出血性攻击
关于股份证明区块链

盖彼得ž
日
电子邮件：peter.gazi@iohk.io

阿格洛斯基亚亚斯
爱丁堡大学和IOHK大学
电子邮件：aggelos.kiayias@ed.ac.uk

亚历山大拉塞尔
康涅狄格大学
电子邮件：acr@cse。uconn.edu

摘要：我们描述了一种没有检查点的风险证明(PoS)区块链的一般攻击。我们的攻击利用了交易费用、“断章取义”处理交易的能力，以及完全主导区块链的标准最长链规则。攻击随着诚实交易的数量和对手持有的股份而增长，并且可以由控制任何恒定比例股份的对手发起。

根据区块链协议的统计概况，可以启动区块链操作前几年的攻击；因此，它属于PoS协议的可行性范围。最重要的是，它展示了交易费用和奖励与PoS协议的安全属性是如何紧密结合的。更广泛地说，我们的攻击必须在任何未来的PoS设计中得到反映和反击，以避免检查点，以及从现有协议中删除检查点的任何努力。我们描述了几种防止攻击的机制，其中包括事务的上下文敏感性和链密度统计数据。

Ⅰ.介绍

股权证明(PoS)区块链协议被设想为解决基于工作证明(PoW)的区块链系统中矿工节点的巨大能源需求的一种解决方案。PoS是在比特币论坛的讨论中提出的[1]并采用这样的原则，即生产新区块链块的权利应授予利益相关者，其概率与其当前股份的比例，正如区块链本身所证明的那样。可以想象，这样的区块链学科可以在不消耗大量的真实资源的情况下产生理想的账本属性：不需要投入大量的能源支出来运行该协议。这样的协议自然会用假设系统中诚实的多数股份来取代假设诚实的多数哈希权力的假设。虽然这种PoS协议的潜在优点是实质性的，但早期有人认为，这种方案的设计可能特别具有挑战性(见，e。g.，甚至可能是不可行的(见，e。g.，[坡14])。

在PoS的环境中，一个特别关键的威胁被Buterin[但是14]记录下来，他将其称为“远程攻击”的问题(也与“无成本模拟”的概念有关，例如，[Poe15])。这指的是少数涉众能够从起源块（或任何足够老的状态）开始执行区块链协议，并生成一个有效的系统替代历史。面对着这样的另类历史，而没有其他的外部历史除了起源块之外的信息，一个新连接的节点将没有能力可靠地区分这种交替历史和实际历史。由此可见，通过这样的攻击，少数利益相关者可以重复处理或删除过去的交易，从而违反了生成的账本的基本持久性属性。在同一篇博客文章[但14]，然而，一线希望也提供：观察到区块链等少数的利益相关者可能有特征，可以用来区分他们与实际的区块链由诚实的多数。特别是，如果时间戳包含在每个块，这将是一个简单的模拟协议的少数利益相关者会导致区块链更稀疏的时域，因此，最长链规则在任何特定时刻将有利于区块链由诚实的政党。

许多PoS协议被提出并实现，例如，PPCoin[KN12]和NXT加密货币[Com14]。最近，最近的努力已经开始严格分析PoS设置的安全性，导致了具有正式保证的协议，如阿尔戈兰[Mic16]、[KRDO17]、白雪公主[BPS16]和[DGKR17]。为了即将到来的阐述，将这些协议分成两类将是有用的：[2]

1)**最终共识协议，应用某种形式的最长链规则的区块链。**
在这种设置中，块的不变性随着在其上创建的块的数量而逐渐增加。
2)顺时针-BA协议，在继续生产任何后续块之前，通过完全执行拜占庭协议(BA)的协议来实现每个块的不变性。

在上述的PoS协议中，Algorand是一个块wiseBA协议，而其他所有协议都旨在最终达成共识。展望未来，我们的调查证明与最终共识PoS协议的设计相关；为了比较，我们在这里提到阿尔戈兰。

所有这些协议都必须面对克隆攻击的问题，这最终被认为比最初认为的更严重。另外的复杂性——在[BPS16]中被恰当地称为“后验腐败”——观察到，简单地检查时间戳将不足以处理远程攻击。事实上，攻击者可以尝试

1.参见用户量子机械师https://bitcointalk.org/index的帖子。php?主题=27787.0和随后在2011年进行的讨论。

[2]请注意，我们只包括包含有足够详细的白皮书的PoS协议，cf。图2.

978-1-5386-7204-4/18/$31.00©2018IEEE85
DOI 10.1109/CVCBT.2018.00015

破坏与该系统历史上过去时刻拥有大量股份的账户相对应的密钥。假设这些账户目前的股份很小（甚至为零），它们非常容易受到贿赂（或简单的粗心大意），这样会将他们的密钥暴露给攻击者。有了这样一组（目前是低风险的）密钥，攻击者可以发起远程攻击，在这种情况下，时域中的结果区块链的密度可能与诚实生成的公共区块链难以区分。

为了解决后路腐败和其他远程攻击，已经采用了一些减轻罪行的方法（有时结合使用），可以分为三种类型：

(i)引入某种类型的频繁检查指向机制，它可以通过提供一个相对最新的块来将节点引入到系统中。

(ii)采用密钥进化密码学[Fra06]，要求用户发展他们的密钥，使过去的签名不能被伪造，即使完全在他们当前的秘密状态发生暴露。

(iii)执行严格的链密度统计，其中协议任何步骤的参与参与者的预期数量已知；因此，表现出明显较少参与的替代协议执行历史可以立即被视为对抗性。

在上述PoS方案中，所有最终的共识协议(即NXT、PPCoin、杜鹃花、白雪公主和杜鹃花螯虾)都采用了第一种缓解策略，并采用了某种形式的检查点。Ouraroros采用第一种和第二种方法（密钥进化签名）来额外处理自适应腐败，而阿尔戈兰德采用第二种和第三种方法（严格的链密度统计）。

值得欣赏这些处理后路腐败和远程攻击的方法之间的区别。检查点通过允许节点忽略与节点已知的最近的检查点不一致的替代链，从而完全消除了这个问题。然而，这附带一个重要的模型限制：对于任何类型的检查指向工作，节点必须经常在线（因此他们采用最近的检查点块）或在长时间的离线（重新)引入系统后（或第一次加入时）接收可靠（受信任的）信息。这相当于系统安全运行所必需的额外信任假设，因此在分散的、无许可的设置中显然是不可取的。类似地，执行严格的链密度统计需要可靠地估计协议的任何阶段的参与者数量，并且还限制模型：协议将不能在允许调用任意数量的各方进行执行的环境中运行。另一方面，密钥进化密码学是一种更算法的缓解，对模型有最小的要求：节点应该仅仅有消除私有状态的能力。算法缓解似乎比限制模型的缓解更可取。

重要的是要注意，密钥进化密码学，上面列出的唯一算法缓解，特别关注关于后腐败问题；特别是，尚不清楚关键进化是否能阻止所有可能的远程攻击。因此，我们的工作的动机是基于以下问题：

> *密钥进化的密码学是否足以防止所有可能的远程攻击，并以这种方式实现不需要依赖任何模型限制缓解措施的PoS?*

A.我们的结果

我们通过引入一种新的针对最终共识PoS协议的远程攻击，来回答上述问题。打桩出血是一种有效的不依赖于后路腐败的远程攻击策略；因此，它不能通过密钥进化的密码技术来预防。对该攻击的唯一要求是，底层的区块链协议允许交易费用被用作运行该协议的奖励，这是区块链协议中的一个标准特性，以鼓励参与账本维护。

攻击的想法是：一个攻击利益相关者少数派联盟发起一个远程攻击，同时包括在诚实维护的公共区块链中发布的所有交易。鉴于交易的费用将用于奖励产生的那些块在某种程度上，大量的交易费用在私人攻击者区块链将收集的恶意联盟（费用来自账户不存在于私人链必须被没收）。假设区块链系统已经运行了相当长的一段时间，可以想象，累积的交易费用将把攻击的少数民族联盟变成多数派，能够以比诚实维护的公共区块链更快的速度推进私有区块链。由于远程攻击的低成本模拟性质有可能安装流血攻击从过去的任意点（假设检查点没有使用或充分扩展到过去），因此攻击联盟可以重写事务的历史。

我们证明了攻击者必须回到PoS系统的历史上才能发起攻击的理论界是≈(2-4αA)/f，其中αA表示少数民族联盟的相对股份，f是每单位时间提供的相对费用。

使用比特币区块链作为可行性评估的基础，[3]2017年11月3日，每个区块的1天平均交易费量为2.28BTC。[4]同一天发行的BTC的发行量约为1666万份，[5]相对费率为$1.36 \cdot 10^{-7}$.由此可见，按照目前的速度，一个假设的与比特币具有相同的收费-货币特征的PoS区块链将只具有理论上的意义。然而，每单位的总交易费用增加了20倍

[3]请注意，这只是为了举一个例子，因为比特币区块链对远程攻击免疫。需要考虑的一点是一个假设的PoS-
基于区块链，具有与比特币相同的统计特征
车链

[4]https://www.smartbit.com.au/charts/transaction-fees-per-block

[5]https://blockchain.info/charts/total-bitcoins

攻击者相对利害关系	运营年限
0.1	11.11
0.2	8.33
0.3	5.55
0.4	2.77

图1：区块链历史需要发起利益相关方攻击，假设最低相对交易费量为$2.73 \cdot 10^{-7}$每分钟(根据假设的PoS区块链的最近（2017年11月3日）比特币区块链的价值增加了20倍)。

时间[6]木桩出血攻击是可行的，30%的攻击者需要不到6年的历史。图1。特别是，这表明利益流血攻击必须是长期PoS区块链系统的一般威胁模型的设计考虑。

然后，我们考虑可能的缓解策略。首先，我们可以观察到，桩流血攻击将导致私有区块链最初在时域中显示稀疏块密度，并逐渐增加。这对于诚实维护的区块链可能是不典型的，可以作为链选择规则的一部分来使用。*然而，更容易实现的不同缓解措施是在每个事务中引入上下文：上下文敏感事务是包含最近某一点区块链散列的事务*。很容易看出，这样的交易不能转移到一个由恶意的利益相关者私人维护的替代区块链。我们注意到，这种缓解以前已经考虑过不同的目的；参见[Lar13]，它被用来防止攻击者将“硬币销毁”转移到秘密维护的区块链。

最后，我们在图2中说明了远程攻击的系统化演示、它们的需求以及减轻它们的方法。我们观察到，如果删除检查点机制，木桩出血攻击将对所有目前提出的最终共识PoS协议产生不利影响。因此，在未来的任何努力中，要从这些协议中删除不可取的检查点机制，以及在设计不依赖于检查点的新的最终共识PoS协议时，都必须考虑到这一点。在事务中引入上下文敏感性是一种简单的“算法”缓解机制，因此可以添加到PoS区块链协议的设计武库中，以放松模型假设，如可忽略的交易费用或频繁的检查点。

II .初步的

A.计算模型

即使在一个提供了许多优势的慷慨的计算模型中，也可以发起木桩流血攻击

[6]请注意，这并不一定意味着每笔交易的费用需要增加；区块链系统在每单位时间内处理大量的交易就足够了。实际上，20倍的增长(从1MB增加到20MB)是2015年期间各种激烈辩论的提议之一16，最终导致比特币区块链的硬分叉。有关20倍增长背后的原始理由，请参见http://gavintech.blogspot。co.20兆字节的测试结果。html.

到区块链协议：

对手不需要对消息传递进行控制：攻击可以在一个完全同步的通信和计算环境中启动，所有的消息——包括那些由对手生成的消息——都由可靠的广播传递。

对手不需要动态的腐败：攻击可以由在执行开始时确定的一个固定的对抗方集合发起。

对手不需要引入新的政党或不需要取消诚实的政党：攻击可以由完全参与的政党的静态人口发起。

下面，我们概述了一个简单的、强大的计算模型，反映了上述特征。该模型是通过适当加强[KRDO17]的框架得到的，并足以支持我们的攻击。我们强调，采用这样一个强大的模型只会扩大攻击的适用性和强度，这可以在典型的区块链模型中启动，这些模型可以为对手提供显著更多的能力[GKL15]、[PSS17]、[BPS16]、[DGKR17]。

a)时间、插槽和同步：我们考虑一个设置，其中时间被明确地划分为被称为插槽的离散单元；参与方配备了指示当前插槽的同步时钟。该模型还允许可靠的同步广播：各方可以在每个时槽的开始广播一条消息，然后在时槽结束时可靠地传递给所有其他各方。

b)对抗性腐败：该模型涉及到参与各方八的固定集合。在我们的模型中，对手A与对抗方的固定子集相关联。我们超载符号A来表示对抗方的子集；诚实当事人的集合表示为H。诚实的各方随时活跃，接收其他各方发送的所有信息，并遵守正在考虑的协议。对手在每个槽中被激活，可以任意指导对抗方的行为。请注意，敌对各方发送的消息受广播约束——它们同步传递给所有诚实的各方。

c)INIT功能：初始股份和事务；环境：该模型与（理想化的）初始化功能INIT相关联。INIT功能由初始股份分配参数化。这是一个非负数分配给玩家，我们写成$S_0=((U_1,s_1),\ldots,(U_n,s_n))$.功能$\mathrm{INIT}^{S_0}$操作如下：

在对双方进行任何计算之前，该功能将为每个双方的U∈八确定一对公钥和私钥(pk_U, sk_U).

在协议期间，该功能用sk响应来自表单键的用户U的消息U，即密钥sk_U的用户U。

在协议期间，该功能响应于形式起源的任何信息_带有“起源块”B的块0包括初始股份分配和与用户相关联的公钥。

该模型进一步引入了一个实体：环境Z。在我们的环境中，环境仅仅是负责产生环境的原因

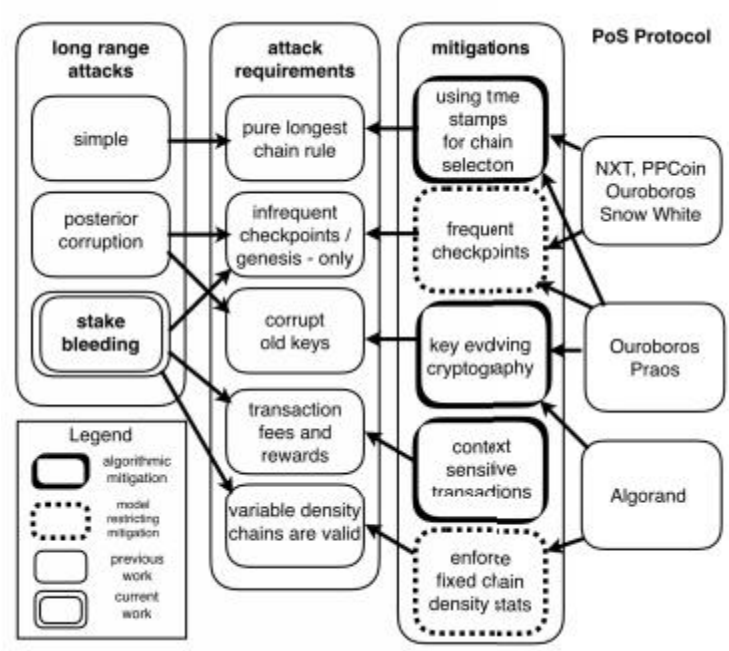

图2：远程攻击的概述，相关的攻击需求，可能的缓解措施和我们的结果。术语“纯最长链规则”指的是将区块链的长度视为唯一标准的链选择规则。如果缓解通过强化协议而不削弱模型的情况下防止攻击，则被归类为算法；如果它加强模型假设，将攻击置于模型之外，或者以一种重要的方式与比特币等分散区块链协议的预期操作设置不一致，这就是对执行环境的模型限制。请注意，Algorand是一个块级ba协议，其他描述的协议都是最终的共识类型。我们包括所有存在足够详细白皮书的PoS协议(具体是PPCoin[KN12]、NXT[Com14]、阿尔戈兰德[Mic16]、机器人[KRDO17]、白雪公主[BPS16]和Praos[DGKR17])。其他的，如Casper和比特股没有充分的记录，不能包括在比较中。*

*具体来说，Casper[BG17]的描述仅仅在一个非指定的PoS系统上提供了一个“最终”层；关于比特共享[SL15]，可以在htth：//docs的分布式共识白皮书中找到。bitshares .org/bitshares/papers/index .HTML不可用（已于2018年3月4日检查）

交易，作为向双方提供的输入。特别是，在每一轮协议中，环境可以为各方提供一个事务集合；这些有形式(U，U\它要求将其股份从U方转移到U方\.(对于我们的攻击，将环境仅仅看作是交付给各方的固定交易时间表就足够了。请注意，典型的区块链安全模型将赋予环境更大的能力：面向对手的信息通道、事务的自适应选择、消息传递的调度等。)

最后，给定一个初始化功能$INIT^{S0}$和一个环境Z，一个协议的执行由起源块B组成0、当事人的密钥、环境传递给玩家的交易序列，以及玩家播放的整个消息序列。

B. 区块链，分类账和股权证明协议

a)事务分类帐属性：区块链是一种数据结构，它与每个时间段（最多）一个块相关联。单个的块由事务的集合组成，

除了特定于协议的元数据之外。在上述模型的背景下，我们假设发生块B0在任何区块链中显示默认初始块，与时间0相关。一家连锁店也会立即诱发一种股权分配，SC，通过将链中的交易应用于起源块的股份分配。对于区块链C，我们让C「!表示去掉最后一个！所得到的C的前缀！赛跑者起跑时脚底所撑的木块

直观地说，区块链协议Π允许一个当事人集合共同维护一个公共分类帐。我们将重点关注，事实上，为每一方（在每个时间点）维护一个单独的账本的协议；公共账本的概念是由协议Π的适当的持久性和活动性特性所保证的：

持久性。一旦系统的一个节点宣布某个事务tx是稳定的，其余的诚实节点，如果被查询，将报告在分类帐中相同位置的tx，或者不会向tx将冲突的任何事务报告为稳定的。在这里，稳定性的概念是一个由安全参数k参数化的谓词；具体来说，a

当且仅当事务出现在C中时，事务才被声明为稳定的(由具有链C的一方)「k.

活力。如果系统中所有诚实的节点都试图包含某个事务，那么在经过u槽对应的时间（称为事务确认时间）后，所有节点如果诚实地查询和响应，将报告该事务是稳定的。

直观地说，一个安全的区块链协议Π保证这些属性由诚实的当事人持有的账本（记录在区块链中）所拥有，在对对手a的适当约束下。

b)链选择规则；最长链规则：我们将注意力集中在由链选择规则定义的协议上：协议的每一步都要求某些玩家播放区块链；然后玩家应用一个选择规则，这可能会导致用一个广播链替换他们的本地链。我们关注的是“最长链规则”：检查广播区块链的有效性——一个依赖于协议的属性——随后，采用最长的有效链，包括玩家持有的链。（长度只是方块的数量；为了具体起见，我们假设联系在字典学上被打破了。）

c)股权证明协议：我们关注通过股权证明协议Π维护的分类账，该协议授予将链扩展到U方的权利，其概率与该方在链中的股份（前缀）成比例。

股份比例增长。一方被允许扩展给定链C的概率(一个表示为扩展机会的事件Π)与该方控制的股份成比例C“问，由C「!.这里是一个特定于协议的参数，通常与上面讨论的安全参数k相关。

我们有意地在上面的描述中模糊了概率空间的细节，因为这取决于潜在的股权证明协议的细节。此外，我们忽略了下面定理1中的“持久性深度”问题，简单地设置！= 0.考虑到这一点将改变结论！因子

d)相对股权和诚实多数：作为一个符号问题，对于一组当事人X和一个股权分配S，我们用S(X)表示双方在X中持有的股份。在执行区块链协议（通常从上下文中理解）的特定时刻，我们让αX∈[0,1]表示双方在X中的相对股份。具体来说，这是数量SC(X)/SC(U)其中C是诚实用户所持有的链。（请注意，由于广播的假设，所有诚实的玩家在每个插槽中都持有相同的最长的有效链。）我们说，一个执行的Π有一个诚实的多数，如果αA<1/2在协议的每个步骤。

*e)区块奖励和交易费用：大多数区块链协议涉及某种形式的块奖励和交易费用。*为了能够对所有考虑过的协议进行通用的语句，让我们介绍以下符号：

费用Π(E，i)表示Z在执行E的插槽i中创建的所有新交易的总费用（作为总股份的一小部分）。

报酬Π(C，i)表示由协议Π创建的硬币总量，并给在槽i中区块链C中创建块的一方的硬币总量。

传输X →Y(C，i)表示插槽i中区块链C中X方转移给Y方的总金额。

III .流血的攻击

A.攻击描述

我们首先非正式地描述了我们的攻击是如何在由协议Π定义的通用股权证明区块链的上下文中操作的。为了简化演示，我们假设整个攻击者控制了一定比例的股份αA< 1/2.

对手A模拟诚实协议Π，并按照该协议的规定维护当前区块链(表示为C)的本地副本。此外，它还维护了一个替代区块链，它最初是空的，并且对诚实的各方隐藏。Ĉ

对手检查每个时隙，是否允许扩展链C还是根据协议Π的规则。Ĉ它跳过了扩展C的所有机会，因此对它的增长没有任何贡献。ĈĈ另一方面，每当扩展的机会，扩展与一个新的块，并插入到这个新块的所有事务从诚实的链尚未包括在有效的上下文（或尽可能多的Π允许的规则）。ĈĈĈĈ这使A有权获得（打开）任何块创建奖励和来自所包含的交易的任何交易费用。

随着协议的进展，C和C都将增长，C增长得更快。ĈĈ虽然A在C上的相对股份可能会因为C中区块创造者的块创造奖励而减少，但由于块奖励和交易费用，它在链上的相对股份将会增加。在一些关于交易费用和区块奖励的相对规模的现实假设下(在第三节-B中阐明)，C的对抗性相对股份最终将超过C的诚实相对股份。ĈĈ从这一点上，链比链C（预期）增长得更快，最终变得更长。如果Π使用将来拒绝块的普通最长链规则，那么A现在很容易通过发布来违反账本的持久性，这将被Π之后的所有诚实的各方所采用。Ĉ此外，如果A在发布前增加了一笔交易，将足够的股份转让给诚实的当事人，以不再控制多数，则不会违反中所述的“诚实多数”假设Ĉ
第二节B。

图3给出了对执行我们攻击的对手的更简洁的描述。该描述使用了一个通用的扩展机会Π(C)谓词，当允许A根据Π的规则扩展给定的链C时，均为真。此外，长度(C)表示从对手的角度来看，链C的长度。

B.攻击分析

股权证明协议Π必须满足几个属性，以便容易受到中描述的攻击

对手A

根据Π和它自己的私人链，对手A保持着它对公共链C的看法；两者最初都是空的。在A以下是Π，但有以下例外情况：

. 在服务机会Π (C)：什么也不做。

. 在服务机会Π（）：扩展一个新块，包含尚未来自C的所有事务，并且不影响根据Π的有效性。保持隐私。

. 长度()，>长度(C)：将多数股权转让给H。根据Π进行发布。

图3：对手A对抗最终达成共识的利益证明协议Π。

第三节-A。主要要求为：

(i)没有频繁的检查点。协议Π必须按照最长链规则运行：在诚实各方看到的所有有效链中，Π规定他们采用最长的链。

虽然可能会偏离这一要求，但Π必须允许长到过去很长时间的重组：如果指定了重组的最大深度且很小(i。e.，Π不允许一个诚实的政党改变其对主链的观点超过几个区块（或插槽）到过去，即使有一个更可取的候选链），那么攻击就不适用了。

(ii)交易费用。该协议Π必须涉及交易费用，或者更广泛地说，从交易各方向维护分类账的各方进行的任何硬币转移。更详细地说，只有最终比C快，攻击才会成功。由于C的生长速度(回复。)与诚实当事人的相对持股比例成正比。在的对手)，我们需要后者最终超过前者。

观察，当它创建一个块时，对手在每个槽i中的相对股份增加：

这个块的奖励Π(,i);

所有从诚实方到敌对方的转移H→A(,i);

沙痂所有的费用

$$\sum_{j=i+1}^{i} \text{费用}\Pi(E,j)$$

对于在槽i之后的所有槽j≤i包含中的前一个块。另一方面，当在C中通过奖励创建一个块时，诚实方在C中的相对比例都会增加Π（C、i）（不收取任何费用Π，因为C中的所有费用都是由诚实的当事人支付的)；并通过转移而减少H→A(C,i).

我们假设

$$\text{传输}A\to H(C、i)=\text{传输}A\to H(,i)=0.$$

(iii)与上下文无关的交易。根据Π产生的有效交易需要忽略在区块链中使用它们的上下文：Π必须允许A从C获取事务并在不同上下文中使用它们。

(iv)低增长链的有效性。Π协议必须支持“沉睡的多数”，以确保只有少数利益相关者扩展的链（因此在一开始表现出小链增长），根据Π的规则仍然被认为是有效的。

在下面的定理中，我们给出了执行攻击所需的槽数的估计，作为初始对抗性股份α的函数A以及在每个时段的交易中产生的费用金额。为了简单起见，我们分析了案例1/3<αA<1/2，即使攻击适用于任何不变的αA>0（有关显式绑定，请参见本部分末尾的注释）。

定理1。*假设Π是一个股权证明区块链协议，其股权比例增长满足上述(i)-(iv)的条件。考虑使用图3中给出的对手a执行协议Π。假定*

$$\text{传输}H\to A(C,i)=0,$$
$$\text{报酬}\Pi(C,i)=\text{为}0,\text{和}$$
$$\text{费用}\Pi(E,i)\geq f$$

在执行E和两个C∈{>，}和所有的i>0。让1/3<αA<1/2表示对手A的初始相对股份。设T表示长度为()>、长度为(C)的插槽。然后我们有

$$E[T]\leq\frac{3-6\alpha A}{f}$$

而T将紧密地集中在它的期望周围。

证明：让α_P对于P∈{A，H}，C∈{C，}和i>0表示链C中玩家P集合的相对股份在槽i中(记得A和H分别表示对手和诚实的一方)。此外，允许长度$_i$(C)表示链C的长度从对手的角度来看。那么不等式E[长度$_T$( )] > E[length$_T$(C))转换为（由于利益相关者比例增长的假设）

$$\sum_{i=1}^{T}\alpha_A[i]>\sum_{i=1}^{T}\alpha[i].\quad(1)$$

因为奖励Π(C, i)=0和C中的费用都由诚实的方支付（和收到），我们有$\alpha_H:=\alpha[i]=1-\alpha_A$对于所有的i>为0，因此

$$\sum_{i=1}^{T}\alpha[i]=T(1-\alpha_A).$$

要下界在（1）左侧的和，请定义T1（分别为T2），为满足α[T]的最小插槽$_A$1] ≥ αH(分别α[T$_A$2] ≥ 2αH-αA).由于相对股份α$_A$每个插槽至少增长f[7](A包括所有

[7]我们在这里忽略了只有在交易被包含在一个块中之后，实际的股份才会增长，但是这对我们的论点没有明显的影响。

从C到的事务)，我们得到了α $\hat{C}_A$+(T1− 1)f ≤ 1 − α A(T也是如此2)，这给了我们

$$T_1\frac{1-2\alpha_A}{f}\leqslant+1\text{和}T_2\frac{2-4\alpha_A}{f}\leqslant\ +1\ .(2)$$

$\overset{C}{A}$现在注意，α [i]的下界是

$$\begin{cases}\alpha_A\text{为我}<T_1.\\ (2-3\alpha_A\text{为我}\geqslant T_2.\end{cases}$$

因此，对于满足的任何T，（1）都将被满足

$$\alpha_A(T_1-1)+(1-\alpha_A)(T_2-T_1)+(2-3\alpha_A)(T-T_2+1)>(1-\alpha_A)T\ .$$

（3）使用（2）和求解T给出了我们所期望的界。

浓度源于C和某些槽i的长度是由一个和决定的$\hat{C}$独立的随机变量为每个槽1≤j≤i。■

我们注意到，我们削弱了定理1的陈述有几种简化证明的方法。

首先，我们关注1/3的<α A<1/2作为定义T的事件2永远不会发生。尽管如此，很容易看出，虽然我们的攻击受益于更高（低于50%）的初始对抗性股份，但它也可以通过α来执行A<1/3与一个稍微修改的分析。

第二，定理1假设为零的方块奖励，并从H转移到A。然而，回想一下转移H→A（C、i）完全由环境控制，仅受第II-A节所述的限制。（这是为了捕捉区块链协议的安全性不依赖于任何关于要存储在分类账中的交易的特定假设；相反，它必须对任何这样的交易序列安全地操作。）因此，对于任何奖励Π(C，i)，同样的分析适用的情况，可以简单地通过设置转移来实现H→A(C，i)，以使C中的诚实股份比率保持不变（因为中的对抗性股份比率将持续增加）。$\hat{C}$另一方面，非零奖励Π$\hat{C}$(，i)只会让攻击更快地成功。

最后，观察到我们在分析中相当悲观，降低值α [i]，好像它们除了在插槽T$\overset{C}{A}$1和T2.通过更仔细的计算，我们可以得到一个更好的界T≈(2-4α A)/f .

C.对现有PoS协议的影响

我们现在总结了第第三-B节中描述的先决条件在多大程度上得到了满足，这些协议来自学术文献和现实世界的部署，这意味着利益流血将是它们的考虑因素。我们主要关注最终的共识协议，但是我们要注意到我们的攻击概念对块级ba设置的适用性。[8]所有最终的共识协议都采用了某种形式的检查指向，大概是为了防止后路腐败攻击；这一般对策也以琐碎（和模型限制）方式防止桩出血攻击（和任何其他远程攻击）。有趣的是，如果我们删除检查点，所有被考虑的最终共识结构都容易受到我们的攻击，因为它们都满足第III-B节中的条件(ii)-(iv)：他们承认交易费用，他们的交易是上下文无关的，低增长的链被认为是有效的。更详细地说，我们有以下内容。

NXT和PPCoin。*NXT协议只允许重新组织最后的720个块，因此形成了一个所谓的移动检查点和违反第III-B节的条件(i)*。在PPCoin[KN12]中也采用了类似的检查指向机制。

素洁白雪公主协议[BPS16]还使用移动检查点来防止后腐败攻击，而且没有它也容易受到木桩流血攻击。

[Ouroboros[KRDO17]使用移动检查点作为其最大有效链选择规则的一部分，中和了克隆体攻击。如果没有检查点，Ouroboros将容易受到后路腐败和木桩出血的攻击，因为它不使用密钥进化的密码学。

它的Praoros[DGKR17]使用了与它相同的最大有效链选择规则，设置移动检查点。如果没有这种对策，欧罗博罗斯普罗斯仍然会中和后腐败攻击，因为它使用了关键进化签名签名块；然而，它很容易受到我们的股份流血攻击。

Algorand[Mic16]，如前所述，并不是一个最终的共识协议，而是遵循块级ba方法。尽管如此，我们还是可以考虑到股份流血攻击的核心思想对阿尔戈兰德的适用性，目的是创建一个替代的区块序列，并利用股份流血来获得暂时的多数股权。然而，在Algorand的情况下，由于需要足够多的利益相关者来证明每个BA的结果，这可以被视为违反了第III-B节中的要求(iv)。事实上，Algorand强制执行了一个严格的参与规则，因此它总是可以以一种模型限制的方式找到正确的协议执行。

如前所述，上述结果表明，任何从这些协议中删除模型限制假设的尝试都需要至少采取一些针对木桩流血攻击的对策。我们将在最后一节中讨论这些问题。

增值缓解措施

补救我们的攻击的一种自然方法是修改协议Π，以违反至少在第III-B节中给出的要求之一。对于需求(i)或(ii)这样做将导致检查点服务的信任假设，或导致另一个限制模型的限制，将整个协议执行过程中的事务费用限制在不重要的金额内。因此，我们更愿意关注两种替代的方法，算法缓解措施，旨在违反要求(iii)和(iv)。

a)时域最小链密度：可以用来减轻桩出血攻击的第一个观察结果是由攻击产生的区块链

[8]请注意，我们只包括包含有足够详细的白皮书的PoS协议，cf。图2。

有一个周期，其中区块链的密度相当稀疏。接下来我们澄清密度的概念：在所有的PoS协议中，允许一些各方可能不会一直在线（尽管他们被选中参与协议）。通过观察区块链，就可以检测到他们没有参与。例如，在Ouroboros[KRDO17]的情况下，将会有许多“插槽”为空，没有相应的块；在其他协议中也存在类似的可观测量。这允许协议检测和清除具有此缺陷的区块链，从而将它们与诚实各方产生的正确区块链区分开来。我们在这里不再进一步追求这个方向。

b)上下文敏感的事务：一个基本的　股权流血攻击的特点是“断章取义”。e.，将其从诚实维护的区块链复制到攻击者维护的私有区块链中。防止这种情况发生的一个非常简单和有效的方法是包括“上下文”，i。e.，最近块的散列。这个想法已经讨论了姿势设置至少早在拉里默的工作[Lar13](参见[Lar18])引入它，以确保攻击者的秘密链不能利用诚实的政党的交易增加秘密链的总价值他们维护（作为“硬币年龄破坏”是一个建议机制的姿势提出）。在这里，我们用它来实现一个不同的目标：防止交易费用在一个私人链中的一段时间内“流血”给恶意的各方。使用上下文敏感性，事务的有效性将需要在区块链中存在该散列。这只会允许反向生成的交易转移到私有区块链，从而完全中和攻击（因为私有区块链不再有诚实的“流血”）。我们注意到，在[BPS16]第2.2.2节中提出了一个看似类似的缓解措施，以解决另一个不同的问题，即攻击者试图分叉区块链以收集事务　诚实的参与者在过去几个街区内所支付的费用。建议的缓解措施要求该交易包括一个最近的区块指数，而且不足以防止股权流失。相比之下，本节中定义的上下文敏感性要求事务包含最近块的散列。

V.结论

我们提出了一种新的远程攻击，称为桩出血攻击，适用于所有调查的最终共识PoS协议操作时，没有任何模型限制假设。考虑到当前加密货币的统计数据，一场木桩流血攻击需要区块链多年的历史才能成功，因此它们不会立即引起关注。然而，他们从密码学的角度指出了一个重要的设计考虑。他们展示了如何在不依赖后腐败的情况下发动克隆攻击，实际上不利用任何腐败的适应性。由此还可以很容易地推断出，密钥进化密码学本身并不足以缓解远程攻击，而且研究在无信任、无许可的环境中阻止长时间愤怒攻击的其他算法缓解措施是很重要的没有诉诸于检查点或其他模型限制假设的环境。

确认。

阿格洛斯·基亚亚斯得到了地平线2020研究和创新计划、项目特权的部分支持，资助协议编号为780477。亚历山大·罗素部分得到了美国国家科学基金会对No.的资助1717432.

参考文献

[bg17] 维塔利克·布特林和维吉尔·格里菲斯。卡斯珀是一个友好的终结小玩意。CoRR，abs/1710.09437，2017年。

bgm14 伊多·本托夫，艾丽尔·加比森和亚历克斯·米兹拉希。没有工作证明的加密货币。CoRR，abs/1406.5694，2014年。

bps16 伊多本托夫，拉斐尔帕斯，和伊莱恩施。白雪公主：可证明的安全证据。密码学ePrint档案，报告2016/919,2016。http://eprint.iacr.org/2016/919.

但14] 维塔利克布特林。远程攻击：具有自适应工作证明的严重问题。https://blog.以太坊。org/2014/05/15/long-range-attacks-theserious-problem-with-adaptive-proof-of-work/，2014.

Com14 NXT社区。NXT白皮书。https://bravenewcoin.com/assets/Whitepapers/NxtWhitepaper-v122-rev4.pdf，2014年7月。

[数据库17] 贝尔纳多大卫，彼得盖，阿格洛斯基亚尼亚斯，和亚历山大罗素。一种自适应安全的、半同步的股权证明协议。密码学ePrint档案，报告2017/573,2017。http://eprint.iacr.org/2017/573.出现在EUROCRYPT 2018.

Fra06 马特富兰克林。对密钥进化密码系统的调查。*Int。J.安全与网络，1（1/2），2006年。*

[gkl15] 胡安A。加雷，阿格洛斯基亚斯和尼科斯莱奥纳多斯。比特币骨干协议：分析和应用程序。《伊丽莎白·奥斯瓦尔德和马克·费施林》，编辑，欧洲墓穴2015，第二部分，LNCS第9057卷，第281-310页。2015年4月，海德堡。更新版本在http://eprint。iacr.org/2014/765.

[kn12] 阳光金和斯科特纳达尔。个人硬币：带有股权证明的点对点加密货币。https://peercoin.资产净值、纸张、佩尔币纸。pdf，2012年8月。

krdo17 阿格洛斯·基亚斯、亚历山大·罗素、贝纳多·大卫和罗曼·奥利尼科夫。一个可证明的安全的股权证明区块链协议。在乔纳森·卡茨和霍瓦夫·沙查姆，编辑，加密货币2017，第一部分，LNCS第10401卷，第357-388页。施普林格，海德堡，2017年8月。

Lar13 丹拉里默。交易作为股权证明。https://bravenewcoin.com/assets/Uploads/TransactionsAsProofOfStake10.pdf，2013年11月。

Lar18 丹拉里默。委托的股权证明共识。https://bitshares.org/technology/delegated-proof-of-stake-consensus/，访问了21.3.2018，2018年。

麦克风16 硅胶。高效和民主的账本。CoRR，abs/1607.01341，2016年。

[坡14] 安德鲁·波尔斯特拉。从股权证明上的分布式共识是不可能的。https://download.wpsoftware.net/bitcoin/old-pos.2014年5月。

[坡15] 安德鲁·波尔斯特拉。关于利害关系和共识。https://download.wpsoftware.net/bitcoin/pos.pdf，2015年3月。

PSS17 拉斐尔·帕斯，利奥尔·西曼和阿比希·谢拉特。对异步网络中的区块链协议的分析。*在让-斯巴斯蒂安·科伦和杰斯珀·布乌斯·尼尔森，编辑，欧洲加密2017，第二部分，LNCS第10211卷，第643-673页*。施普林格，海德堡，2017年5月。

[sl15] 费边·舒赫和丹尼尔·拉里默。比特股票2.0：Gen-局域网概述。https://bravenewcoin.com/assets/Whitepapers/bitshares-general.pdf，2015年12月。