区块链技术（4）-去中心化的共识机制

2018-04-10 陈皓

区块链技术（4）-去中心化的共识机制
陈皓
- 00:02 / 22:37

其实，去中心化的共识机制也是要解决拜占庭将军问题（The Byzantine Generals Problem），它是莱斯利·兰伯特（Leslie Lamport）1982年提出，用来解释一致性问题的一个虚构模型。它是分布式领域中最复杂、最严格的容错模型。

分布式一致性算法

拜占庭的将军们没有一个中心化的领导机构，所以，如果他们需要攻击某个城市，所有将军需要对任何将军可能提出的攻击时间达成共识。也就是说，只有所有的将军都达成了共识，在同一个攻击时间攻击，就有非常大的胜率。但是，问题来了。这时，可能会有多个将军同时发出不同的攻击计划，而且这些将军中还有叛徒。那么，将军们怎样达成共识呢？

莱斯利·兰伯特证明，当叛变者不超过 1/3时，存在有效的算法。不论叛变者如何折腾，忠诚的将军们总能达成一致的结果。如果叛变者过多，则无法保证一定能达到一致性。

拜占庭问题之所以难解，在于任何时候系统中都可能存在多个提案（因为提案成本很低），并且要完成最终的一致性确认过程十分困难，容易受干扰。但一旦确认，即为最终确认。

比特币的区块链网络在设计时使用的 PoW（Proof of Work） 算法思路。一个是限制一段时间内整个网络中出现提案的个数（增加提案成本），另外一个是放宽对最终一致性确认的需求，约定好大家都确认并沿着已知最长的链进行拓宽。

也就是说，如果比特币系统在某一个时刻同时出现了两个都合法的区块，那么两个都承认。于是，区块链上会出现两个合法的分支（术语叫"分叉"）。此时矿工可以选择任何一个分支继续，在某个分支的长度超过了另一个分支时，短的那个分支马上作废。

如果你看过我之前写的《分布式系统架构的本质》，那么一定知道Paxos协议，这也是一种分布式一致性的共识算法。但为什么不用Paxos和Raft来做区块链的一致性算法的协议呢？这两个算法对资源的消耗比PoW要小得多呢。

如果你熟悉这几个算法，那么你就知道PoW和Paxos/Raft的算法在本质上有下面这些不同。

- 对于Paxos/Raft，其需要Leader选举，而对于比特币或者以太坊这样的无中心化的方式是没有leader的。
- 对于Paxos/Raft，加入其网络（集群）的结点前提假设都是受信的。然而，对于比特币/以太坊来说，其前提假设都是不受信的，它们只相信，超过一半的结点所同意的东西。
- 对于Paxos/Raft，需要事先对整个集群中的结点数有定义，而无中心化的比特币和以太坊中的结点是想来就来，想走就走，来去自由。如果Paxos/Raft在这样的环境下，其会处于一个非常尴尬的境地——要能随时进行伸缩。而且，Paxos/Raft并不适合在一个非常大的网络中玩（比如上百万的结点）。

但是它们有一些是相同的。

- 它们都是一致性的算法。
- 对系统的修改总是需要一个人来干（区块链用PoW消耗资源，让提案变得困难，Paxos/Raft用领导选举）。
- 系统中暂时的不一致是可以被修正的（区块链会考虑最长链，牺牲了强一致性，保证了可用性，Paxos/Raft如果没有超过半数的结点在线，会停止工作，牺牲了可用性，保证了强一性）。

总之，区块链所面对的无中心化的P2P网络要比Paxos/Raft所面对的相对中心式分布式网络要复杂多得多。所以，不太可能使用Paxos/Raft协议来替代PoW协议。除非，你想干一个相对中心化的区块链，然而这就成了区块链的一个悖论了。

无论你是搞区块链，还是搞分布式，你都需要知道拜占庭容错系统研究中的三个重要理论：CAP、FLP 和 DLS。

- CAP理论 - "在网络发生阻断（partition）时，你只能选择数据的一致性（consistency）或可用性（availability），无法两者兼得"。论点比较直观：如果网络因阻断而分隔为二，在其中一边我送出一笔交易："将我的十元给A"；在另一半我送出另一笔交易："将我的十元给B "。此时系统要么是，a）无可用性，即这两笔交易至少会有一笔交易不会被接受；要么就是，b）无一致性，一半看到的是A多了十元而另一半则看到B多了十元。要注意的是，CAP理论和扩展性（scalability）是无关的，在分片（sharded）或非分片的系统皆适用。
- FLP impossibility-在异步环境中，如果节点间的网络延迟没有上限，只要有一个恶意节点存在，就没有算法能在有限的时间内达成共识。但值得注意的是， "Las Vegas"

algorithms（这个算法又叫撞大运算法，其保证结果正确，只是在运算时所用资源上进行赌博。一个简单的例子是随机快速排序，它的pivot是随机选的，但排序结果永远一致）在每一轮皆有一定机率达成共识，随着时间增加，机率会越趋近于1。而这也是许多成功的共识演算法会采用的解决办法。

- 容错的上限-由DLS论文我们可以得到以下结论。
  - 在部分同步（partially synchronous）的网络环境中（即网络延迟有一定的上限，但我们无法事先知道上限是多少），协议可以容忍最多1/3的拜占庭故障（Byzantine fault）。
  - 在异步（asynchronous）网络环境中，具确定性质的协议无法容忍任何错误，但这篇论文并没有提及 randomized algorithms 在这种情况可以容忍最多1/3的拜占庭故障。
  - 在同步（synchronous）网络环境中（网络延迟有上限且上限是已知的），协议可以容忍100%的拜占庭故障。但当超过1/2的节点为恶意节点时，会有一些限制条件。要注意的是，我们考虑的是"具认证特性的拜占庭模型（authenticated Byzantine）"，而不是"一般的拜占庭模型"。具认证特性指的是将如今已经过大量研究且成本低廉的公私钥加密机制应用在我们的算法中。

工作量证明

比特币的挖矿算法并不是比特币开创的，其原型叫 Hashcash。这个想法最初是由哈佛大学的女计算机科学家辛西娅·德沃克(Cynthia Dwork)、加州伯克立大学的Moni Naor和Eli Ponyatovski于1992年的"Pricing via Processing or Combatting Junk Mail"论文中提出来的。是的，一开始这个算法是用来限制垃圾邮件的。

简单说来，Hashcash一开始要求邮件发送方对邮件头（其中包括时间和收件人地址）计算一个160bit的SHA-1哈希值。其前面需要有5个零，也就是20bit的0。接收端会检查这个事。

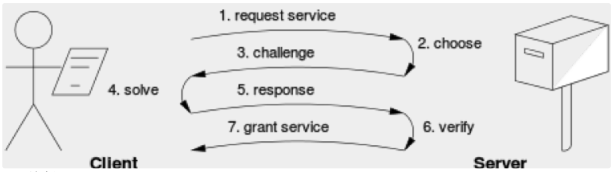
为什么要设计成这个样子？因为如果我们发垃圾邮件，这点算力对于发送方来说，没有什么。但对于需要大量发送垃圾邮件的人来说，这就是一个很大的成本了。就算是那些控制着用户的僵尸网络的黑客来说，发送垃圾邮件时，导致CPU使用率过高，会马上引起电脑所有者的警觉，而且还很容易定位相应的恶意程序。

对于一些受信的邮件服务器，我们可以把其放进白名单中，这样，就不需要它们接受Hashcash挑战，它们也不用为之付出成本。

于是，这种玩法叫做Proof-of-Work，简称为PoW，工作量证明。我们用这种消耗对手能源的手段来阻止一些恶意的攻击或是像垃圾邮件这样的对服务的滥用。

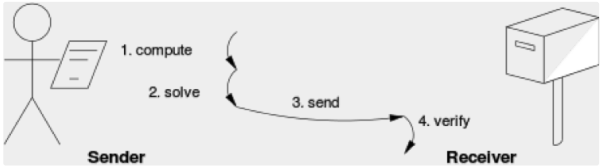
PoW有两种协议。

- 一种叫Challenge-Response协议，用于Client-Server。如图所示，如果Client需要使用服务，那么需要被Challenge去花费一些资源。如果证明自己的资源已被花费了，则通过认证，授权使用。



（图片来源：Wikipedia）

- 另一种叫Solution-Verification协议，用于验证使用。Hashcash就是这种协议。下图可以帮助你更形象地理解。



（图片来源：Wikipedia）

通过前面的描述，可以得知，我们需要为用户记录的交易是不能被修改的，所以使用hash方法为每个账本做了"签名"，还把其不断地打包再hash形成merkle root，然后再形成一个串链。于是，修改一个地方就会导致所有地方的"签名（hash值）"都需要跟着一起修改，于是形成了复杂度。

然而，这样的复杂度对于计算机来说并不高，找上一台或是几台主流点的电脑，分分钟就破解掉了。因为hash运维这个事对于计算机来说，是一件非常高效根本不费事的事。

于是乎，我们通过挖矿——PoW这样的协议来大幅度地提高修改成本，使得有恶意的人要改一个地方，需要花很大很大的成本来修改。这几乎是一件不可能的事情。

因为比特币是去中心化的P2P系统，任何人都可以方便地获得所有的数据，所以为了防止有恶意的人修改数据，使用PoW的"挖矿"机制，可以大幅度提高想要通过修改和攻击这个系统的人的成本。

当然，PoW的初衷是通过消耗资源的方式来阻止一些恶意攻击。然而在区块链的去中心化的世界里，PoW还有另一个功能，那就是让这些不受控制的分布式P2P网络里的结点统一思想。也就是说我们常说的，分布式一致性。这对分布式系统中的交易系统来说是一件非常重要的事。

总结一下，工作量证明就是为了下面几件事。

1. 提高对数据篡改的成本。让你修改数据需要付出大量的算力，而区块链的数据相互依赖，导致"一处改处处改"，因此你要完全修改就需要付出大量的算力。
2. 提高网络中有不同声音的成本。试想，如果一个网络有不同的人给出来了不同的账本，而且都合法，你会信谁的？所以，挖矿可以解决这个事。让你要做一个伪造账本的成本极其地大，而校验账本的成本很小。
3. 解决分歧。当有不同声音的时候，即区块链出现分叉时，所有的矿工只能选择其中一个分支（因为没人有算力可以同时发出两个不同的声音）。于是，大多数人选择的那个分支就会成为事实，少数人选的那头就被遗忘了。这让整个去中心化系统的一致性，不再以人数多认可的数据为准，而是以算力多的人认可的数据为准。

只要网络越来越大，能掌握半数以上算力的人基本上是不可能的。是这样的吗？我表示怀疑。

PoW解决这种无中心化网络的作弊、分歧这样的问题是目前最有效的，其他不用PoW这样的玩法的都存在很大的安全问题。但是，现在的PoW也有几个非常严重的问题。

1. 越来越中心化地记账。本来是要大众一起参与去中心化的事，现在因为算力的问题，因为GPU的出现，导致一般人几乎无法参与其中了。

2. 越来越跑不动。比特币今天的链越来越长，导致要验证数据是否正确的成本越来越高，一般人的电脑基本都快要跑不起来了。

所以，比特币社区也开始分裂成好几个衍生品，用不同的手段在解决这个问题。但是，目前为止，我没有看到什么比较好的方式。因为这世界上不存在完美的解决方案，你要一头，另一头就没了。

股权证明协议

PoW这个机制，要找到符合条件的Hash值，在目前来看，其耗费的电力和时间成本是越来越大了。所以，为了每个Block更快的生成，出现了PoS （Proof of Stake）协议，中文翻译为股权证明协议。

在PoS机制下，矿工不在叫矿工，而是叫Validator（校验者）。假设现在有一个区域需要被生成，而现在有4个Validator，每一个Validator需要以"交押金"的方式来取得记账权。假如，A交的押金占了38%，B占25%，C点21%，D占16%。那么，他们按照股权的比权来获得记账权。比如，A有38%的概率可以获得记账权（不是由系统随机分配，还是要算hash值，只不过是财富越多的人挖矿的难度越小）。而如果你发起恶意攻击的话，你的钱就会被系统没收充公。而Validator记账后没有奖金，只有手续费。

也就是说，在PoS机制下，记账权不再像PoW那样由谁的算力大谁就越有机会来记账，而是由谁的财富多，谁就越有可能来记账。于是，记账权按大家财富的比例来分配。

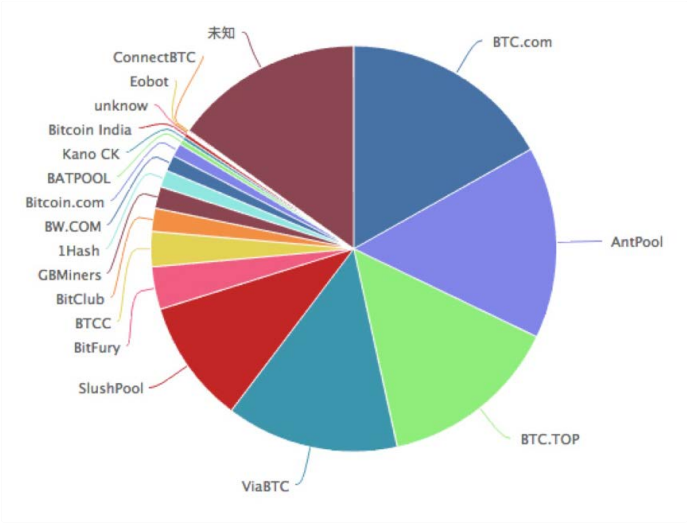
PoW好像是"多劳多得"的社会，而PoS更像是"资本主义"社会，钱越多的人越有话语权。这其实也没有什么不对的。从博弈论的角度上来说，钱越多的人越有动力维护社会的稳定，因为如果社会不稳定了，他是损失最为惨重的人。

（这里有一个逻辑问题：如果钱越多的人越有动力维护社会稳定，那么，是不是中心化的机构也越有动力维护整个系统的健康度？如果是这样的话，我们为什么要去中心化呢？更多的逻辑问题会在本文最后提出。）

在以太坊下，是根据拥有以太币的总量，来决定成为Validator的机率。

PoS宣称至少有如下的几个好处。

1. 第一个好处很明显。不需要那么费劲的挖矿了。那样浪费电力不环保地挖矿的确有点太糟糕了。PoS很明显地解决了这个问题。
2. 在P2P这种无中心化的网络下，如果你要控制整个网络，就需要超过半数以上的能力。在PoW下，你需要51%的算力。在今天，这会是一个非常大的成本。但是我们看一下，下面的全球比特币的算力图，我们发现只要前四家公司联合起来作弊，就可以完成对比特币的攻击（据说中国有60%左右的算力，看来只要中国政府愿意，要拿下比特币也不是什么难事，呵呵）。而在PoS下，你需要有51%的财富，你才可以发起攻击，这相对于算力而言需要更多的成本。设想一下，你得拥有51%的比特币，你才能黑了比特币，然而，如果你有51%的财富，你为什么要黑了这个系统，自己把自己干死呢？这就是博弈论。



（图片来自：http://qukuai.com/pools ）

PoS机制潜在的问题

世界上没有免费的午餐，也没有绝对完美的事，所以PoS也有其潜在的问题。最明显的一个问题就是，当不需要太多算力的时候，如果账本出现分叉的情况，也就是系统出现两个冲突且合法的区块的时候，在比特币这种算力密集的PoW机制下，所有的矿工必需赌其中一个分支往下走。

因为算力的问题，所以基本上来说不太可能同时在两个分支上发展。而其中一个分支如果长于另一个分支，较短的那个分支就会被孤立出去，其上的账本就都不作数了，而矿工的奖励也没有了。这是PoW机制的好处。

而在PoS这种不需要算力的机制下，就可以让记账人们在两个分支上同时进行，以争取实现利益的最大化（无论哪个分支最终胜出，我都可以有利）。这样一来，攻击者就可以利用这种情况来发起Nothin-At-Stake攻击。

也就是说，如果绝大多数人都在发展两个分支，假设有99%的人发展A分支，99%的人也同时发展B分支，而有1%股份的人在分支A中写一笔交易，然后在B分支没有这笔交易，当其在A分支上达成合约后（比如，收到商品），加入B分支，然后B分支胜出，导致其没有交易。

另外，两个分支发展还可以发起双重支付。就是说，Bob把他的10元钱借给了Alice，也给了Marry，在不同的分支上。这就是所谓的"双重支付"问题（Double Spend Problem）。

在CAP理论中，如果出现网络分区的情况（Partition），你要么选择数据的一致性（Consistency），那么你就得让整个系统不可用（Availability）；要么选择系统的可用性（Availability），那么你就得牺牲数据的一致性（Consistency）。所以，在无中心化下，我们通过分叉来牺牲数据的一致性，于是，在一个分叉上，Bob把10元给了Alice，另一个分叉上，Bob把10元给了Marry。

甚至可以发起"贿赂攻击（Bribe Attack）"，攻击者可以在一个分支上声称购买了某个商品。然后，收到货后，以提高手续费的方式只养另一个没有购买这个商品交易的分支，然后把没有这个交易的链养得足够长，长到系统最终选择了没有交易的这条链。

在PoW机制下，这种"分叉攻击"的玩法基本上来说不可能，但在PoS的玩法下，这种攻击就很有可能。在以太坊下，如果发现有人玩同时养分叉的玩法，就会予以惩罚。然而，如果这个攻击者有多个账户呢？我用多个马甲来玩不同的分叉.....

另外，PoS这种通过财富的占比来决定记账概率的玩法，可以让结点进行预计算，也就是可以计算下一个的hash值，这样一来，相当于我可以偷偷养分叉。

看来，PoS的问题也很多，所以有人又提出来了一个进化版，叫DPoS（Delegated Proof of Stake，委托股权证明）。它是 PoS 的进化方案。

以太坊的官方Wiki上有一份Proof-of-Stake的FAQ， 你可以前往一读。

DPoS机制

在常规PoW和PoS中，一大影响效率之处在于任何一个新加入的区块，都需要被整个网络所有节点做确认。DPoS优化方案在于：通过不同的策略，不定时地选中一小群节点，这一小群节点做新区块的创建、验证、签名和相互监督。这样就大幅度减少了区块创建和确认所需要消耗的时间和算力成本。

这就像选举人团代议制度，和美国选总统一样。DPoS下每个token都是选票，大家票选20个选举人团+1个随机选举人=21个选举人代表网络。然后每隔一段时间，在这21个人中挑选一个出来维护账本并获得收益。

近日，推崇DPoS的EOS开始了其21个超级节点的选举。作为超级节点，他们将获得 EOS 每年增发 5% 的收益中的大部分，大约每一个节点每年可以获得 238 万个 EOS的收益，按照当前价格（EOS/RMB ¥34），一个节点每年可以分到 1 亿元人民币的奖励。

（注明一下，EOS是以准备颠覆以及坊以及整个区块链生态的姿态，打着提高交易吞吐量到百万级TPS的技术口号，的进入这个世界的，本文成稿时，EOS还没有正式发布，相关细节，你可以看看 EOS白皮书的中文版翻译 。）

比较有趣的是，在这次超级节点的竞选上，主要竞选节点来自中国、美国和韩国。这三方的优势是，韩国人拥有最大的EOS交易量，而中国人拥有更多的EOS之外的资本，而美国人则有规则制定权。看起来就是，美国有政治权力，韩国有经济权力，中国这边有外围经济权。看上去是比较完美的制衡，就像三国演义一样。

为了赢得选举，中国竞选人开始进行了我们熟悉的套路——贿选。所谓贿选，就是指将上文提到的当选超级节点后每年应分得的「巨额工资」返还给每一位投自己票的人。通过这样的贿选就可以破坏上述看起来比较制衡的政治局面。这样搞下去，很有可能，那21超级个节点就会成为一家公司所控制。

所以，很快，创始人BM（Dan Larimer）就现身表示，不支持节点对投票人实行分红的做法。然后，Thomas Cox 也在社区内发帖《为什么付费投票是坏的》来谴责贿选，并在开始陆续发布 EOS.IO 的 0.1 版本「宪法」的第一条款《不说谎》.....（相关的报道可参看《EOS超级节点投票：「千亿」利润下的币圈国家战争》。）

顺便八卦一下，EOS创建人BM在2014年的时候，创建比特股时打出超级比特币的概念，然后，因为Bug大多，体验非常地差，后面他和公司不合离开了比特股。2016年，他创建了社交平台Steemit，想颠覆传统媒体，结果也失败了，并于2017年创建EOS，瞄准以太坊，想做区块链接基础设施（包括并行运算、数据库、账户系统等等）。老实说，我觉得这个对他来说更难。

在我看来，有两点让这区块链这个技术开始有些变味了。

- DPoS已经开始把区块链的去中心化的初衷开始向中心化的地方演进了。
- 政治在未来区块链的世界里是一个必不可少的技能，这意味着不可控的复杂性。我感觉这些技术宅是一定Hold不住的。

小结

对我来说，目前为止，PoW还是一个比较稳健的共识方式，PoS/DPoS还需要更多的实践和改进，当然，也许混合PoW和PoS/DPoS也不错呢。"去中心化"和"高吞吐"这两个事，我觉得是很难协调的。

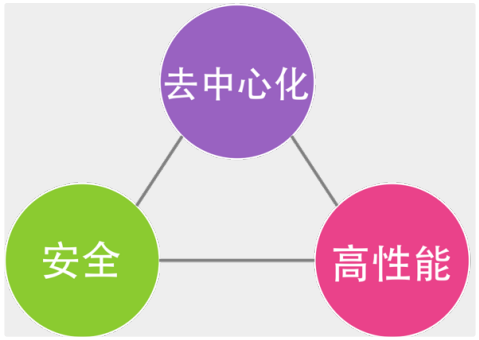
总结一下。

1. PoW就是蛮荒社会。谁的拳头大谁说话。是真正意义上的无政府的去中心化的社会。
2. PoS就是资本主义社会。谁的钱多谁说话，还是无政府的社会，但是资本家控制的。
3. DPoS就是政治主义社会。谁的选票多谁说话，我也不知道怎么个选举，竞选活动吗？有电视辩论吗？还是投票玩玩？但是感觉又回到了中心化架构中的Leader选举。

无论怎么样，人类社会进化的影子在去中心化的社会中又开始出现了。那么，另一个逻辑问题来了，如果这种"去中心化的社会"本质上是在重复一遍"中心化"的演进过程，那么，还有什么意义？

上面的这个逻辑问题我们留到最后，这里还是看一下技术方面的事儿。

我们都知道，分布式系统的CAP原则，在一致性、可用性和分区容忍性上只能三选两。在区块链的P2P网络下也是很类似的，在去中心化、安全和高性能中，我们也只能选两个。



- 如果我们想要一个既安全，性能也很高的系统，那么得放弃去中心化的架构，如DPoS这样的中心化系统，直接放弃区块链走传统的中心化架构。
- 如果我们想要一个去中心化和安全的系统，主要去挖矿，那么放弃高性能。这就是目前的比特币架构。
- 如果我们想要一个去中心化和高性能的系统，那么就得放弃安全。没有安全的系统，基本上来说是不会有人用的。

文末给出了《区块链技术》系列文章的目录，希望你能在这个列表里找到自己感兴趣的内容。

- 区块链技术（1）-区块链的革命性及技术概要
- 区块链技术（2）-区块链技术细节：哈希算法
- 区块链技术（3）-区块链技术细节：加密和挖矿
- 区块链技术（4）-去中心化的共识机制
- 区块链技术（5）-智能合约
- 区块链技术（6）-传统金融和虚拟货币

hua168

2018-04-11

大神，分布式方面，能不能讲下安全，像国内大网站经常会被攻击他们是怎么防攻击，像防DDOS做CDN+DDOS防火墙效果也不怎么好，都在哪些地方做安全……能简单讲下吗？谢谢……

neohope

2018-06-22

哈哈哈，您预测的很准，EOS的主链刚上线就挂了。我觉得BM能力是有的，但对团队的管理水平就有些差了。 应该多看看您的文章。

.

2018-06-06

讲的好清楚！
补充亮点
在bitcoin挖矿中，GPU已经被更专业的ASIC取代了
在改进版的POS中，要求参与者抵押资产来解决nothing at stake的问题

作者回复

2018-06-07

谢谢补充

derek

2018-04-11

老师有了解墨客吗？作为母链，可在之上构建各种子链，子链可使用自己的共识机制，并实现了分层分片

cat0

2018-06-27

看了很多介绍比特币技术的文章，能站在社会发展历史的宏观角度探谈比特币技术的，耗子叔是我见到的第一个。读你的专栏越读越觉得物超所值，你的音频也是我听过的技术类最棒的，看得出用心做了

晓聪

2018-04-29

行家出手，比起之前看过的文章更有高度

杨洪林

2018-04-22

非常佩服作者的理解深度，我有一个问题请教。区块链技术的去中心，高性能和 安全 怎么和CAP 中的 Consistency, availability and partition tolerance ——对应呢？consistency 对应安全性，partition tolerance 对应去中心化， availability 对应性能？ 不知道我的理解对不对？

总指挥

2018-04-14

很有意思啊哈哈

云学

2018-04-13

很欣赏这种辩证看技术的文章，不知不觉中解决了之前的很多疑问，对区块链也比较理性了，相比于去中性化，防篡改和可追溯更有应用价值

dilei

2018-04-11

有个疑问 最初的比特币是咋来的，当时还没有交易吧

macworks

2018-04-10

有人的地方就有政治，这点任何协议都不能免除。至于去中心化和中心化的演进其实很正常。有些去中心化解决不了的问题，需要引入中心化的方案，而中心化的引入又会带来风险，所以又会有新的去中心化的提议出现。如果你仔细想想，法币，例如美金，很大程度上也是去中心化的。能搞定去中心化和安全本身已经是很了不起的事情了，性能问题是可以通过引入中心化的方案，例如担保机构来解决。这在一定程度上是可以接受的。

毕小涛

2018-04-10

请教一下，去中心化的协议还有gossip，为什么不是用gossip呢？

Yole

2018-04-10

其实Paxos/Raft也能作为区块链网络中的共识算法，只是不能使用在公有链里面，不能BFT。联盟链CFT应该就够了。

作者回复

2018-04-12

两个问题，1）为什么要联盟链？2）为什么数据结构要存成链？

王亚南

2018-04-10

有几个疑问，可能比较初级：1、比特币能成为货币必然需要发行，那现在比特币的唯一发行增量就是挖矿产生的奖金了？2、如果每一笔交易都需要获得全网确认一致的话，比特币交易不是会很慢，现在采用比特币交易的平台体验会很差吧？

酱了个油

2018-04-10

耗子叔，关于链长导致的效率问题，是说每个区块生成后都需要把整条链走一遍来验证合法性吗，这一步主要是做什么校验呀

作者回复

2018-04-12

验证你账户上的钱是怎么来的？