弄清加密经济学

原创： Josh Stark 以太坊爱好者 *2017-12-26*

-塞戈维亚的罗马水道，一项工程界的早期奇迹-

几个月前，著名的硅谷风险投资公司Parker Thrpson在推特上说：“加密经济学（Cryto-economics）这一说法极为愚蠢，就是经济学而已。自己捏造单词只是一个用来忽视本来很容易理解的概念的借口。“

“加密经济学”一词造成了很多混淆。 人们往往不清楚它究竟是什么意思。这个词本身有可能是误导性的，因为它暗指整个经济学都有一个平行的“加密”版本，这是完全错误的，所以帕克完全有理由嘲笑这样的概念。

简而言之，加密经济学就是利用激励机制和密码学来设计新的系统、应用和网络。具体来讲，加密经济学与建立事物相关，与机制设计（mechanism design）（数学和经济理论领域）有许多共同之处。

加密经济学不是经济学的一个子领域，而是应用密码学的一个领域，且将经济激励和经济理论考虑在内。 比特币，以太坊，zcash和所有其他的公共区块链都是加密经济学的产物。

加密经济学使区块链变的有趣，并使区块链与其他技术区别开来。 从{中本聪的白皮书](https://bitcoin.org/bitcoin.pdf)中我们了解到，通过密码学，网络理论，计算机科学和经济激励的巧妙结合，我们可以建立新的技术。这些新的加密经济系统可以完成这些学科本身无法实现的事情。而区块链只是这种新的实用科学的一个产物。

本文旨在以清晰，简单的术语解释加密经济学。 **首先**，我们以比特币为例来看看加密经济的设计。 **其次**，我们思考了加密经济学与经济理论是如何联系起来的。 **最后**，我们看看如今仍然活跃的三个不同的加密经济设计和研究领域。

1.什么是加密经济学？-以比特币为例

比特币是加密经济学的产物。

比特币的创新之处在于它允许许多彼此陌生的实体就比特币区块链的状态达成共识，而这是通过经济激励和基本密码学工具的结合来实现的。

比特币的设计依赖于经济激励和惩罚。 经济激励被用来招募矿工，从而支持整个网络。 矿工们贡献自己的硬件和电力，因为只要他们生产出新的矿块，就会得到大量的比特币作为奖励。

其次，经济成本或惩罚是比特币安全模型的一部分。攻击比特币区块链最显而易见的方式是控制大部分网络的哈希算力 - 也就是所谓的51％攻击 ——攻击者因此能审查交易，甚至改变区块链的历史状态。

但是，控制哈希算力的代价是金钱，通常要花费大量金钱在硬件和电力上。比特币的协议有意使得挖矿变得困难，这也就意味着要想获得对大部分网络的控制，花费将十分昂贵，也就是说发起攻击几乎无法获利。 截至2017年8月16日，在比特币上发起51％攻击需要每天花费18.8亿美元在硬件上，340万美元在电力上。

如果没有这些经过仔细推敲的经济激励措施，比特币将无法工作。如果挖矿成本不高，就很容易触发51％攻击。而如果没有挖矿奖励，就不会有人购买硬件和电力来支持网络运行。

比特币也依赖于加密协议而存在。 公私钥加密技术用于保障个人安全，让用户拥有对比特币唯一的控制权。哈希函数用于“链接”比特币区块链中的每个区块，证明事件发生的顺序和历史数据的完整性。

这些加密协议为我们提供了构建像比特币这样可靠而安全的系统所需的基本工具。如果没有公私密钥基础设施这样的东西，我们就不能保证用户对比特币的唯一控制权。 如果没有哈希函数，节点就无法保证比特币区块链中比特币交易历史的完整性。

如果没有像哈希函数或公私密钥加密那样的硬性加密协议，我们就没有可靠的记账单位（编者按：比特币）来奖励矿工，无法确保我们的帐户历史记录是真实的，且完全由合法所有者所控制的。 如果没有一套经过认真调整的激励措施来奖励矿工行业，那么该记账单位就失去了其市场价值，因为谁都无法保证这个体系可以延续下去。

通过这种方式，设计比特币既需要理解密码学，也要理解激励机制是如何影响用密码学构建的系统的安全属性和功能的。 加密经济学是陌生的，反直觉的。 我们中的大多数人不习惯把金钱看作一个设计或工程问题，也不习惯将经济激励作为新技术的一个重要组成部分。 而加密经济学恰恰要求我们从经济角度思考信息安全问题。

在这个行业中，最常见的错误之一是由那些只通过计算机科学或应用密码学的观点来看待区块链的人造成的。 我们倾向于把对于我们来说最舒适的事情放在首位，而忽视把我们专业领域之外的事情。

在区块链技术中，刚才提到的那个错误导致许多人臆断并剥离出经济激励的关键作用，这就是我们看到诸如“区块链是无需信任的”、“区块链只靠数学支撑而无需其他”和“区块链是完全不可更改的”这样无意义的句子的其中一个原因。**它们各自都有错误之处，却都同样具有混淆一个人们组成的大型网络的本质作用的效果——在那样的网络中，人们的必要参与是通过经济激励来维持的。**

比特币这样的加密经济系统对于那些只把它看作是计算机科学产品的人来说，就像是魔法一样，因为比特币可以完成纯计算机科学无法完成的任务。加密经济学不是魔术 - 它只不过是跨学科的而已。

2.更广义上说，加密经济学与经济学有什么关系？

“加密经济学”这个词可能存在一定误导性，因为它似乎在与整个经济学作比较，这就是为什么像Parker这样的人会否定这个词。 经济学是对于选择性的研究：对个体和组织如何回应激励的研究。 加密货币和区块链技术的发明不需要用任何人类选择的新理论——人类根本就没有发生改变。 加密经济学并不是将宏观经济学和微观经济学理论应用于加密货币或代币市场。

加密经济学与机制设计最为相像，机制设计是一个与博弈论有关的领域。 在博弈论中，我们研究某一给定的战略互动（即一个“博弈”），然后尝试理解每个参与者可以选用的最佳策略，以及如果两个参与者遵循这些策略可能产生的结果。 比如，我们可以用博弈论来看待两个公司之间的谈判，国家之间的关系甚至演化生物学。

机制设计通常被称为反向博弈论（博弈论的逆向应用），之所以叫这个名字是因为我们从一个期望的结果开始，反向设计一个游戏，如果玩家追求利益，就会最终产生我们想要的结果。 例如，设想一下如果我们负责设计拍卖规则会发生什么情况？ 我们有一个目标，希望投标人的投标价等于一个项目的实际价值。为了达到这个目标，我们运用经济理论将拍卖设计为一种博弈，使得任何玩家的主导策略都是投出标的物的真实价值。维克里（Vickrey）拍卖是其中一个解决方案，其出价是不公开的，拍得的玩家（定义为出价最高的玩家）只支付第二高的出价金额。

像机制设计一样，加密经济学着重于设计和创建系统。 正如在拍卖案例中一样，我们用经济理论来设计产生一定均衡结果的“规则”或机制。 **但是在加密经济学中，用于创造经济激励的机制是使用密码学和软件建立的，我们设计的系统几乎总是分布式的或去中心化的。**

比特币便是加密经济学的产物。 Satoshi希望比特币具有某些特性——比如，它能够就其内部状态达成共识，且是抵制审查的。 随后，Satoshi假设人们会以理性的方式回应经济激励，并着手设计了一个系统来实现这些属性。

多数情况下，加密经济学是用来为分布式系统提供**安全保证**的。我们有一个加密经济安全保证：除非有人愿意花费数十亿美元，否则比特币区块链对于51％攻击就是安全的。换言之，在状态通道 ，我们稍后会讨论这个话题，我们都可以拥有加密经济安全保证，保证链下过程几乎与链上交易一样安全。

值得注意的是，机制设计并不是万能的。 **我们依靠激励来预测未来的行为是有限度的。** 正如Nick Szabo指出的那样，我们最终将猜测人们未来的精神状态，并假设他们对某些激励措施有何反应。加密经济系统的安全保障一定程度上取决于人们对经济激励措施反应强度的假设。

3.加密经济学的三个实例

目前至少有三种正在设计中的系统可以被称为“加密经济”。

示例1：共识协议

区块链不必依靠中心信任方便能够达成可靠的共识，是密码经济设计的产物。 我们上文探讨过的比特币解决方案叫做“工作量证明”共识，因为矿工必须进行工作（投入硬件和电力），才能参与网络并获得挖矿奖励。

改进工作量证明系统和设计替代方案是加密经济研究和设计的一个领域。以太坊目前的工作量证明共识机制包含了许多对原始设计的变化和改进，从而实现更快的出块时间，并更能抵抗由ASIC导致的采矿集中。

在不久的将来，以太坊计划迁移到一个名为Casper的“权益证明”共识协议。 这个协议可以替代工作证明，不需要进行大家熟知的挖矿，因此也就无需专门的挖矿硬件也不需要大量的电力支出。

要知道，要求矿工购买硬件和花费电力的目的是为了增加矿工的成本，作为提高51％攻击的累积成本的一种方式，导致其成本太高。利益证明制度是使用加密货币保证金来创造相同的抑制性，而不是像硬件和电力这样在真实世界投资。

为了在证明利益系统中“挖矿”，你必须将一定数量的以太币存进“保证金”智能合约。就像在工作量证明中一样，这么做大大提高了51％攻击的成本，攻击者将不得不投入大量的以太币来成功攻击网络，而他们将在随后永远失去这部分以太币。

Casper由 Vlad Zamfir ， Vitalik Buterin 和其他几个以太坊基金会成员设计。 你可以在 Zamfir 的这个系列文章（编者按：EthFans中译本见文末）中获得关于Casper设计历史的更多内容，他在最近的播客中也经常谈论这个。Buterin在这里（编者按：EthFans中译本见文末链接）写了一篇关于Casper的设计哲学的长文，并在 ethereum GitHub wiki 上解答了有用的常见问题。

例2：加密经济的应用设计

一旦我们解决了区块链共识的根本性问题，我们就能够在类似“以太坊”这样的区块链上构建应用程序。底层区块链为我们提供了（1）一个可以用来创造激励和惩罚的价值单位，以及（2）一个工具包，我们可以用“智能合约代码”的形式来设计条件逻辑。 这些工具也可能是加密经济设计的产物。

例如，预测市场 Augur 依赖加密经济机制才能发挥作用。 Augur 使用它的本地代币 REP 创建一个奖励系统，如果用户向应用程序报告“真相”，就可以获得奖励，随后这个“真相”会被用来结算预测市场的赌注。这一创新之处使去中心化预测市场成为可能。 另一预测市场 Gnosis 也使用了类似的方法，虽然也让用户指定其他机制来确定真正的结果（通常称为“预言机”）。

加密经济学也被用于设计代币销售或ICO。 例如，Gnosis 使用“荷兰式拍卖”作为其代币拍卖的模型，理论上来说，这样可以带来更加公平的分配（一个结果好坏参半的实验）。我们前面提到，机制设计的实际运用领域之一是拍卖，代币销售为我们提供了一个应用这一理论的新机会。

与建立底层共识协议相比，代币销售机制是一个不同的问题，但是两者有着足够多的相似之处，都可以看作是加密经济。 建立这些应用程序需要了解激励机制是如何影响用户行为的，还需要能够可靠地产生某种结果的经济机制的设计。他们还需要了解构建应用程序的底层区块链有哪些功能和限制。

还有许多区块链应用程序并不是加密经济学的产物。例如，Status 和 MetaMask ，这些应用程序属于允许用户与以太坊区块链进行交互的钱包或平台。除了那些已经属于底层区块链的一部分加密经济之外，这些机制不涉及任何其他的加密经济机制。

例3：状态通道

加密经济学还包括在个体间设计更小的交互实践， 其中最著名的是状态通道。 状态通道不是一个应用程序，而是一个有价值的技术，大多数区块链应用程序可以使用该技术来提高效率。

区块链应用的根本局限在于区块链很贵。 发送交易需要费用，使用以太坊运行智能合约代码对于其他类型的计算来说成本相对较高。 状态通道让我们可以通过将多个进程移动到链下来提高区块链的效率，同时保持通过使用加密经济设计区块链值得信赖这一特征。

假设Alice和Bob想要进行大量但每次小额的加密货币交易，正常情况下，他们会通过将交易发送到区块链来完成交易。但这样做效率很低，需要支付交易费用，并等待新区块的确认。

想象一下，如果Alice和Bob签署本可以直接上链却没有上链的交易呢？他们可以把交易来回发送，而且想多快都行，这一步没有任何费用，因为没有交易触及到区块链。 每次交易都会“胜过”前一次，并更新双方的余额。

当Alice和Bob完成小额支付交易时，他们向区块链提交最终状态（即最近签署的交易）并“关闭”该通道，仅需支付单次交易费，他们就可以进行无限次的交易。 他们可以相信这个流程，因为双方都知道在他们之间的每次交易都可能在区块链上更新。 如果通道设计得当，没人可以作弊，比方说，尝试提交以前更新的状态，并把这种状态当做最新的状态，因为区块链一直都是可用的。

为了便于说明，你可以将其视为与我们与其他可信来源（如法律系统）进行互动的方式。 当双方签订了合同，他们在大部分情况下不需要将合同提交给法院，请法官来解释并强制执行合同。 如果合同设计得恰到好处，双方只要做他们承诺要做的事情，根本不需要劳烦法院。 由于任何一方都有可能把对方告上法庭，并请求强制执行合同，这足以使合同有效。

这种技术（状态通道）不仅对支付有用，而且对于以太坊计划状态的任何更新都是有用的，因此称其为“状态通道”要比称为狭义的“支付通道”更贴切。除了可以来回发送支付交易，用户还可以来回发送更新到智能合约上。有必要的话我们甚至可以发送整个以太坊智能合约到区块链来执行。这些程序即便不执行也有用。他们所需要的只是一个足够高的保证——如果有必要的话一定可以执行的保证。

未来，大多数区块链应用程序将以某种形式使用状态通道。较少的链上操作几乎已成为强制性的改进，如今在链上完成的许多操作以后可以移入状态通道，同时保持足够程度的安全性。

上面的描述跳过了很多不同状态通道运行的重要细节和的细微的差别。Ledger Labs 在去年夏天建立了一个模型，展示了基本的概念，在那儿你可以了解到更多的细节。

结论

用加密经济学思考区块链空间有很大的帮助。 **一旦你对加密经济学有了一定的了解，就能解开我们这个行业的许多争议和争论。**

例如，中心化管理且不使用工作量证明的“许可链”自从首次被提出就一直饱受争议， 这一领域通常被称为“分布式账本技术”，专注于金融和企业用例。不少区块链技术的支持者不喜欢这种技术，这些“许可链”从字面上来看也是区块链，但其中的某些东西总是让人觉得怪怪的。“许可链”似乎在拒绝一个所有人都认为是区块链的重点的东西：不依靠中央可信赖方或传统金融体系就能达成共识。

一个更简单的区分方法是看这个区块链是不是加密经济的产物。 只是简单的分布式账本，不依赖于加密经济学设计来达到共识或调整激励措施的区块链，对于某些应用可能有用。但它与使用密码学和经济激励来产生之前不存在的共识的区块链（比如比特币和以太坊）是完全不同的。 这是两种不同的技术，而区分它们最好的方式是看它们是否是加密经济学的产物。

其次，我们应该期待将来会有不依赖于“区块”和“链”的加密经济共识协议。 显然，这种技术与块链技术有一些共同之处，但是能把它们称为区块链是不准确的。 我想再次强调的是，我们要着眼于看这样一个协议是否是加密经济学的产物，而不是看它是否是区块链。

ICO的关注点也集中于这点区别，但很少有清楚的表述。 许多人独立地意识到代币的价值最强烈的表现之一就是它是否构成了它所连接的应用程序的必要组成部分。 更确切地说，代币是否是应用程序中必要的加密经济机制的一部分？ 因此，了解持有ICO项目的机制设计，对于确定代币效用以及价值来讲至关重要。

过去的几年里，我们从只站在一个应用（比特币）的角度来思考这个新领域领域，转变到了从底层技术（区块链）的角度来思考。我们现在需要退一步，用统一的方法来看待这类解决发难，那就是：加密经济学。

感谢eff Coleman，Ethan Wilding和Vlad Zamfir对本文初稿给出的相关建议。

原文链接: https://medium.com/l4-media/making-sense-of-cryptoeconomics-c6455776669 **作者:** Josh Stark **翻译&校对:** 娇娇 & Elisa