加密经济学：区块链技术前景之路基

原创： Kyle Wang 以太坊爱好者 *2017-08-20*

> **如果你不能乐在其中，那就没有意义了。**
>
> ——“约翰·纳什”，《美丽心灵》（2001）

浏览现下的关于区块链的文章，你将看到关于其应用的有益的讨论，以及，关于某些人最喜爱的加密货币的未来价格走势的无穷无尽的争论。但在所有这些主题中，人们仍然很少提及居于这场运动核心的最迷人的概念——区块链作为一样新奇事物，意味着以物质激励我们所期望的人类行为。

从许多方面来说，区块链技术的神奇之处在于，它使我们可以在荒漠上种庄稼、在狐狸洞里养鸡。伴随对密码学的使用，区块链概念允许我们可靠地证明，历史上什么交易真实地发生了。通过将博弈论和经济学组合进区块链协议的设计中，该系统激励了稳定性，并让这一公共利益走向未来。这一切，居然可以发生在遍布黑客、骗子、盗版和暴民的匿名且敌视的电子世界里！

这就是加密经济学（cryptoeconomics），一个新鲜到运行拼写检查时你需要点选“添加到词典”的术语。如果你对潜藏于区块链技术及其具体系统之下的这一概念探究得足够仔细，你会发现，他们都大量包含了加密经济学的工具。这些工具本是特地设计出来以最小化恶意行为者的影响的。

虽然加密经济学有许多的定义，这些定义相互之间都有细微的不同，为了本文的目的，我将我们的讨论建立在以太坊百科给出的定义上。

加密经济学综合自密码学、计算机网络和博弈论（它为安全体系提供一些经济激励/反激励集合的展示）。

在这篇文章中，我将讨论这些经济激励（因为他们与区块链相关），发掘加密经济学背后的一些安全性假设，然后描述以太坊平台的新版本，Caspe“小精灵”协议，是如何伴随着对这些观念的深入考虑而设计出来的。

激励与拜占庭容错机制

激励乃是博弈论和经济学在塑造朝向共同利益的人类行为时候的一个核心组成部分。虽然密码学，或者说，为了有效地创造一个可验证的历史而对链上的区块进行的加密与解密，是被普遍接受的，我们之间仍然存在一些分歧与争论，在谈到“为了创造成功的加密货币或平台，激励系统是否真是必要的”的时候。

不简要地讨论支撑去中心化数字经济的问题，即拜占庭将军问题，的话，我们就没法继续下去了。

光荣的拜占庭军队被包围了，并且被围困有一个城堡里。将军们控制着这支军队的不同部分，他们意识到，他们需要决定共同进攻，或者共同撤退；但在物理上，他们却是相互隔离的。重要的是大多数人都同意此种或彼种策略，因为错失时机或者半心半意的攻击对拜占庭人来说将意味着重大伤亡或者一个更为糟糕的结果。

不幸的是，拜占庭军队中，卖国将领的数量是不确定的，他们最想要的就是这场战争悲惨地结束。他们可能给不同的将军发送相互矛盾的信息，企图破坏大家的努力。而且，因为信息必须通过传信官来传达，不可能去断定这些信息是伪造的还是可信的。

所谓的核心问题就在这里：在一个一致意见具有绝对必要性的系统里，如何能够在缺乏信任机制的情况下，通过一个可信的过程，将一个一致意见传达给所有人？换句话来说，这些将军如何能够战胜藏在他们中间的叛徒，形成一个一致的、多数的意见？

在计算机科学里，一个系统的从错误组件（即阻碍其他重要组件形成必要共识的组件）中避免错误的能力，被称为拜占庭容错机制（BFT）。那么，它跟区块链和围绕激励的讨论有什么样的关联呢？

在一个加密货币，比如比特币（Bitcoin），中，如果缺乏一个可以实现BFT的协议，又没有一个中心化的权威，我们就将完全陷入黑暗。就像那些将军，比特币的节点（分享和扩大该区块链的计算机）需要知道哪些交易是有效的。打个比方，就像那些卖国的将军和他们可疑的信息，人们也可以花了比特币却简单地告诉其他节点他们没有花。去中心化的数字货币的关键问题是：没人知道可以相信谁、可以相信什么。

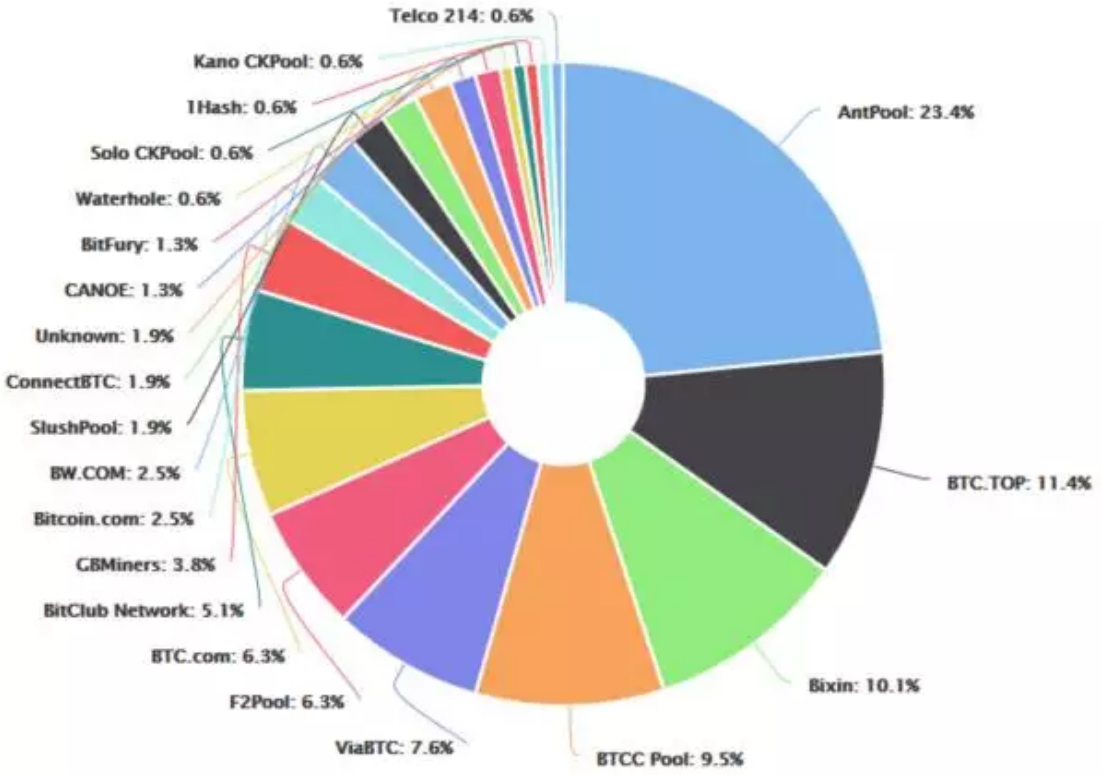
比特币对拜占庭将军问题的应答是位于区块链顶层的工作量证明（PoW）协议。正如你会发现大量关于PoW的讨论和其他材料，这一协议背后的一般理念是：让操纵投票变得尽可能困难，出于所需资源（时间，电力以及处理能力）的大量付出。要记录一场投票，每个“将军”都必须完成一个非常复杂的数学问题，该问题会在一瞬间被分享给其他人，待它被解决后，这些人又必须解决另一个复杂的问题。“工作”的链条将创造一个坚固的交易记录，同时，让攻击者们的操纵变得过分昂贵且费时。

激励在此时加入进来，以鼓励参与者们维护该协议——比特币“矿工”，也就是记录那些交易的人，在每一次他们使用他们的计算机算力并且成功地将已验证的交易提交到区块链的时候，都会被奖以12.5个比特币和交易费用作为激励。通过这种方式，他们因向比特币履行了一项关键服务、传播写满了有效且被验证过的交易的区块链而受到奖励。

在以太坊平台上，人们提议的权益证明（PoS）协议走得更远，它使用惩罚来反激励恶意行为。在PoS中，为了参与该系统，验证者们必须缴纳一大笔以太币保证金，作为电力和算力的替代。当验证者们不为该系统的利益采取行动时，他们就冒着失去他们全部权益，或者说保证金，的风险。

那么，加入鼓励机制有任何缺点吗？因为加密空间里的两个主要角色的协议都对加密经济学表现出强烈的关注，看起来精心设计的激励系统对于区块链技术的成功来说是关键的了。但MIT的教授Silvio Micali，一个密码学世界里的核心权威，并不同意这一点。

正如这篇文章所报道的，Micali认为，激励应被当作最后手段来使用，因为它们可以导致许多负面的外部性；他还举比特币作为例子。在比特币工作量证明系统中的激励，导致了“工业化规模的矿池”，比特币矿工们将他们的资源聚集在一起然后分享奖励。下图可看出这些矿池的主导地位：



激励变得扭曲？比特币算力分配，2017年7月

这些体量巨大的矿池的出现，以及随之而来被分配给它们背后的组织的权力，真切地开始冲击比特币作为一个去中心化的加密货币的理念，同时提高了51%攻击（我们稍后将讨论它）的可能性。简而言之，如果这一趋势持续下去，我们将到达这样一种境地：新比特币的发行将几乎完全由最大的矿工主导。

Micali转而建议Algorand，一个更少激励机制的公有区块链，它通过一个随机过程在每一轮中交换将军，借此解决拜占庭将军问题。我将不会在这里讨论该机制的细节，但这一方法避免了工作量证明需要的计算资源的数量，结果产生了更快速的交易。

这些不同的方法，围绕着那个有趣的哲学问题，即：“总体来说，人是被他们的利他主义还是一己私利主导的”，而被反复考虑。Micali的的支持者指出，在Bittorrent和其它分散式的计算机项目比如Genome@Home上长期驻留的无私奉献者证明了我们并不总是需要激励来促进利他行为。同时，以太坊基金会（Ethereum Foundation）的Vitalik Buterin和Vlad Zamfir坚定地站在相反立场上，他们认定：没有激励与惩罚，人们在最好的时候就是无动于衷（为什么要做记录呢？），在最坏的时候是穷凶极恶。

尽管大部分区块链运动都拥抱了激励和加密经济学的理念，Micali的系统肯定是可行的，而它的变体也许会在与现有的区块链平行的道路上生根发芽。

是否需要激励，这是一个开放性的问题；而且我不认为它可以在一个学术模型中得到解决。实际上它正通过证据得到解答。你大可开发出一些东西，静观其变。

——Charles Hoskinson，以太坊前CEO

尽管比特币的工作量证明机制不是完美的，事实证明，它所建基的范式转换和加密经济学原理（密码学保护过去，经济学保证未来）已然导致了其将近十年的生存与应用。

关于行为的加密经济学假设

加密经济学的现状是：其术语和理论正被区块链的开发者们和思想领袖们日复一日地加以倡导。要强调这个领域内的前沿创新，在写作这篇文章的时候，某些联系着加密经济学的术语的谷歌搜索结果还不到100条！虽然这一领域中的许多观念都是非常理论化的，其余的部分却保证了它们的应用会在区块链技术的发展和应用中取得惊人的成果。

也就是说，加密经济学关心的是设计强悍的协议，主导去中心化的P2P系统和数字经济。换句话来说，加密经济学的概念和技术应被用于塑造导向合意结果的行为。

今天，作为中本聪（Satoshi Nakamoto）的创新的结果，比特币在一个工作量证明激励系统上运行，而该系统几乎既解决了拜占庭将军问题，又鼓励了人们维护该系统的努力。但是，因为Micali指出的负面外部性，比如倒向具有可观影响力的中心化矿池，工作量证明协议不能被认为是有效率的，在加密经济学的意义上。虽然Micali以此为证据指出激励系统完全是有害的，加密经济学的支持却转而主张：激励或者惩罚走得还不够远、还没有被最优地运用。

所以，我们应该通过何种镜头来评估一个协议呢？以太坊基金会的开发者们在他们的分析中使用下列安全模型。这些针对参与者行为所作的假设便是协议设计的基础。

安全模型

诚实的大多数模型——传统的容错假设，即51%乃至更多的参与者在根本上是诚实的，是“好人”。在加密经济学社区，这一模型在很大程度上是不受欢迎的，经常被认为是在匿名、去中心化的图景中的一厢情愿。

相反，在加密经济学研究中，我们岂止是愤世嫉俗。我们执着于有关攻击者的假设——即他们是如何协作的，为了发动攻击他们必须投入的预算，以及攻击导致的实际成本。

协调选择模型——假设所有的协议参与者都被同一个联合或者代理统一起来了。

在这里，最大的比特币矿池就是一个好例子。因为大多数比特币算力都被控制在一小部分人手中，串谋是一个非常现实且具有威胁性的方案。随着矿池的增大，一个51%攻击，也就是一个机构（或者串谋的代理们）可以通过控制超过一半的挖矿算力来操控比特币区块链，在现实中是完全可行的。

虽然代理不能够重写以往的交易、从人们的钱包里面偷币，或者制造大灾变作为报复，他/她还是能够阻碍其他矿工上传交易到区块，以及“双花”使用所有链的比特币。总的来说，这种威胁看起来暗示了行动者自己的弄巧成拙——这样一种勾结的或巨大的努力将只会使整个比特币贬值，因为参与者们将对这个系统失去信心，并且在这段时间里拒绝确认交易。

罕见瞬间：90%的比特币挖矿算力齐聚一堂

不协调选择模型——假设所有协议参与者都不彼此合作，他们小于一个特定规模，且各怀目的。

这是藏在"去样一个假设之上：宇宙中遍布弱小的、自利的并且无意或者无法相互合作的参与者。

贿赂攻击者模型——该假设建立在不协调选择模型之上，但也假设存在一个拥有足够资源、通过有条件的贿赂来激励其他参与者采取特定行动的攻击者。

这一模型已经在Vitalik以及其他作者提出的SchellingCoin案例中得到详尽的描述。为了增加一点趣味性，我将提供一个短小精悍的例子：

让我们假设，在不协调选择模型的宇宙中，存在一个王座争夺游戏。游戏的参与者们将对他们想坐上钢铁王座还是泡沫王座投票。每一个投票给多数方的人都将赢得100美元，而少数方的所有人将什么也得不到。

在这个游戏中，假设你将投票坐上钢铁王座，因为你想统治七大王国，也因为坐在泡沫王座上实在不讲究。你相信大多数人会因为同样的理由做出同样的选择。因为其他每个人都得出了跟你一样的结论，多数票将投给坐在钢铁王座上，每个人都能拿到100美元。

但是，让我们假设，有个恶意的泡沫经理人试图推销他的不可降解的器皿。经过一番狡猾的算计，他向每个人都发送了一份有条件的要约："投票给泡沫一方，如果你变成了少数方，我将私下给你110美元！"因为他有一段长期还债的历史，每个人都知道他看重这一承诺，也有财力来支付它。

如图所示，你的收益取决于王座游戏中其他人采取的行动

突然，均衡点就转移了。现在，你投票给泡沫王座就有意义了——如果你是多数方，你拿到100美元；如果你在少数方，你将揣着110美元回家。因为其他每个人再一次得出了与你相同的结论，多数人将投票给泡沫，而那个经理人将允许自己大笑三声，全数不用支付还以零成本达成了他的目标。实际上，他那慷慨的威胁才是他的杀手锏。

这种形式，便是我们所知的P + epsilon攻击，比特币协议就对被这种策略很敏感！将钢铁王座替换成主区块链，泡沫王座替换成攻击者的链，你应该可以看到其弱点——一个恶意行为者激励其他矿工中的大多数接受一个变异的链。尽管如此，因为一个攻击者为了发动攻击必须有能力可靠地展示大量的预算，比特币的工作量证明还是无视这一缺陷，坚持了下来。

关于行为的加密以太坊的权益证明机制：下一个实验

我希望你深刻地意识到，区块链技术的发展受到这些安全模型的意涵的驱动。正如控制者团队（the control）的Nick Tomaino写的那样，“加密经济学是这整场运动的基本催化剂”。

要评估设计协议的缓解这些安全模型中现存的和理论上的缺陷的能力，开发者们使用这两个概念：

第一个，加密经济学安全边际，衡量那些违反一个协议保证所带来的结果（以损失的美元计）。理论上来说，因为攻击者可以0成本发动P + epsilon攻击，只要他/她有那个预算，比特币的工作量证明系统可以说只有0的加密经济学安全边际！

加密经济学证明在某种程度上也是相似的；这是一份来自网络中某参与者的保证或者信息，断言某物为真。若在某个事件中证明它并不为真，该参与者就将失去一定数量的金钱。

让我们来检验一下今时今日区块链技术领域最具雄心的项目——即将到来的以太坊Casper更新，它尝试通过将平台从工作量证明调整为权益证明来直捣黄龙。一场关于Casper的权益证明（PoS）机制的复杂之处的讨论将超出这篇文章的范围，但简而言之，权益证明尝试提供一个非常巨大的加密经济学安全边际，通过强制要求大笔的以太坊安全保证金，代替计算机算力，以实现验证者的功能。这一安全保证金，或说加密经济学证明，成了一个强有力的威慑。其含义是一目了然的——制造麻烦，你就将失去一切！

Casper强制参与者加入一个谢林币（SchellingCoin）游戏（如我们的钢铁-泡沫王座例子概述的那样）。参与者们被强制要求将他们的安全保证金押在多数人将下注的事情上。使用同样的（我们在钢铁王座游戏中用到的）递归逻辑，多数参与者将准确地投票给有效的交易，因为每个参与者都预期其他人得出同样的结论。情形就是如此，权益证明可以抵抗P + epsilon攻击，因为在他们最终将投票给少数方的情形中，攻击者将不得不可信地展示巨额的预算以补贴参与者的安全保证金。

在这些安全模型的环境下，我们可以看出Casper的弹性集中在不协调选择模型中，且源自贿赂攻击者。Casper在理论上同样对起源于合作攻击者模型的51%攻击敏感。但是，就像比特币，以太坊将做出如此攻击的成本提高到如此高昂的地步，以至于几乎完全地遏制了它。在Casper的环境下，失去所有相关权益的威胁是一个更强有力的震慑。要获取更多关于Casper进展的信息，请经常查看Vlad Zamfir的文章。

虽然Casper的许多元素是高度理论化的，权益证明协议自身也激起了关于公平份额的辩论，但有证据表明：这一转变几乎完全在加密经济学的意料之中，也意味着解决了工作量证明系统的许多不足。缓慢但坚定地，区块链空间里的思考者们在我们对去中心化数字经济中最优协议设计的认识上进一步覆地翻天。

一些针对整个区块链技术的批评者们对这样一种理念感到很不自在：今天，太多攻击途径仅在理论上是可行的。我认为这样一种想法没什么意思：只要有足够的金钱和时间，一个攻击者将总是能够破坏任何系统。在最坏的情况下，加密经济学也如坚实壁垒般伫立，努力让这些攻击变得尽可能昂贵、困难而且不可取。

因为我们将走向一个图灵完备的智能合约时代，这一领域必将变得更加复杂而激动人心。

我希望这篇文章给你一些对生机勃勃、丰饶多姿的加密经济学领域的了解。作为结束，我这里已没有什么资源了，所以我想分享一些对我来说受益匪浅的链接。

加密经济学101，Nick Tomaino著：https://thecontrol.co/cryptoeconomics-101-e5c883e9a8ff ——本文的灵感来源之一。他也有一些很棒的链接。

加密经济学傻瓜入门，K著：https://medium.com/@j32804/cryptoeconomics-for-dummies-part-0-7172efa81507 ——关于如何进入这个主题的有趣文章。

加密经济学导论（视频）：https://www.youtube.com/watch?v=pKqdjaH1dRo ——高手直接布道。Vitalik Buterin舌灿莲花。

为什么加密经济学和X-Risk研究者们应该多听听对方的意见：https://medium.com/@VitalikButerin/why-cryptoeconomics-and-x-risk-researchers-should-listen-to-each-other-more-a2db72b3e86b ——Vitalik Buterin论加密经济学与人工智能研究交叉的文章。

以太坊的基本问题：https://github.com/ethereum/research/wiki/Problems ——近来以太坊要解决的问题的候选名单。包含了一些关于加密经济学的有益讨论。

纳什均衡与谢林点：http://lesswrong.com/lw/dc7/nash_equilibria_and_schelling_points/ ——有关Buterin写作的一篇文章（https://blog.ethereum.org/2014/03/28/schellingcoin-a-minimal-trust-universal-data-feed/），但自身也是关于博弈论的优秀读物。

冲突的战略：https://www.amazon.com/Strategy-Conflict-Thomas-C-Schelling-ebook/dp/B01ASPM5A4/ref=mt_kindle?_encoding=UTF8&me= ——一本老的但是绝佳的关于博弈论的书。作者是托马斯·谢林，核战略的理论大师（我可是认真的！）。

原文链接: https://hackernoon.com/cryptoeconomics-paving-the-future-of-blockchain-technology-13b04dab971

作者: Kyle Wang

翻译&校对: 阿剑 & Elisa