共识机制的安全问题

一、简介

区块链是一种新兴技术，允许在短时间内执行数字交易。它是一种安全介质，通过对等 (P2P) 网络共享信息来工作。单个实体的共享信息可以到达网络中的所有参与者，而且不会被私自篡改数据。除了加密交易之外，它还被用于各种其他目的，例如确保知识产权、生成金融合同、追踪食品生产和追踪供应链。这项技术时常受到各种恶意攻击的阻碍：诸如 Sybil 攻击、Eclipse 攻击、边界网关协议 (BGP) 劫持和 51% 攻击等。其中，51%攻击被安全研究人员忽视，主要是因为攻击成本巨大。然而，最近的攻击已经证明 51% 攻击可以在各种现代加密货币上执行。与其他共识协议相比，工作量证明 (PoW) 共识协议是 51% 攻击的直接威胁。最近的攻击主要针对依赖 PoW 的加密货币。

二、共识机制的问题

1、工作量证明（PoW）

工作量证明 (PoW) 是一种基于求解数学方程的共识机制。PoW 最初由比特币发起，随后被许多主要的加密货币迅速推行。矿工是 PoW 共识的主要支柱。授权和记录交易的过程是由矿工批准的。PoW 共识要求矿工付出相当大的努力来挖掘一个区块。该过程主要是在反复试验的基础上尝试答案的随机方法。因此，求解方程可能需要进行一次甚至数千次尝试。为了识别“目标哈希”，它必须包含比块的哈希值小的数字。PoW 共识假设一半的网络节点始终是诚实的矿工；因此，获得超过一半的哈希算力会使这种共识变得脆弱。PoW 的显着缺点之一是能源成本和硬件要求。研究表明，全球比特币挖矿过程的用电量远远超过 159 个国家。其实，由于各个加密货币使用的算法不同，挖掘要求和挖掘时间可能会有所不同。

与其他共识协议相比，PoW 的挖掘过程相对较慢。由于少数矿池拥有大量挖矿能力，因此对这些矿池的攻击可能会对比特币网络造成严重破坏。最近的攻击证明，PoW 容易受到 51% 攻击。使用 PoW 共识的低哈希加密货币更容易受到 51% 攻击，因为可以轻松获得所需的哈希。P + epsilon 攻击可以在拥有所需预算的情况下免费执行。

Sybil 攻击可以通过形成大量恶意节点来成功利用 PoW。以太坊协议和私有区块链容易受到余额攻击。此外，DDoS 攻击和 BGP 劫持也可以用来中断这种共识机制的常规流。AntPool、BW.com、NiceHash、CKPool 和 GHash.io 是一些已经受到 DDoS 攻击的矿池。

2、权益证明（PoS）

权益证明 (PoS) 是一种共识机制，它根据参与者投入网络的权益来授权区块。拥有大量硬币的矿工比其他参与者拥有更多的权力。Peercoin 是 2012 年第一个使用这种共识的加密货币。遵循随机过程来考虑下一个区块的创建者。该过程涉及获取有关加密货币总量的详细信息，以及它的维护时间。PoS 共识的优势在于它不需要参与者通过 PoW 等昂贵的挖矿过程。

PoS 由于其中心化属性而易受攻击。在持续投入大量财富的同时，参与者成为网络中的强大实体，也能够影响网络的福祉。通过获得大部分供应，恶意的利益相关者可以利用无利害关系的问题。PoS 的主观性较弱，实施过程也非常复杂和具有挑战性。要进行 51% 攻击，攻击者需要获得 51% 的不同加密货币。然而，获得总股份的 51% 的成本可能是巨大的。因此，与 PoW 相比，51% 攻击的威胁级别可能较低。研究表明，PoS 可以被远程攻击利用。P + epsilon 攻击无法执行，因为攻击者需要获得大量预算来为参与者提供保证金，同时投票给少数人。PoS 可以被 Sybil 攻击利用，DDoS 攻击也可以破坏部分网络。

3、委托权益证明（DPoS）

委托权益证明 (DPoS) 是一种共识机制，允许股东为证人投票。DPoS 的主要思想是减少能源浪费，提高交易速度。整体出块过程使得这种共识机制比 PoW 共识快很多倍。DPoS 包含每股一票的政策，这使利益相关者可以选择在拥有更多硬币的同时投更多票。见证人因生成区块而获得奖励，但当他们未能执行所需任务时，他们也会受到惩罚，导致他们无法获得报酬并被投票淘汰。证人必须从随机的利益相关者那里获得最多的选票才能执行指示的任务。利益相关者还投票支持代表对网络进行改革和改变，并对其进行审查以做出最终决定。

DPoS 的开发旨在提高交易效率并克服各种其他共识机制引入的限制；但是，它包含严重的缺陷。它未能实现充分的去中心化，并且由于验证者数量众多，网络速度变慢。由于集中的方面，它可能成为随机攻击者的焦点。DPoS 容易受到

51% 攻击。攻击者可以说服利益相关者获得 51% 的投票权来执行 51% 攻击。这种共识机制也容易受到其他主要攻击，例如远程攻击、DDoS 攻击、P + epsilon 攻击、Sybil 攻击和平衡攻击。

值得注意的是，所有三种共识机制都可以被 51% 攻击利用，这使得这种攻击对攻击者非常有吸引力，特别是对于 PoW，获得必要的哈希算力成本较低。

三、51%攻击解决方案

1.延迟提交区块的惩罚系统

延迟块提交的惩罚系统建议修改 Satoshi 共识以保护网络免受 51% 攻击。惩罚系统建议广泛增加攻击成本，以使潜在优势无法获得利用。考虑一个块从区块链网络中隐藏的时间量而应用惩罚。时间是根据块之间的间隔持续时间计算的。这种安全保护技术将持续分叉通知全网，并在此期间限制参与者、矿工和交易所进行欺诈交易，直到延迟解除。这种防御机制主要针对私人开采的链，如果网络遭受分叉，则不予关注。

惩罚系统遵循方程（1），一个二次函数，确定要施加的惩罚水平。例如，假设一条真正的链包含从 553 到 558 的块，并且有一个攻击者设法产生了从 553 到 559 的块，那么将考虑攻击者引入的第一个块高度来计算惩罚。

$$DelayBlock = \frac{\sum_{i=1}^{n} n\,(n+1)}{2}$$

式（1）

2. 延迟工作证明 (dPoW)

延迟工作证明 (dPoW) 是 Komodo 的一种安全解决方案。他们开发了 dPoW 来防止双重支出问题。这种安全技术已经在大约 20 个区块链中使用。它适用于基于未使用交易输出（UTXO）的加密货币。dPoW 共识机制利用分配的 PoW 区块链来保存 Komodo 交易。因此，为了防御对 Komodo 区块链的 51% 攻击，任何现有的 Komodo 链副本都允许整个链控制恶意活动。该安全链的主要属性是它不识别最长链规则。它添加了一个安全层来防止攻击者执行 51% 攻击。但是，它还提供集成公证节点，以证明哈希对网络是否安全。dPoW 在全球部署了 64 个特殊节点，节点每年都会被选举出来以执行所需的任务。

3. PrilGuard

PirlGuard 是一种安全协议，旨在缓解 51% 攻击。它修改了共识算法以防止 51% 攻击。PirlGuard 协议基于 Horizen 的惩罚协议的属性，但主要是为 Ethash 构建的。当攻击者通过确认其私人构建的块开始与网络对等时，PirlGuard 通过惩罚立即放弃对等方以挖掘 x 个块。惩罚区块的数量取决于对手设法秘密挖掘的区块数量。

PirlGuard 还引入了由主节点控制的公证合同。主节点的主要任务包括对区块链进行公证，并通过检索 Pirl 区块链上的合法共识来惩罚恶意行为者。公证合同在 Pirl 和 Ethereum 区块链上实施。

4. ChainLocks

ChainLocks 是一种为保护 DASH 而开发的安全技术。它是实施长寿主节点仲裁（LLMQ）以减轻 51% 攻击的结果。ChainLocks 执行全网投票过程，其中包含“先见”策略。对于每个特定的区块，都会批准一个由大量主节点组成的 LLMQ。它要求每个参与者签署被注意到的块，以便可以扩展活动链。大多数参与者（60% 或更多）验证不同的块并生成 P2P 消息（CLSIG）以通知网络中的每个其他节点该事件。除非有足够多的成员遵守，否则无法生成（CLSIG）消息。该消息涉及真实性的有效签名，并且可由网络内的所有节点验证。在这种安全保护技术中，交易在第一次确认后得到确认。一旦确认，它就不能被撤销，因为签名的块不能在以后被确认。

5. 合并挖掘

合并挖掘是一种允许将多种加密货币合并到同时进行挖掘的技术。包含相同共识的低哈希加密货币受益于合并挖掘。他们可以通过引导包含更高哈希能力的其他货币来增加哈希能力。合并挖掘不是一种安全技术，但它是一种在使用时可以帮助缓解 51% 攻击的方法。两个网络中的交易按顺序进行，区块链分为父区块链和辅助区块链。除了增强安全性之外，另一个好处是矿工可以同时开采多个区块的能力。由于矿工对两种货币的整体哈希率做出贡献，这种技术建立了更高的安全性。