黑币POS协议2.0版白皮书

Pavel Vasin
www.blackcoin.co

摘要—目前的PoS协议存在一些潜在的安全问题：币龄（coin age）可能会被恶意的节点滥用以获得更高的网络权重并成功实施双花（double spend）。另外，由于币龄的问题，诚实的节点可以通过定期开启钱包进行权益累积（staking）而滥用这一系统。这样就不能确保黑币网络的安全。最后，在当前的系统当中，所有权益证明的组件都是可以充分预测的，这样就可以对将来的权益证明进行提前计算。在本白皮书中提出了一套系统以解决上述问题。

I. 介绍

目前虚拟币社区普遍认为PoS系统还没有充分证明其安全性、经济价值以及长期的总体能源效率。黑币本来是为了证明PoS的概念是有效的这一目的而被创造出来的，并坚持让它在未来的虚拟货币当中具有现实世界的用途。在过去的120天里，黑币以它1500万～2000万美元的市值证明了这个系统是安全的。由于我们预计黑币生态系统在未来将会持续增长，我们希望确保PoS系统能够尽可能的安全。这就是为什么我们将要引入PoS协议2.0版（或者简称为PoS2.0）的原因。未来我们将会持续扩展和加强这个新系统，以确保各种攻击途径在被恶意的滥用之前就被关闭。

本白皮书的结构如下：第 II 章会对PoS的概念进行解释；第 III 章将会对现有系统的缺陷进行描述；第 IV 章将会讲述哪些地方将要做出改变；最后在第 V 章进行总结。

II. 股权证明机制（PoS）

类似于比特币[1]这样的去中心化数字货币的获得方式是：通过来解决艰巨的计算任务来获得整个网络的认可，从而产生区块，其中包含了各个区块分别是由哪个节点所生成的证据。然而不幸的是，基于PoW（工作量证明机制）的系统最终将倾向于自我毁灭[2]。

PoS的目标是取代这种在分配体系中达成一致的方式。PoW的机制是，在一定数额的币被整个网络接受以前，各个节点通过生成区块的方式来证明自己对这些币的所有权。生成一个区块的过程包含把这部分的币发送给自己，以证明所有权。所需要的币数（也叫做目标）是由网络通过类似于PoW的难度调节机制来规定的，以此来确保大致恒定不变的出块时间。

与PoW机制一样，在PoS中生成区块的过程将会得到转账费用的奖励，此外还有一个通过底层协议所定义的供应模型，也就是通常所说的利率。虚拟币的初始分配通常是在一个叫做PoW挖矿的时间段进行的。

A. 相关工作

第一个基于PoS的虚拟币是点点币（PPC）[3]，目前仍然在PoW挖矿阶段。基于对点点币的PoS协议的进一步开发又产生了新星币（NVC）[4]，它使用一种混合的PoW／PoS系统。

黑币是第一个采用基于上述项目发展而来的纯粹PoS协议的虚拟货币。

III. PoS的安全问题

除了PoS对于PoW在整个网络上建立共识的方法上所具有的明显优势，PoS也亟须解决一些问题，从而极大地提高其网络安全性。

A. 币龄

在点点币的协议当中区块的生成是基于币龄的，这是一个随着时间的流逝而线性的增加未花费的币的权重的因子，其证明必须与一个新区块一起提供，并满足以下条件：

$$\text{proofhash} < \underbrace{\text{币数} \cdot \text{币的年龄}}_{\text{币龄}} \cdot \text{目标} \tag{1}$$

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。

通过这个系统，攻击者可以把足够的币龄积攒起来，从而成为网络上拥有最高权重的节点。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。

值得一提的是，这种情况发生的可能性很低，攻击者也没有足够的动机（积攒足够的币龄以成为网络中权重最高的节点，为实现这一目标，需要花费大量时间，或者拥有大量黑币——换言之即大量金钱。其次，发动这样的攻击很可能使得整个黑币系统的价值降低，长期来看难以从中获利）。

另一种情况是这些币龄属于贪婪但却诚实的节点。有一些节点并没有恶意，但是他们的钱包平时都是离线的，只是偶尔进行同步以获得利息。当前的系统事实上鼓励了这些节点滥用这一机制，他们平时保持离线，只在累积了可观的币龄以后才连线以获得利息，然后再次关闭。

B. 区块链提前计算和长距离攻击

在本文撰写之际，对于如何在一个巨大的分布式网络当中确保时间戳的安全性，还没有已知的解决方案。当前的区块时间戳规则给了攻击者一定程度的自由来选择公式1当中提到的proofhash，并因此提高了让过去几个区块成功分叉的可能性。

此外，目前的权重修正因子没有对哈希功能进行足够的模糊处理以防止攻击者提前计算出未来的权益累积证明。因此恶意的攻击者将能够计算出权益累积证明的解答的下一次间隔，从而能够连续生成多个区块并实施能够危害到整个网络的恶意攻击。

IV. 协议中的变化

下面我们来描述一下黑币协议的变化，这些变化能处理前面几节当中提到的问题。

A. 将币龄从等式中拿掉

运行一套PoS系统最安全的方法是将尽可能多的节点纳入网络，越多节点在线进行权利累积，系统遭受安全问题（例如51%攻击）的可能性就越低，通过节点确认的交易确认速度也越快。

因此，拿掉币龄就需要所有节点必须更多的保持在线以进行权益累积。积攒币龄的方法在新系统里将不再可能，新系统采用以下公式计算权益累积的机会：

$$\text{proofhash} < \text{币数} \cdot \text{目标} \tag{2}$$

需要注意的是公式2的系统不会改变实际的权益奖励值

B. 改变权益修正因子

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。

C. 时间戳规则

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。对区块时间戳规则的修改建议概要如下。

比特币	
以前的限制	前11个区块时间的中间值
未来的限制	+2 小时
粒度	1 秒
预计的区块时间	10 分钟

黑币	（新规则）
以前的限制	上一个区块时间
未来的限制	+15 秒
粒度	16 秒
预计的区块时间	64 秒

D. 哈希功能

新星币的原始协议使用Scrypt[5]算法来进行工作量证明，同时也用来进行区块哈希。但前期实施的时候这里有一些问题。使用Scrypt算法对于PoS来说没有什么实际好处，而且相对于其他算法来说也慢很多。因为黑币已经结束了PoW阶段，所以唯一需要做的主要改变是确定区块哈希的算法。因此区块哈希算法已经被改回到SHA256d。对应的区块版本已经升级到第7版。

V. 总结

以上的修改提议应该会提高黑币PoS协议的安全性，并进行了优化。新的协议能够将攻击途径减少到最低限度，并且能够显著提高网络当中保持运行的节点数量。这将会使黑币和PoS在继续扩大应用范围的同时封堵和缓解潜在的风险。

VI. 鸣谢

非常感谢Rob ‘Soepkip’ Schins、Maarten ‘maarx’ Visser、Steven ‘McKie’ McKie和Patrick Doetsch帮助编写了V2版协议。

翻译：James、kikoxxxbc（黑币中文社区）

校对：BCDolphin、SyllaBear

参考文献

[1] 中本聪. 《比特币：一种点对点的电子现金系统》 bitcoin.org, 2008.

[2] Nicolas T. Courtois. 《最长链规则与虚拟币的程式化自我毁灭》，2014.

[3] Sunny King 和 Scott Nadal. 《点点币：采用PoS机制的点对点的虚拟货币》 peercoin.net, 2013.

[4] 新星币 http://coinwiki.info/en/novacoin.

[5] Scrypt 工作量证明. https://en.bitcoin.it/wiki/scrypt_proof_of_work.