什么是加密经济学?

Blockgeeks 以太坊爱好者 *2017-12-14*

什么是加密经济学（cryptoeconomics）？以太坊社区开发者Vlad Zamfir解释道：

> “这是一门独立的学科，旨在研究去中心化数字经济学中的协议，这些协议被用于管理商品及服务的生产、分配和消费。它也是一门实用科学，重点研究对这些协议的设计和界定方法。”

区块链技术是运行在加密经济学理论基础之上的。

我们不妨将此概念分解一下。加密经济学（Cryptoeconomics）来源于两个词汇：密码学（Cryptography）和经济学（Economics）。人们常常会忽略其中“经济学”的成份，而恰恰正是这一成份赋予了区块链以独特性。区块链并非是首个使用“去中心化的点对点系统”的技术，洪流网站（torrent sites）在文件共享上对此技术的使用由来已久。然而，从某种意义上来说，这是一次失败的应用。

为什么点对点的文件共享是个失败的应用?

在一个洪流系统（torrent system）中，任何人都能通过一个去中心化的网络来共享文件。这个想法旨在让每个下载者在下载的同时也保持着向网络里的其他下载者提供种子（上传已下载的数据）。问题是，这一系统的运作逻辑是建立在荣誉系统制度上的。如果你下载了一个文件，系统预期你也会提供种子。但是在没有经济激励的情况下，人们认为持续上传种子是件毫无意义的事情，尤其是当这一行为还将占据电脑里更多的存储空间时。

中本聪和区块链技术

2008年10月，中本聪（一位匿名男士、女士，或组织）发布了一篇论文，此文为比特币（Bitcoin）后续的发展奠定了基础。这篇论文将会动摇网络社区的根基，因为这是我们有史以来第一次拥有了一个以加密经济学为理论依据的工作模型。与之前的点对点去中心化系统不同的是，人们现在有了经济激励去“遵守规则”。不仅如此，区块链技术的真正天才之处在于其克服了拜占庭将军问题，并创造了一个完美的共识系统（详见下文）。

比特币的加密经济学属性

那么，像比特币这样的，基于加密经济学理论的加密货币，究竟有哪些属性呢?

让我们一一阐述：

- 它是基于区块链技术而产生的货币。其中，每个区块都包含前一个区块的哈希值，从而形成一条连续链。
- 每个区块都包含多笔交易。
- 新产生的交易会使所有区块的特定状态得以更新。例如，如果A有50个比特币，且想把其中的20个比特币发送给B，那么在新的状态下就会显示：A只剩下30个比特币，而B拥有20个新的比特币。
- 区块链必须是不可变的。只可能新增区块，而不可篡改旧的区块。
- 仅允许有效交易。
- 区块链应当是可下载的，任何人在任何地点都可以轻松接入并查询某笔特定的交易。
- 如果支付了足够高的交易费用，则交易可以被快速添加至区块链上。

正如其名，加密经济学有两大支柱：

- 密码学
- 经济学

区块链技术的运行中使用了多项密码学函数。让我们看一下其中一些主要的函数：

密码学

区块链技术的运行中使用了多项密码学函数。让我们看一下其中一些主要的函数：

- 哈希算法
- 签名
- 工作量证明
- 零知识证明

哈希算法

简言之，哈希算法是将任意长度的字符串映射为较短的固定长度的字符串。比特币则是使用SHA-256摘要算法对任意长度的输入给出的是256bit的输出。那么，加密货币中哈希算法的应用有哪些？

- 加密哈希函数
- 数据结构
- 挖矿

加密哈希函数：

一个加密哈希函数有如下特性：

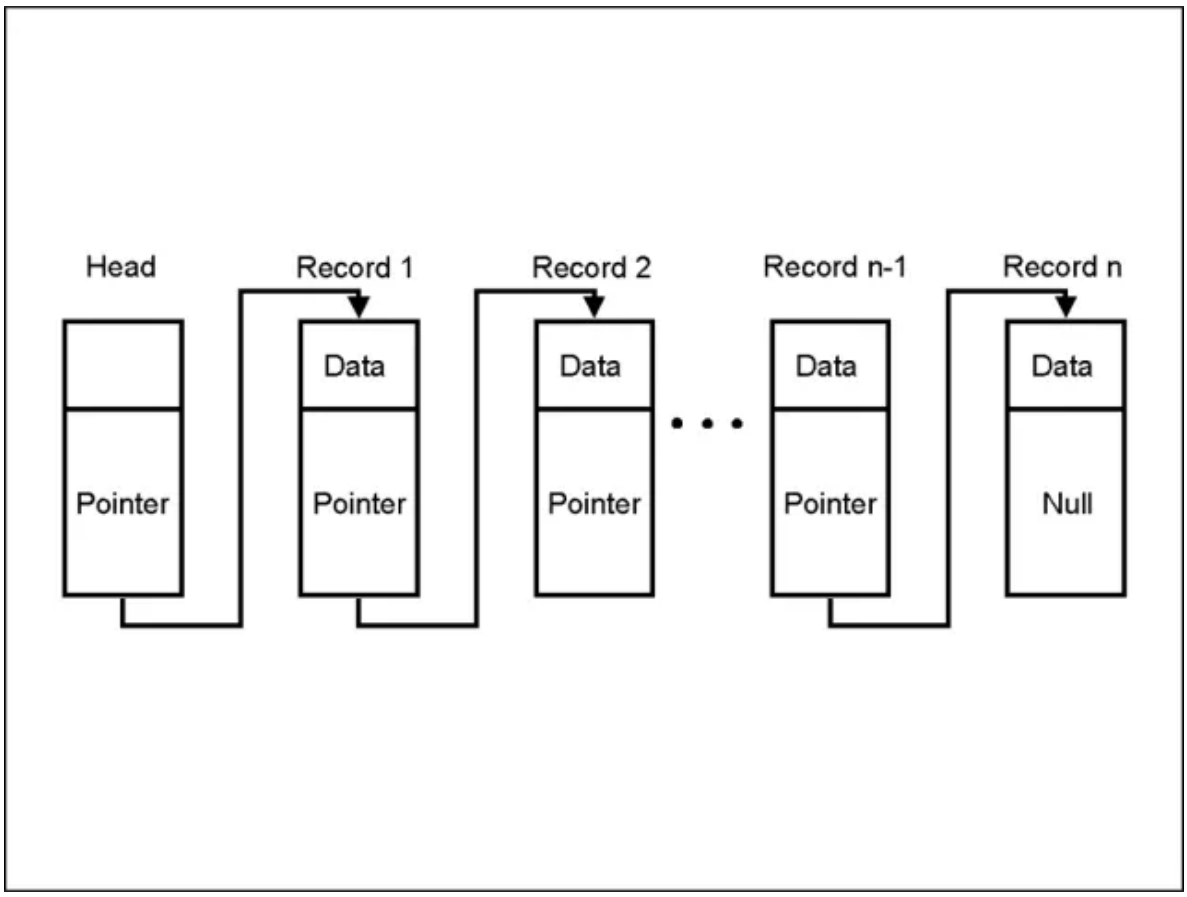
- **确定性**：无论在同一个哈希函数中解析多少次，输入同一个A总是能得到相同的输出h(A)。
- **高效运算**：计算哈希值的过程是高效的。
- **抗原像攻击（隐匿性）**：对一个给定的输出结果h(A)，想要逆推出输入A，在计算上是不可行的。
- **抗碰撞性（抗弱碰撞性）**：对任何给定的A和B，找到满足B≠A且h(A)=h(B)的B，在计算上是不可行的。
- **细微变化影响**：任何输入端的细微变化都会对哈希函数的输出结果产生剧烈影响。
- **谜题友好性**：对任意给定的Hash码Y和输入值x而言，找到一个满足h(k|x)=Y的k值在计算上是不可行的。

加密哈希函数对区块链的安全性和挖矿有巨大的帮助。

数据结构：

有两种数据结构对于理解区块链非常重要：链表和哈希指针。

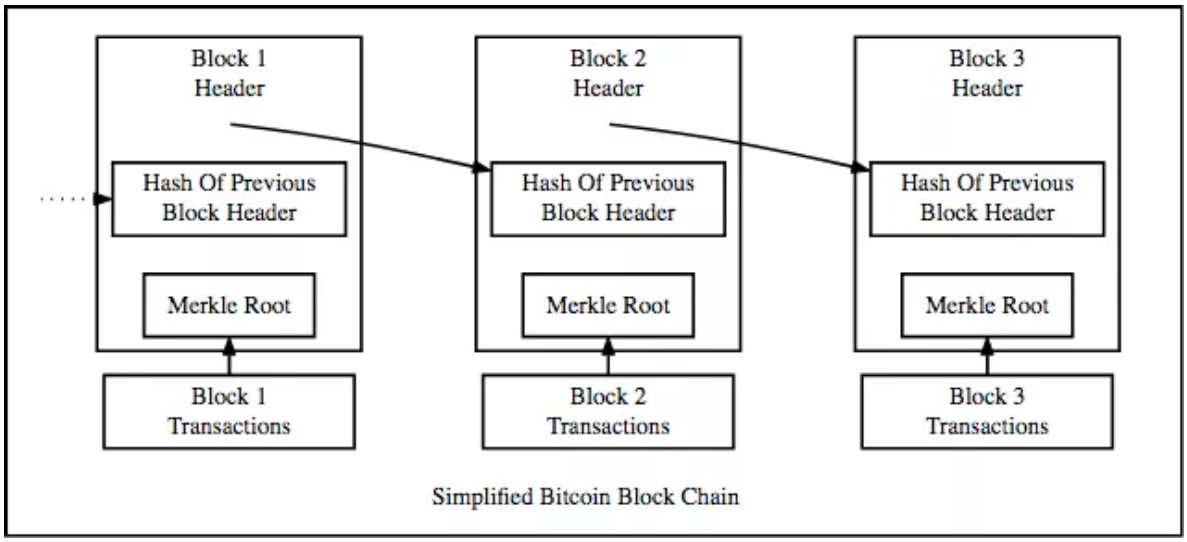
- 链表：链表是依次按顺序连接而成的数据区块，如下图所示：



在链表中的每个区块都通过一个指针指向另一个区块。

- 指针：指针是包含其他变量地址的变量。因此，正如其名，指针就是指向其他变量的变量。
- 哈希指针：哈希指针不仅有其他变量的地址，还有该变量中数据的哈希值。那么，这对区块链而言有何帮助呢?

区块链的构成如下图所示：



区块链本质上是一个链表，其中的每个新区块都包含一个哈希指针。指针指向前一区块及其含有的所有数据的哈希值。借此特性，区块链拥有了不可更改性（immutability）的伟大特质。

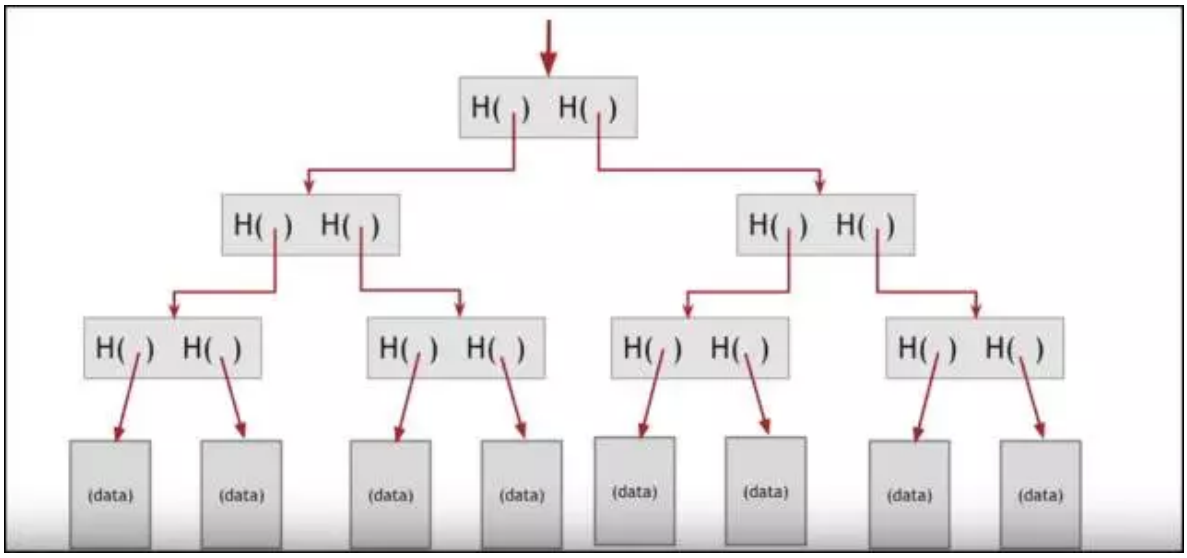
区块链如何实现其不可更改性?

假设在上面的图表中，有人尝试篡改1号区块中的数据。请记住加密哈希函数的一个重要特质是任何输入端的细微变化都会对哈希函数的输出结果产生剧烈影响。

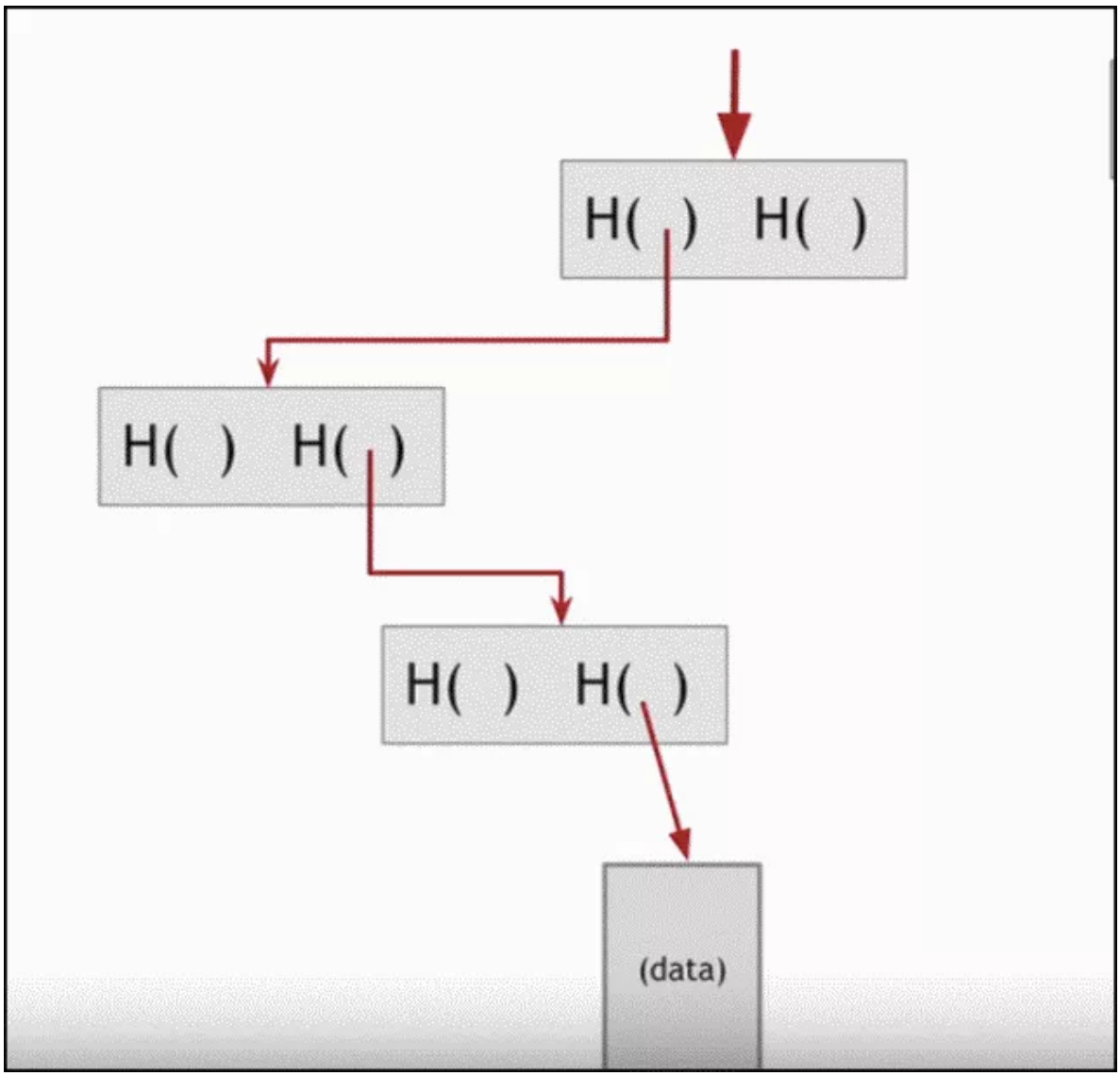
那么，即便有人尝试对1号区块里的数据进行细微的改写，也会使得存储在2号区块里的1号区块的哈希值产生巨大的变化。接下来，这将导致2号区块的哈希值发生变化，进而影响存储在3号区块的哈希值。以此类推，最终整条区块链上的数据都会发生变化。这种通过冻结整条链条来修改数据的方式几乎是不可能做到的。正因如此，区块链被认定为是不可篡改的。

每个区块都有自己的梅克尔根（Merkle Root）。现在，正如你已知道的，每个区块里都包含多笔交易。如果将这些交易按线性存储，那么在所有交易中寻找一笔特定交易的过程会变得无比冗长。

而这就是我们使用梅克尔树的原因。



在梅克尔树中，所有个体交易通过哈希算法都能向上追溯至同一个根。这就使得搜索变得非常容易。因此，如果想要在区块里获取某一特定的数据，我们可以直接通过梅克尔树里的哈希值来进行搜索，而不用进行线性访问。



挖矿

加密谜题被用来挖掘新的区块，因此哈希算法仍然至关重要。其工作原理是调整难度值的设定。随后，一个被命名为“nonce”的随机字符串被添加到新区块的哈希值上，然后被再次哈希。接着，再来检验其是否低于已设定的难度值水平。如果低于，那么产生的新区块会被添加至链上，而负责挖矿的矿工就会获得奖励。如果没有低于，则矿工继续修改随即字符串“nouce”，直至低于难度值水平的值出现。

正如你所见，哈希算法是区块链和加密经济学中一个至关重要的部分。

签名

在加密货币中，签名是其中一个最为重要的密码学工具。在现实生活中，签名的概念是什么？又有哪些特性？想象一下，你在一张纸上签名后，如何鉴定这是一个好的签名？

- 可被验证的。这个签名要可以证明确实是你在纸上签名了。
- 不可伪造的。没有其他人能够伪造及复制你的签名。
- 不可抵赖的。如果你使用自己的签名进行签署，你就无法将其收回或声称他人代替你签名。

但是，在现实生活中，无论签名有多复杂，都有被伪造的可能性。你无法通过简单的视觉辅助工具来真正地验证签名的有效性，这样做既无效率也不可靠。

密码学给了我们一种通过公钥和私钥来解决问题的方案。让我们来看看这两种秘钥的工作原理和其对加密货币系统的促进作用。假设有两个人，Alan和Tyrone。Alan想要发送一些非常重要的数据，而Tyrone想要鉴别这一数据确实来自Alan，他们可以通过使用Alan的公钥和私钥来实现这一目标。

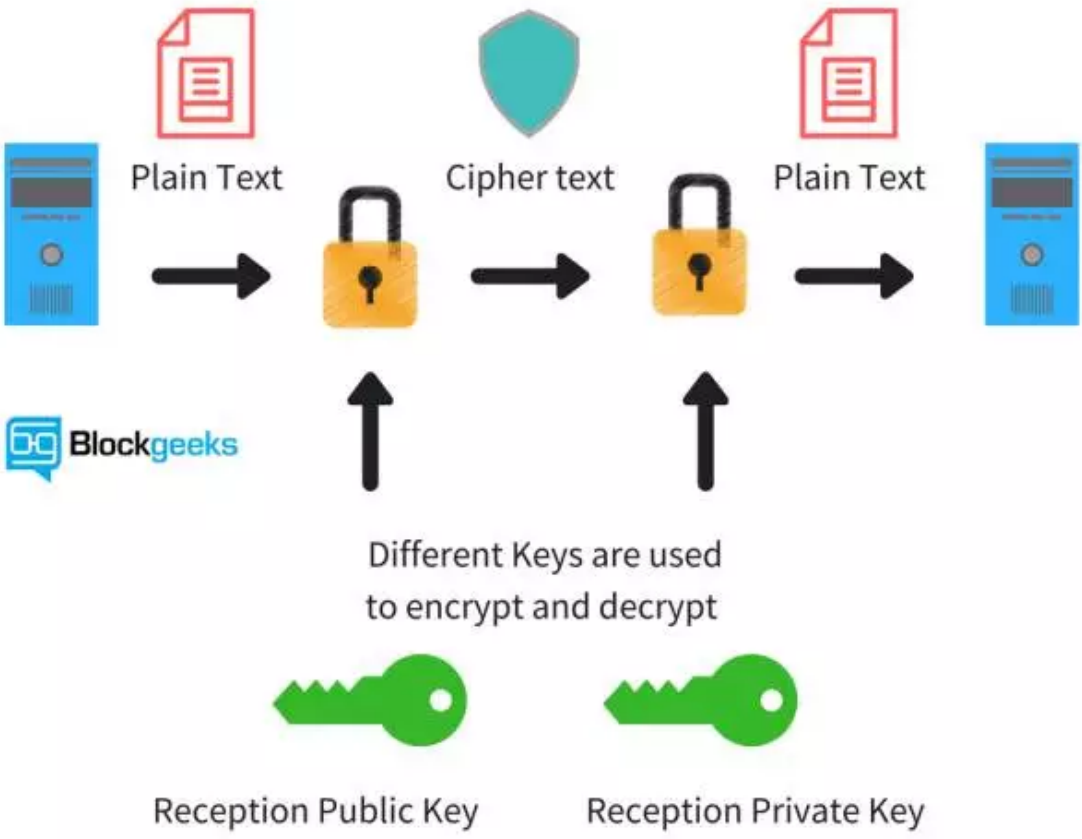
有一点必须指出，通过某人的私钥来确定其公钥是不可行的。公钥正如其名，指公开的密钥，可以被任何人获取。而私钥是仅个人拥有的密钥，你不可以将其与他人分享。 那么，让我们再回到Alan和Tyrone的话题，如果他们要使用密钥来交换信息，具体该如何操作呢？

假设Alan想把信息“m”发送出去，Alan有一把私钥Ka-和一把公钥Ka+。那么，当他把信息发送给Tyrone时，他会用私钥将该条信息加密，于是信息变成了Ka-(m)。当Tyrone收到这条信息时，他可以使用Alan的公钥来取回信息，Ka+(Ka-(m))，于是便得到了原始信息“m”。

总结一下：

- Alan有一条信息“m”，当他用私钥Ka-对其进行加密之后，得到加密信息Ka-(m)。
- Tyrone随后使用Alan的公钥Ka+来解密这条加密信息Ka+(Ka-(m))，从而得到原始信息“m”。

通过下图可以得到上述过程的直观表示：



可验证性：如果加密信息能够用Alan的公钥进行解密，那就可以100%确定是Alan发送了该条信息。

不可伪造性：如果说有其他人，例如Bob，拦截了该条信息，并用自己的私钥发送了一条自己的信息，那么Alan的公钥将无法对其解密。Alan的公钥只能用来解密Alan用自己的私钥加密过的信息。

不可抵赖性：同样的，如果Alan宣称，“我没有发送信息，是Bob发的”，但Tyrone却能够用Alan的公钥来解密信息，那就证明Alan在撒谎。如此，Alan就无法收回他之前发出的信息，并将其归咎于他人。

加密货币的应用：现在，假设Alan正在发送一笔交易“m”给Tyrone。首先，他要用哈希函数对该交易进行哈希，然后使用私钥对其加密。Tyrone知道他正在收到一笔交易“m”，因此他能用Alan的公钥对其解密，并将解密后得到的哈希结果与他已有的交易“m”的哈希结果进行比对。由于哈希函数具有确定性，并且对于同样的输入总是给出相同的输出，那Tyrone可以直接确定，Alan确实发送了同一笔交易，且其中没有任何作恶。

更简单地来说：

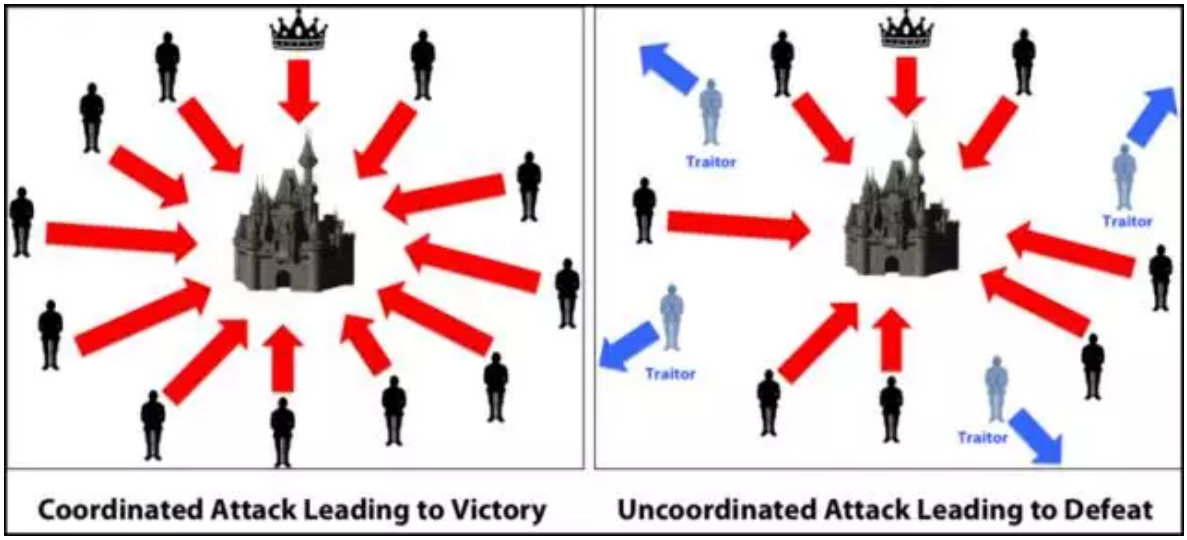
- Alan有一笔交易“m”，并且Tyrone知道他正在接收该笔交易。
- Alan对m进行哈希运算，得到h(m)。
- Alan用自己的私钥对哈希结果进行加密，得到Ka-(h(m))。

- Alan将加密数据发送给Tyrone。
- Tyrone使用Alan的公钥来解密，Ka+(Ka-(h(m)))，并得到原来的哈希结果h(m)。
- Tyrone用已知的“m”进行哈希运算，可以得到h(m)。
- 哈希函数的确定性特征决定了如果h(m)=h(m)，就意味着这笔交易是真实有效的。

工作量证明

当矿工们通过“挖矿”来产生新区块并添加至区块链上时，其中验证及添加区块涉及到的共识系统被称为“工作量证明”。矿工们使用庞大的计算机算力来解决这道密码学谜题，而难度值决定了这道题的所需要的计算量。这是区块链技术中最具开拓意义的机制之一。早期的去中心化点对点数字货币系统之所以会失败，是由于“拜占庭将军问题”导致的，而工作量证明的共识系统为该问题提供了一种解决方案。

什么是拜占庭将军问题?



好了，让我们想象一下，有一群拜占庭将军想要攻打一座城市，他们将面临两个不同的问题：

- 每个将军及其军队在地理上相距甚远，因此通过中央集权来指挥是不可行的，这使得协同作战变得异常困难。
- 被攻打的城市拥有一只庞大的军队，他们能获得胜利的唯一方式是所有人在同一时刻一同发起进攻。

为了让合作成功，位于城堡左边的军队派遣一位信使，向城堡右边的军队发送了一则内容为“周三攻击”的信息。然而，假设右边的军队没有做好攻击准备，并让信使携带一则内容为“不，周五攻击”的信息返回。而信使需要通过穿越被攻打的城市返回到左边的军队，那么，问题就来了。在这位可怜的信使身上，很多事情都有可能会发生。例如，他有可能被抓获、泄露信息、或被攻打的城市杀害后将其替换了。这将导致军队获得被篡改过的信息，从而使作战计划无法达成一致而失败。

上述例子对区块链有明显借鉴意义。区块链是一个巨型网络，你要如何信任他们呢？如果你想从钱包里发送4个以太币给某人，你如何确认网络中的某人不会篡改信息，将4个以太币改成40个？中本聪发明了工作量证明机制来绕过拜占庭将军问题。其运行原理是：假设左边的军队想要发送内容为“周一进攻”的信息给右边的军队，他们需要执行如下步骤：

- 首先，他们会给初始文本添加一个“nonce”，这个nonce可以是任何一个随机十六进制值。
- 其次，他们将添加了“nonce”的文本进行哈希，得到一个结果。假设说他们决定仅当哈希结果前5位是零的时候，才进行信息共享。
- 如果哈希结果满足条件，他们就会让信使带着有哈希结果的信息出发。否则，他们会持续随机改变nonce的值，直到得到想要的结果。这一过程不仅冗长耗时，且占用大量的算力。
- 如果敌人抓到了信使，并企图篡改信息，那么根据哈希函数的特性，哈希结果将会剧烈变化。如果城市右边的将军看到信息没有以规定数量的0作为开头，那么他们就会叫停攻击。

然而，这里有可能有个漏洞。

哈希函数并不是100%免碰撞的。那么，如果城市中的敌人拿到信息之后将之篡改，并通过不断改变nonce值，获得了以规定数量的0作为开头的结果，那该怎么办？虽然极度耗时，但是仍然可行。针对这种情况，将军们可以使用数字的力量。

假设，如果不是1个左边的将军给1个右边的将军发送信息，而是有3个左边的将军来给右边的将军们发送信息。为了实现上述目的，他们可以制作自己的信息，然后对累积的信息进行哈希。紧接着，再给哈希结果添加nonce值后，再次进行哈希。这次，他们希望产生一个以6个0开头的信息。

显而易见，这将会非常耗时。但这次，如果信使被城市抓获，那么敌人想要篡改信息，并且找到符合结果的nonce值，将会耗费无限长的时间，可能历时数年。例如，将军们派遣多个信使，那么，城市在计算到一半的过程中就可能会遭受攻击并且被摧毁。

右边的将军们要做的非常简单。他们只要将之前给他们的正确的nonce值添加在信息上，并进行哈希，然后对照其结果是否匹配即可。对一个字符串进行哈希是非常容易的。那么，从本质上来说，工作量证明的过程是：

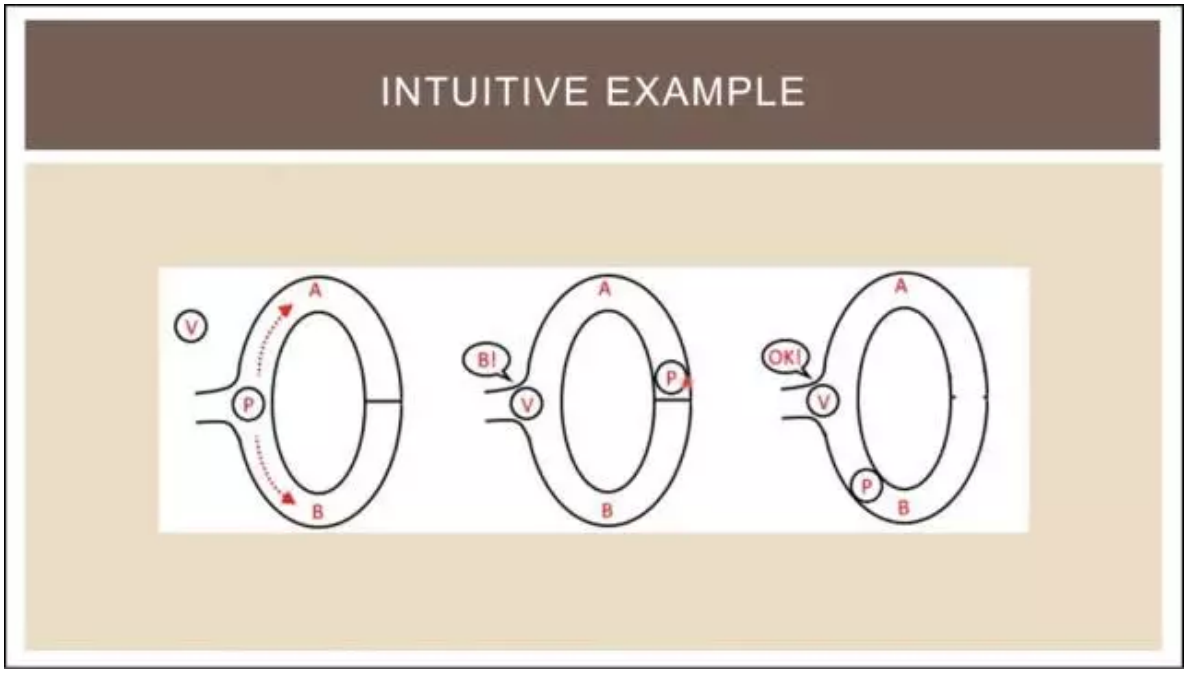
- 寻找一个符合哈希目标的nonce值，是一个非常困难且耗时的过程。
- 然而，验证结果中是否有作恶行为却是非常简单的。

零知识证明

什么是零知识证明（Zero Knowledge Proof, ZKP）？ZKP意味着A可以向B证明，他知道特定的信息，而不必告诉对方自己具体知道些什么。在这个例子中，A是证明者，B是验证者。在密码学中，这尤为有用，因为这将为证明者提供一层额外的隐私保护。 运行一个ZKP，要满足以下这些参数：

- 完整性：如果陈述属实，那么诚实的验证者能被诚实的证明者说服。
- 可靠性：如果证明者不诚实，他们无法通过说谎来说服验证者相信陈述是可靠的。
- 零知识：如果陈述属实，那么验证者无法得知陈述的内容是什么。

举一个零知识证明的例子。让我们观察一下阿里巴巴洞穴是如何运作的。在这个例子中，证明者（P）对验证者（V）说，他知道洞穴后面暗门的密码，并提出在不向验证者透露密码的情况下证明此事。那么，其验证过程如下图所示：



证明者可以走路径A或者路径B，假设他们一开始决定通过路径A到达暗门。同时，验证者V来到入口，他对证明者选择哪条路径并不知情，并宣称他们希望见到证明者在路径B出现。

如图所示，证明者确实出现在路径B上，但万一这仅是巧合呢？也有可能是证明者凭运气在出发时选择了路径B，却因不知道密码被困在了门口。

所以，我们需要通过多次试验来确定测试的有效性。如果证明者每次都能出现在正确的路径上，那么证明者的确可以在不向验证者透露密码的情况下，证明自己知道密码。

区块链中的零知识证明是如何应用的?

许多基于区块链的技术都在使用Zk-Snarks。事实上，以太坊在大都会阶段就计划引入Zk-Snarks，并且将其加入以太坊的功能库。Zk-Snarks是"零知识简洁无交互知识认证"的简称，是一种在无需泄露数据本身情况下证明某些数据运算的一种零知识证明。

以上内容可用来生成一个证明，通过对每笔交易创建一个简单的快照来验证其有效性。这足以向信息接收方证明交易的有效性，而无需泄露交易的实质内容。

这就实现了以下两种情况：

- 实现了交易的完整性和隐私性。
- 实现了系统的抽象性。由于无需展示整个交易内部的工作方式，因此系统非常易用。 因此，以上就是区块链使用的一些重要的加密函数。现在，让我们观察其第二个支柱，经济学。

经济学

正如开篇所述，区块链与其他去中心化点对点系统的区别在于，它给用户提供了金融和经济激励去完成某项工作。和其他牢固的经济系统一样，我们都需要通过激励和奖赏的方式让人们去完成工作。同样的，如果矿工行为不道德或者不尽职，那就要对矿工采取惩罚措施。接下来，让我们去观察一下区块链是如何将所有的经济学基础原理融合进来的。

必读：加密货币博弈：

https://blockgeeks.com/guides/cryptocurrency-game-theory/

区块链用到了以下两种激励组合：

第一种激励组合：

- **代币**：加密货币作为奖励分配给那些活跃度高且为区块链做出贡献的参与者。
- **特权**：参与者可以获得决策权，这将给予他们收取租金的权利。例如，挖出新区块的矿工们可以成为新区块的临时决策者，将短暂地成为新区块的独裁者，并有权决定将哪些交易添加至该区块。他们可以对收录在区块内的所有交易收取手续费。

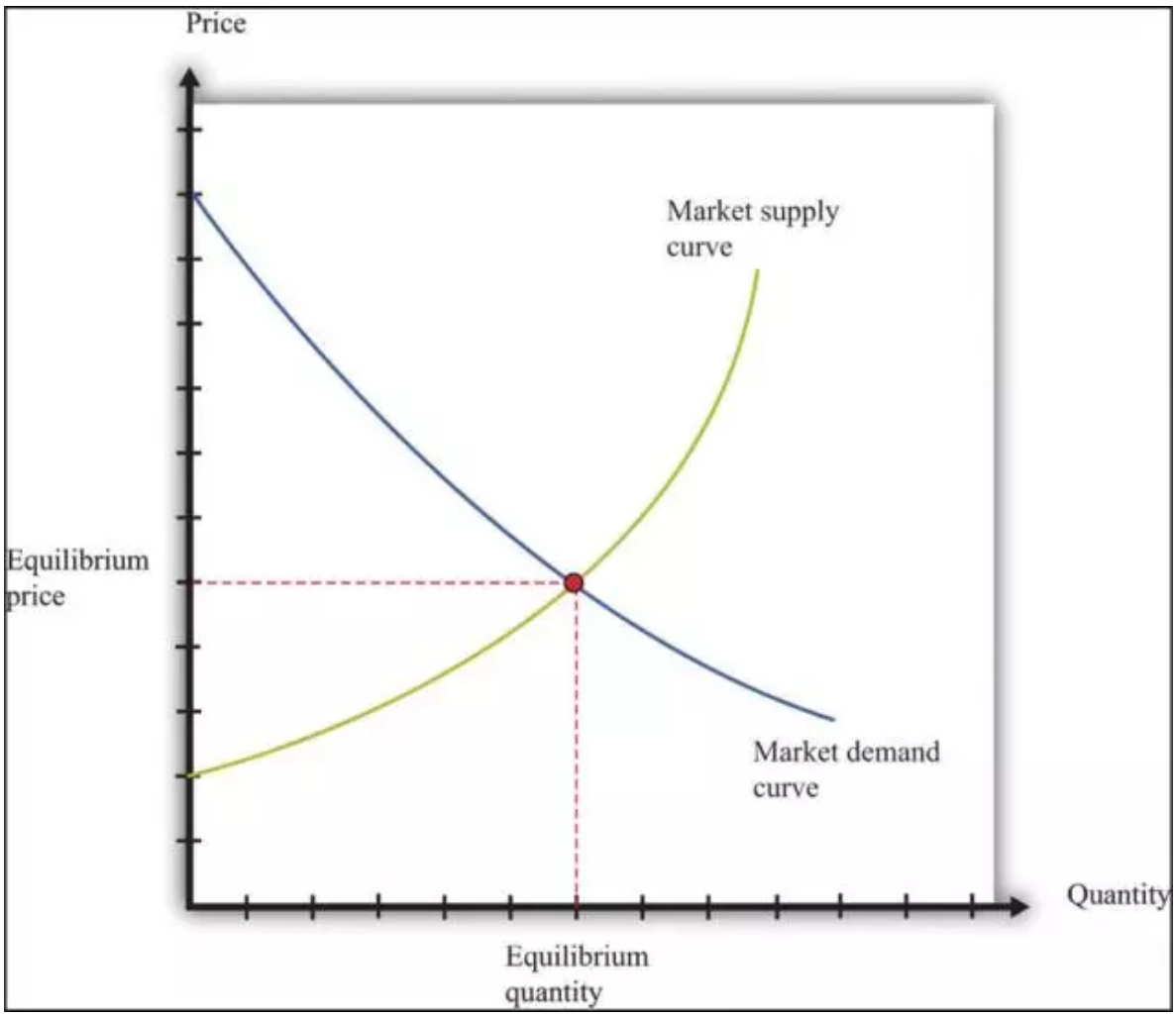
第二种激励组合：

- **奖励**：好的参与者可以获得货币奖励，或因尽职而得到决策权。
- **惩罚**：坏的参与者必须支付货币罚款，或因作恶而丧失权利。

加密货币如何实现价值?

加密货币和普通货币拥有价值的原因大体上是一样的，即基于信任。当人们信任某一种商品并赋予其价值，它就成为一种通货。这就是起初法币和黄金有价值的原因。因此，当某个给定的商品拥有一个给定的价值时，价值就会随着供求关系而发生改变。供求关系是经济学中最古老的规则。

什么是供求关系?



这是供需曲线，也是经济学中最常见的一张图表。如上图所示，商品的需求与供应呈反比关系。两条曲线的交汇处是均衡点，也是你想要达到的甜蜜点。那么，让我们用这个逻辑来观察一下加密货币，比如说比特币。

比特币的发行总量固定在2100万枚。这即是所有比特币的市值。由于总量是固定的，那么当涉及到比特币的供应时，有几件事必须要考虑清楚。首先，需要制定一些规则来使比特币的挖矿变得逐渐困难。否则，矿工们将会肆意挖矿，把剩余的比特币开采出来，并投放至市场，从而降低整体价值。

为了确保矿工们不会马上把所有剩余的比特币都开采出来， 我们需要采用如下手段：

- 首先，每隔10分钟将一个新的区块添加至链上，每添加一个区块可以获得25枚比特币作为奖励。时间间隔必须是固定的，以确保矿工们不会无规则地在链上持续添加区块。
- 其次，比特币协议要求难度值必须不断地被提高。如先前所说，在挖矿过程中，区块的哈希值及其nonce值需要低于某个特定的数值。该数值被称为“难度水平”，通常以数个0作为开头。当难度提高时，0的数量也在增加。

有了以上两种方式，挖矿过程变得十分专业，且投入巨大。整个过程确保可以核实市场上所有比特币的供应量。这也同样适用于其他基于工作量证明机制的加密货币。

加密货币的需求有很多决定因素：

- 该货币有怎样的历史？
- 最近是否被黑客攻击过？
- 是否能够持续产生结果？
- 背后的开发团队实力如何？
- 是否有变得更好的潜力？
- 宣传力度如何？

所有这些因素都决定了该货币的“热度”如何。其结果是价值围绕着需求而波动。

区块链中的博弈论

那么，一个无序的、去中心化的点对点系统是如何保持其诚信的呢？矿工权利很大，且很容易作恶并逃脱。这就是先前尝试构建去中心化系统失败的地方。毕竟，用户是人类，而人类就有作恶的倾向。因此，你如何建立一个有人类诚信的去中心化系统？答案就在一个最基本的经济学概念中：博弈论。

博弈论本质上是对战略决策的研究。其核心是做对自己最有利的决策，并记住对手的决策。博弈论中一个最基本的概念是："纳什均衡"。

纳什均衡是一种状态。在此状态下，每个参与者的策略是对其他参与者策略的最优反应。没有一个参与者可以通过独自变换策略来增加收益。让我们来观察一个纳什均衡的例子。

	B Takes Action	B Doesn't Take Action
A Takes Action	(4,4)	(4,0)
A Doesn't Take Action	(0,4)	(0,0)

如上表所示，我们将其称为"收益矩阵"。上表中的数字代表参与方采取（或不采取）行动而得到的收益数量。让我们逐一分析：

假设A采取行动： 那么如果B也采取行动，收益将是4；否则，收益是0。因此，对B来说最佳策略是采取行动。

如果A不采取行动： 那么如果B不采取行动，收益将是0；否则，收益是4。

因此，我们可以得出结论：无论A如何选择，B的最佳策略就是采取行动。现在，同样的，我们来观察下A的最佳策略是什么。

如果B采取行动*：* **如果A不采取行动，收益将是0；否则，收益是4。那么，对A来说最佳策略是采取行动。** 如果B不采取行动**： 如果A不采取行动，收益将是0；否则，收益将是4。那么，无论B如何选择，A的最佳策略就是采取行动。

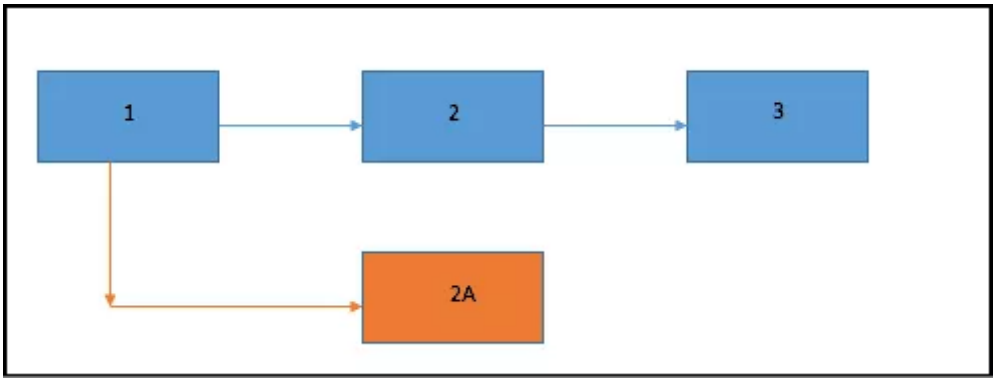
因此，我们可以得出结论，对A和B来说，最好的策略都是采取行动。

因此纳什均衡是：

	B Takes Action	B Doesn't Take Action
A Takes Action	(4,4)	(4,0)
A Doesn't Take Action	(0,4)	(0,0)

那么，区块链是如何运用纳什均衡的呢？因为链自身在一个自我强加性的纳什均衡里，所以不夸张的说，区块链是真实存在的，而矿工们也可以维持诚信。

让我们举个例子：



如上图所示，蓝色的1，2和3号区块是主链的一部分。现在，假设有个恶意的矿工挖出了一个2A区块，并企图用一次硬分叉来满足自己的财务收益。那么，用什么来阻止其他矿工加入他，并在新的区块后面挖矿？

其实，矿工们有一个非常困难但却很快的鉴定规则，那就是任意一个区块在无效区块上挖矿，即被认定为无效区块。因此，其他矿工只需忽略无效区块，并继续在老链上挖矿即可。记住，所有货币都是建立在信任和认知价值上的。因此，为什么会有人将那么多的资源浪费在一块有效性无法被确认的区块上？

现在你要思考的是：万一有许多矿工决定加入新的矿群，并在其新区块上挖矿。这个问题在于，区块链网络是一个巨大且广泛分布的网络，在里面进行交流和协作几乎是不可行的。大部分矿工只会选择能将其收益最大化的那条路径，正因如此，主链的纳什均衡也就得以实现了。

区块链中的惩罚

就像其他任何一个有效的经济系统一样，应当有正向激励和负向激励。在博弈论模型中如何实现惩罚？想象一个收益矩阵，其中参与者的收益很高，则其对社会的影响也非常高。例如：

假设有A和B两个人，他们都将要犯罪。现在，根据收益矩阵，当他们犯罪时，他们的收益都很高。因此他们的纳什均衡点是都去犯罪。虽然这在逻辑上是有意义的，但会带来非常恶劣的社会影响。人类多半是被个人贪婪所驱动的，而非利他主义。如果这是真的，那么世界将变成一个很糟糕的地方。那么，人类如何应对的？答案是引入惩罚机制。

假设我们有一个系统，每当有-0.5个因子的公共设施从公众手里被取走，就要相应的对任何犯罪的人记录-5个因子的惩罚。那么，让我们将惩罚因子加入上面的收益矩阵中，再观察下表的变化：

	B doesn't commit crime	B commits crime
A doesn't commit crime	(1,1)	(1,-1)
A commits crime	(-1,1)	(-1,-1)

如上表所示，收益发生了巨大变化。纳什均衡变成了（1,1），不犯罪是最佳策略。现在，惩罚的代价是高昂的，但是社会毕竟损失了0.5个因子的公共设施。那是什么激励着社会加入这场惩罚博弈？这个问题的答案是将惩罚作为针对每个人的强制措施，即任何一个没有参与到惩罚博弈中的人也将会被惩罚。例如说，用税收供养的警力。警察可以惩罚罪犯，但公共设施的损失会以税收的形式从公众手里取走。任何参与博弈但没有付税的人，都会被认作为是罪犯并受到惩罚。

在区块链里，任何不遵守规则并且非法开采的矿工都会受到惩罚。他们会被剥夺特权和承受被社会排斥的风险。这种惩罚会变得更加严厉，一旦权益证明被采用后（稍后详述）。通过使用简单的博弈论和惩罚系统，矿工们就能保持诚信。

矿工们更多的动机

当矿工（们）成功地挖到了一个区块，他们成为了这个区块的临时决策者。无论是选择哪笔交易放入区块中，还是提高该笔交易的速度，他们都拥有完全的管辖权。他们可以对收录的交易收取手续费。这对矿工们是一种激励，因为他们除了能够获得挖到一个新区块的奖励之外（比特币的新区块奖励是25个BTC，以太坊是5个ETH），还能得到额外的经济奖励。

为了让系统公平，同时也确保每次不是同一批矿工挖到新的区块，并获得奖励，系统会阶段性调整挖矿的难度水平。这就确保挖到新区块的矿工是完全随机的。长远来看，挖矿是一个零和博弈，换言之，矿工通过挖出新区块而得到的利润终究将根据挖矿的成本来进行调整。

P+Epsilon攻击

但是，一个工作量证明系统，容易受到一种名为"P+Epsilon攻击"的特殊类型攻击。为了理解这种攻击的原理，我们必须事先定义以下名词。

非协作选择模型：在一个非协调选择模型中，所有的参与者都没有动机与其他人进行合作。参与者可能形成群体，但在任何时候，这个群体都不会大到占据多数。

协作选择模型：在这个模型中，所有参与者都会为一个共同的激励而协作。 现在，假设区块链是一个非协调选择模型，但如果有一个动机能够让矿工们采取行动去损害区块链的完整性，那该怎么办？如果可以通过贿赂使矿工们采取某一特定行动，那该怎么办？此时就要引用贿赂攻击者模型。

现在，假设区块链是一个非协调选择模型，但如果有一个动机能够让矿工们采取行动去损害区块链的完整性，那该怎么办？如果可以通过贿赂使矿工们采取某一特定行动，那该怎么办？此时就要引用贿赂攻击者模型。

什么是贿赂攻击者模型?

象一个非协调选择模型。现在，假设有一个攻击者进入了系统，并贿赂矿工们去相互协作，那该怎么办？这个新的模型就是贿赂攻击者模型。为了成功地贿赂系统，攻击者必须拥有以下两种资源：

- **预算**：攻击者愿意支付给矿工们去执行某个特定行动的现金总额
- **成本**：最后实际支付给矿工们的金额。

然而，如果一个攻击者决定对区块链发起攻击，我们会得到一个有趣的谜题....，此时就会出现“P+Epsilon攻击”。我们可以参考下图：

Base game:

	You vote 0	You vote 1
Others vote 0	P	0
Others vote 1	0	P

想象一个简单的博弈，例如选举。如果人们投票给某个人，并和其他人一样投票给同一个人，那么就能获得收益，否则就没有收益。那么想象一下，一个贿赂者接入系统，并对某个个体制定了这个规则。如果你投票时其他人没有投，那么你会得到“P + ε”的收益。除了普通收益P之外，还有一个额外的贿赂收益 ε。

那么现在，收益矩阵如下图所示：

With bribe:

	You vote 0	You vote 1
Others vote 0	P	P + ε
Others vote 1	0	P

现在想象一下这个场景，博弈中的每个人都知道假设他们投票了，那么都有可能得到收益，但如果他们不投票，那就只有50%的概率得到收益。

你认为参与者会怎么做？当然，他们会通过投票来确保收益。这正是有趣的地方所在。正如矩阵中所示，贿赂者只需支付费用“ε”，当有人投票了，而其他人没有投票的时候。但是，在这种情况下，因为所有人都投票了，纳什均衡点转变为：

With bribe:

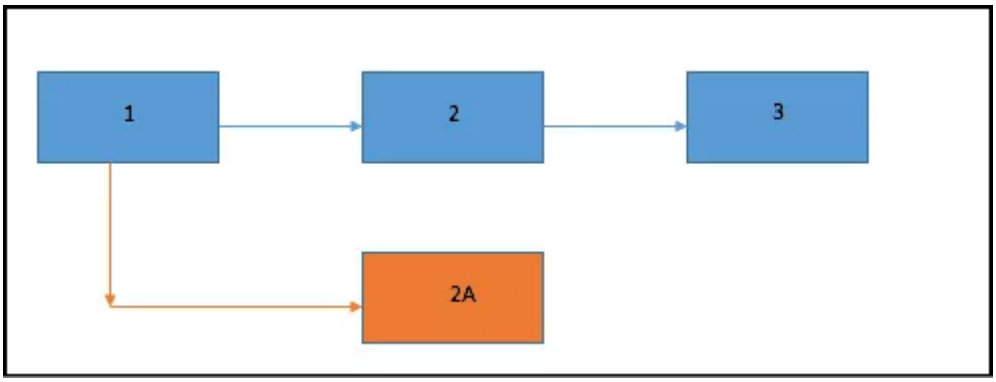
	You vote 0	You vote 1
Others vote 0	P	P + ε
Others vote 1	0	P

是的，贿赂者都不需要支付贿赂费用！

因此，让我们从贿赂者的视角来看待这个问题：

- 说服群体按照某种方式去投票。
- 无需支付贿赂费用即可实现目标。

这对贿赂者来说是一个巨大的双赢局面，同时，这对区块链影响重大，尤其是在基于工作量证明的系统中。让我们把之前的虚拟区块链再拿出来检验一下：



假设贿赂者真的想让区块链进行硬分叉，同时宣布对那些选择加入新链的矿工们给予贿赂费用 ε，这将激励整个矿工社区进行协作并加入新链。显然，这需要极高的贿赂费用来实现上述情形，但正如我们在上面的贿赂攻击模型中所看到的那样，攻击者甚至不用给出该数量的金额。根据Vitalik Buterin所说，这就是工作量证明系统最大的问题之一，即易受到“P+Epsilon攻击”。

解决方案在于权益证明

权益证明机制是针对这类以激励驱动的攻击的解决方案。在该类系统中，矿工们需要提取一定比例的私人财富，并将其投资于未来的区块中。这将是一个更好的经济系统，因为其中的惩罚更为严厉。矿工们将面临其权益和财富被剥夺的可能性。而不是像之前一样，仅仅被剥夺权利或在受到指责后逃脱。

因此，这是如何防治“P+Epsilon攻击”的？假设你是一名矿工，你有一部分的财富被投资于即将添加到主链上的一个区块中。现在，来了一个贿赂者来告诉你，你能够得到一个额外的收益，如果你将区块加入主链。但是，如果新链未被确认，那么你就有很大的风险会损失你投资在区块上的所有金钱。此外，正如“P+Epsilon攻击”所述，你不会从贿赂者那里得到额外的收益。显而易见的，对于一个矿工来说，一旦他们投资了一个权益，他们将会继续在主链上工作，而不是参与作恶。

结论

如你所见，密码学和经济学以一种非常美妙且复杂的方式结合起来创造了区块链技术。在过去几年中，它所经历的成长令人难以置信。未来，它将变得更加强大，且应用更为广泛。

原文链接: https://blockgeeks.com/guides/what-is-cryptoeconomics/ **作者:** Blockgeeks **翻译:** Nicole Yao