TECHNICAL NOTES

Seesaw Reward Balance System

Whitepaper
aka the
'Purplepaper'

Revision 0.8a March 23 2017 Pivx.org

PIVX

PRIVATE INSTANT VERIFIED TRANSACTION

这些技术指导备注旨在正式记录和描述私人即时验证交易加密货币的特征和概念。
本文件将详细解释跷跷板奖励平衡系统的技术细节及其预期收益。

简介

大多数加密货币把主节点划分为多个区块，在保障挖矿方式和主节点分配机制的两种奖励方式的平衡下平均的分配每个区块的奖励额度。
这种力求公平的奖励分配方式有可能被日益增多的持有大量主节的投资人所颠覆，可能引起潜在的预算系统的集中化，这种情况类似于在公司中有一个主导性的大股东一样。持有主节点的额外收益可能导致持有权益证明进行挖矿的用户数量的减少，从而降低了PoS网络的安全性。

主节点持有者确实提供了有价值的服务，也理所应当从该服务中获得收益，但我们需要明确，我们的奖励目的不是对他们提供的额外价值进行奖励。因为我们认为，如果这样做会使主节点持有者拥有超越该体系下其他类型用户的收益并且该收益分化比例会非常大,并最终导致更大程度的集权。

为了解决这个问题，本文中概述的功能特点是力求确保PoS网络的安全性而开发和使用的。 PoS网络的安全性是通过激励赌币来实现的，进而促进交易的流通性，并控制主节点网络的增长率和数量核计。

普维币概览

私人即时验证交易，即普维币，是一种确保安全性和私密性，采用权力下放机制，开源的加密货币。在它2016年2月1日之前以Darknet（DNET）的名义发布，之后正式更名为普维币。当DNET转为现行的股权证书（PoS）阶段时， 初期采用工作量证书（PoW）进行分配的阶段也相应的于2016年8月终止 。

普维币采用黑币的权益证明（PoS ）2.0 [1] 协议，基于比特币核心0.10.x代码库进行运行。它利用主节点网络[2]，以实现公开的分权监管方式，同时增强交易的隐私性。

普维币的主要目标是实现近乎即时的私人交易，并构筑一个保障所有用户利益的可持续的网络管理机制 。目前我们正致力于实现这些目标，虽然一些功能正在开发中，但他们将在不久的未来一一实现。

第四页 普维币概览内容

普维币拥一个自由开放的任务和开发环境，以及一个高度亲和性的开发团队。 我们使用多种社交网络渠道和社交媒体平台，以便用户能更便捷的取得联系。开发团队欢迎任何贡献自己的技术专长并加入我们，一起致力于普维币的发展。我们鼓励人们勇往无前的踏实工作。在这里，无需要顾虑人事监督，层级结构，和等级机构所产生的权限制约 。

有关普维币的更多具体细节，请访问pivx.org。 技术说明详见– 跷跷板奖励平衡系统4 P

股权证书2.0概览

为了达成共识; 股权证书 (PoS) 2.0的需要运行钱包软件的节点，以证明用户拥有块链中的硬币从而进行区块交易的验证。 作为交易筹码的节点会获得一定数量的区块比例。 该比例是根据特定时间段的股权来划分的。用户也相应的根据该比例获得奖励收益。

这意味着随着用户的增多 (参与的节点量增加，产生的货币量增加)，囤积该网络中大多数硬币的难度增加，网络也因此变得更安全。

主节点概述

主节点是在同一区块链上使用相同的钱包软件运行的节点，以向网络提供额外的服务。这些服务包括为增强交易的隐私性而进行的硬币混合，以及即时交易和权力下放的管理方式 。其中，权力下放的管理方式提供一个分散的预算制度以及稳定不变的提案提请和投票系统。

为了提供这样的服务，主节点持有者能对持有的每一个区活得一定比例的奖励。 这种相应的的奖励能抵消主节点持有者运行节点的费用 。

主要特点概述

为了促进网络中股权节点和主节点之间的比例均衡，普维币团队开发了一个可变的跷跷板奖励平衡系统，可以动态的调节主节点和股权节点之间的区块奖励份额。

每个普维币股权证书（PoS）区块奖励拿出10%专门用于预算系统，90%专门用于主节点和股权采矿的收益奖励。奖励部分通过跷跷板奖励平衡系统在主节点和股权节点之间进行近一步动态分配。

该分配方式逻辑在根源上是很简单的。 主节点持有数越高，每个股权证书（PoS）区块的奖励部分越少，即支付给主节点的奖励比例也减少，用于股权节点的奖励比例进而增多。相反，当主节点数量下降时，主节点奖励比例增加，而股权节点奖励比例相应的减小。

当主节点所定的的硬币数量低于总硬币供应量的1%时，股权证书（PoS）区块奖励以9比1的比例开始。

但是，随着锁定到主节点的硬币数量超过了普维币硬币总量的41.5%，区块奖励总量将根据大于50%的区块奖励额度而向股权节点转移。

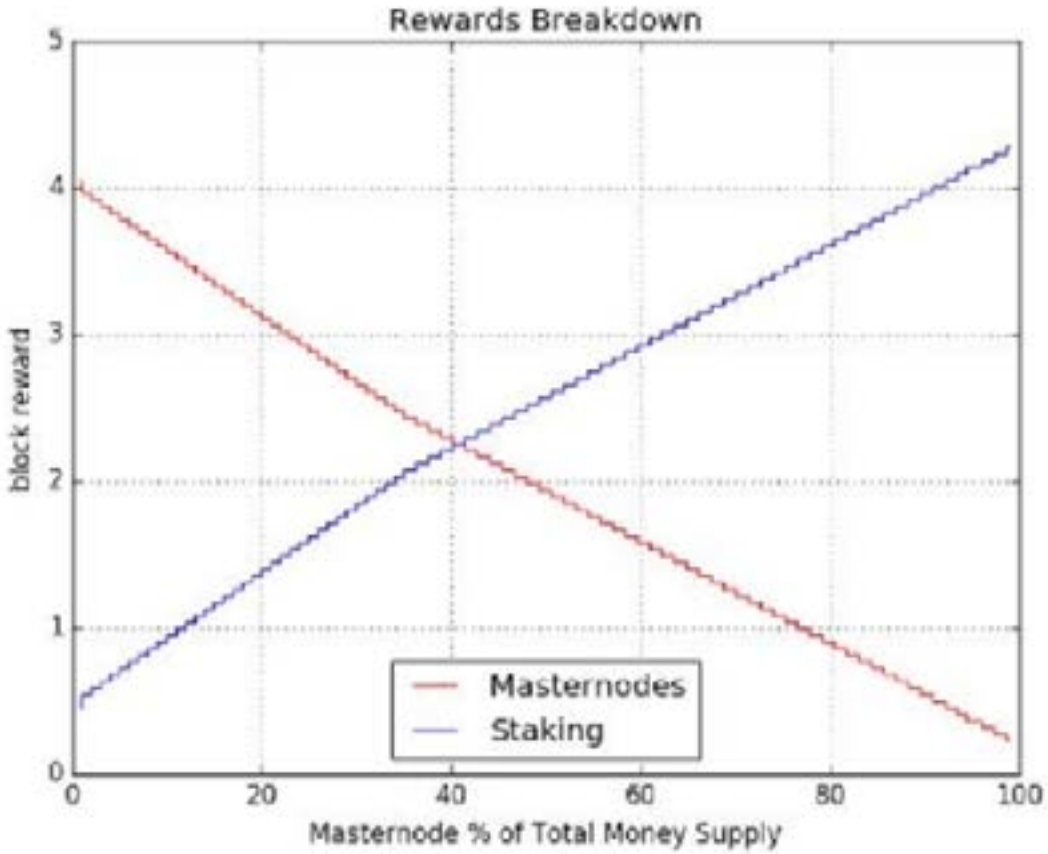
这样做会导致主节点的吸引力的下降，因为与具有较少维护成本的投资相比，它更可能会降低其盈利能力。这个阈值被选中，因为它将促成一个强大的盈利颇丰的主节点网络，因为它可以刺激生成总硬币供应量的60%的硬币，这些硬币将能用于固定网络和维持货币的流动性。

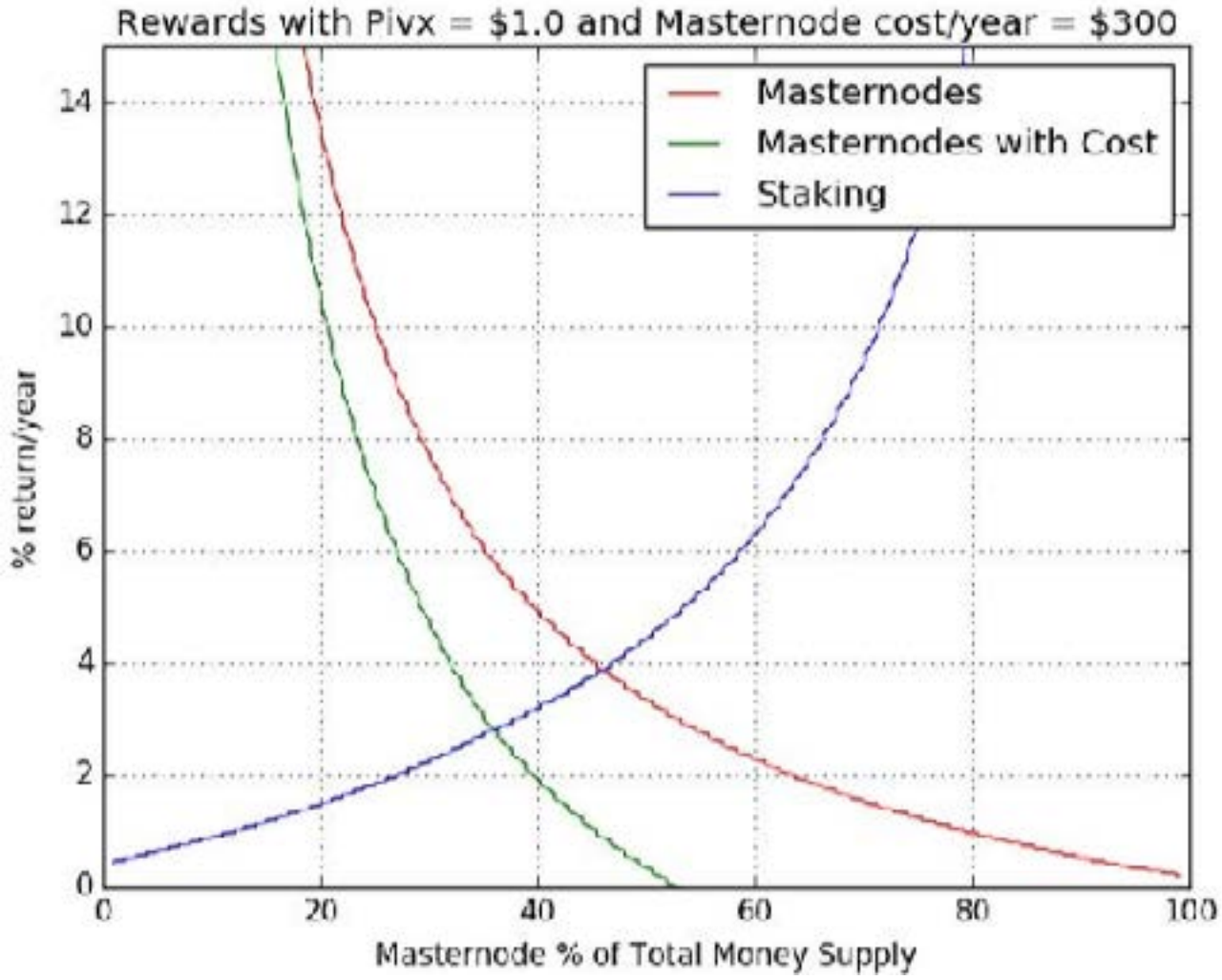
跷跷板奖励平衡系统的另一个预期收益和目标是确保在正常情况下低于平衡阈值的情况下，主节点持有者的用户比持有同等数量硬币的股权持有者用户更有利可图。 造成这种情况的原因在于主节点持有者相较于股权持有者投入了额外的成本，承担了维护主节点更大的风险和时间。

跷跷板效果

下图显示了从648,000区块 (2017年5月中旬) 开始，主节点 (红色) 和股权节点 (蓝色) 的块奖励金额 (Y轴) 相对于由主节点 (X轴) 锁定的总硬币供应的百分比，其中每个块 奖励固定为5 PIV。

下图显示了从块648,000开始的理论上年度百分比回报，其中每个区块设置





红线表示每个主节点的维护成本为零时主节点持有者的回报，而绿线是假设情景下的逻辑主节点回归曲线，每个主节点维护人员每年维护成本为300美元，相应的每个PIV的价格为1美元。

代码走查逻辑。

逻辑力求简单而有效。这是为了确保其稳定性，并能够容易地确定其结果，并在需要时改进其逻辑。

```
if (mNodeCoins <= (nMoneySupply * .01) && mNodeCoins > 0) {
   ret = blockValue * .90;
}
```

节点硬币是每个块的硬币总数。
该值是由主节点硬币（m节点硬币）相对于总硬币供应量（n硬币供应量）确定的可变比率想乘而得。

结果值是根据所持有的主节点份额所获得的硬币奖励数量。
上面的例子显示了用于定义／确定最高的主节点份额进行支付的第一个逻辑。您可以看到，如果主节点硬币小于或等于硬币供应量的1%，且大于0，则主节点的所获的区块值将为股权证书持有者（PoS）区块的90%（ret = 区块值* .90 ）。

该逻辑会继续执行，从特定比例开始增加直到节点硬币小于或等于硬币供应的99%。

```
else if (mNodeCoins <= (nMoneySupply * .99)
         && mNodeCoins > (nMoneySupply *.987)) {
   ret = blockValue * .05;
}
```

超过总硬币供应量99%的任何节点硬币值将以等于区块值的1%的固定值回馈给用户。期望的是，它永远不会到这一点，但运算逻辑在设计上涵盖了所有可能的结果。

```
else {
   ret = blockValue *      .01;
}
```

这个跷跷板奖励平衡系统算法最初只使用了16百分比布长; 迄今为止，经过改进，它现在对动态的跷跷板算法总共执行了105个百分比的步长，并能支持更细微的步长量。

未来计划总结

普维币利用的跷跷板奖励平衡系统具备了超越众多使用的主节点奖励分割方法的股权证书加密币的许多优点。

1. 它可以通过改变其奖励大小来间接地影响网络中的主节点总数，以调节其奖励额度与赌注额度。

2.当主节点数额过高，通过增加股权持有者的奖励支付份额，促进股权持有者的数量，从而保持高网络的高度安全。

3. 只要主节点数值低于平衡阈值（大约40%的硬币供应量），主节点持有者的收益就会持续高于股权持有者的收益。

4.保障所有硬币持有者获得奖励，而不仅仅是主节点持有者。 从而导致更公平和集权度相对比较低的系统。

未来计划

由于跷跷板奖励平衡系统还比较新（在撰写本文档时只有5个月）；随着网络的增长，更细致的调整和更优的阈值将被采用以保证系统的卓越性 。

但即使在使用股权证书（PoS）的头5个月内，已有超过1400个主节点，它占目前硬币供应量的30%以上。而 该算法已被证明能够按照设计无缝地进行使用。

源代码

GITHUB
https://github.com/PIVX-Project/PIVX/blob/v2.1.6/src/main.cpp#L1786

链接
BTC ANNOUNCE THREAD
https://bitcointalk.org/index.php?topic=1262920.0

官方网站 https://pivx.org
Masternode Payment Information http://178.254.23.111/~pub/DN/DN_masternode_payments_stats.html

未来计划

由于跷跷板奖励平衡系统还比较新 (在撰写本文档时只有5个月) ; 随着网络的增长, 更细致的调整和更优的阈值将被采用以保证系统的卓越性 。

但即使在使用股权证书 (PoS) 的头5个月内, 已有超过1400个主节点, 它占目前硬币供应量的30%以上。而 该算法已被证明能够按照设计无缝地进行使用。

参考文献

[1]股权证书2.0 白皮书http://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper-cn.pdf

[2] 达世币主节点 https://dashpay.atlassian.net/wiki/display/DOC/Masternode

作者
著作人: 雅基曼
编辑: 沃瓦特曼， 紫纸斯波克
格式设计: 钱炼金术士
翻译: 文朵儿

www.pivx.org