> 这不是一篇学术论文，但我仍希望它能得到一些具有学术性的反馈。这篇文章尝试将我对密码学、分布式系统的粗浅理解和简单的逻辑学结合在一起以获得观念上的突破，但我自己也觉得论证效果不够好。也许日后我再也不会尝试用如此愚笨的方式来处理如此巨大的题材，也许我以后将不再触碰，因此在这场攻打风车的尝试中，我希望学到越多越好。

权益证明的核心疑难

本文源于一种长期的不满，而这种不满是分为两方面的：一方面，不满于当今业内有许多团队不顾历史的教训，为 PoS 研究投入了大量精力，并且不断用各种定义模糊、站不住脚的理论攻击工作量证明（PoW）；另一方面，也不满于尚未由社区成员提炼出本文将要提出的论点予以反击[1]。

当我们已知一套理论时，我们便知道了两种不可能：一种是理论上的不可能（比如抓住自己的头发提着自己离开地面），另一种是（当前）实践上的不可能（例如在很薄的地基上盖摩天大楼）。我认为理论家的工作是重视第一种不可能，因为第二种不可能只意味着工程上尚未解决的问题，前者却意味着方向上的错误。

有鉴于此，我并不准备在本文中提及 PoS 在实践上可能遇到的问题（比如持币者的币量分布不均匀），我假定这些问题都可以解决。我将仅从基本的逻辑出发，论证权益证明方案中仍存在一些疑难问题。

一. 权益证明理念简介

权益证明（Proof of Stake，PoS）的观念主要来源于人们对比特币挖矿的能源耗费的担忧。在比特币发展早期，一些密码学货币支持者认为比特币的普及将伴随着挖矿产业能源耗费的不断提高，这种情形是不可持续且不环保的。于是他们设想：**能否使用系统内部的资源数量来界定投票权重，用投票来解决出块问题**？“Proof of Stake” 这个名字便来源于这个过程与持股投票、获得分红的相似性。并且，由于人们不需要为此一过程投入外部硬件，整个系统便将脱离对外部硬件的依赖，进而一劳永逸地消除硬件竞赛和能源 “浪费”。

这种思路最早的实践便是 PPCoin（点点币）。在点点币中，每一笔 UTXO 在每一秒种都有一次机会尝试出块，而出块会将该 UTXO 的币龄（UTXO 值乘以该 UTXO 存留的时间）清空，同时为该 UTXO 持有者发放一笔与币龄成比例的奖励。

PPCoin 初步实现了 PoS 的设想：用系统内部资源占有量的多少来界定出块权和收益权。但与此同时也暴露出 PoS 系统的一些问题，其中最突出的便是 “理性分叉” 问题（也叫 “Nothing-at-Stake”，或者 “短程攻击”），在 PPCoin 中，其具体形式是：由于每张 UTXO 在一秒内有一次出块机会，若不能出块便只有等多一秒，在该秒内，节点的计算能力是完全闲置的，而在其它链上出块又没有损失，因此 UTXO 持有者都会在不同链上尝试出块，使整个系统经常陷入恶性分叉中。后来，人们将这一问题归结为“分叉没有成本”，即违反协议也不需要付出代价[2]。

以太坊的权益证明方案继承了这一源流，并加入了一个关键的措施来抵御 “Nothing-at-Stake” 风险：罚没保证金。出块者用于出块和赢取报酬的资源必须先质押进某个地址，一旦发现出块者出现了一票多投的行为便罚没这部分保证金。出块期结束后还有一个冷却期，冷却期之后出块者才能取出这部分保证金。

与 Casper 同期还有另一种引人注目的 PoS 算法：Tendermint。Tendermint 的灵感来源于几十年前提出的 PBFT （实用拜占庭容错）算法，因此，也有人将权益证明分为两类：链式结构型（“Chain-based”）和拜占庭容错型（“BFT-style”）[3]。尽管多年演化之后，Casper 仍应算作是链式结构型，但在笔者看来，这样的分类正在失去意义——两种思路正在逐步趋同[4]，或者说，即便有许多不同，算法运行的过程还是有非常多的相似之处，并且这些相似之处多数都是受传统共识研究（也就是 BFT 共识）的启发。

需要说明的是，笔者并未研究过 Definity 的算法，因此不能确定本文论述的相关性。至于 Algorand，相信读者从上文中就可读出我的意见。

接下来，我想邀请读者用更抽象的角度来看待问题。

二. 分布式系统的根本问题（或：出块时间稳定性问题）

（一）分布式系统的根本问题

公链网络是一个开放的分布式系统，这意味着它有几点重要属性：没有全局时钟、节点独立运行并且可能出现故障、消息需要时间来传递（对所需时间上下限的可知与不可知可以延伸出进一步的假设）。

没有全局时钟意味着各个节点有各自的始终，没有办法保证这些时钟在任一刻的状态都为彼此所致。Lamport 曾论证这是分布式系统的根本问题：**作为一个系统，最重要的功能便是对系统中发生的事务（transaction）进行排序**，可是，大家的时钟走得都不一样，而且发送事务时还可以伪造时间戳，那怎么办呢[5]？

在中本聪共识出现以前，有两种方案：

1）选择可信第三方来发布、确认时间，比如在中国，中科院授时中心负责为全中国发布标准时间，一切与之冲突的时间都不能算数；

2）在一个节点有限且可知的计算机系统内部，由于节点不会随意进出，稳定的节点集合可以得出网络延迟的上限，即满足同步假设；满足了同步假设，就意味着大家都知道某一节点发出的信息，另一个节点会在多长时间内收到；确定了这一点之后，我们就可以设计出一些具有容错能力的算法，为系统中的时事件排序（即达成共识）。

那么上述两种方案有什么共同特征？

他们都是中心化的，即都具有单点故障。在第一个方案中，授时中心就是那个单点；而在第二个方案中，需要先有一套方案来解决节点间的信任问题（“你凭什么可以加入这个系统”），在这套社会解决方案中，也很难完全消除掉中心。

上述理由同样可以解释为什么在比特币以前没有出现过开放性的分布式系统：随意进出的节点可以轻易打破同步假设，使共识进程崩溃。

（二）工作量证明和中本聪共识

中本聪共识解决这个问题的方法就是要求系统的每一次状态更新都必须提供工作量证明。**分布式系统中由于通信问题而导致的暂时性的不一致（即网络正常运行中出现的 “分叉”）可以用最长链规则加以解决，而工作量证明则为块的提出作了根本性的限制**。如此一来，系统的参与者会自然形成一条主链，包含事务的区块前后相继，使我们能轻易判别出事务发生的先后顺序（尽管在同一区块内仍判别不了，并且在任意时刻达成的共识都有可能被推翻）。工作量证明的计算密集性，使得人们除非有天大的利益，不会尝试挖出另一条长链；而算法的随机性又使得人们不可能提前预知块哈希，无法提前伪造某事务已经上链的证明。

这种解决方案的优雅性集中体现在稳定的出块时间这一点上。众所周知，工作量证明系统会有一个相对稳定的出块时间，但是，**难道有人规定了这个系统在 10 分钟之内必出一个块并且只能出一个块吗**？不是的。它的实现方法是：出块者提交区块时，会在区块头内附加一个时间戳；各节点接收到区块后开始验证区块内事务和区块本身的有效性，若都有效便接受；接收的区块达一定数量后便统计、计算出平均出块时间，根据此平均出块时间和工作量算法的难度要求反推出全网算力，再根据此全网算力值更新工作量证明的难度要求。

由于各节点接受到的主链块都是一样的，因此难度调整也是一样的；难度调整会对出块时间有直接的影响，如此动态地调整出块时间使之趋向目标值。就这样，网络中独立验证的节点共同构筑了一个去中心化的时钟。换言之，不是某个中心度量出来的 10 分钟决定了比特币的出块间隔，而是比特币网络度量了时间[6][7]！

（中本聪显然也认识到了这一点，因为他从未用过 “blockchain” 一词来指代工作量证明系统；他用的是 “Hash-chain” 甚至是 “time-chain”！）

那么，PoS 有办法度量时间吗？

（三）PoS 与单点时钟

在 PoS 系统中，为了防范 “Nothing-at-Stake” 问题，人们不能任意提出区块，必须限定出块资格，即对人们的出块行为施加技术上 或者/以及 经济上的限制（比如质押货币）；其次，为了解决 “Long-range Atteck” 问题（即攻击者从非常久远的区块上构造出一条链来的攻击），PoS 系统必须引入一种限制回滚深度的机制（比如让节点不再接受 4 个月以前的区块[8]，即技术上的回滚深度不能超过 4 个月），因为货币的质押期和冷却期都是有期限的，过了这段时间，协议对攻击者在经济上的限制就消失了。

那么问题来了，这些期限在技术上是如何实现的？最简单的方式就是用区块本身来实现，比如距当前 100 个区块以前的链就不再接受更新了。但问题还没完，出块的时间怎么稳定下来呢？出块时间如果不稳定，那这种时间上的限制也很容易被打破。

实际上，对于出块的时间区间确实要做一些限制，如果出块时间没有上限，那么 “可终及性（termination）” 就很难保证（就是单个共识周期没准一直跑不完）；如果出块时间没有下限，那验证者就可以合起伙来加速出块，使货币增发失去限制，也让这些验证者的权益增速失去限制，拉低系统的处理能力和安全性。

但是在一个点对点的网络中，如上所述，没有全局时钟；那怎么产生出这种对时间的度量和控制呢？验证者迟迟不签名，既有可能是被审查了，也可能自己掉线了，无法判别；如果不加约束，达成确定性的时间就会远大于设计好的单个共识进程的时间，而趋近于预期出块时间与最大回滚深度的积。实现这种约束，只有一个办法，就是处在一个同步的网络中，让验证者无法用 “被审查” 来推诿，只能承认自己是掉线了或者没有尽到职责，然后受罚。

在点对点网络的汪洋大海中，这种同步网络如何出现？PoS 设计者说：简单，先选举出一个验证者委员会，在委员会内部建立稳定的连接并形成同步网络。

那么，为了在单个共识过程中形成共识，确保满足安全性和可终及性，需要同步网络；可是只要共识节点并不永远是同一组，就一定面临两个同步网络间的更替问题；在这个更替过程中同样面临时间度量和控制的问题；该时间间隙不能是一个共识过程，否则你就只是增加了另一个同步过程，增加了另外两段间隙；可是它若不是一个共识过程，又如何形成一个非单点的时钟呢？

而且，即便让第二组委员会在第一组委员会的轮次尚未结束前便准备好也是没用的。因为两组委员会之间不是同步的，第二组委员会压根不知道第一组的轮次何时结束，更谈不上密缝无间地跟上。

如此推理下去，你会发现，真正要实现对时间的度量和控制（即对系统内发生的所有事件实现无冲突的排序），权益证明算法要求的是整个验证者网络都是同步模型，要实现这一点，比较常见的办法是限制验证者的数量，比如 Cosmos 就限制了系统中最多只能有 100 个验证者（当然这样设计还有另一个原因是 PBFT 算法的效率其实不高，通信量要达到 n^2）……你想起什么来了吗？

对的。DPoS。DPoS 就是 PoS 系统走下去的一个 “正确” 的答案。

可是没有一种理论能告诉我，100 个验证者，跟 21 个验证者，区别到底在哪里。

说 PoS 中心化，不是因为财富的分布，而是因为严格的技术理由——它摆脱不了单点故障。

三. 随机数问题

在工作量证明协议中，随机数是共识过程的终点，并且其产生过程无需节点在线交互（矿工自己计算即可），验证其有效性也是很容易的。如上几点使得随机数的寻找在协议中显得自然而又经济。它不需要额外的传输，也无需人们信任某一个熵源。

而在权益证明协议中，随机数是共识过程的起点，需要随机数来选出委员会。如果随机数方案要实现去中心化，就意味着系统不能从某个系统外的熵源获得随机数，也不能 “硬点” 系统内部的某个（或某群）固定的节点来产生随机数。这意味着：要么系统通过系统内的开放过程生成随机数；要么让共识结果本身成为熵源。

前一种方法貌似可行，但你仔细想想又不对了。这个开放过程（也是一个多方计算协议）在哪个环境中运行呢？线下的多方计算可以实现信任最小化（即只需至少一个诚实参与者即可保证结果不可被操纵）（例子如 Zcash 为产生 zk-SNARK 参数而设计的 MPC 协议），但经常需要进行线下的多方计算是不现实的。若在线上，并且不在可信任计算的环境中运行，则很容易被攻击；若是在一个可信任计算的环境中，那又意味着 PoS 进程本身是依赖于另一个可信任计算进程的。

因此，大多数 PoS 都选择了后一条路。

但问题还没完。使用共识结果（比如区块哈希值或由验证者提议的某个值）作为熵源的弊端在于：（1）从随机数揭晓到验证者就位之间存在窗口期，让攻击者可以尝试对验证者发动 DoS 攻击；（2）参与共识的验证者会试着操纵随机数。前者在严重时会使系统停止运行，后者会使奖励分配不均，使得先获得出块权的验证者比后来者更具有优势。理论上也许可以通过激励方案的设计来缓解这一情形。

（并不是说 PoW 中就不存在此种情形，而是这种情形被计算密集性遏制了，不间断地竞争使矿工并没有多少时间和机会操控区块哈希值；但在 PoW 中，出块是在一定时间范围内进行的，并且计算难度也不高，这就让验证者大有余裕可以多试几次。当然，其它验证者也可以联合拒绝掉）

四. 节点竞争问题

所谓节点竞争，指的是节点为获得系统奖励而开展的共识资源占有量竞争，在 PoW 系统中的表现是升级矿机和加矿机。

但在 PoS 系统中，节点竞争有了更多形式，不仅包括吸收他人委托的代币、改善节点的安全和通讯设施，还包括攻击其它验证者。这并非开玩笑，因为当期全网质押的代币数量越少，验证者的收益率就越高。如果动用网络攻击的同时还能借协议之手罚没对手的共识资源，何乐而不为呢？

我并不是说 PoW 中就不会出现 DoS 攻击，而是说，PoW 中的 DoS 不会改变攻守双方的共识资源数量。打个比方就是，PoW 中的 DoS 只是暂时阻碍防守方参与挖矿，相当于把路堵了，但不会让你家工厂没了，而且大多数时候被攻击的都是矿池而非某个矿工，总而言之不会对系统安全性造成长远影响，要攻击整个系统的攻击者还是必须一五一十地付出边际上的费用才能阻碍矿池参与共识，但矿工还可以切换到别的地方去；但在 PoS 中，DoS 攻击可能导致防守方的权益被罚没，相当于直接把你家工厂给推了，推完之后，整个系统的安全性永久性地下降了。进一步地说，这意味着 PoS 系统的安全性会逐步衰减，而衰减的速度会与网络中防御力最弱节点持有的代币量相关。

Vlad 曾有句名言：在质押保证金的 PoS 系统中，发动 51% 攻击会让你的 ASIC 矿场被烧毁。仔细想想，这实际上意味着协议层在鼓励节点动用系统外的手段来钓鱼、攻击其它验证者。协议层永远有边界，边界外的行为，协议层是无法了解的，因此也根本不可能指望协议层总是能 “明辨是非”。

讨论节点竞争不仅是为了讨论节点竞争，而是为了指出 PoS 设计者观念结构中值得怀疑的地方：只需动用具有负向激励的手段限制系统内参与者的行动，任何目的都有可能达成，创造出系统外的人也能接受的价值更是不在话下。

在 PoS 的设计中处处可见这种观念：对相互冲突的区块双重签名了，罚他；验证者掉线了，罚他；分不清是他掉线了还是别人审查他，那就双方一起罚。设计者似乎认为只要设置了负向激励便可让所有人都遵守协议，全然不理为了实施这些措施到底需要哪些条件、又会对性能造成什么样的影响、如何保证这些措施不会被滥用，以及，最重要的，这样做是不是真的能够创造价值。

依此视角，你会发现，PoW 的设计者谨守分布式系统的底线，不依赖全局时钟，也不对单点运行系统所需的信息作太多要求（即尊重了点对点网络的带宽有限性和时延性），利用 “计算-验证” 的非对称性压缩节点的负担，并最终用近乎规律的出块创造了一种货币。反观 PoS，设计者一方面罔顾实行罚没措施所要求的信息（双签确实是可以检测出来的，前提是你要收到了双签的区块）、也不考虑非交易处理导致的状态变更所造成的负担，更是完全不点明，作了这些变更之后，这样的系统还有没有价值。

五. 题外话

有一个公开的秘密：以太坊社区喜欢嘲笑 EOS 及其拥趸，说中心化的 EOS 与联盟链无异。尽管这种嘲讽没有什么建设性，但确实道出了以太坊立足于密码学货币世界的一个原因。

我在此要说的是（也许会扫了很多人的兴）：你觉得 Cosmos （100 个出块节点）如何呢？以太坊转轨 PoS 之后，我们还有嘲笑 EOS 的资格吗？

但我想，这种担忧近乎杞人了，因为这篇文章公开之后，也许在很多人眼中我就不再属于以太坊社区，而成为 “敌人” 之流了。

---

1. 实际上，本文所要提到的大部分论点都不是笔者首创，之所以这么说，是因为它们都不来自于以太坊社区。在下文论述的相关部分，我将给出参考的文献和观念的出处。 ↩

2. 详情请见《从当年 PPCoin 的 PoS 模式看 PoS 的演化》；另，Conflux 研究员杨光在近期的公开演讲中将这一问题归结为 “权益重用”，我认为比 “Nothing-at-Stake” 要准确得多。 ↩

3. Vitalik, etc. 权益证明 FAQ [EB/OL]. https://ethfans.org/posts/Proof-of-Stake-FAQ-new-2018-3-15, 2018-03-15/2019-03-21 ↩

4. Vitalik. Casper 的前世今生[EB/OL]. https://ethfans.org/posts/vitalik-on-casper-development-history-and-state, 2018-08-16/2019-03-21 ↩

5. Preethi Kasireddy. 分布式共识的工作原理[EB/OL]. https://ethfans.org/posts/lets-take-a-crack-at-understanding-distributed-consensus-part-1, 2019-01-17/2019-03-21 ↩

6. Gregory Trubetskoy. PoW 本质上是一个去中心化的时钟[EB/OL]. https://ethfans.org/posts/blockchain-pow-is-a-decentralized-clock, 2018-05-11/2019-03-29 ↩

7. 比特币这个时钟的实际表现如何？不算太好。现在的比特币比预期多出了 3 万个区块。详情请见《盘点比特币给用户带来的保障》 ↩

8. Vitalik. Casper 的前世今生[EB/OL]. https://ethfans.org/posts/vitalik-on-casper-development-history-and-state, 2018-08-16/2019-03-29 ↩