授权股权证明机制白皮书

(Delegated Proof-of-Stake ， DPOS)

作者： **Daniel Larimer**

2014 年 4 月 3 日

翻译：yidaidaxia_郝晓曦

比特坊数字资产研究俱乐部 翻译作品（www.bitfarm.io）

摘要

本白皮书介绍一种股权证明机制的新实现方式，该方式可以对交易进行秒级验证，并且能够在更短的时间内提供比现有任何股权证明系统都更好的安全性。在比特币网络产生一个区块的时间过后，一个授权股权证明系统(DPOS)能使你的交易得到 20%股东的核实，而在比特币网络声明交易已几乎不可逆(6 个区块，约 1 小时)的时间过后，在 DPOS 机制下，通过其代表，你的交易已经得到 100%股东的核实。

1.0 背景

分布式交易总账需要在尽可能短的时间内做到安全、明确及不可逆，便于提供一个最坚实且去中心化的系统。在实践中，该流程分为两个方面：选择一个独特的节点来产生一个区块，并使得交易总账不可逆。

1.1 工作量证明机制(Proof of Work, POW)

第一个成功解决该问题的尝试是比特币系统(Bitcoin)，比特币系统使用工作量证明机制使更长总账的产生具有计算性难度。工作量证明机制就好比是乐透，平均每 10 分钟有一个节点找到一个区块。如果两个节点在同一个时间找到区块，那么网络将根据后续节点的决定来确定以哪个区块构建总账。从统计学角度讲，一笔交易在 6 个区块(约 1 个小时)后被认为是明确确认且不可逆的。然而，核心开发者认为，需要 120 个区块(约一天)，才能充分保护网络不受来自潜在更长的已将新产生的币花掉的攻击区块链的威胁。

尽管出现更长的区块链会变得不太可能，但任何拥有巨大经济资源的人都仍有可能制造一个更长的区块链或者具备足够的哈希算力来冻结用户的账户。

1.2 股权证明机制(Proof of Stake, POS)

股权证明机制已有很多不同变种，但基本概念是产生区块的难度应该与你在网络里所占的股权(所有权占比)成比例。到目前为止，已有两个系统开始运行：点点币(Peercoin)和未来币(NXT)。点点币使用一种混合模式，用你的股权调整你

的挖矿难度。未来币使用一个确定性算法以随机选择一个股东来产生下一个区块。未来币算法基于你的账户余额来调整你被选中的可能性。

未来币和点点币都分别解决了谁来生产下一个区块的问题，但他们没有找到在适当的时间内使区块链具备不可逆的安全性的方法。根据我们能找到的信息，做到这点，点点币需要至少 6 个区块(约一小时)，未来币需要 10 个区块。我们找不到在 10 个区块后未来币能提供什么级别安全性的根据。

我们之前发布了基于交易的股权证明机制(Transactions as Proof of Stake, TaPOS)的白皮书，在该机制中，每笔交易都包含区块链中前一个区块的哈希值。通过该系统，对任何人而言，网络变得越来越安全而不可逆，因为最终每个区块都经过了股东投票。股权证明机制面临的挑战是它没有定义谁来产生下一个区块。

1.3 瑞波共识机制(Ripple Consensus)

瑞波共识算法，使一组节点能够基于特殊节点列表达成共识。初始特殊节点列表就像一个俱乐部，要接纳一个新成员，必须由 51%的该俱乐部会员投票通过。共识遵循这核心成员的 51%权力，外部人员则没有影响力。由于该俱乐部由“中心化”开始，它将一直是“中心化的”，而如果它开始腐化，股东们什么也做不了。与比特币及点点币一样，瑞波系统将股东们与其投票权隔开，并因此比其他系统更中心化。

2.0 授权股权证明机制(DPOS)

当使用去中心化自治公司(Decentralized Autonomous Company, DAC)这一说法时，去中心化表示每个股东按其持股比例拥有影响力，51%股东投票的结果将是不可逆且有约束力的。其挑战是通过及时而高效的方法达到 51%批准。

为达到这个目标，每个股东可以将其投票权授予一名代表。获票数最多的前 100 位代表按既定时间表轮流产生区块。每名代表分配到一个时间段来生产区块。所有的代表将收到等同于一个平均水平的区块所含交易费的 10%作为报酬。如果一个平均水平的区块含有 100 股作为交易费，一名代表将获得 1 股作为报酬。

网络延迟有可能使某些代表没能及时广播他们的区块，而这将导致区块链分叉。然而，这不太可能发生，因为制造区块的代表可以与制造前后区块的代表建立直接连接。建立这种与你之后的代表(也许也包括其后的那名代表)的直接连接是为了确保你能得到报酬。

该模式可以每 30 秒产生一个新区块，并且在正常的网络条件下区块链分叉的可能性极其小，即使发生也可以在几分钟内得到解决。

2.1 成为一名代表

成为一名代表，你必须在网络上注册你的公钥，然后分配到一个 32 位的特有标识符。然后该标识符会被每笔交易数据的“头部”引用。

2.2 授权你的选票

每个钱包有一个参数设置窗口，在该窗口里用户可以选择一个或更多的代表，并将其分级。一经设定，用户所做的每笔交易将把选票从“输入代表”转移至“输出代表”。一般情况下，用户不会创建特别以投票为目的的交易，因为那将耗费他们一笔交易费。但在紧急情况下，某些用户可能觉得通过支付费用这一更积极的方式来改变他们的投票是值得的。

2.3 保持代表诚实

每个钱包将显示一个状态指示器，让用户知道他们的代表表现如何。如果他们错过了太多的区块，那么系统将会推荐用户去换一个新的代表。如果任何代表被发现签发了一个无效的区块，那么所有标准钱包将在每个钱包进行更多交易前要求选出一个新代表。

2.4 解决区块链分叉

和工作量证明系统及其他股权证明系统一样，最佳区块链是最长的有效区块链。任何时候，一名代表错过签发一个区块的机会，该区块链将比潜在竞争对手短。只要在你的交易被写入区块后的 100 个区块中的 51%被生产出来了，那么你就可以安全地认为你在主区块链上。

也许，在防止区块链分叉所导致的损失方面，最重要的事是在事发后第一时间得知消息。因为代表们通过生产区块得到很好的报酬，他们将保持接近 100%的在线时间来防止因被投票罢免而损失收入。你可以安全地认为如果在过去的 10 个区块中，有一两个区块错过生产，则互联网的某些部分可能正发生连接问题，那么用户应该对此特别警觉并要求额外的确认数。如果 10 区块中有超过 5 个错

过生产，那么这意味着你很可能在一条支链上，因此应该停止所有交易，直到分叉得到解决。

以一种及时的方式(少于 5 分钟)简单地发现并警示用户网络分叉，是可以最小化潜在损失的非常重要的能力。而知道你是否正处在一条支链上则更为重要。

2.5 100 名代表是去中心化的吗？

因为去中心化已经成为一个流行术语，所以其定义很难完全固定。我们将自由市场看作去中心化的基本形式，并将对进入自由市场设置障碍看作是所有中心化的基础。像任何事物一样，中心化有程度之分，所以我们把授权股权证明机制与其它方案的中心化程度进行对比。

2.5.1 比特币

比特币系统目前正以授权工作量证明(Delegated Proof of Work, DPOW)为基础而运行，因此有大约 10 名代表控制了绝大多数的哈希算力。在那些为其竞争而能使用规模经济进行无收益挖矿的人手中，哈希算力本身就是中心化的。最后，工作量证明机制为进入市场设置障碍，使得“在职”的区块制造者无法轻易被取代。与比特币系统相比，DPOS 在区块生产方面至少去中西化了 10 倍，并且也许在市场竞争方面去中心化了无数倍。

尽管在哈希算力方面有一定量的去中心化，当想到掌控比特币系统的股东(比特币持有者)所持股份的占比，我们认为比特币系统是最中心化的。如果你考虑使用比特币体系的用户总数，其中参与挖矿的人很可能少于百分之一。

2.5.2 点点币

点点币是一个混合系统，所以它由于工作量证明机制而是部分中心化的。和比特币系统一样，它也有矿池。与比特币相比，点点币无疑是更去中心化的，然而，因为股权证明机制矿池需要用户保持他们的电脑在线且钱包解锁，只有一小部分的股东参与了任何形式的挖矿。

2.5.3 未来币

未来币使用透明锻造，以确定的选出下一个制造节点。可以将其类比为，使用授权股权证明机制但你只能将你的投票权授予你自己，而你获得锻造区块机会的频率直接取决于你的账户余额。在这个意义上来说，未来币比点点币和比特币更为去中心化。但由于对安全风险的顾虑以及事实上大多数常规用户不会整天开启他们的电脑来籍此获得锻造机会方面的优势，它仍然遭受着少的可怜的挖矿参与度。

从这个角度来讲，我们可以断定未来币网络是由一小部分股东来保障网络安全的。事实上，如果你不上线投票，那么你将失去你的选票。为了解决这个问题，一些未来币用户用他们的股权建立股权池，并信任第三方来为他们挖矿。这是以一种形式的授权股权证明来提高股东参与度，但这也使他们的账户余额在他们参加这些矿池时承受风险。

3.0 攻击

一般而言，网络必须抵御两种类型的攻击：拒绝服务攻击和双重支付攻击。一个攻击者通过不把一些或全部的交易加入总账来进行拒绝服务攻击。这种攻击可以由任何拥有 51%网络(无论比特币、未来币或其它)的人进行。而利用在网络正试图达成共识时的短期优势，可以进行双重支付攻击。

为抵御这些攻击，网络必须使 51%的股东尽快达成协议。

3.1 防止排除交易

拥有全部经股东投票选出的 100 名代表，并且按要求轮流生产区块，意味着任何一笔由至少 1%的股东批准的交易能够在 30 分钟内加入总账。这意味着没有代表可以通过将投票支持其他代表的交易排除在外来获取利益。

3.2 将一些代表的权力中心化

与其所被授权的投票权无关，这前 100 人所获得的权力权重是相同的，每名代表都有一份相等的投票权。因此，无法通过获得超过 1%的选票而将权力集中到一个单一代表手上。

个人或者组织控制区块链的多名代表是有可能的。但是这个过程将需要欺骗很大比例的股东数去支持“傀儡”。

即使可以建立这 51%傀儡，他们扰乱网络的能力仍将是有限的、能够被快速识别快速纠正的。没有工作量证明机制设置的进入障碍，占据多数的诚实用户会

把攻击鉴别出来，然后将代码分叉并无视攻击者生产的区块。这种攻击可以扰乱网络，但不会是致命的。

3.3 针对代表的分布式拒绝服务攻击(DDOS)

因为只有 100 名代表，　可以想象一个攻击者对每名轮到生产区块的代表依次进行拒绝服务攻击。幸运的是，由于事实上每名代表的标识是其公钥而非 IP 地址，这种特定攻击的威胁很容易被减轻。这将使确定 DDOS 攻击目标更为困难。而代表之间的潜在直接连接，将使妨碍他们生产区块变得更为困难。

4.0 基于交易的股权证明机制(TaPOS)

代表制是一个短时间内达成坚固共识的高效方式，而 TaPOS 为股东们提供了一个长效机制来直接批准他们的代表的行为。平均而言，51%的股东在 6 个月内会直接确认每个区块。而取决于活跃流通的股份所占的比例，差不多 10%的股东可以在几天内确认区块链。这种直接确认保障了网络的长期安全，并使所有的攻击尝试变得极度清晰易见。

5.0 高质量的服务

假设一个 DPOS 系统拥有 10 亿美元的市场总量，平均每年的交易费为 0.25%，代表们合计获得所有交易费的 10%，那么每名代表每年能获得 25,000 美元以使其节点保持在线。

这是一个利润可观的角色，许多人将为获取它持续竞争。这意味着每个想要获得这份工作的人都会想方设法从拥有这份工作的人那里把它“偷走”。为做到这

点，他们将对代表行为进行统计学分析，以找到对于标准算法的任何偏离行为。一旦找到这种偏离，他们就能有希望赢得一些选票。

那些拥有这份工作的人，可能会全力以赴地证明他们正在按标准软件运行。他们越有效地证明其对区块生产的正直性，越有可能保住他们的工作。你可以想象开发者会很快制作出系统，代表们可以通过这些系统快速证明哪些交易得到了广泛的散播。

事实上，市场竞争将产生用以证明代表们的正直性与可靠性的最具创造性的解决方案。让网络变得更安全的工作可以获得很多收益，而尝试绕轮网络则得不到什么好处。

6.0 结论

DPOS 流程与 TaPOS 结合所产生的网络，其网络共识的可证明性将至少 3 倍于比特币、点点币及未来币网络。DPOS 能够更快地达成共识，同时消除随机小股东带来小规模干扰的可能性。经济激励确保了代表们致力于证明他们有良好行为，并可能采用类似于瑞波系统的共识算法(来实现这种证明)。DPOS，事实上，是一种通过无网络分叉之虞的去中心化方式来产生瑞波特殊节点列表的方法。

注：译者完成翻译后发现 Bitsharestalk.org 上“麦可猫”也已经完成了翻译并发布在论坛。具体链接如下，供参考。

https://bitsharestalk.org/index.php?topic=4031.0