A：POS
大户坐着获得的资本利得，是小散无法逾越的鸿沟，且无法约束他的权利。

B：这个问题是社会正常现象吧，有钱的人挣钱本身就是比平民容易，
他投入这么多钱收入却比别人少，那才是不公平啊，
现在是大家获得的比例是一样的，大户投入的钱多，就是会获得更多的回报。

以上是一个 PoW 和 PoS 讨论中常见的对话。A
提出了两个问题，第一个是公平性问题：PoS
大户坐着获利，普通人没有;第二个是无法制约问题：PoS 大户的权利无法约束。B
回答了第一个问题。

对于问题 1, 我同意 B 的看法。投入多回报多是合理的，无论是 PoW 还是 PoS 都是这样，区块链是帮助实现过程公平而不是结果公平的工具。在区块链里面我们依然会看到马太效应。试图用区块链去解决结果公平的后果是区块链治理的内涵无限扩大，将本该由协议解决的各种问题(后面会看到)统统推给投票去解决。

然而无论是历史还是理论早就告诉我们，世界上并没有完美的群体选择制度。区块链是一个能够记录数据，保证数据不被篡改，为所有人提供数据的工具，通过这样一个工具帮助我们更好的实现过程公平，已经是非常非常大的进步了。

问题 2 是一个在讨论中被忽略的关键问题。投入资源换取回报天经地义，但前提是你想投入就能投入吗?举个例子，一个明星创业团队融资，是不是任何 VC
想投就能投进去呢?PoW
具有非常好的开放性，使得后来的共识参与者总是可以加入共识群体，而 PoS
不具有这样的开放性。引用这里的讨论：

在 PoS 中，未来的共识群体是由今天的共识群体决定的。任何新的节点想要参与共识都需要通过至少一个交易来实现(e.g. 抵押，投票，etc.)，而这个交易是否被处理是由今天的共识群体决定，他们可以处理这个交易，也可以不处理这个交易，如果不处理这个交易，新的节点永远都无法参与共识。

同时，「不处理交易」是容易伪装而难于惩罚的行为，我还没有看到能在共识协议中解决这个问题的方案。PoS 往往是根据 stake
的权重来分配出块比例(和节点数量没关系)，考虑到大部分系统中 stake
的集中程度，这是一个非常实际的问题。

PoW 是彻底的 Permissionless。无论什么时候，只要你愿意，都可以买矿机和电力加入出块者的行列，不需要今天的矿工给你任何形式的许可。你也许会说，我还是需要购买矿机和电力呀，这是不是一种形式的许可呢?

是的，从更低一层来说，这也是一种许可。但遗憾的是，在所有的 Proof of XXX 中，这已经是最去中心化的许可形式了，毕竟矿机生产和电力资源的去中心化程度远高于各种 tokens (的分散程度)。我们总是应该追求尽可能的去中心化，否则用回中心化系统就好了。

「是否能够投入」本身可以看作一种 option，有非常高的价值。PoW 能有这样的性质，是因为工作量证明的计算是一种不依赖历史的计算，无论你在任何时间点购买算力加入计算，你都和其他矿工在同一个起跑线上 ,这是一个非常独特的、反直觉的性质，正是这个性质使得后来者总是能打破了早期参与者的优势。

PoS 不同，因为 stake 是系统中内生的资产，资产的所有权是由系统历史决定的，交易顺序是由系统历史决定的，因此无论是需要抵押 token 加入的
pos，还是只需要持有 token 就可以参与的 pos，其 validator
集合都是这个系统自身的历史决定，PoS 和 PoW 在「参与共识是否需要依赖历史」上是截然不同的。我们很容易能看出，这是一个本质不同，无论什么样的上层设计都解决不了这一点。

因此 PoW 和 PoS 的设计，从根本上是两种不同的思路，体现两种不同的理念：

1、(PoS) 系统应该让先发者获得天然的优势

2、(PoW) 系统不应该让先发者获得天然的优势

注意主语是「系统」，共识参与者在系统外的优势不是任何协议设计可以解决的。如果你认为 1 是对的，自然应该支持 PoS，反之你应该会更赞同 PoW。CKB

在设计中选择 PoW，是因为 CKB 的设计目标是 Layer1，一个全世界共用的基础设施，我们希望它可以长久而且中立的运行，要做到这一点，系统不应该让先发者(包括系统设计者自己)获得天然的优势。

A: PoS 买币 staking 不就是投入了吗

确实是投入，但是这里的「投入获得回报」中的「回报」已经变了。对于投入获得的回报我们需要分开来看，一种回报是 token 收益，最近的 PoS 基本都支持 delegate，所以基本上所有人都有这个
option。另一种是参与共识的权利，根据上面的回答，它可以被现有的 validator 垄断，大部分人没有
option。权利有很多种，分红只是其中一种，而且不是关键的那一种。

那么共识的权利为什么重要，它有什么用呢?它意味着你可以对交易排序，而交易排序决定了链上众筹时你的交易能不能及时上链，在 DEX
里面交易时你的订单能不能及时成交，等等等等。在 PoS 的系统上做 DeFi?你需要认真考虑一下 validator
本身是做什么的，是否和你的发送的交易有利益相关?

我们知道，DeFi 的交易很可能是价值含量非常高的交易，e.g. DEX
里面一个巨大的买单，这时候 validator 如果安排一个插队的交易怎么办?仅仅是交易顺序的不同就可以造成巨大的获利，何况共识节点能做的远大于此?

聪明的你一定会想到：「那 PoW 的矿工 /
矿池不是一样有这样的问题吗?」没错，PoW 的矿工一样有这样的权利，但 PoW 有两个优点可以削弱这个问题：

1、出块节点和生态中的关键用户是解耦的。生态中的关键用户，指的是交易所、钱包等围绕区块链提供服务的服务商，它们为大量的用户提供优质的服务，聚集了大量的用户和交易;

2、在 PoS 中，由于拥有大量用户和交易，stake
会自然的往生态中的关键用户集中，形成天然的 stake pool，因此关键用户在业务上的优势可以转化成在共识和治理上的优势(在某些链里面已经体现的非常明显了)，使得先行者的优势更加强化。

在 PoW 中，矿工群体和交易所 / 钱包是独立的，他们有不同的专业分工，通过不同的专业知识，不同的方式获取回报，关键用户不能将自己的业务优势转化为协议中的优势，矿工也没办法将自己在协议中的优势转化为上层业务的优势。在 PoW

中，开发者、用户和共识节点之间可以形成制衡。

3、PoW 的共识是开放的(见上文)，充满了激烈的竞争。也许一个矿池 / 矿工可以在短时间内做到这一点，但由于新的矿工总是可以自由加入，想要长久的做到这一点是非常困难的，激烈竞争将会造就一个越来越公平的充分竞争的市场，这需要时间(30 年?maybe)。

反过来，在 PoS 中，由于天然的先行者的优势，以及业务优势和共识优势的绑定，先行者的优势只会越来越大，竞争将逐渐消失，最后形成垄断或寡头。在基础设施级的协议里面，我们应该尽可能的去避免垄断。

区块链本身是一个大的排队机，决定排序的权利是这个系统中最关键的权利。

A：(Bitcoin)一小时 51 攻击的成本区区 44.3 万美金 ...

A 想要表达的是，Bitcoin 并不安全，因为只要 44.3 万美金就能攻击它了，然后 PoS 的 token 是有限的，没有攻击者可以从市场上购买到足够多的 stake 来攻击。

这个观点忽略了一个问题：在某一时刻，地球上的算力同样是有上限的。如果一条 PoW 的链只有 10% 的 SHA256 算力，这样算是没有问题的。但是如果比特币已经集中了 90%(估计值)的 SHA256 算力，你从哪里去获得另外 90% 的 SHA256 算力呢?量变会引起质变，算力地位的变化会影响安全性。

不安全的不是 PoW，是没有获得足够算力的 PoW 链。使用 PoW 的区块链都会遇到比使用 PoS 的区块链更大的起步问题，然而正是这样真实而残酷的考验才能证明区块链的安全。不然，我也跑一条 PoS 链，99% 的 token 都归我自己，1% 在市场上想炒多高炒多高，安全性岂不是分分钟超过 Bitcoin?

Bitcoin 已经运行 10 年了，上面承载的价值这么多，为什么攻击没发生呢?相反，某些链运行了不到一年，上面存了价值区区几十万元的智能合约被偷了无数次。理论需要不断用事实修正，当理论和事实不符的时候，一定是理论错了。

同样是有上限，在 PoW 链中参与共识所需要的资源上限是随着时间变化的，由科技的进步、人类的进取心和激烈的竞争不断推动前进，所需要的自然资源的获取是完全去中心化的;而 PoS 链中所需要的资源上限是协议规定好的，增发的 token 全部进入现有 validator 的手中，再通过 validator 在市场上的售卖或是 staking pool 的分红分发出去，会不会有些似曾相识?

A: 这两者抽象到最后都是资本，PoW 是以资本开支和 opex 计算资本成本;PoS 是以抵押物市场价值计算机会成本。这两种成本都是不可逆的。

我不赞同这种逻辑，忽略中间过程直接捅到本质恰好忽略了关键。过程是关键，过程会产生摩擦，过程会产生损耗。即使都是资本，资本的流动性和产生垄断的速度也是有差异的，协议是否能从垄断中回复也是有差异的，见前文。

A: 我不觉得 PoS 的持币者会一直不卖;

A: 过度集中 谁会给生态贡献;

A: 如果筹码 90% 在你手里 这个生态也就做不下去;

A: 对你来说，高度集中持币是没有价值的;

A: 你都垄断 90% 代币，没有人给你交租;

垄断也是可以建立生态的，腾讯、苹果都是例子。无论是历史还是经济学原理还是《从 0 到 1》都很清楚的告诉我们，垄断才能获取暴利。

同时，垄断存在不代表你知道有垄断存在。token 是世界上最具有流动性的资本，即使我拥有 90% 的 token，我也会把它分散投入到 100 个 staking pool 里面去，而不会集中在一个 staking pool 里面。垄断者不会喜欢跳出来说「hey，我垄断了这个系统!」。

A: 潜在作恶垄断者会因为短期利益卖出 token;

A: 作恶就是为了短期利益;

A: 即，潜在谋求短期利益垄断者会因为短期利益卖出 token;

B: 头部抵押者都被看的很清楚，解抵押了，或者提币去交易所了，本身会导致价格下跌，他还没砸呢，就已经反映了;

A: 我也是这个意思，垄断者不作恶不也是安全的么?

这里混淆了垄断和作恶的概念。作恶指的是显式的攻击，例如双花一笔交易，作恶是可以被观察到的，系统或者生态也可以作出相应的反制。垄断是隐式的，垄断者不需要也不会攻击这个系统，但是它依然可以利用自己的共识权利获得更多的利益

，正如前文说的，只要能操控交易排序，你就能操控一切。

操控交易排序是无法被发现的。在 PoS 系统中，操控交易排序也意味着操控未来的 validator 集合，意味着垄断地位可以轻易的维持，这是根据系统历史来保证系统安全的必然结果，这一点在 PoW 中是不存在的。

我们现在还没有找到一个方法可以在所有时间排除一切垄断的可能，但是 PoW 至少给了我们一个更长的时间维度上使得垄断难以存在的设计，我觉得这一点对于 Layer1 至关重要。

A: 第一点，PoS 链后来者为什么不能参与?买币比买矿机门槛低多了，PoS 里面长期存在垄断者这个结论我是不认同的，没有经济规模效应;第二点，攻击 PoS 的成本比较，收购 stake 只是一方面，还有 reputation 系统，pos 里面节点是非常在意自己 reputation 的，这个成本对节点是巨大的。

第一点问题中，垄断的问题上面已经有回答。关于门槛问题，我认为这是很多人甚至包括协议设计者常常犯的错误。区块链的首要目标是安全和去中心化，而门槛以至于一切易用性问题都不是区块链的目标。

在区块链协议里面讨论门槛问题就像是在说「你让普通人怎么去构造 TCP 请求包」一样，将不同层次的目标混为一谈。要降低门槛，提高易用性，我们可以在上层做很多工作，做钱包，做云挖矿，设计各种金融产品，为什么要在区块链协议里面考虑门槛的事情呢?

Nervos 追求分层的协议架构，也是因为看到了易用性问题和安全问题必须分开考虑，易用性 / 门槛和安全从本质上就存在矛盾，强行扭在一起只会让我们一无所获。未来区块链协议的直接参与者一定是专业用户，这些专业用户通过搭建(可信的)服务、降低使用门槛、提供易用性来获取生态中普通用户的支持和收益。

第二点，reputation
是一个无法量化，区块链协议也无法判断的东西。将区块链的安全寄托在 reputation 上，只会让区块链走回现有信任体系的老路。同时 reputation 还有无法转让的特点，基于一个无法转让的事物建立安全模型，会不会又有些似曾相识?

A: 其实这里面有很多隐含的假设，如果一个 PoS 链出现你说的一个 cartel 控制 1/3 的 token，社区是可以通过应分叉 fork out cartel;我不觉得一个 PoW 链被 51% 算力控制的链，也面临同样严重的问题;另外我觉得节点隐藏最后长时间形成多数控制这种可能性是不大的;

将协议中解决不了的问题推给链外治理(注意在 cartel 控制 1/3 stake 并且产生足够大的威胁以至于社区想要 fork 的时候，链上治理已经没有用了)和硬分叉，确实可以解决一切问题，但这应该是一种成本极大的最后手段，不应该成为随便使用的工具，区块链的协议应该尽可能的避免陷入这个场景。

使用链外治理和硬分叉等价于承认协议的不足，需要人来接手了。我赞同一个区块链生态最终是需要人来治理的，但是我认为人介入的频率越低越好，如果不追求这一点，为什么还需要区块链呢?只有降低人参与的频率，协作的自动化成本才能降低，协作所需要的信任基础才能减小。

「节点隐藏最后长时间形成多数控制这种可能性是不大的」 —— 只要时间足够长，无论多小概率的时间都会发生。金融市场的黑天鹅告诉过我们无数次了，愿我们的记忆不只是 7 秒。

A: xxx 的筹码在不断分散;

A: xxx 的钱包地址从 ICO 1000 多个，不到一个月上万个;

根据 top 100 的地址或者 top 20 staking pool 的分散程度是无法证明 token 是分散的。道理很简单，我们谈论的都是无需许可(permissionless)的系统，地址代表的只是一个公私钥对而已，不代表一个身份。产生地址几乎是零成本的，存有 stake 的地址数量无法代表持有这些 stake 的是不同的用户。不要混淆地址和用户。

在 PoS 中，validator 集合中的 validator 数目是无关紧要的，并不能代表 stake 分散。如前文所说，如果你有 99% 的 stake，你应该把它们分散到 100 个甚至 1000 个 validator 上去。

PoW 中同样会有算力集中在大矿工手中的问题，但是由于 PoW 的开放性以及系统没有给后来者制造劣势(见上文)，这样的集中只会是暂时的，算力将在激烈的竞争中不停的从一个人手中转移到另一个人手中。PoW 赞美竞争，PoW 是一个开放的系统，只有开放的系统才可能远离热力学的终局，保持长久的生机。

PoS 有其价值，也有其问题，因此无法适用所有场景。Layer 1 的区块链协议必须使用 PoW，只有使用 PoW 的 Layer 1 才能解决我们希望解决的问题，实现我们希望的未来。