① 风险提示: 防范以"虚拟货币""区块链"名义进行非法集资的风险 —银保监会等五部门

NEW 资讯 ▼ 快讯 视频 ~ 学院 ▼ 产业区块链 海盗号 更多 -

搜索... Q

☆ 学院首页 > 区块链教程 > 新手入门 > 什么是区块链共识?

## 什么是区块链共识?

等一轮残月 管理员 船龄 7.1年 2016-04-13 15:26:00 来源 **区块链金融科技** 

共识 (Consensus) 过程是一个非常有趣的过程。

在我们的日常生活中,几乎所有的事情都是达成共识的过程。

达成共识越分散的过程, 其效率就越低, 但满意度越高, 因此也越稳定; 相反, 达成共识越集中的过程, 效率越 高,也越容易出现独裁和腐败现象。

- 达成共识常用的一种方法就是通过物质上的激励以对某个事件达成共识; 但是这种共识存在的问题就是容易 被外界其它更大的物质激励所破坏。
- 还有一种就是群体中的个体按照符合自身利益或整个群体利益的方向来对某个事件自发地达成共识;当然形 成这种自发式的以维护群体利益为核心的共识过程还是需要时间和环境因素的,但是一旦达成这样的共识趋 势,其共识结果也越稳定,越不容易被破坏。

在比特币和其它区块链币中,也存在如何达成共识的问题。或者说,**比特币或其它区块链币最核心的问题也是如** 何在去中心化的环境中达成共识。

区块链是比特市背后的核心技术,也是支撑比特币的基础架构。因此在谈区块链共识,就必然要谈比特币的共 识。

比特币最核心的突破是在去中心化的情况下对交易事件达成了共识,即在没有中心组织的情况下对某个交易的有 效性达成了一致。

比特币实现这个共识的方法主要包括两个部分:

- 1. 激励;即通过每个区块产生一定量的新比特币来激励参与者;
- 2. 引入外部资源确保安全;即通过大量的外部计算来确保共识的安全性,也就是工作量证明 (Proof of Powe r) ;

这也是几乎所有PoW币种所采用的的方法。

而这套方法要能持续长期运行下去的前提就是:

- 1. 这种激励对参与者要有足够的吸引力;也就是说比特币要一直涨价,才能吸引参与者持续参与挖矿计算,以 维护整个网络的运行;否则就会导致参与的人减少,破坏网络安全;
- 2. 没有外部攻击;由于比特币引入了外部计算来确保安全,因此只要有足够的挖矿算力(超过维护系统算力的 51%) 就能对系统成功进行攻击,这也是比特币长期存在的安全隐患之一;因为只要有钱,就能买到设备 和算力。

正是由于比特币存在的问题,例如消耗大量的资源、外部51%攻击等,出现了PoS (Proof of Stake) 共识机 理。

总体上, PoS共识理论和实践目前仍处在探索阶段。

## 推荐教程

BFT-DPOS共识机制的进化过程及背

区块链中最重要的便是共识算法,比特币修 W (ProofofWork, 工作量证明) , 以太市

比特币官网是什么?

什么是Bitlicense?

达世币 (X11 算法) 矿池挖矿教程

在ubuntu上部署OBC

怎样通过p2p网络自动下载最新版比

什么是羽毛币 (FTC)

地中海币新应用-小费自动发放系统制

BTSX新手教程一: 创建钱包注册账

比特信: 一种 P2P 消息验证和传输系

凸点赞0

☆ 5 次收藏 ペ分享

下一篇: 比特币术语解释

有引入外部的资源,因此不会担心外部攻击,例如外界的算力攻击。

看起来PoS是很完美的,但是它存在一个严重漏洞。

PoS存在内部的Nothing-at-Stake攻击。

什么是Nothing-at-Stake (常写作N@S) 攻击?

假设系统中出现了两个分支链,那么对于持有币的"挖矿者"来讲,最佳的操作策略就是同时在两个分支上进行 "挖矿",这样,无论哪个分支胜出,对币种持有者来讲,都会获得本属于他的利益,即不会有利益损失。而且 由于不需要算力消耗,因此PoS中在两个分支上挖矿是可行的。

这导致的问题是,只要系统存在分叉,"矿工们"都会同时在这几个分支上挖矿;因此在某个情况下,发起攻击 的分叉链是极有可能成功的,因为所有人也都在这个分叉链上达成了共识;而且甚至不用持有51%的币量,就可 以成功发起分叉攻击;

而这在PoW中是不可行的,因为挖矿需要消耗算力,矿工只能在一个分支上进行挖矿。

第二个问题是重写历史攻击;即攻击者可以通过购买原始持有币种的账户来从头发起攻击,重新分叉一个区块 链。因为原始的币种持有者可以将币转移至其它账户,因此他是可以在没有损失的情况下将原始账户出售给攻击 者的。攻击者需要的就是有足够数量币的原始账户;当然了,这也只是概率问题,因为有可能原始账户持有者不 会出售他们的账户,但是理论上确实存在这种攻击。

第三个问题是,尽管PoS中的挖矿不用消耗算力,运行成本很低,但是也存在如何激励矿工的问题。因为一般的P oS系统是没有新币产生的,矿工只能赚取交易费,而且在交易费不高的情况下,对矿工的激励也是很有限的。

当然了,也有很多PoS币种解决这个问题的办法就是持续的再产生新币来激励挖矿者,这导致的问题就是通胀。

上述3个问题是PoS要解决的,尤其是N@S的问题尤为重要,因为如果没有其它约束机制,这种攻击是完全有可 能实现的。

从以上可以看出,无论是PoW还是PoS机理的共识过程,其必要条件有两个:

- 1. 信息公开共享;
- 2. 个体参与;

以现实为例,事件的信息越透明、所涉及到的人员参与度越高,最终形成的共识也就越稳定、越持久。这与区块 链共识是一致的。

以上是个人的对区块链共识的一些学习心得,期望能看到更多这方面的讨论和研究文章,与爱好者一起分享。

## 全部 最佳



forestong 水手 船龄 **4.2年** 2016-04-17 21:41:56

说得很好,这也是我担忧的。存在这样天然的缺陷,是不是区块链就没有前途了呢?

△1赞 ◆回复 ♀0踩



下一篇: 比特币术语解释

凸点赞0

☆ 5 次收藏 ペ分享



巴比特学院是巴比特旗下的教育培训品牌,由巴比特主办,与专业培训机构合作,邀请业内区块链专家和实践者作为培训导师,通过导师现场授课、行业高端论坛、企业调研走访等方式,打造国内一流区块链培训品牌,推动区块链在中国的发展与创新。2018年,巴比特学院的品牌影响力将向杭州以外的北京、上海、南京、成都、深圳、广州等地辐射。

关于我们 关于巴比特

联系我们

联系人: 学院课代表

微信: btczs001

地址: 杭州市西湖区西溪首座

版权声明品牌素材

使用条款

扫码咨询



Copyright © 2011-2020 · 巴比特 · 署名-非商业性使用-相同方式共享(BY-NC-SA 3.0 CN) · 浙ICP备14013035号-8 · 🚇 浙公网安备 33010602002085号 · 站长统计 · 文章存档



凸 点赞 0

☆ 5 次收藏 ペ分享

下一篇: 比特币术语解释