IPFS星际联盟 Lv2
2020年01月06日 阅读 140

关注

Filecoin的预期共识机制

本文作者：星际联盟 原创作品，转载请注明出处

共识机制的概念

- **什么是共识机制**

  “共识机制”即是在区块链系统通过特殊节点的投票，在很短的时间内完成对交易的验证和确认；对一笔交易，如果利益不相干的若干个节点能够达成共识，我们就可以认为全网对此也能够达成共识。

- **为什么需要共识机制**

  区块链是一种去中心化的分布式账本，在区块链上，每个节点都会维护一份记录链上所有交易的账本，链上产生一笔新的交易时，各个节点接收到这个信息的时间可能不同，有些恶意节点有可能在这时发布一些错误的信息，这时就需要有节点把所有节点接收到的信息进行验证，最后公布最正确的信息。这一套系统的运行需要各个节点的参与，系统也会为节点的工作给予奖励，此时就需要共识机

共识机制能确保只有真实的事务记录在区块链上，可以在区块链技术应用的过程中有效平衡效率与安全之间的关系。

- **共识机制的目标**

1. 达成一致: 共识机制试图解决围绕分布式系统的最复杂问题之一：数据的真实性和准确性达成统一协议。与中心化系统不同，用户不必信任系统中的任何人。嵌入网络的协议规则确保了公共分类帐的状态总是随着大众的共识而更新。

2. 防止双花攻击: 共识机制防止任何用户重复消费，这是在比特币出现之前一直存在的数字货币问题。“双花攻击”指的是数字货币有可能被两次消费。区块链共识机制中嵌入的协议规则确保只有有效和真实的交易才记在公共透明的账簿中。随着矿工算力扩大以保护交易（以及网络），双花攻击或改变交易的指数变得越来越难。

3. 激励机制: 创建一个自我调节的无信任系统需要调动网络参与者的积极性。共识机制通过激励好的行为，在某些情况下，惩罚坏的行为者来实现这一点。比特币(Bitcoin)使用的第一种共识机制(工作量证明(Proof-of-Work))，通过奖励比特币(Bitcoins)给矿工，奖励他们每一笔交易的担保和验证。任何针对网络的行动(通过黑客攻击或双花攻击)都需要大量的算力和钱财，这些资源将更好地用于为系统工作(因为他们的努力会得到回报)，而不是针对系统。

4. 公平公正: 区块链的去中心化的一个重要优势是分配授权，任何人都能在同一个基础上参与进来。公共区块链的开源特性使任何人都可以检查和验证底层源代码对网络中的所有参与者是否公平。如果你愿意，就可以轻松地设置一个节点并成为参与者甚至矿工。简而言之，共识机制确保区块链不存在区别对待。

5. 容错机制: 在算法领域，容错是指分布式系统在面临威胁或故障时仍能无限运行。共识机制确保区块链是容错的，因此是可靠和一致的。

理想的共识机制需要具备的几大特性

特性	说明
Secret	选举秘密进行
Fair	选举是公平的，基于一套规则，在规则的基础上概率起作用
Single Leader	最好每轮选举出一个领导人
Unpredictable	无法预测
Verifiable	十分容易验证
Anti-attack	能够承受攻击
Efficient	消耗资源不大

三种常见共识机制

- **POW-工作量证明**

> POW是proof of work的缩写，是系统中生成要加入到区块链中的新区块时必须满足的要求。在基于工作量证明机制构建的区块链网络中，节点通过计算随机哈希散列的数值解争夺记账权，求得正确的数值解以生成区块的能力是节点算力的具体表现。 通过数学运算来争夺记账权（随机值），拥有记账权的节点就可以将打包的区块向全网进行广播并且并入到区块链上，节点会获得奖励作为参

- **POS-权益证明**

> POS即proof of stake，表现为在创建区块时要求矿工首先拥有一定量的数字货币(可通过购买方式获得)，系统根据矿工钱包中代币的多少以及存放时间来计算币龄，币龄越高，获得打包区块的概率也就越高，类似于把资产存在银行里，银行会通过你持有数字资产的数量和时间给你分配相应的收益。

- **DPOS-代理权益证明**

> DPOS的英文全写为Delegated Proof of Stake，区块链系统中持币用户可以投票来选举拥有拥有新区块打包权和验证权代表节点，系统所有交易的打包验证全部依赖这些选举出来的节点，并且节点可投票来废除某些未尽到自己义务的节点，由备用节点顶替。

- **机制缺点简要对比**

共识机制	描述	缺点
POW	工作量证明	效率严重低下；资源消耗过大；分叉概率高
POS	权益证明	不容易保持一致性；持币越多的人获得记账权的概率越大
DPOS	授权股权证明	安全性不高；与区块链去中心化的理念相悖

###Filecoin共识机制--EC预期共识

> Filecoin把矿工在网络中的当前存储数据相对于整个网络的存储比例转化为矿工投票权（voting power of the miner）

> Filecoin有抵押机制，强制参与者选择一条链，通过巧妙地结合抵押机制，对于同时挖多个链的矿工进行惩罚，这样可以非常快速地促进收敛。

> 预期共识的实现非常简单，它不需要交互，节点自己可以计算是否自己成为领导人，而且公布之后他人可以十分方便地验证。

- ## 算法描述

> 预期共识机制可使用如下公式进行描述，如果在一轮计算中，某矿工能使下式成立，则其具有出块资格

$$\mathcal{H}\left(\langle t||\text{rand}(t)\rangle_{\mathcal{M}_i}\right)/2^L \leq \frac{p_i^t}{\Sigma_j p_j^t}$$

> 左侧部分：H 为不可逆hash函数（比如 SHA256），L为 H 函数值的所占二进制的位数，可保证左侧部分的取值在0%到100%之间；
>
> H 函数内的 <t||rand(t)>是在第 t 轮的一个全网统一的随机数，这个在第 t 轮才会公布；
>
> 右侧部分：本矿机有效版算力在全网中总有效算力的占比

- ## 预期共识机制的缺点

> 预期共识机制实现了公平性、保密性、公开可验证性等特性，但它并非是完美的，其最大的问题在于出块的不稳定性；在每一个周期里面，预期选举出来的领导矿工是1个，但是在某些情况下也会选举出来多个领导矿工。

- **Filecoin共识机制改进--增加出块量**

> 既然已经明白预期共识机制存在这样的问题，那如何针对不稳定进行改进呢？一个比较直接的想法就是增加出块量；Filecoin引入了常数BlocksPerEpoch，此处简称为e，每一轮预期的出块数设定为 e 个，e的取值目前还在实验和讨论中。 我们这里进行简单地推算： 当 e=1 时，也就是最初的方案，每轮一个区块，空块率超过 1/3； 当 e=2 时，理论上可以计算出，空块轮次出现的概率将降低到 1/8 ～ 1/7； 当 e=3 时，空块轮次出现的比例将降低到 1/20

> 增加出块量的方法很简单，但可以很好地提高网络出块的稳定性。但这样又会使链上保存更多的区块数，同样，每个节点也需要做更多的同步和验证工作。鱼与熊掌，不可兼得。

- **SSLE**

> Secret Single Leader Election，即秘密单个领导人选举，是很多共识机制努力要实现的目标，为此出现了很多的研究，如 Algorand，Snow White， Stellar Consensus， BAR-Fault Tolerance Consensus， Mergeable Consensus ，也包括本文介绍的预期共识机制。

> **关注下面的标签，发现更多相似文章**

区块链

评论

输入评论...

相关推荐

专栏 · 起个帅的名 · 3天前 · 区块链
以太坊智能合约开发实战
1

专栏 · flydean · 9天前 · 区块链
区块链从入门到放弃系列教程-涵盖密码学,超级账本,以太坊,Libra,比特币等持续更新
7 2

专栏 · 十壹 · 25天前 · 区块链
前端er应该知道的区块链技术
7

专栏 · 林冠宏_指尖下的幽灵 · 7月前 · 前端 / 区块链

专栏 · 胡七筒 · 1年前 · Node.js / Go

程序猿生存指南-25 逃离帝都

106 72

专栏 · flydean · 1月前 · 区块链

一篇文章让你彻底弄懂SSL/TLS协议

5

稀土君 · 1年前 · 区块链

PRS Dapp 线上征集评选活动

专栏 · 胡七筒 · 1年前 · MySQL / Redis

程序猿生存指南-14 钱迷心窍

103 82