白币 POS 3.0 协议的安全性分析

http://www.whitecoin.info

摘要：经过了多年的测试，股权证明机制（POS）的安全性正在逐步得到证实。白币的 POS3.0 协议采用先进技术解决了困扰的币龄、区块奖励和区块链提前计算等问题。此协议通过抑制非活动节点，激励更多节点接入到网络中，具有很强的鲁棒性。本文着重介绍 POS3 的优势并进行安全性分析。最后罗列了进一步增强白币安全性的想法。

I 介绍

密码学已经设法改变了金融和资金的定义方式。最近，比特币[1]的出现展示了点对点网络如何通过解决“拜占庭将军问题”来防止伪造。此后，利用比特币的开源代码产生了许多不同的数字币。在网络上生成新权益有两种主要方法。第一个是“工作量证明”，第二个是“股权证明”。工作证明采用计算竞争的原理，第一个解决问题的计算机会收获币。工作量证明机制背后的理论有点类似举办数学竞赛。解决难题的第一台电脑收到奖励。这使得权益的分配是一个完全公平的过程。然而，这也造成了浪费能量的问题。为了竞争，需要更好的计算机硬件。因此，新币的产生需要浪费钱和能量。股权证明是股东之间的竞争，根据网络的连接和随机机会，可以收到新币。利息是根据持有多少股权生成的。这解决了比特币的能源浪费问题，但在网络安全方面引入了新的挑战。对于白币，我们对本协议中的优势进行技术分析，并讨论潜在的改进和陷阱。第一个基于股权证明的虚拟币是点点 [2]，随后，黑币的 POS2.0[2]和 POS3.0 取得了重大突破。白币已经实施了 POS 3.0 系统，因为我们认为它是世界上最安全有效的虚拟币产生方法。接下来，我们将概述和突出说明该系统的安全性及其解决的技术问题。

II。安全，币龄和攻击

竞争生成币的整个目的是为了避免攻击。交易的确认是给予区块产生的奖励。但是，如果这个系统具有游戏规则，那么它是有缺陷的。在股权证明机制中，你首先证明你可以使用币，也就是你可以参与竞争去随机的赢得区块。越多的人竞争区块越安全。币龄意味着，你持有币的时间越长，你可以赢得区块的概率越高。原来的意图是激励休眠的币持有者。然而，这并不鼓励节点保持与网络的连接，因为它们可以等待奖励增加。此外，股东可以长时间断开网络连接，然后重新连接并获得足够的数据块，从而增加了对网络造成 50％的攻击的风险。时间计算方法将影响支付阻止连接。此外，连接的节点越少，获得大多数块伪造共识就越容易。此外，可以提前计算利益以使攻击更有效。时间戳用于股权证明，以获得时间的一般概念。漂移计算用于防止伪造错误的时间戳。在工作量证明中，根据生产块的速度而增加或减少难度。然而，作为防止任何种类“定时攻击”的预防方法，使用集中检查点。

III。问题解决方案

A.币龄

币龄的计算是基于未花费的币的数量和休眠时间。计算采用简单的公式：“proofhash<币数•年龄•目标”。proofhash 对应于一个取决于权重修正因子、未花费的产出和当前时间的模糊和的哈希值。通过足够的币龄积攒来进行攻击是不太容易实现的[3]。如果攻击是恶意

的，攻击者可以对区块链进行分叉并达成双花。但是，此次攻击过后，攻击者必须重新积攒币龄才能再次发起攻击，因为当区块生成后权益累积就会归零，所以执行连续的双重支出是非常困难的。然而这种情况也不是完全不可能，因为输入可以分为 1000s 的输出。这可能会导致连续双重支出攻击的可能性。但是这也不太容易实现的，因为攻击者需要大量的币来保持网络中更大的权重。虽然理论上可行。但是，如果我们看看白币和其他受欢迎的 POS 系统，我们发现节点数量相当低，使得一些小的节点具有较大的权重。许多持币者可能不想执行这种攻击，因为如果检测到这种攻击，它们可能失去其享有的价值。尽管这种情况发生的可能性微乎其微，但是仍然存在攻击可能。POS 2.0 的解决方案：从原来方程式中移除币龄：
- “roofhash<币数•目标”。

B. 区块链预先计算

区块链时间戳是 POS 系统的关键。 理论上可以通过更改以前的时间戳来对币进行分叉。攻击者可以提前计算所有的区块，这样可以高概率来生成多个连续的块。POS2.0 的解决方案：为了降低预先计算攻击的可能性，权重修正因子在每一次修正因子间歇时都会改变，以便对将要用来下一个权益累积证明的时间戳的计算结果进行更好的模糊处理。我们对区块时间戳做了适当的改变，使其在 PoS 机制下更有效的工作。预计区块时间将在原本的 60 秒的基础上有所增加，以匹配粒度。需要注意，假设节点有外部时间来源，并且节点的内部时间与全网整体时间之间的差异太大，则此节点产生的区块将很可能成为孤块

过去限制：上一区块时间
未来限制：+15 秒
粒度：16 秒（有效地从 1 秒增加）
预计阻止时间：64 秒

C. 积分奖励
不幸的是，大多数 POS 系统中的块奖励是币龄。 理论上说，这是通过允许节点接收潜在的付款到期而公平分配利息。 这是一个保持普通 APR 的尝试。 然而，存在一定的问题，因为节点可以保持断开连接并且具有许多分离输入，重新连接到网络得到奖励。 此外，它不给予节点任何激励来保持连接。 在一个分布式的系统中，越多的节点连接安全性越好，因为它将信任从单个实体转移到网络本身。 POS 3.0 的解决方案：每个块的积分奖励为 1.5 个币。 这是与维持利率 1％的币供应成正比的。

IV。多签名

协议的最后一个值得注意的是执行“多重签名”。许多算法的一个缺点是它们只支持使用单个密钥进行加密。使用双方托管系统也称为“Double deposit escrow“和更安全的双重密钥帐户，让这些帐户参与保护网络变得重要。除了双重密匙账户之外，还有许多其他类型的输入使用 p2sh 和锁定时间，而且也必须允许这些输入来保护网络。另一个问题是，在单个密匙帐户中，黑客可以使用密钥记录器获得密码，当您的钱包为了获取权益处于解锁状态时，损害您的钱包。POS3.0 的解决方案：我们允许用户将块签名密钥放在“6a”的输出中，称为刻录地址，以便通过发送标准事务来获取权益。这允许任何符合资格的输入进行提交。这是白币的一个巨大的优势，用于定制软件，投票和传说中的“Cold Staking”。“Code Staking”技术涉及多台计算机。当多重签名可行时，签名将在许多计算机之间分开。这使得帐户实际

上不可能被破解，因为即使单个密钥被泄密，其他密钥在局域网或多个服务器上也是完全不同的位置。

五，安全分析

将区块奖励中时间因素去掉是一个明显的改善。因此，如果节点数量下降，每年的利息会与断开的节点成比例。例如，如果只有 1/5 的网络是在获取权益，你可以期待高达 5 倍的奖励！由于许多币没有足够的节点，所以即使是小股东也是一个很大的优势。虽然统计所有相关币的数据很花时间，但不言而喻，通常情况下不少于股东的 20％享受利息。我们认为这种激励措施的增加肯定会使节点更具竞争力。粒度的变化对于防止“Stake Grinding”是有用的。在 Neucoin [4]中对这种攻击的概率进行了很好的分析。他们的说法是，即使使用 Bitcoin 网络的所有哈希功能，攻击也是不可能的。但是，几分钟的等待可能会导致网络的新用户不确定哪个链接加入。因此，POS 使用“检查点”是基于主要开发者的集中控制，以选择试图做到这一点的链。当然，这不是一个理想的解决方案。有一个很好的建议在 Ethereum [5]。为此。他们提出，网络的一个新节点要求其他节点“离线”，如果它们确实在正确的链路上。使用我们的去中心化市场，可以让节点定期分享这个信息。解决方案还将需要进一步研究。一般来说，额外移除币龄是一个安全的决定。可以执行检查时间服务器的混合系统，以帮助计算漂移，并要求节点与时间的普遍共识保持紧密同步。基于块链本身的其他随机因子的添加也可能是一个考虑。

VI。 结论

白币是世界上最安全的 POS 系统之一。 我们还有几个候选解决方案和想法来进一步提高其安全性。白币会保证您的安全，尽可能地保持匿名性，尽可能多地连接节点，保证分布式和避免所有攻击。去中心化是比特币最初的核心思想，虽然觉得这个体系还没有完全实现。 一个安全和公平的金融体系的整个目的就是把它控制在人民手中。POS 3.0 与比特币相比具有经济优势，因为它不浪费电力来生成新的块，也不会对新币造成不公平的竞争。 而现在有了使节点保持连接的动力，股东们全面获益。

REFERENCES

[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/peercoin-paper.pdf, 2012

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

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

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