Security Analysis of Proof-of-Stake Protocol v3.0

(原文地址：https://bravenewcoin.com/assets/Whitepapers/Blackcoin-POS-3.pdf)

摘要

PoS 经过多年的测试已经证明其安全性。黑币的 PoS 3.0 技术中的优势已经解决了币龄（Coin-Age）、区块奖励（Block Reward）以及区块链预计算（Blockchain Precomputation）面临的问题。该协议是鲁棒的并且可以保持节点连接到网络。其抑制不活跃的节点。在这篇文章中，我们将高亮并概述其优势并且对该系统进行安全性分析。我们还概述了黑币中的想法，潜在地增加更高的安全性。

1. 介绍

密码学已经改变了金融和金钱的定义方式。最近，比特币[1]的出现已经展示了一个点对点网络可以如何通过解决“拜占庭将军问题”来组织伪造攻击（forgery）。从那时起，许多不同的在比特币基础上创造的币开放了源代码。主要有两种方法在网络上产生新的资金。第一种是“PoW”，第二种是“PoS”。PoW 后面的理论是维持一个数学的竞赛。第一个解决问题的计算机获得币奖励。这便使得币的分布变得完全公平。然而，这同时制造了一个能源浪费的问题。计算机为了竞争，便有了硬件的创造和装备竞赛。因此，金钱和能源在产生新币的时候被浪费。PoS 是在股东之间的竞争，其基于与网络的连通性和随机的机会，你就可以获得新的币。利息根据你的持有量产生。这就解决了比特币中的能源浪费问题，并引入了网络安全性新的挑战。在黑币中，我们将写一份该协议优势的技术分析并且为了尊重我们的前辈，会讨论潜在的提升和缺陷。PoS 最先在“点点币”[2]中实现。随后，PoS 的主要突破在黑币中产生，命名为“PoS 2.0”[3]和“PoS 3.0”。我们已经实现了 PoS 3.0 系统因为我们相信它将成为世界上最安全最高效的产生币的方法。我们将会概述并高亮这个系统的伟大安全性以及其解决的问题。

2. 安全性，币龄和攻击

维持币的竞赛的完全目的是为了避免攻击。交易的确认是给区块的获胜者的一项荣耀。然而，如果这个系统可以被用来赌博，那么它就会存在缺陷。在 PoS 中，你首先证明你有币的权限，并从那时起你可以精竞争并随机的赢得区块。越多的人参与竞争，则该区块越安全。币龄的概念是你持有币的时间越久你越有机会赢取一个区块。它的初始目的是刺激休眠的币持有人。然而，这实际上并没有鼓励一个节点保持连接到网络因为他们可以等奖励增加。并且，股东可以长时间断开网络连接，然后重连并赢得足够多的区块来冒着网络上 50%攻击的风险。时间计算会影响支出从而降低连接。而且，越少的节点连接，越容易获得大多数区块来伪造共识。并且，股份可以提前计算来使得攻击更有效率。时间戳被用在 PoS 中以获得时间的普遍观念。趋势计算被用来阻止伪造错误的时间戳。在 PoW 中，一个难度系数的增长或降低是由一个区块被多快时间产生决定的。然而，作为一种预防方法来阻止各种“定时攻击”，PoS 币使用中心化的检查点。

3. 所有问题都有一个解决办法

A. 币龄（Coin Age）

币龄由未使用的币的权重和它们闲置的时间来计算。计算公式就是“proofhash < coins • age • target”。

证据哈希（proof hash）是依赖一个股份修改器、未花费的输出以及当前时间的一个模糊总和的哈希。储存币龄的攻击在之前就被概述为不可能的[3]。其论证就是因为，由于币龄会在第一次消费之后重置所以很难实现联系不断的重复花费。然而，这也并非完全清晰的，因为一个输入可以被分成 1000 个输出。这或许为连续不断的重复花费攻击提供了可能性。但是，这仍然是一个难题，因为攻击者会需要维持极其大数量的资金使得其权重高于网络。理论上，这是说得通的。然而，如果我们注意黑币的分叉数量和其他主流的 PoS 系统，我们可以发现节点的数量是相当少的，并且这位一小部分的节点提供了特别大的权重。一个拥有很多币的持有者可能不想执行这个攻击，因为如果被发现，他们将会有损失他们股份的可能。但是这看上去可能是合理的，因为它仍然是一个攻击向量并且事实上是一个非常真实的攻击，所以这很可能是一个谬论。更重要的是，随着每天有如此多的币发行，保持尽可能多的节点连接是保持安全性所必需的。PoS 2.0 的解决方案：从等式中移除币龄——“proofhash < coins • target”。

B. 区块链预计算

区块时间戳是 PoS 系统的关键。它使得理论上可能通过改变之前的时间戳来分叉一个币。股份修改器不会模糊高效阻止已知未来证据的哈希。所以一个攻击者可以提前尝试计算所有区块并运行一个更高的可能性来伪造多个连续不断的区块。PoS 2.0 的解决方案：股分修改器在每个修改器间隔被改变来更好的模糊任何会被用来为下一个 PoS 查明时间的计算。预期的区块时间会从最初的 60 秒增加来匹配粒度。

过去限制：上一区块的时间

未来限制：+15 秒

粒度：16 秒（有效地从 1 秒增加）

预期区块时间：64 秒

C. 区块奖励

不幸地，大部分 PoS 系统的区块奖励是基于币龄的。理论上，这是为了通过允许节点获得潜在的支出回报来公平地分布利息。这是一个维持通用 APR（common APR）的尝试。但是，这个系统并不好用，因为节点可以断开连接并分成许多个输入，然后重连到网络并赌博奖励系统。而且，它不给节点提供任何激励来保持连接。在一个去中心化的系统中，有越多的节点连接，安全性就越好，因为它把信任从一个单独的实体转移到网络本身。PoS 3.0 的解决方案：区块奖励被指定为一个常量 1.5 个币每区块。这基于币维持在 1%利息的供应的比例。

4. 多重签名/冷分股（Multisignature/Cold Staking）

该协议最后值得注意的补充是“多重签名分股 Multisignature Staking”的实现。许多分股算法（staking algorithm）的一个缺点是它们只支持以一个单独的密钥来分股。由于比如像 BlackHalo[4]这样的软件的普及和使用——它使用一个两方托管系统，或者也称作“双方押金托管”，以及更安全的双重密钥账户——它已经变得允许这些账户参与到保护网络的安全非常重要。不只双重密钥账户，还有许多其他类型的使用 p2sh 和锁定的时间以及那些必须也被允许保护网络安全的输入。另一个问题是，在一个单密钥账户中，一个骇客可以使用密钥日志来获取你的密码并在解锁分股的时候危害你的钱包。PoS 3.0 的解决方案：我们允许用户把区块签名密钥放在被认为地址被销毁的“6a”的输出，因此他们可以通过发送一个标准的交易来分股。这允许任何输入都有资格提交。这给黑币提供了一个巨大的优势来自定义分股软件、投票以及传说的“冷分股 Cold Staking”。“冷分股”技术涉及到多台计算机。基

本上，当一个多重签名输入有资格分股时，该签名被在多台计算机之间分离。这使得一个账户事实上不可能被攻击，因为即使一个单密钥被损坏，其他密钥还处在一个完全不同的位置，既不在本地局域网也不在多台服务器上。这个技术已经在 BlackHalo 的最近发布版本中实现。

5. 安全性分析

基于时间的区块奖励的淘汰是一个显著的提升。因此，如果分股的节点数量下降了，年利会与断开连接的节点数成比例地增加。举个例子，如果只有五分之一的网络分股，你可以预期最多五倍的奖励！由于许多币没有足够的节点，这是一个巨大的优势，甚至对小的股份持有人也是。尽管获取所有相关币种的统计数据会很耗时，但是不言而喻的是，通常有低于20%很多的股份持有人分股。我们认为这种以激励的方式的增长必定会保持节点更具竞争力。粒度的改变对于阻止“磨碎股份 Stake Grinding”很有帮助。一个对于这个攻击的可能性的好的分析在 Neucoin[5]中完成。他们的声明是即使拥有比特币网络的所有散列能力，攻击也不可能成功。然而，一个几分钟的回滚会引起网络的新用户不确定加入哪条链。因此，PoS 系统使用基本上就是主要开发者的中心化控制的“检查点 Checkpointing”来选择尝试这么做的链。当然，这不是一个理想的解决办法。对此，在以太坊[6]中实现了一个好的提议。他们提议，网络的新节点询问其它节点“离带 off-band”他们是否确实在正确链上。使用我们的去中心化的市场，我们是可能得到节点来周期地分享这些信息。这个解决办法需要更深入的调查研究。对于币龄额外的移除大体上讲是一个安全的决定。实现一个检查普及时间的服务器的混合系统以及帮助计算趋势并需要节点来保持与一个时间的普遍共识紧密同步，是可能实现的。基于区块链本身的其他随机因素的补充可能也会是一个考虑。

6. 结论

世界上最安全的 PoS 系统之一正在这里被黑币所使用。我们也有几个备用方案和主意来更加提高安全性。在黑币这里，我们非常注重你们的安全性。我们已经做了每件可能的事情来维护匿名，尽可能多地保持节点的连接，保证去中心化和削弱所有的攻击。去中心化是比特币最初的核心观念，尽管我们认为这个观念还未被完全实现。一个安全兵器公平的金融系统的所有目的就是把控制权掌握在人们的手中。PoS 3.0 对于比特币有经济学上的优势因为它不会浪费电力来产生新的区块，也不会给新币制造不公平的竞争。并且现在以激励的方式保持连接，股份持有人会全面地获得更大的利益。

参考文献

[1] Satoshi Nakamoto ~~~ Bitcoin: A peer-to-peer electronic cash system. bitcoin.org, 2008

[2] Sunny King, Scott Nadal ~~~ PeerCoin: https://peercoin.net/assets/paper/peercoinpaper.pdf, 2012

[3] Pavel Vasin ~~~ Proof of Stake 3.0: http://bravenewcoin.com/assets/Whitepapers/blackcoin-pos-protocol-v2-whitepaper.pdf, 2013

[4] https://www.blackhalo.info/

[5] Kourosh Davarpanah, Dan Kaufman, Ophelie Pubellier ~~~ NeuCoin: the First Secure, Cost-efficient and Decentralized Cryptocurrency: http://www.neucoin.org/en/whitepaper/download, 2015

[6] https://www.ethereum.org/