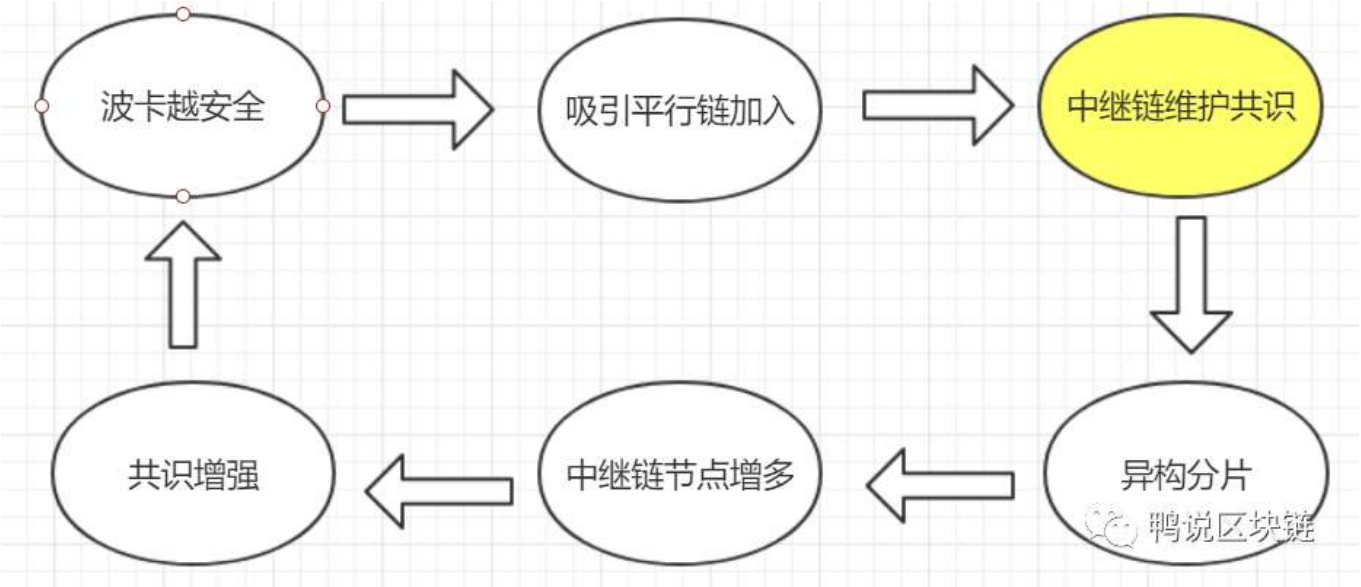
0到1全面认知波卡——提名权益证明（五）

原创 可达鸭Joie 鸭说区块链 2020-07-19 19:37

往期回顾：
0到1全面认知波卡——概述（一）
0到1全面认知波卡——跨链可组合性（二）
0到1全面认知波卡——异构分片（三）
0到1全面认知波卡——共享安全（四）

上节课我们介绍了波卡的共享安全，项目方都可以加入波卡让波卡维护共识，所有平行链共同享受波卡的安全性，只需要专注自己本身的应用。并且随着加入的平行链越多，由于波卡的异构分片模型，波卡的中继链节点就会越多，波卡就会越安全。越安全反而又吸引更多平行链加入，**这是一个良性循环发展。**



可以看出，波卡给人最大的安全感就是因为**中继链维护共识的能力**，那么中继链是如何维护共识的呢，如果中继链的节点不够分散，被一些节点垄断了，即使节点再多也不会有安全感。今天我们来聊聊波卡的**中继链如何让节点足够分散并且足够去中心化**，这是波卡**共享安全最核心的要素。**

PS.读懂本篇，需要小学数学水平（谨慎阅读）

一、共识机制

什么是共识机制呢?

以前我们把钱存在银行，我们相信有国家做担保，银行不会倒闭，钱存银行里面很放心。现在有了区块链，因为区块链是去中心化的，没有一个中间机构让大家建立信任。所以**必须要有一个规则，让节点达成共识，这个区块链才能不依托中间机构建立信任。**这个规则就叫共识机制。

比特币的共识机制是**工作量证明POW**，按劳分配，谁干得多获得记账的机会就大。最公平，但是**消耗能源多。**
点点币的共识机制是**权益证明POS**，按财分配，谁质押的币多获得记账的机会就大，它能节省能源，**但是富者更富，容易形成垄断节点。**
EOS的共识机制是**股份授权证明DPOS**，按权分配，谁获得的选票多，谁就有记账权。它的效率最高，但是只有21个节点，**不够去中心化。**

波卡的共识机制是**提名权益证明（NPOS）**，在POS的基础上改良，**完美解决了节点垄断的问题，使得网络足够去中心化，杜绝节点窜通作恶现象。**

二、验证人和提名人

在波卡的提名权益证明中，存在两个角色。

一个是**验证人**。可以认为就是做节点的矿工，任何人对维护波卡的网络感兴趣，都可以申请作验证人节点。
一个是**提名人**。可以认为就是持有DOT的散户，作为提名人，你可以用DOT投票给你信任的验证人节点，把DOT质押在这个验证人节点，获得利息。
注意，**DOT并没有转给验证人，只是质押在波卡网络，验证人无权动用质押的DOT。**

在波卡初始阶段，**正式验证人节点席位是有限的**，假如是200个。
如果你想成为正式验证人节点，那么需要提名人投票给你节点的**DOT总数能排在前列**，也就是要排在前200名，这样才会成为**正式验证人**，否则只能是**候选验证人，没有收益。**

请记住，成功当选为正式验证人并不是高枕无忧了，**提名人有权随时切换投票到其他节点**，一旦提名人不信任你，投票给你节点的DOT总数掉落在200名以外，不好意思，你就失去正式验证人资格，成为候选验证人。

波卡网络会**根据生态的发展，来动态调整正式验证人的席位。**上面说的200个正式验证人席位只是假设的，不是固定的。可以点击阅读原文查询验证人席位的数量，如下图所示，正式验证人数量是197，候选验证人数量是179。

上节课说过，**平行链越多，正式验证人节点就会越多**，因此，在目前的波卡网络初始阶段，还没有平行链所以不需要太多的正式验证人节点。这样通过动态调整，根据当前网络的需要，合理安排正式验证人席位数量，**以保证网络效率的最大化。**

三、有趣的市场调节

提名权益证明NPOS是如何让网络足够去中心化，防止垄断节点的出现的呢？

有的小伙伴说，某个验证人节点如果被很多提名人投票，比如说交易所，把用户充值的DOT投给自己做验证人节点，不就有可能成为垄断节点吗？

这里需要讲解下验证人和提名人的**利息收益是如何分配的。**

1、单个节点的收益

在POS共识机制，利息分配方式是节点质押的币越多，分得的利息越多。
而在波卡的NPOS共识机制，**利息分配不看节点质押的DOT总量，所有正式验证人节点平均分配。**

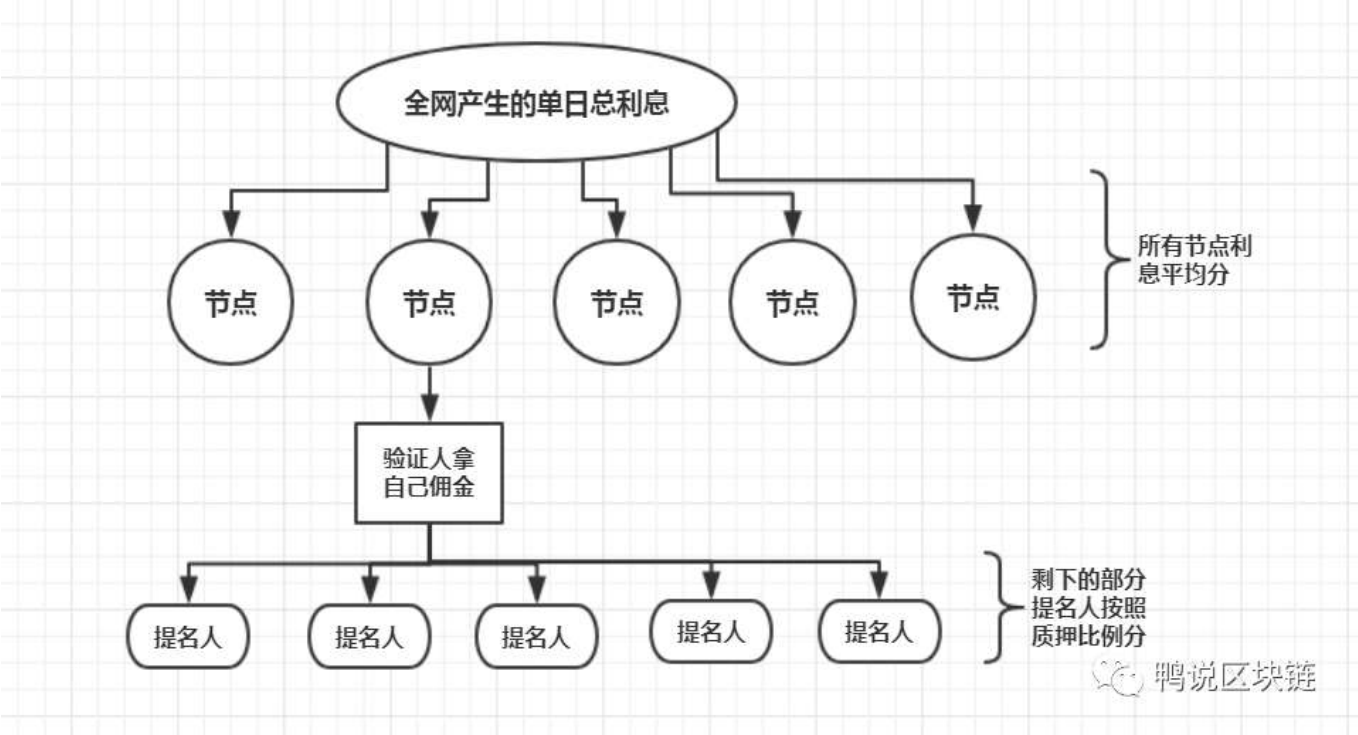
单个节点日收益 = 波卡全网当日总利息 / 正式验证人节点数

2、验证人和提名人的收益

单个节点日收益，当然是要被验证人和提名人共同瓜分的。也就是验证人和提名人要一起分这个单个节点日收益。

正式验证人的收益 = **自己设定的佣金**，在0%-100%自由设定，比如设置10%就是单个节点日收益的10%。

提名人的收益 = **单个节点的日收益** 减去 **验证人佣金**后，剩下的部分按所有提名人质押的比例分配。



3、市场调节

对于验证人来说，佣金是可以自由设定的，有的节点佣金高，有的节点佣金低，市场自由竞争。这就造成下面的情况：

1、佣金如果高了，提名人就不会投你，切换投票到佣金更低的验证人节点，**就有出局的风险。**

2、佣金如果低了，作为验证人肯定也不爽。

所以根据市场调节后，验证人佣金会**逐渐回归到一个合适的范围**，比方说5%-10%。

那么问题来了，如果你是提名人，在大多数验证人节点佣金差不多的情况下，你会投给哪个节点呢？

聪明的提名人一定会投给质押DOT总数低的节点。

为什么？因为由于平均分配，单个节点日收益都是一样的，每个验证人节点的佣金又都差不多，投给质押DOT总数低的节点，你质押的DOT占比就会更大，在所有提名人的分配中占据优势。

划重点：正因为**提名人会更愿意投票给质押总数低的节点**，才会**创建有平等质押量的验证人节点池，足够去中心化**（好好理解这句话，想想为什么）

四、特殊情况

有一种特殊情况，如果验证人节点自己投给自己，就像前面说的交易所做节点，把用户的DOT投票给自己，那如何预防垄断呢？

首先，单个节点DOT质押总量特别大的话，作为验证人节点会**损失一大笔利息。**因为每个单个节点的收益都是一样的（平均分配），明明有条件可以做多个节点，为什么要把DOT集中到一个节点去只拿一个节点的收益呢。

如果节点作恶，运行不良，比如经常掉线、死机等情况，波卡会对验证人节点进行惩罚，**质押总量越多的节点惩罚越多，**这样从规避风险的角度来看，也不会把DOT都集中到一个节点上，对于提名人来说投质押总数低的节点惩罚后损失也会降低，降低风险。

更靠谱的是，如果验证人节点之间联合作恶，那么达到一定比例，惩罚量甚至可以惩罚掉所有质押的DOT。**这更加确保波卡网络不可能会发生类似51%攻击（双花攻击）的事件。**

波卡的提名权益证明通过人性的逐利行为使节点足够分散，从落地的那一刻开始，标志着真正的去中心化网络的诞生。

——END

阅读原文