“计算-验证非对称性” 与 Moneyness

兼论 PoW 与 PoS

本文应 李阳@橙皮书 的邀请而作，缘起是橙皮书组织的微信群 “新经济学人” 内关于 PoW 和 PoS 长短的辩论。

本文亦感谢 Jan@Nervos 以及 Henry-民道@dForce，他们两位皆为各自的立场提供了漂亮且深入的论证，笔者亦从他们的论证中得到很多启发。

最后，本文的另一目的是表达对一位哲人的敬意，他发明了一个可供我们不断对话的原型机，而且我们越与之对话，越明白这个原型机的精巧。所谓 “大巧不工”，化繁为简需要极为强大的系统性思维，而他当得起 “大师” 的称谓。

一. 前言

2019 年 5 月上旬 “新经济学人” 群内辩论的主题为 PoW（Proof of Work，工作量证明）和 PoS（Proof of Stake，权益证明）的短长。但在我看来，微信群内的讨论很难形成聚焦，因此大家实际上在讨论两个不同的问题：（1）PoS（PoW）的技术局限性，即在技术上它们到底能不能实现某种属性；（2）PoS（PoW）系统的健康度问题，比如会不会形成 持币者/挖矿者/设备制造商 等在政治地域或收入阶层上的集中，以及这种集中会不会造成不良影响，虽然大家对什么是 “健康”、“不良” 并没有一致的定义。

在前一个问题上，我认为最好的论证是由 Jan 提供的。**他指出参与 PoW 系统是完全 permission-less 的**（这个 “参与” 就是指 “出块”），无需向任何人申请，即可 购买矿机/组建矿池 来参与 PoW 系统；**而 PoS 系统为了安全性牺牲了这种免许可性**：如果有人想加入这个系统成为验证者，他必须先质押，而质押作为一笔交易必须被打包上链才有效，等于是说他至少得取得部分现有验证者的同意才能成为验证者（出块者）。（这一点是很有道理的，PoS 要解决 “Nothing-at-Stake” 问题的最简单方法就是安排 “质押-罚没” 制度，而资金进入权益池是必须交易上链来确认的）。

在后一个问题上，最好的论证是由民道提供的。他指出，**出于分散风险的目的，持币大户不会拿住手上的币不卖**。币的价格上涨，则此种资产在持有者总资产中的比重也会变大，这个过程也是风险增大的过程，因此持币者会倾向于卖出自己手中的币，因此对财富集中的担心是不必要的。

仅就后者而言，许多问题我认为近乎无法 研究/比较，举例而言，说 PoS 中会出现币的集中，但难道 PoW 中没有矿场规模大小的区别吗？说 PoS 没钱不能参与，但难道在 PoW 里面矿机不用花钱买吗？至于集中度的大小，虽然我并不认为在某一时刻这种统计数字有太大的意义，但就拿统计数字来比较好了，本就没有人能提出一种最优分布，那么如何比较呢，更平均一定更好吗？

绕一圈你会发现，虽然只讨论前者不讨论后者是不行的，但在前者的讨论中我们有更明确的方法可以依靠，而且只有 Jan 说的那一点是最为确实的。

而在与民道讨论的过程中，我发现按照一般的方式根本比较不出 PoW 与 PoS 的区别：因为两种方式皆是 “抗女巫机制（Sybil Control Mechanism）”（女巫攻击即单个参与者可以不受限制地访问系统资源），两种方式皆必然要求参与者投钱进去（否则就无法达成抗女巫的目的了），两种方式皆可完成货币分发（矿工要卖币，验证者也要卖币），两种方式皆有可能形成一定程度的集中（正如某些地域电价较低，也必然有某些地域或某些人群资金成本较低）。更重要的是，从非常抽象的角度来看，两种系统都是以货币增发来购买参与者的支持，PoW 发币给矿工，PoS 发币给验证者。**这些角度都仅能比较出量的区别，而不可能比较出质的区别**。

这些问题迫使我选择另一条路径，而我开始思考一个问题：PoW 和 PoS 哪种更适合用于建构货币呢？货币性（Moneyness）的核心是什么？

二. 为什么会有货币？

为什么会有货币？为什么比如钻石这样的稀缺物品没有成为货币？石油会是一种好的货币吗？

在交易行为中，交易双方都免不了要判断对手所供商品或服务的费用，而在判断商品质量过程中付出的交易费用，我们称为 “判质费用”。交易的规模和频次总的来说当然受制于作为整体的交易费用（“信息费用”、“缔约费用”、“判质费用”），但只要我们将目光集中在以下情境中，问题就会变得更加清晰一些：当人们已经决定要相互交易，为什么有某种双方都接受的商品会更好？这种商品要具备什么条件（或者说为什么某种商品会比其它商品更符合这个条件）？

很快你便会意识到，这基本上与 “缔约费用” 无关，采用彼此都喜欢的某种商品（“货币”）并不能改变缔约费用；与 “信息费用” 的关系也没有那么密切，因为形成了大规模的市场后，货币作为一种商品，其信息费用（发现市场价格的费用）跟其它商品相比可能不会差别太大。因此，关键在于 “判质费用”。即，如果双方以物换物，双方都必须付出许多成本来判定对手给的东西的质量，有时候这种质量检验是消耗性的（比如检验石油的质量），但也许存在某种商品，其质量的变化幅度很小、很容易检验出其质量，那么大家可以很容易拿这种东西来交易，至少其中一方不用付出那么多的判质费用了。**又因为不同商品的判质费用不同，故适合用作货币的优势也不同**。

人类历史上出现过无数种货币：黄金、白银、石头、甚至香烟、鸡蛋；**但所有这些货币在相应的社会中都有明确的特征：在一定科技条件下，它们的判质费用是最低的**，黄金和白银只有纯度这一个维度，并且检验费用很低，熔化即可；美国产的香烟都是标准化产品，因此在战后德国某段时间被民间用作货币。

因此，判定 Moneyness 的强弱，其实无异于要去确定该物判质费用的高低。判质费用越低，越适合用作货币。

这就是产权经济学大师阿尔钦的洞见。（另说一句，此种货币理论子孙稀少，连阿尔钦爱徒张五常先生亦更多承袭费雪的货币篮子观念，而没有取阿尔钦的见解。）

好的，道理我都懂，这跟 PoW 和 PoS 有什么关系？

三. PoW 与 PoS 的真正区别

密码学货币的品质优劣到底体现在哪里？

密码学货币不是金属，没有物理实体，因此也没有了 “纯度” 的概念，不过，因为区块链的公开账本属性，UTXO 倒是有个 “干净度” 的概念——有些比特币曾经流入黑市，有些人可能介意。

但其实这种差别极为微小，根本不构成重要考量。**真正的质量其实在 “账本安全性”。同样是纯粹的、储存在全网无数台电脑上的数字，但不同的数字之间还是有 “账本安全性” 的区别**。

还没完。如上所述，**重点并不在于质量**（90% 的黄金和 95% 的黄金只有市场价格的区别），**而在于判质费用的高低**（黄金的判质费用比钻石低）。因此，并不是安全性的高低决定了哪种分布式账本适合承载货币，而是判定账本安全性的费用决定了它们的 Moneyness。

在 PoW 中，判定账本安全性的工作极为简单，验证块哈希并查看全网的难度要求即可；难度要求虽然不能直接地反映改写账本到底有多难，但直接地呈现了大概需要多少次哈希计算。

而在 PoS 中，至少就我所知，没有能够如此简单检验账本安全性的方法：

（1）在**非质押型** PoS 系统中，对出块合法性的校验依赖于状态数据，因为只有状态数据才能告诉你哪一刻哪个地址里有多少钱、TA 到底能不能出块，但是每出一次块都会多一部分状态数据；在最糟糕的情况下，这种困难性可以使 PoS 完全失去抗女巫的作用（攻击者可以用一段高度以前的分叉链攻击节点并且不必付出任何代价）；

（2）在**质押型** PoS 系统中，出块过程是验证者经由 “发起-预投-投票（签名）” 来完成的，而验证账本安全性中也必然有一步是校验验证者的签名。而且，无论聚不聚合签名，验证所需的计算量都很难降下来。

重点是，即便验签很简单，你也没法直接看出这些节点到底有多安全。你只知道确实是这 80 个节点签了名，如此而已。

（对不同方案验证性能的实证研究，应该是密码学者的研究课题了。我没有研究过，不能妄下结论）

综上，我认为，PoW 与 PoS（以及 “不好的 PoW”）的真正区别不在于它们是否能够提供安全性，而在于提供安全性的同时是否能让我们容易验证此中的安全性。客观来说，我在此比较的都是我看到的 PoS 系统，并不能演绎地推导出 PoW 一定比 PoS 做得更好，只能证明现在部分 PoW 比部分 PoS 要好，但能走到这一点我也就心满意足了，我也没有意愿讨论现在还不存在的解决方案。

接下来我想讨论另一个概念。

四. “计算-验证非对称性”

“**计算-验证非对称性**” 是指在某一类数学问题中，求出具体的解，与验证该解是不是一个解，所需付出的计算量是不一样的。我在这里谈的是 “难于计算、易于验证” 这种类型的非对称性。

举例而言，比如数学问题 `3X = 9` ，求解这个 X 的过程，与验证该解（ `X = 3` ）是不是正确解的过程，是完全一样的，在这个例子中，计算和验证是完全对称的。

但如果是一个数独谜题的话（9 个 9 宫格组成一个大网格，要求每行、每列、每个九宫格内 1-9 不能重复出现），你要算出一个数独谜题的解要花很多功夫，但验证起来极其简单，这是非对称的。

当然，还存在着验证极为简单，但计算求解近于不可能的问题，比如在椭圆曲线上用公钥推导出私钥。

（“计算” 和 “验证” 的概念在不同的语境下亦有不同含义，有一位精通密码学的朋友曾跟我解释过，然而我学识粗浅，实在无法重述，故留待社区中朋友们的解释和阐发）

在分布式账本中，“难于计算、易于验证” 的重要性在于：**它决定了当账本安全性上升的时候，验证的成本是否也随之上升**。

在比特币的 PoW 算法中，计算-验证非对称性非常强：无论安全性如何上升，验证的成本都不变。

但在我们现在看到的 PoS 方案（主要为质押型 PoS）中，这一点并不明显。因为签名（为出块赋予合法性）并不比验签（验证这种合法性）更难（更花时间），相反，在有些算法（比如基于椭圆曲线的签名算法）中，验签甚至比签名还要难，它是 “易于计算、难于验证”！

在限制了验证者数量的 PoS 系统中，可以说这种验证成本是有上限的，但在没有限制验证者数量的 PoS 系统中，验证的成本会随着验证者数量的上升而上升，即验证效率与出块权的去中心化（甚至网络的安全性本身）发生了冲突。

意识到了这一点，我们才能理解大师的智慧：

只要协议发了钱，人们总是要投入资源来竞争的；既然这样可以买到安全性，那我可以好好挑一挑，到此用哪种资源来提供安全性；另一方面，要出块就总是需要验证，或者说，验证才能真正约束出块者的行为，那就选验证成本低的吧；最后，既然验证的需求长期存在，不如想一种办法让验证的成本始终很低，这样才能更好地容纳安全性的增长。

这种 “难于计算而易于验证” 的属性，说起来很简单，所有了解现代密码学的人都理解，但却很有可能是 PoW 最核心的秘密。

五. Crypto-economics

我一直很反对给 economics 加前缀，虽然经济学作为一门社会科学，关于研究方法的争论吵过很长时间，但在我看来，这种争论早已有了结果，平时说某某经济学，只是方便交流而已。同样地，我也不太喜欢 “Crypto-economics” 一词，但同时我也认为，如果这个词真的有意义的话，我目前了解到的观念鲜少够得上这个词应有的规格，因为大多数时候，讨论 Crypto-economics 的人经济学都不怎么好。

若要有意义，密码经济学唯一的好去处是用成熟的经济学去判断不同的组件在分布式系统中到底承担着什么样的角色，甚至断言其优劣。

比如，PoW 和 PoS，在密码学（或者分布式系统）中是抗女巫机制，但在经济学视角下，它是安全资源，是系统的安全性的（一个）来源。而验证，在密码学视角下是对证明者的挑战，但在经济学视角下就成了判质过程，这个过程所需付出的代价就是判质费用。等等。

在大多数时候，技术归技术，经济学归经济学，但当我们需要评判某个组件在系统设计中的优劣时，我们可能需要两者的交叉。如果有密码经济学这回事，我相信这会是其中一个重要含义。

六. 结语

综上，我认为，PoS 作为一种抗女巫机制是可行的，只不过它所要求的共识算法可能会更复杂一些；但如果我们从 Moneyness 角度出发，我们会发现 PoW 货币在判质费用上更低，而且因为一些技术属性使得我们可以相信它会长期保持比较低的水平；而 PoS 系统至少就目前为止，没有出现可媲美 PoW 的低验证费用，甚至其验证费用还会上升。

愿 PoW 与 PoS 大辩论之火长燃不熄！

参考文献：

弗里德曼《货币的祸害》

阿尔钦：为什么需要货币？

对链式结构型 PoS 系统的 “虚假权益” 攻击

理解 BLS 签名算法