比特币的治理

作者：Pierre Rochard；来源：刘教链

我们为什么在意？

比特币的治理（governance）之所以重要，是因为比特币是第一个成功的、流动性最强的、最广为人知的加密货币。用Michael Goldstein的话说，“健全的货币是文明的基础支柱，比特币重拾了这一强大的社会协调工具。” 如果比特币的治理模式存在缺陷，就会阻碍比特币充分发挥其潜力。如果比特币的治理模式存在缺陷，比特币的利益相关者就应该努力修复它。

关于比特币治理的讨论往往集中在谁是最终的决策者，反复出现的候选者包括矿工、节点和投资者。治理的目的和机制往往只是被暗示，甚至与现实脱节。对过去治理效率的看法往往是谁“赢了”或“输了”某个具体决策，而不是决策过程本身是否充分。

什么是比特币的治理？

比特币的治理是一套交易和区块验证规则的决定、实施和执行过程，个人采用这些规则来验证他们在交易和区块中收到的付款是否符合他们对“比特币”的主观定义。如果两个或两个以上的人采用同一套验证规则，他们就形成了关于“比特币”的主观社会共识。

比特币治理的目的是什么？

关于比特币治理的目的，有各种各样的观点。治理应该为了哪些结果而优化？

Matt Corallo 认为，无信任（trustlessness）是比特币最重要的特性。Matt 将无信任定义为“在使用比特币时，除了你运行的开源软件外，无需信任其他任何东西”。如果没有无信任属性，所有其他积极的结果都会受到损害。

Daniel Krawisz 认为，比特币价值最大化是治理事实上的优化目标。Daniel 说：“比特币升级的一般规则[......]是，能提高比特币价值的升级会被采用，而不能提高比特币价值的升级不会被采用。”

在比特币治理的背景下，这两种观点分别反映了义务论准则和结果论准则之间的经典分歧。我倾向于 Matt 的义务论准则，即关注无信任。纵观货币史，从古代钱币生产者到现代中央银行，信任他人生产货币的结果就是滥用信任。在无信任度上妥协可能会帮助比特币价格找到一个局部最大值，但代价是找到一个更高的全局最大值。此外，没有证据表明比特币的价格与比特币协议的升级有关。也许比特币的基本价值会受到升级的影响，但比特币的流动性和波动性很低，价格并不能可靠地反映基本价值。如果我们无法观察到升级对比特币价值的影响，那么结果论准则似乎就不够充分了。

在评估当前的比特币治理程序是否符合维护比特币的无信任特性或提高比特币价值的既定目标之前，我们应该尝试定义当前的比特币治理程序是如何实际运作的。

当前的比特币治理程序是如何运作的？

比特币治理程序维护着一套验证规则。从高层次来看，这套长长的验证规则涵盖了语法、数据结构、资源使用限制、合理性检查、时间锁定、与内存池和主分支的调节、coinbase 奖励和费用计算以及区块头验证。要不折不扣地修改这些规则并非易事。

这些规则大多继承自中本聪。有些规则是为了解决漏洞和拒绝服务漏洞而添加或修订的。其他规则的修改是为了实现创新的新项目。例如，为启用新脚本添加了新的CheckSequenceVerify操作码。

研究

每项规则的改变都始于研究。例如，隔离见证（SegWit）就是从研究修复交易可篡改性（transaction malleability）开始的。交易可篡改性已经成为一个严重的问题，因为它阻碍了闪电网络（Lightning Network）在比特币上的部署。行业和独立研究人员共同合作，最终形成了隔离见证。

批评者指出，研究人员想要研究的东西、用户的期望和对网络特性有利的东西之间偶尔会出现脱节。此外，学术界的计算机科学家更喜欢“科学模拟”，而不是“工程实验”。这一直是科研社区紧张关系的根源。

提案

当研究人员发现了一个问题的解决方案时，他们会与其他协议开发者分享他们提出的修改建议。分享的形式可以是向 bitcoin-dev 邮件列表发送电子邮件、正式白皮书和/或 Bitcoin Improvement Proposal (BIP)。

实施

提出提案的研究人员或对该提案感兴趣的其他协议开发人员将在节点软件中实施该提案。如果研究人员无法实施提案，或者提案没有得到同行的好评，那么提案就会停留在这个阶段，直到被放弃或修改。

虽然这可能会给人一种印象，即比特币协议开发的贡献者可以否决提案，但研究者可以向公众说明自己的理由，并绕过现有的开发者。在这种情况下，如果研究人员缺乏声誉和信誉，就会处于不利地位。

实施阶段的另一个问题是，如果比特币协议开发者和更广泛的比特币社区普遍认为某个实施方案有争议，那么参考实现的维护者就不会合并该实施方案。参考实现的维护者有一个深思熟虑的政策，即遵循共识的变化，而不是试图强加这些变化。C++ 参考实现托管在 github.com/bitcoin/bitcoin，是中本聪代码库的直接继承者。由于其成熟性和可靠性，它仍然是最受欢迎的比特币节点实现。

要绕过参考实现的维护者，不顾一切地修改共识，就像复制比特币代码库并发布提议的修改一样简单。这种情况就发生在 BIP-148 用户激活软分叉（UASF）中。

修改验证规则的提议可以通过软分叉或硬分叉实现。有些提议只能以硬分叉的方式实施。从预分叉节点的角度来看，软分叉实现是前向兼容的。采用软叉后，分叉前的节点无需升级软件就能继续验证分叉前的共识规则。但是，这些分叉前的节点并不验证软分叉所做的规则变更。从分叉前的节点的角度来看，硬分叉不是向前兼容的。分叉前的节点最终将与分叉后的节点出现在不同的网络上。

硬分叉和软分叉对网络和用户的影响一直存在争议。软叉被认为比硬叉更安全，因为软叉不需要明确的选择加入，但这也可能被视为一种胁迫。如果有人不同意软分叉，就必须硬分叉来推翻它。

部署

节点软件实施后，必须说服用户使用节点软件。并非所有节点用户的重要性都相同。例如，“区块链浏览器”也有更大的权力，因为许多用户依赖于他们的节点。此外，交易所可以决定哪个验证规则集属于哪个代币符号。投机交易者、大户持有者和其他交易所对代币符号的这种权力进行制衡。

虽然个人用户可能会在社交媒体上发出信号，表示他们使用的是某一版本的节点软件，但这可能会遭到女巫攻击。共识的最终检验标准是，你的节点软件能否接收你认为是比特币的付款，而你能否发送对方节点软件认为是比特币的付款。

软分叉有一个链上治理功能，叫做带超时和延迟的 BIP-9 版本比特位。该功能以滚动方式衡量矿工对软分叉的支持。矿工对提案的支持度被用作更广泛社区支持度的替代衡量标准。遗憾的是，由于挖矿集中化以及矿工和用户之间的利益冲突，这种代理衡量可能并不准确。矿工的链上“投票”也延续了比特币是矿工民主的神话，只有矿工才能决定交易和区块的有效性。只要我们承认并接受代理测量的局限性，BIP-9 就是有用的。

执行

验证规则的更改由完全验证节点的去中心化点到点网络执行。节点使用验证规则独立验证其操作者收到的付款是否属于有效的比特币交易，是否包含在有效的比特币区块中。节点不会传播违反规则的交易和区块。事实上，节点会断开并禁止发送无效交易和区块的对等节点。正如 StopAndDecrypt 所说：“比特币是一座坚不可摧的验证堡垒。” 如果每个人都认定挖出的区块无效，那么矿工的 coinbase 奖励 + 费用就一文不值。

矿工的作用是提供时间戳功能，并通过工作量证明来确保安全。所提供的哈希率，一方面来自于硬件和电力的成本，另一方面来自于coinbase 奖励和费用的收入。矿工是雇佣兵，过去他们提供的时间戳功能没有经过完整的规则验证。由于挖矿集中化，无法信任矿工自己执行验证规则。

当前的比特币治理模式是否导致了更多的不信任？

在我看来，目前的比特币治理模式已经防止了无信任度的下降。在过去的 5 年中，比特币链上交易的急剧增加似乎看不到尽头。如果比特币的治理模式没有抵制去年矿工发出的将最大区块重量增加一倍的信号，那么就会开创将交易吞吐量的价值置于无信任度之上的先例。

目前的比特币治理模式是否导致了比特币价值的升级？

我认为不可能建立因果关系。比特币的价格比两年前要高得多，但这似乎是一个由交易者心理而非技术基本面驱动的内生过程。关于基本面，不可否认的是，比特币的治理已经实现了共识的改变，而闪电网络的运行依赖于共识的改变。我一直在尝试建立通道和进行闪电支付：毫无疑问，闪电网络提高了比特币的价值。