最近有一位之前找过的用户问了我们小编的一个问题，我相信这也是很多币圈朋友经常会疑惑的问题：去中心化存储相关问题，去中心化存储龙头相关问题，带着这一个问题，让专业的小编告诉您原因。

说到区块链，我们常常会碰到“去中心化”这个概念。那么到底什么是去中心化？中本聪解决了自己定义的难题“点对点的电子现金”，在这个过程中，他“发明”了区块链技术。比特币系统融合密码学、博弈论和软件工程等三个领域的技术与理论，区块链技术是已有技术巧妙地组合形成的创新。中本聪不是凭空解决“点对点电子现金”这个难题的，他沿着前人的足迹前进，只是他完成了最后一跃。

“去中心化”是摘除掉中心化的中心节点的竞争优势。它不代表没有中心，只是中心节点是一种相对中立的存在。这些中心节点不会是强制性的存在。而对于完全去中心化的系统，节点和节点之间的联系不通过特定的节点完成，所有的节点都可以在系统上存储和更新数据，从而实现公开化。

区块链的去中心化区块链本质上是一个去中心化的分布式账本数据库。简单的理解就是区块链的数据是分散的存储在网络中许多节点上的。而传统的数据存储方式，则是存在网络中1个或几个大节点上的。由此看来，所谓的中心化与去中心化，说白了就是存储数据的节点的多少的区别。所以，区块链的去中心化是相对的。数据只存在1个节点上，肯定就是中心化的。但如果存在100个节点上，它们相对于1个节点就可以说是去中心化，只是去中心化的程度不一样而已。同时，中心化与去中心化也并不矛盾，并不是完全对立的，因为去中心化中的“去”字是表示弱化、消除中心的过程，而不是绝对没有中心，与无中心化是完全对立的概念。

链乔教育在线旗下学硕创新区块链技术工作站是中国教育部学校规划建设发展中心开展的“智慧学习工场2020-学硕创新工作站”唯一获准的“区块链技术专业”试点工作站。专业站立足为学生提供多样化成长路径，推进专业学位研究生产学研结合培养模式改革，构建应用型、复合型人才培养体系。

有用的工作量证明（Proof of Useful Work）是由著名的去中心化存储项目 FileCoin 在它的白皮书里提出来的一个概念。工作量证明，Proof of Work，POW 是实现区块链的一个重要共识方式，FileCoin 要实现一个基于区块链的存储平台。所以它也要做共识，它选择的就是工作量证明共识。

首先我们来解释一下常规的工作量证明。它是区块链实现共识的一种方式。是比特币采用的方式，所以，工作量证明就是俗称的“挖矿”。比特币做为一个去中心化的点对点交易系统，要在不同的节点上维护一个共同的完全相同的帐本，来记录所有的交易，而且确保交易不会重复，不会一笔钱多花，就需要一个维护这个账本一

致性的规则。大家一起遵守这个规则，就是共识。区块链常用的方法是，把这个账本分成很多页，每个页就是一个区块。每个区块由一个节点来记账，然后分发给其他节点复制，这样所有节点上的账本都是一样的。但是每个区块都由哪个节点来记录，就需要一个大家都能遵守的规则。比特币采用的方法，是让所有的节点做一道简单的数学题，题目很简单，但是计算量很大，一般要10分钟左右才能做出答案来。得到答案虽然很费时间，但是验证答案是否正确很容易。然后所有的节点同时做题，第一个做出来的节点，就得到下一个区块的记账权。因为每个区块都只有唯一一个最早做出题的节点，所以，每个区块的记账权是唯一的，而且也是很容易被其他节点验证的。节点一旦验证到其他节点得到了区块记账权，就必须复制区块，加到本地区块链中，同时开始下一个区块记账权的竞争。通过这种方式，比特币就能确保所有节点的区块链是一致的。

节点通过大量计算竞争区块记账权的的过程，就是工作量证明。所以，工作量证明系统（或者说协议、函数），是一种应对拒绝服务攻击和其他服务滥用的经济对策。它要求发起者进行一定量的运算，也就意味着需要消耗计算机一定的时间。这个概念由 Cynthia Dwork 和 Moni Naor 1993
年在学术论文中首次提出。而工作量证明（POW）这个名词，则是在 1999 年 Markus Jakobsson 和 Ari Juels 的文章中才被真正提出。

实现区块链共识的方式还有很多，如POS，DPOS，POA，PBFT等等，但是工作量证明是唯一被时间验证过（11年）的在公链上运行的区块链共识机制。

工作量证明存在一个什么样的问题呢？还是用比特币为例。比特币节点为了获取出块权做得那个数学题，叫哈希运算。计算量非常大，每一台参与比特币挖矿的矿机都要时刻进行这个计算，耗费大量的电力。这个计算不像其他的如大数据处理的计算，可以产生一些价值，它的唯一目的，就是竞争出一个节点，成为下一区块的出块者。目前比特币每年消耗电量约25.5亿瓦，这相当于全球电量的0.5%，是爱尔兰一年的耗电量。反对POW的人纷纷指责挖矿将电力资源浪费在虚无缥缈的数字货币上，还称之为自由主义的“泔水”。

但是，认为POW是浪费的电的人不知道，正是能源和算力打造了比特币安全不可攻破的体系。

一张100元的现金不只是你我认为他值100，而是整个社会群体都认为他值100，价值就是来自于共识。比特币是社区行为，来自不同国家的人聚集到社区，用互联网来建立秩序，它的意义也是来自于群体共识，只要大家都相信比特币有价值，只共识存在，那么他就有价值，和法币一模一样。所以产生价值认同并不一定需要国家来驱动，比特币改革了一种传递信任的载体和媒介，千百年来，人类社会通过多少流血战争建立的政权和共识，现在兵不血刃，只是耗费些电力就实现，岂不是更

先进。

总结而言，要想设计一个去中心化而且安全的数字货币，能源和算力是必要的代价。工作量证明是以去中心化形式构建安全产权认证系统的唯一方案。所以认为POW是浪费的电的人不知道，正是能源和算力打造了比特币安全不可攻破的体系。现在比特币全网算力已经达到一个非常恐怖的地步，任何人想要发动51%算力攻击已经是不可能的事情了，POW算法使比特币系统牢不可破。

为缔造价值而产生的消耗不叫浪费。

但是，如此多的算力，是否可以用来创造更多的价值呢？用 FileCoin 的话说，工作量证明，还有没有其他用途呢？

FileCoin 是分布式存储行业的明星项目。他的开发团队 Protocol Lab 就是开发 IPFS 协议的团队，以至于很多人都分不清FileCoin 和 IPFS 的区别。可以说是2017年 FileCoin 的1CO，把这个行业推向巅峰，也引出了一系列的同类型项目。本文无意于赞誉或者贬低这个项目，只想结合自己从事这个行业的经验，表达一些自己的观点，尽量做到客观公正。希望对从事这个行业的人有一些启发。

FileCoin 在白皮书中提出要实现一个有用的工作量证明，实际上就是认可了，要打造一个安全不可攻破的区块链，就必须消耗工作量。但是，他们不希望为这个工作量做出的计算完全被浪费，所以想把这个工作量利用起来。所以，他们想到的方法是，在工作量证明里加入存储空间的使用率。这样，所有的节点为了形成共识，就必须提供存储空间来存文件。这个存储空间就可以存用户数据，就是有用的。

那我们来看一下FileCoin是怎样实现这种有用的工作量证明共识的。

Filecoin采用的共识机制并不是简单的工作量证明，而是一种叫做预期共识（Expected Consensus，简称 EC）的机制。和其他主流共识机制目标一样，让矿工争夺某一个高度唯一的出块权而获得奖励。这个获得出块权的矿工叫做 Leader。在每一轮的出块争夺中，为了保证账本的可靠性，都有一个唯一的 leader 来进行记账。

也就是说，共识的核心就是选择谁来当 Leader。选 Leader 的方式一般有两种，交互式或者非交互式。交互式是要矿工之间互相投票的。比如 PBFT 就是交互式的，几个参与选举的人通过互发信息，得到多数票（ 超过 2/3 ）的人就是 Leader。预期共识采用了非交互式的方式来选举 Leader。参与的各方根本不给彼此发消息，而是每个节点各自独立私下进行运算。最后某个节点说，我

赢得了选举，然后提供一个证明，其他人可以很容易就验证，他确实赢得了选举。这个验证方法就是零知识证明。

预期共识机制会为区块链网络预设一个出块的期望值。比如每1个纪元（epoch）生成1个区块（block），但也有一个纪元可能出现空块或多个区块的情况。所以在Filecoin 中，每个高度不是一个区块，而是一个区块集，叫做 TipSet，这个TipSet 中可能包含了多个区块。所以实际上 Filecoin 是 TipSet链。预期共识无法保证每一轮只选举出一个 Leader，所以会出现一轮中有多个Leader 的可能，这样链式结构就变成了DAG的网状结构。所以 FileCoin 还会对block 赋权重，实现有效收敛。

FileCoin 采用的 EC 共识有一个好处。对于传统的 POS 共识机制来说，有一个重大问题就是无法控制分叉。也就是说，由于挖矿成本低，参与者可以同时挖多个链获取利益。而预期共识对这一点做了设计，那就是通过权重和抵押机制来促使矿工选择一条最好的链，对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。这说明 POW 和 POS 共同使用会是一种好的方式。

每一个矿工获得出块的可能与其当前有效存储量占全网总存储量正相关。这种期望共识机制其实是更像是 POS 权益证明，只是它将POS里边的权益（Staking）换成了有效存储占比。但是矿工的有效存储从何而来呢？是通过存储用户数据得来。如何证明矿工存储了用户的数据，FileCoin 创造出一个新的证明机制叫 POST时空复制证明。这个 POST 就是 FileCoin 的工作量了。把耗电的算力换成存储有用数据的存储空间，无意义的军备竞争变成了存储服务市场竞争。这确实是FileCoin 的进步之处。只不过，为了成功的出块，矿工通过预期共识被选为出块节点后，必须在一个块的时间里（现在是45秒）做个 POST 证明，成功提交，才能出块。否则就失去机会。所以，为了确保矿工能在指定时间内出块，最终官方还是决定要使用 GPU。虽然这 GPU 不是像工作量证明那样一直不停的工作，但是在整个实现共识的过程中还是出现了跟有用的工作量证明思想相违背的耗能计算。

还有，谈到预期共识的时候，我们说到每一个纪元出块都不是一个块，而是一组块，那么纪元这个概念就很重要了。怎么控制纪元呢？每个矿工在参与选举前，需要先生成一个 Ticket，这个 Ticket 实际上是一个随机数，他需要走一个 VDF 和 VRF的流程，这个 VDF 全称 Verifiable Delay Function，可验证的延时函数。他的计算流程是串行的，需要花费一定的时间，并且这个时间无法通过多核并行的方式进行缩减。这保证了每个矿工产生 Ticket 时必须要消耗的时间，没有人可以通过优化硬件的方式来获得加速。听上去这函数很完美，可是，这个 VDF根本还不存在！现在 FileCoin 测试网直接使用了一个等待函数 sleep，这是UDF，Unverifiable Delay Function。现在最接近的 VDF解决方案，也是需要消耗大量计算资源的。说白了，还是要耗电，还是不环保。

所以，有用的工作量证明，依然只是一个美好的愿望，理想很丰满，但现实很骨感。被誉为下一个比特币的 FIL，还要继续为实现这个颠覆性的共识而努力。

总结一下FileCoin存储矿工获取激励的流程：用户存储数据，支付FIL费用 – 矿工存储数据 – 生成复制证明 – 完成时空证明 – 经过EC共识，选出出块Leader – 获取打包权 – 矿工获取FIL奖励

在这个流程图上，可以看到，矿工可以在两个地方获取奖励。一个是存储用户文件的时候可以得到用户的FIL奖励。一个是在获取区块打包权后获得FIL。而得到区块打包权的一个前提就是存有足够多的用户数据。所以，在存储需求不够大的情况下，矿工会从用户那里收取很低廉的费用。在用户不够的情况下，甚至会倒贴钱自己付FIL存数据，只为能够存足够多的数据，在 EC 共识中被选成 Leader 得到打包奖励。这样产生的效果是，FileCoin 对用户非常友好，存储费用非常低。所以，一定会吸引很多的应用来这个平台上做开发。但是缺点也很明显，如果存储量不够大，矿工根本没法跟其他人争夺出块权，所以得不到奖励。最后整个平台会朝着大矿工，大矿池的方向发展，这跟 FileCoin 想把所有闲散服务器利用起来实现分布式存储的初衷是违背的。或者说，一定要等到这个行业具有一定规模，技术更成熟，才有小矿机挖矿的机会。

我们先来简单的讲一讲中心化存储和去中心化存储各自的利弊。中心化存储设备统一管理，可靠性好，性能高，去中心化存储数据天然分散，易于流通，容灾性好，但是可靠性低。从经济角度来说，中心化存储是重资产投入，成本高。去中心化存储通过区块链激励层，用户自行加入，轻资产，可降低存储总成本。未来应用数据的存储和处理还会是以中心化存储为主，而去中心化存储因为是分布式网络，主要可用于热门数据流量分发。同时，因为没有中心化所有权，可以成为去中心化应用的首选。

市场上有一种说法是，去中心化网络适合冷数据的备份，其实这并不是去中心化存储的优点，实在是因为把热数据放到去中心化网络上太不可靠，处理性能也跟不上。所以，如果去中心化存储能实现一定的规模效应，大大降低存储成本，把冷数据备份当作核心业务，并把目标定位在今天因为成本太高没被企业存储的冷数据，会是一个很好的发展方向。

如此说来，从技术上讲，去中心化存储并不一定比中心化存储有优势。如果能推行一种新的模式，把去中心化的经济激励和中心化的存储合在一起，就能吸收两者的长处。真正实现有用的工作量。FileCoin 未来可能促成的大矿场模式的数据中心，可能更有市场。

在11年后的今天，比特币并没有实现它成为一个点对点的电子支付货币的初衷，

但阻止不了人类前赴后继的去买它，拥有它。同样，我相信 FileCoin 已经得到足够大的社群，矿工和开发者的支持，即使在可预见的未来，它不会促成分布式存储应用的全面落地（也许这从来不是 FileCoin 的目标），但我还是相信会有很多人会因为它的共识去购买它，持有它。上升到哲学层面，人类在为真理买单。

那么在实际生活中，何为有用，或者说，我们到底是在用存储做共识还是用共识做存储？FileCoin 是前者。FileCoin 想要基于存储工作量实现的去中心化的共识，理论上是完美的，追求完美，人类是要付出代价的。这也是为什么在这个项目上我们等待了这么长的时间。但是一旦实现，它可能会为人类带来巨大价值，对市场带来无穷大的号召力。

只不过去中心化不是万物的灵药。中心化的一个最大优势是它的效率非常高。像dPOS或者联盟链这样的弱中心化共识兼顾两者优势，能更快速的把应用推向市场，提前启动分布式存储行业，推进分布式存储应用落地。所以，我们既追求用存储做共识，也追求用共识做存储，根据实际需求来做出我们的选择。在这个过程中，相信区块链也会进一步发展，逐步优化，变得越来越有用。

IPFS(InterPlanetary File System，星际文件系统），它是一种全新的超媒体文本传输协议，可以把它理解为一种支持分布式存储的网站。IPFS
诞生于2015年、2017年8月，IPFS 的激励层filecoin，公开众筹在很短时间内，就募集了超过2.57亿美金，相当于接近20个亿人民币的投资！所以它引起了全世界投资人的高度关注！与此同时它打破纪录，创造了当年全球ICO的奇迹，当之无愧的成为了一个全球瞩目堪比当年以太坊的明星项目！

相对应的就是现在大家所熟悉的以 http 开头的中心化存储网站。这跟我们平时使用的百度云，阿里云这些网站有什么不一样呢？各位不妨思考一下，你存储在U盘，网盘上的这些数据 是绝对的安全吗？答案是否定的！它会丢失，甚至会被和谐掉，对吗？比如从前的金山网盘，360网盘，官方通道已经关闭了，文件需要大量的转移，时间精力都浪费了，另外像百度网盘，免费用户使用的空间也是有限的，如果你想增加储存容量就必须得充值，而且安全性也是有待考究的。

而 IPFS 的网络存储文件，使用的是去中心化分片加密存储技术，把文件分割成了多个片段，存储在网络的各个节点上，而这些节点就是我们使用的电脑，当你下载文件的时候，或者想

要打开文件的时候，IPFS 网络会自动把文件还原，给你使用、供你下载，可以防止某个人或者某个机构控制你的数据，也可以防止被黑客攻击，这样就可以保护我们的存储数据，不会被随意篡改、删除了！此外，使用IPFS
网络进行文件存储、文件下载，在速度方面 可是相当的快！IPFS

最大的神奇之处呢，是彻底告别了传统的HTTP协议常见的卡顿和404错误。

互联网的发展一共经历的三个阶段：

所谓的Web1.0，就是互联网的早期形态。

提出年代：20世纪90年代中期

特征表现：国内以搜狐、网易、新浪、腾讯为代表的一批门户型网站诞生，人们对新闻信息的获取是其利用网络的主要驱动力，巨大的点击流量诞生了新的商业模式。

由网站的运营者生产内容。那时候的网站几乎不记录用户数据。这使得想在网上进行复杂的活动几乎不可能。因为你不知道谁来过，看得啥，做了什么。

随着微博，微信的崛起，我们进入了现在所处的Web2.0时代。

提出年代：21世纪初期

特征表现：BBS、博客、RSS（聚合内容）兴起与繁荣。人的重要性与参与性上升，用户既是互联网内容的浏览者，也是制造者。

在这个时代，每个人都是内容的生产者。如果说Web1.0时代给了我们一个绚丽的画廊，我们只是过客。只能被动的观看画廊中布置的作品。

那么进入Web2.0时代，我们迎来了一个可以自由创新的共享空间。在这里我们即欣赏他人创作，可共享我们的创意。但这个空间的主人并不是我们。比如有一天你不用微信了，那么你在上面的所有信息也就没有了。换句话说，在Web2.0时代，你的网络身份不属于你自己。而是属于这些科技巨头。我们有没有可能主宰自己的数据呢？

有！这就是Web3.0

提出年代：2010年左右

特征表现：网络模式实现不同终端的兼容，从PC互联网到WAP手机，移动互联让普通人群的参与方式呈现更多的可能。基于物联技术的飞跃，跨平台支付、大数据经济等发力迅猛。

Web3.0的提法来自区块链，以太坊的联合创始人Gavin Wood博士。第一个提出了Web3.0的概念在这个网络中一切都是去中心化。

没有服务器，没有中心化机构。更没有权威或垄断组织掌控信息流。而要构造这个一个庞大的Web3.0，信息存储和文件传输的去中心化就是核心之一。

人类社会自进入互联网时代以来，信息爆发式增长，过去两年，新产生的数据占据了人类文明的90%，传统的硬盘级别磁盘列阵存储方式。也渐渐被在最新的云存储技术所替代。云存储就是把存储资源放到云上，然后供人存取。各种不同类型的存储设备通过应用软件集合起来协同工作，保证数据的安全性并节约了存储空间。使用者可以在任何时间任何地点通过任何可联网的装置，使用云上数据。

云存储同时也带来了很多隐患，最大的就是数据存储安全方面的问题。分为以下四类。

第一类：最常见的就是服务器被攻击，数据被盗取的风险。

第二类：属于操作失误或运作流程的缺陷比如腾讯云因为操作失误，导致创业公司，前言数控技术。存在在上面价值上千万的核心数据全部丢失，导致该公司直接停业。

第三类：属于服务器自身故障，导致数据丢失或错误。比如亚马逊云。2019年8月，币安在使用过程中由于出现故障，导致比特币交易价格由正常的接近一万美元变为0.32美元 造成巨大损失

第四类：如果服务商，因为亏损或者政策等原因停止运营，那用户的数据像何处迁移。数据安全由谁负责，这些都是云存储服务提供商所面临的困境。再说说中心化文件传输方案所面临的问题。主要是文件获取效率低下。有两种情况：1，当我们浏览或者下载一部高清电影。那么这台计算机服务器的响应速度和他 网络通信环境就限制了我们浏览和下载文件的速度。第二张我们要获取的这个文件。可能存储在地球的另一端的服务器上，在这种情况下。获取文件的速度也会低下。面对传统互联网安全性能查和效率低下的问题。有没有更好的解决办法呢？有，这就是基于点对点网络的去中心化文件存储及传输协议IPFS。

IPFS，全称是星际文件系统（interplanetary file eystem）由毕业于斯坦福大学的创始人Juan Benet（胡安，贝内特）和他的团队创办。IPFS协议，主要从数据存储和文件传输。两个方面做了架构性的革新。比如大卫要在IFPS系统中保存一段视频，系统会把文件打碎成若干个大小一样的碎片。然后对每个碎片进行哈希运算得到一个数值，称为哈希值，然后再将所有这些碎片

的哈希值及相关数据一起整理并在此进行哈希运算。得到一个最终的哈希值。然后被传输到IPFS系统中。很有可能你的文件中一部分碎片就存储在你邻居家的硬盘中。可是他既不知道这些碎片的内容是什么，也不知道替谁存储了文件，只要没有该文件对应的哈希值任何个人和机构就无法查看你的文件内容，这样我们就不用担心自己我数据被人利用。文件的碎片会被备份多次保留在IPFS系统中的多个节点上。这样即使黑客能攻击其中的个别节点。或者发生区域性的自然灾害，甚至类似911的这种。其他节点依然能保持文件的完整性，在文件传输方面。当我们使用IPFS访问或者下载文件时。我们像系统提交的是改文件的哈希值，因此，只要文件存在于整个IPFS系统中。系统就能帮我们通过最近的网络距离找出这个内容。

这样的处理方式，至少在两个方面都比传统互联网有优势，在搜索方面。HTTP是根据地质寻找内容，比如在没有电话，电报的年代。张三的朋友李四住在北京东城区灯草胡同730号。如果张三要从杭州去找李四就得根据这个地址千里走单骑，结果好不容易到了地方。发现房子还在可是李四已经搬走了。这就是我们传统互联网搜索内容经常会碰到的问题。而在IPFS中，文件是按照内容进行搜索的。甭管李四在世界的哪个角落，我都可以通过各种通信设备找到他，而不再是通过古老的地址检索，在效率方面。比如张三要下载一份视频资料，一共10GB大小，如果这份资料存储在地球另一端某个服务器上。那得经过若干路由从遥远的服务器中，像蚂蚁搬家那样一点点的下载。就好比一艘货轮拉了满仓货物通过海洋慢慢的给运过来。而在IPFS中，系统会从离我们网络距离若干节点，同时向我们传输这个文件的碎片。由于每个碎片只有256KB大小，所以速度将快的惊人。因此无论从传输距离还是从传输容量上。IPFS都大大优于HTTP协议。尽管IPFS有大大了优点，但同时也有缺陷。比如在隐私的保护方面。

由于在IPFS中，文件的检索是根据文件内容的哈希值来进行的，因此这个哈希值如果泄露给第三方。那么第三方就可以毫无门槛的下载这个文件，对此有没有解决办法呢？

有！那就是用户把文件上传到IPFS之前，先对他进行加密。将即使第三方下载了这个文件，他也看不到原始内容。

因此在Web3.0即将开启的时代，IPFS在数据确权，存储安全文件封发及传输效率方面都比Web2.0大大的迈进了一步，新生的IPFS虽然还不尽完善，但这并不影响他的贡献和价值。1991年，蒂姆 博纳斯 李发明的HTTP协议搭建了互联网世界的高速公路，从此我们对信息的传递可以在一瞬间抵达世界的各个角落。30年后，胡安 贝内特和他的团队创建了IPFS协议将重塑这个新世界的数据航道，让人类信息得以永存！正是因为有这样的一群人，推进着科技文明的进步。才得以让我们对未来的探索，有了更多的可能。然而如此宏大的系统要实现稳健运行，就得需要充足的燃料来维持，IPFS要想在完整的应用生态中发挥作用，还需要激励机制和一套完整

的运行系统。

为此Filecoin应运而生。

去中心化存储是很多人头疼的问题，尤其是在理解和现实的冲突方面，去中心化存储龙头也同样面临着相似的问题，关注我们，为您服务，是我们的荣幸！