大家好，感谢邀请，今天来为大家分享一下区块链 共识算法的问题，以及和区块链共识算法的一些困惑，大家要是还不太明白的话，也没有关系，因为接下来将为大家分享，希望可以帮助到大家，解决大家的问题，下面就开始吧！

本文目录

区块链的基本要素包括密码技术、共识算法

基本要素包括：密码技术；共识算法；嵌入式数据库；智能合约；P2P网络。

狭义区块链是按照时间顺序，将数据区块以顺序相连的方式组合成的链式数据结构，并以密码学方式保证的不可篡改和不可伪造的分布式账本。

广义区块链技术是利用块链式数据结构验证与存储数据，利用分布式节点共识算法生成和更新数据，利用密码学的方式保证数据传输和访问的安全、利用由自动化脚本代码组成的智能合约，编程和操作数据的全新的分布式基础架构与计算范式。

区块链中的共识机制是什么

我在上一篇文章讨论了什么是区块链。为了方便大家理解，文章中并没有使用过多技术术语。今天我们来聊聊区块链中的灵魂——共识机制。还不了解区块链的小伙伴可以点击链接回顾上一篇的内容10分钟快速了解是什么是区块链，同样你也可以参考下面的内容，快速回顾区块链的定义以及特点。

区块链它是一个去中心化的分布式加密的共享账本（或数据库），存储在其中的数据或信息，具有不可篡改、不可伪造、全程留痕、可追溯、公开透明，集体维护等特点。

什么是共识机制

所谓共识机制，是一种多方协作的机制。旨在保障多方在安全可信、难以欺诈的模式下，最终达成相互认可的一致性结果，从而解决多方信任问题。

用一句话描述在区块链中的共识机制，其实就是用来决定多节点参与的情况下最终有哪个节点参与记账的技术手段与机制。

例如：

我们经常在港剧看到，法官会在正式裁决之前，先聆听陪审团的结论。而陪审团会就案件整体的证据链做出客观的判断。最终陪审团的全部成员会对指控达成一直结论，并对被告人的某项罪名成立与否向法官和听审人员做出陈述。那么他们如果说对被告人的指控不成立，那么基本上法官也会参考陪审团的决议。

陪审团成员会参与庭审，同时可以获得完整的证据链。其次他们都有一个共同的目标，就现有的证据而言做出理性的分析，判断被告人的罪名是否成立。而后经过成员会互相阐述各自的观点，并相互监督。最后将达成一致的结果提交给法官，这个过程就是共识过程。

（这常见于英美的司法体系中，我们知道香港在回归祖国之前曾经是英国统治，所以使用的英美的司法体系，1997年香港回归祖国，在‘一国两制’的背景下，香港的司法制度得以延续。）

为什么共识机制是区块链中的灵魂？

由于区块链是一个去中心化的分布式账本，其应用场景大多是需要多方参与的情况。设想一下如果每个人都可以自由的操控区块链里面的数据，当一笔交易到来需要在区块链中记账，那么所有网络的参与节点都将尝试对此进行处理，那又如何来确定应该使用哪一个节点所反馈的结果呢？

中本聪伟大的地方在于，它采用了巧妙的设计来解决这一个问题。我们都知道比特币是基于区块链技术的数字货币的一种应用，其发行过程不依赖于任何机构，而是通过挖矿。那挖矿是什么呢？其实所谓的挖矿本身是分布式网络节点共同参与的名为POW（ProofofWork，工作量证明）的共识过程来完成交易的验证与获得记账权的。

在比特币中共识过程本身就是挖矿，参与挖矿的节点称之为矿工。矿工的职责是完成继续所出的一套数学题，谁最先完成运算谁将获得最终的记账权。我们来一起看下究竟是怎么样的数学题才能完美解决记账权争夺战。

具体如下：

生成交易，并与其它所有准备打包进区块的交易组成交易列表，生成Merkle根哈希值。

将Merkle根哈希值，与区块头其它字段组成区块头，80字节长度的区块头作为Po

w算法的输入。

区块头=Nonce+上一个区块HASH值+当前Merkle跟HASH+难度值+时间戳+版本

不断变更区块头中的随机数Nonce，对变更后的区块头做双重SHA256哈希运算，与当前难度的目标值做比对，如果小于目标难度，即Pow完成。

SHA256（SHA256(version,hashPrevBlock,hashMerkleRoot,time,bits,nonce))<TARGET

Pow完成的区块向全网广播，其他节点将验证其是否符合规则，如果验证有效，其他节点将接收此区块，并附加在已有区块链之后，之后将进入下一轮挖矿。

PoW优缺点

优点：

去中心化，将记账权公平的分派到其他节点记账权是通过看节点的PoW，谁挖矿最快，谁就能拿到记账权。

安全性高，作恶需要花费高昂的成本，因为获得正确哈希值的概率和算力成正比，如果没有掌握51%的算力就不能作弊，由于作恶的成本远远高于诚实挖矿的成本，因此安全性高。

缺点：

会造成资源浪费因为挖矿需要大量的哈希运算，需要电力和各种算力资源，而且找到合适的哈希值实际上并没有其他的作用。

网络性能太低因为比特币出块的时间是10分钟，所以交易确认至少需要10分钟，而且目前支持支持每秒7笔交易的速度，不适合商业用处。

PoW共识算法算力集中化。目前挖矿矿池是主力，算力高的矿池有选择权，持本人么有参与决定的权利。

常用的几种共识机制

今天我们通过一个例子了解了什么是共识机制，以及共识机制在区块链中的意义。

通过对POW的机制的研究，了解到比特币通过挖矿的机制保障节点间共识。在文章的最后我列举了常见的共识机制以后有机会我们深入探讨。

欢迎关注我的头条号，我们可以进一步讨论。

OK，本文到此结束，希望对大家有所帮助。