通讯混淆协议BSO（Blockchain Security Obscure Protocol），协议设计思想是让P2P网路在通讯传输时无明显特征，混淆在一般的网络通讯中。增加网络层寻识特征的难度，提高网络层识别、篡改或拦截的成本，从而保护

混淆协议属于一种安全对抗工程，一般有两种对抗方向，一种是正面对抗，通过设计一种新的强加密协议，让中间人无法通过分析流量内容识别出应用业务，但是新协议本身

BSO混淆协议只是一个起步，未来混淆和机器学习将是一个在长期对抗中共同演进的技术，而区块链网络可以通过不断软分叉方式不断完善，健壮起来。

分布式网络治理和监控

区块链生长于网络之上，算力节点在网络上的分布生态是一个未被足够关注的问题。分布式系统的共识离不开信道安全，甚至需要网络保护。

运行在区块链上的数据，资产，应当如同承载在互联网上的信息一样，被全世界所有国家的政府、网络管理机构、运营商来保护，并承诺安全。

所有的加密货币和区块链应用，必须争取获得获得国家和政府的认可、监管并且保护。因为加密货币并不像看上去那样，可以无法无天无人可管，又令管制机构无可奈何。可

从事区块链、加密货币研究的企业、机构，更应该呼吁和推动政府部门尽快出台相关法律法规和监管政策，规范、保护并约束一个良好的生态环境。

另一个维度，区块链是需要运维的。这个观点与追求"维持开放、无需权限和分布式"的理念似乎有点格格不入。但当千百亿资本涌入那些加密货币，专业的攻击者也会盯上这

信仰代码

哈耶克终身都在反对人为建构的秩序，认为人类理性不及，需要由市场自生自发的秩序来认知和管理世界，并提出了《货币的去国家化》的开创性构想，他在序言写下：

"当下的政治必然性不应当是经济学家关注的问题。他的任务应当是像我不厌其烦地重复过的那样，是从今天的政治角度看来不可行的政策，具有政治上的可能性。决定此时

作为技术开发者，引起我们共鸣的是：应从技术的角度探求，使得今天可能在政治上不可能的事情具有政治上的可能性。剩下的交给政治家。

最后，期待人们仍可以回到对代码的信仰上。在它完善之后。

附录：致谢和参与者

由衷的感谢下面的人，他们慷慨的分享和贡献了他们的时间和见解：

Satoshi Nakamoto Bitcoin: A Peer-to-Peer Electronic Cash System 2008
Zach Julian An Overview of BGP Hijacking AUGUST 17, 2015
Dave Hudson Look back to Satoshi's White Paper to Find the Essence of Blockchain 2016
Maria Apostolaki,Aviv Zohar,Laurent Vanbever Hijacking Bitcoin: Routing Attacks on Cryptocurrencies May 2017
Liang Wang,Kevin P. Dyer,Aditya Akella,Thomas Ristenpart,Thomas Shrimpton Seeing through Network-Protocol Obfuscation
Adem Efe Gencer, Soumya Basu, Ittay Eyal, Robbert van Renesse, and Emin Gün Sirer Decentralization in Bitcoin and Ethereum Networks
Byron Gibson Bitcoin and the byzantine generals problem
Tan Qingfeng, Shi Jinqiao, Fang Binxing, Guo Li, Zhang Wentao, Wang Xuebin, Wei Bingjie Towards Measuring Unobservability in Anonymous Communication Systems
Zhu Yixiang，Li Ziyang，Liang Yingfeng，Chen Yexuan，Wang Si，Eleven zhang，Jiang Zhuojian Security analysis and improvement of Blockchain network communication focus on Bitcoin 2018

上一篇：对某cms过滤函数的突破及思考 下一篇：Linux花式读取文件内容的几个命令

1. 1 条回复

微位科技weway 2018-04-26 19:38:03

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板