

共识机制

代炜琦

wqdai@hust.edu.cn

华中科技大学

Huazhong University of Science and Technology

区块链核心技术--共识

区块链的证明机制也就是其证明算法，通过某一种证明算法以证明区块的正确性和拥有权，以使各个节点达成共识。



区块链为什么需要共识

- 之前讲到比特村通过村民记账来解决信任问题，但是所有节点都参与记录数据，那么最终以谁的记录为准？
- 或者说，怎么保证所有节点最终都记录一份相同的正确数据，即达成共识？



强行达成共识

区块链为什么需要共识

在传统的中心化系统中，因为有权威的中心节点背书，因此可以以中心节点记录的数据为准，其他节点仅简单复制中心节点的数据即可，很容易达成共识。



区块链为什么需要共识

然而在区块链这样的去中心化系统中，并不存在中心权威节点，所有节点对等地参与到共识过程之中。大家都一样，我凭啥听你的？有可能谁也不服谁。



区块链为什么需要共识

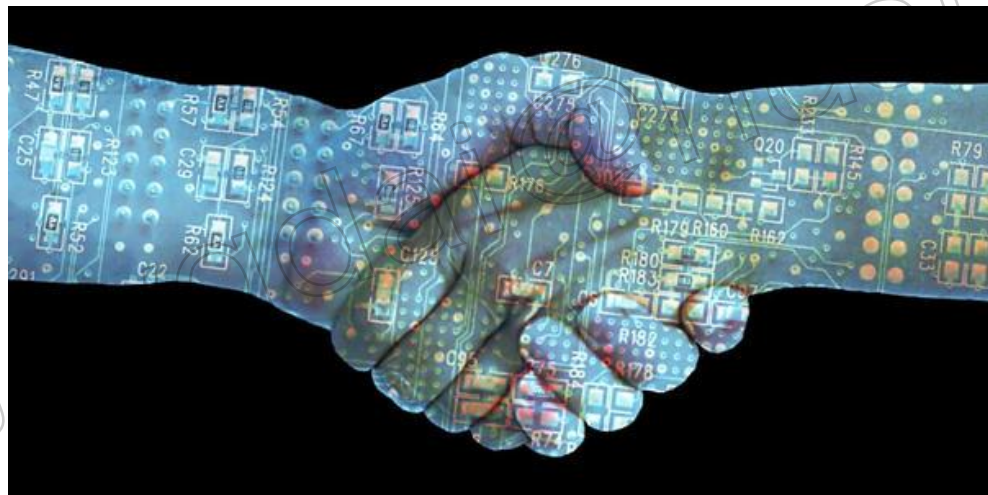
由于参与的各个节点的自身状态和所处网络环境不尽相同，而交易信息的传递又需要时间，并且消息传递本身不可靠，因此，每个节点接收到的需要记录的交易内容和顺序也难以保持一致。



就如同大家都在一个场地开会，但大家的身份、想法、使用的手机型号都不一样，全部达成统一的概率很小，但区块链每一次记账必须达成共识。

区块链为什么需要共识

因此，区块链系统的记账一致性问题，或者说共识问题，是一个十分关键的问题，它关系着整个区块链系统的正确性和安全性。



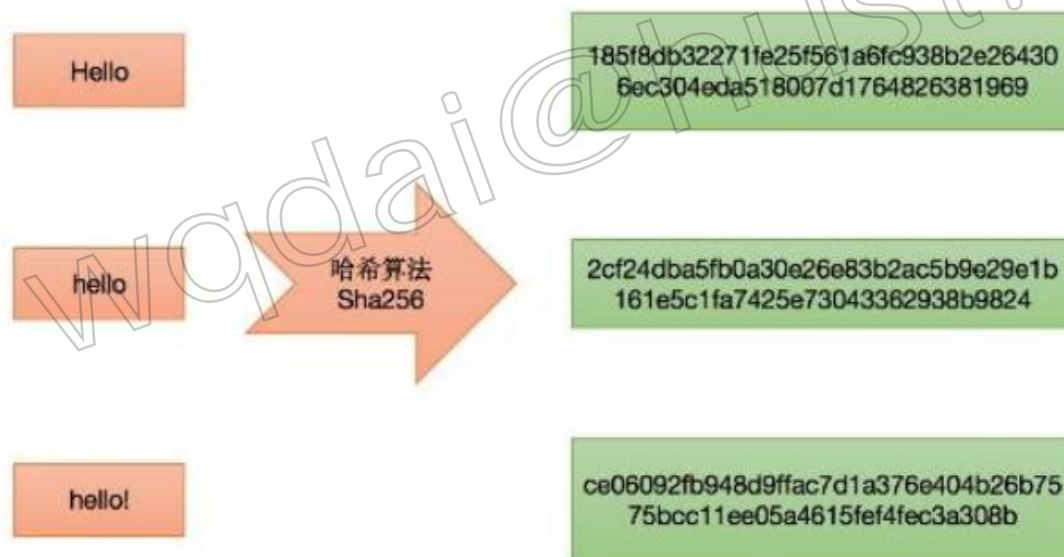
如何实现共识机制？

比特币是一个分布式系统，中本聪利用密码学只是解决了分布式共识问题，而且是零信任环境。他巧妙地利用加密哈希算法特性（SHA-256），对于给定的哈希值，没有实用的方法可以反向计算出原始输入，也就是说很难伪造，且不同的原始输入值对应的哈希值差异大，无规律可循。



如何实现共识机制？

从上图中，我们可以看到只有细微差异的三个输入值：“hello”、“Hello”、“Hello!”，其对应的哈希值天壤之别。

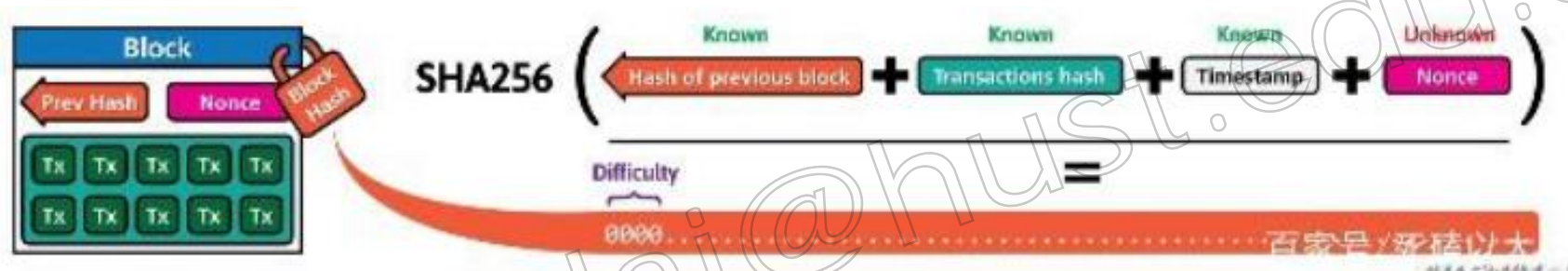


如何实现共识机制？



比特币系统中会自动使用一个系数（难度值），要求每个区块的哈希值必须符合要求系数，且每两周更新一次系数。因为哈希算法的单向性操作，无法逆向根据哈希值计算原始输入。因此为了寻找一个符合要求的哈希值，矿工就不得不在利用已知的前区块哈希、交易集哈希、时间戳再上附加一个数字，不断地更换数字，使用这个值计算出的哈希值能满足难度要求。

如何实现共识机制？



找出那个数字的耗时只取决于计算机哈希计算速度和难度系数，计算速度越快能越早找出，难度越大，查找的次数越多，时间越长。这个数字是不确定的，是1到2的256次方之间的数，称之为随机数nonce。

如何实现共识机制？

有了这个随机数，矿工立即将随机数记录到区块上并立即广播这个区块，其他节点收到这个区块后，只需要执行一次哈希运算就可以验证这个区块是否符合难度要求。

一旦符合要求，节点便放弃本地的挖矿工作，立即进入下一个区块的挖矿。如果全网51%以上的节点都接收了这个区块，全网便已达成共识。找出这个随机数的矿工，将获得奖励（比特币）



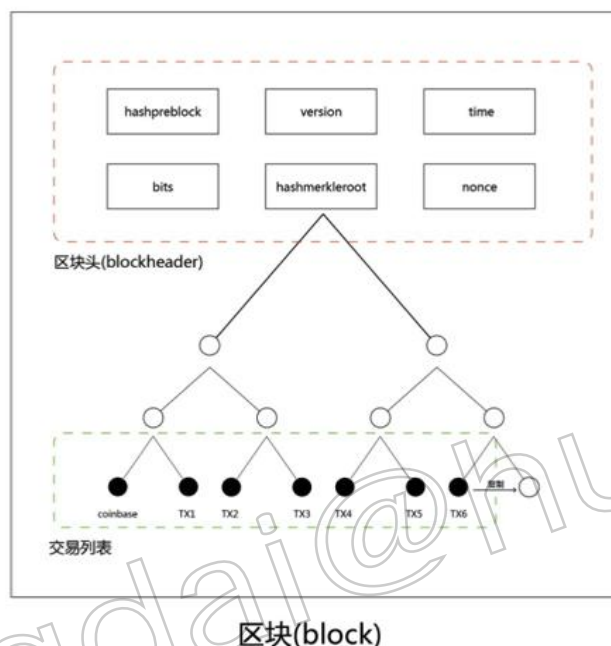
共识机制-POW共识

这就是工作证明，简称PoW（proof of work），也称为工作量证明，只有劳动才有收获，多劳多得，没有不劳而获。



POW的具体实现方式，比特币采用**哈希（Hash）算法**。逻辑上比特币是对整个区块进行哈希运算，但真正实现并非将整个区块数据作为哈希函数的参数，区块大体可分为**区块链头**和**交易列表**两部分，交易列表通过构造Merkle树最终浓缩成Merkleroot内置于区块头，区块头只有6个字段，共有80个字节，如此设计首先带来的好处是方便哈希运算，每次运算只要80字节的参数输入，而不是整个区块的数据，但交易列表的任何变化又能体现在哈希运行结果上。

共识机制-POW共识



比特币采用SHA256哈希运算，且每次都是连续进行两次SHA256运算才能作为最终结果，前一次运算的结果作为后一次运算的输入，即Double SHA256，一般简称SHA256D，扩展上面的公式，比特币合格区块判断依据如下：

$$\text{SHA256D}(\text{nVersion}, \text{hashPreBlock}, \text{hashMerkleRoot}, \text{nTimes}, \text{nBits}, \text{Nonce}) < \text{MAXTARGET} / \text{Diff}$$

其中式子左边的6个参数（区块头）在前一篇文章已经解释，MAXTARGET为最大目标值，常量；Diff代表难度，全网难度一致。MAXTARGET/Diff即通常所说的当前目标值。

共识机制-POW共识优缺点

- **优点**

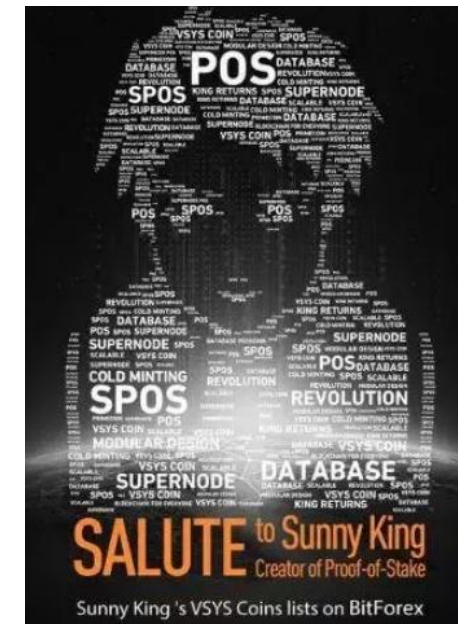
- 体现在协议的相对公平性与安全性，节点挖出新区块获得记账权及预设奖励的概率与其算力占全网总算力的百分比具有一致性；相应地，攻击者的算力需要占据全网50%以上的算力，才能同全网其他诚实节点竞争而实施攻击，工作量证明也一定程度地增加了攻击的难度。

- **缺点**

- 资源消耗巨大是POW共识机制最显著的缺点，而且由于节点还需要一定的时间付出算力资源以作为工作量证明，完成特定随机数的计算才能成功创建区块，同时需要得到其他节点的验证，降低了区块链系统的效率，无法做到交易数据的实时确认。
- POW共识算法不适合私有链和联盟链

共识机制--POS共识

- POS共识机制在2012年8月由极客SunnyKing发布的点点币中首次实现。POS共识机制是出自这个新型区块链系统中的一种特殊交易形式，称为币权交易。
- 在币权交易中，规定货币所有者可以将其持有的货币发送给自己的账户，从而消耗币龄获得铸币的权限并获取部分利息，也保证用户在创建新区块后币龄归零。
- POS共识机制实质上是要求用户证明自己拥有一定数量的数字货币的所有权，也就是“权益”。在实施权益证明机制的数字货币中，创建区块的过程由于并不需要耗费大量算力，因此一般不叫“挖矿”而成为“铸币”。
- POS共识机制中还引入了“币龄”的概念。币龄是指货币数量与货币持有时间的乘积。
- POS共识机制将主链定义为消耗币龄高的链，每个区块的交易都会将其销号的币龄提交给该区块以作为区块的积分，累计积分最高的即总消耗币龄最大的区块链。



共识机制--POS共识

POS实现原理及公式：

$$F(\text{Timestamp}) < \text{Target} * \text{Balance}$$

币龄的计算：coinage = 币的个数*币的剩余使用时间

其中，coinage表示币龄，这将意味着，币龄越大，越容易得到答案。而其中币龄的计算是通过挖矿者拥有的币乘以每个币的剩下使用时间得到，这也将意味着拥有的币越多，也越容易得到答案。这样，pos解决了pow中浪费资源的问题，同时挖矿者不可能拥有全网51%的币，所以也解决了51%攻击的问题。

共识机制--POS共识（点点币）

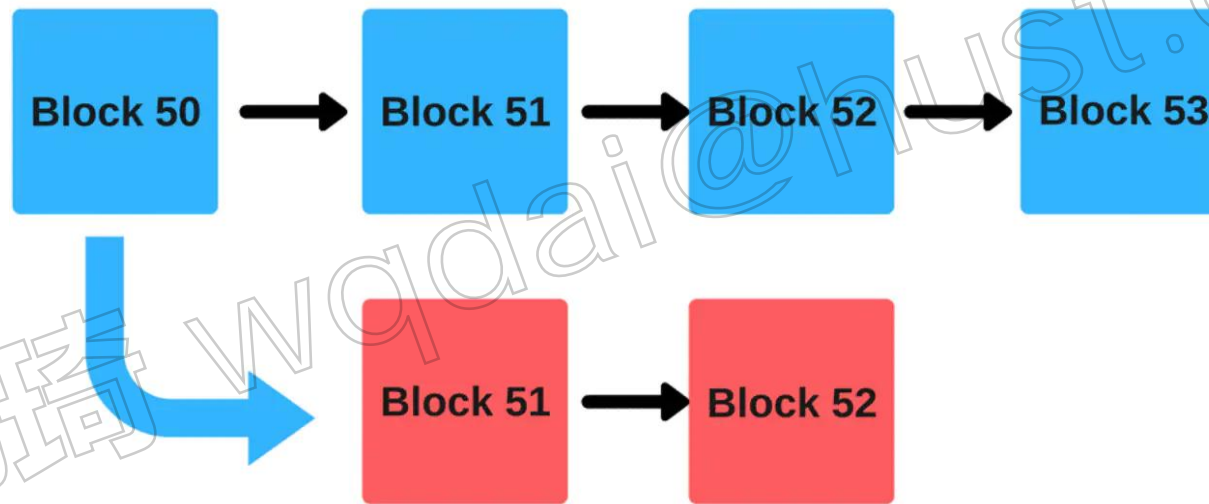
Peercoin（点点币，PPC）于2012年8月发布，最大创新是其采矿方式混合了POW工作量证明及POS权益证明方式，其中POW主要用于发行货币，未来预计随着挖矿难度上升，产量降低，系统安全主要由POS维护。目前区块链中存在两种类型的区块，POW区块和POS区块。PPC的作者为同样不愿意公开身份的密码货币极客Sunny King，同时也是Primecoin的发明者。



共识机制--POS共识（casper协议）

1. 什么是无成本利益关系问题

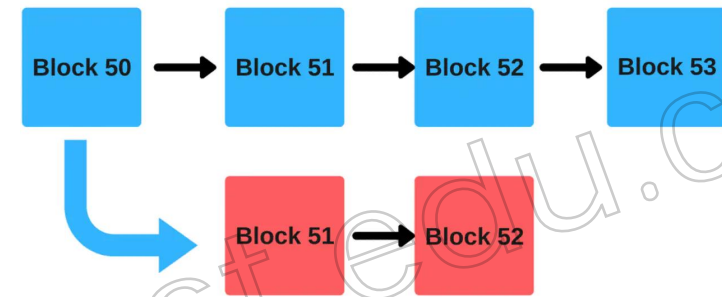
在解决无成本利益关系这个问题前，我们先来看看什么是无成本利益关系问题，因此，我们可以先模拟下这种场景，如下图所示：



假设我们处在上面的这种情况下，有一条蓝色的主链和一条红色的从主链中分出来的链条，如何禁止一个恶意的矿工在红色区块上挖矿然后推动一次硬分叉（Hard Fork）呢？

共识机制--POS共识（casper协议）

1. 什么是无成本利益关系问题



在一个工作量证明系统上，这一风险是可以被减轻的。

假设恶意矿工想在红色链上挖矿。即便她投入了她所有的哈希算力，也不会有任何矿工加入她在新链上挖矿。每个其他人都将继续在蓝色链上挖矿，因为在最长的链上挖矿收益更可观，而且没有风险。

记住，工作量证明在资源方面是非常昂贵的。对一个矿工来说，花费许多资源在一个将会被网络拒绝的区块上是没有任何意义的。因此，链分裂在一个工作量证明系统中是被避免了的，因为攻击者将不得不付出大量金钱。

但是，当你把这种情形放到权益证明下的时候，事情看起来就有些不一样了。如果你是一个验证者，你可以简单地把钱投到红蓝两条链上，完全无需担心间接的不良后果。不管发生什么事，你都总是可以赢，不会失去任何东西，不管你的行为有多恶意。

这就是所谓的“无成本利益关系（Nothing at Stake）”问题，也是以太坊必须解决的问题。他们需要一种协议，可以实行权益证明，同时减少“无成本利益关系”问题。

共识机制--POS共识（casper协议）

2.引入casper协议解决无成本利益关系问题

Casper是以太坊选择实行的PoS协议，既然有人恶意去使得我们的区块链产生分叉，那么我们想方设法去对恶意制造者加以惩罚，这样不就可以解决我们说的无成本利益关系问题了吗？

1. 验证者押下一定比例的他们拥有的以太币作为保证金。
2. 然后，他们将开始验证区块。也就是说，当他们发现一个可以他们认为可以被加到链上的区块的时候，他们将以通过押下赌注来验证它。
3. 如果该区块被加到链上，然后验证者们将得到一个跟他们的赌注成比例的奖励。
4. 但是，如果一个验证者采用一种恶意的方式行动、试图做“无利害关系”的事，他们将立即遭到惩罚，他们所有的权益都会被砍掉。

正是利用了这样的对赌协议，帮我们对恶意制造者加以了惩罚，使得我们的区块链尽量保障不会产生分叉。

共识机制--POS共识

POS共识机制与POW共识机制相比，具有以下优势：

- POS共识技术使POW共识机制算力资源浪费的问题有所缓解。在权益证明系统中，区块生成的概率和币龄成正比，因此用户不需要耗费大量的算力资源来抢夺铸币权，矿工们也不再需要消耗大量资源进行算力军备竞赛。
- 由于章我大量货币成为了攻击者实施成功攻击的必要条件，供给制对货币系统的攻击代价大大提高，攻击持续的难度也有所增加。
- 货币所有者和利益县官人一般持有大量数字货币，他们会更倾向于维护区块链数字货币系统的安全。

共识机制--POS共识

POS共识机制存在以下缺陷：

- 基于权益证明机制的加密货币一般使用以下两种方式对初始币进行分发：一种是初期借用POW机制进行挖矿；另一种是采用首次公开募股（Initial Public Offerings, IPO）的方式。但是采用IPO的方式发行货币会使货币集中在开发者和少数人手中，使得货币系统缺乏信任基础。
- 囤币行为的自发形成，导致区块链系统交易活跃性下降，同时掌握大量货币的用户可能会直接垄断记账权。

共识机制--评价标准

区块链上采用不同的共识机制，在满足一致性和有效性的同时会对系统整体性能产生不同影响。综合考虑各个共识机制的特点，从以下4个维度评价各共识机制的技术水平：

1. **安全性。**即是否可以防止二次支付、自私挖矿等攻击，是否有良好的容错能力。以金融交易为驱动的区块链系统在实现一致性的过程中，最主要的安全问题就是如何防止和检测二次支付行为。自私挖矿通过采用适当的策略发布自己产生的区块，获得更高的相对收益，是一种威胁比特币系统安全性和公平性的理论攻击方法。此外，Eclipse攻击控制目标对象的网络通信，形成网络分区，阻隔交易传播。Sybil攻击通过生产大量无意义的节点影响系统安全性。
2. **扩展性。**即是否支持网络节点扩展。扩展性是区块链设计要考虑的关键因素之一。根据对象不同，扩展性又分为系统成员数量的增加和待确认交易数量的增加两部分。扩展性主要考虑当系统成员数量、待确认交易数量增加时，随之带来的系统负载和网络通信量的变化，通常以网络吞吐量来衡量。

共识机制--评价标准

3 **性能效率**。即从交易达成共识被记录在区块链中至被最终确认的时间延迟，也可以理解为系统每秒可处理确认的交易数量。与传统第三方支持的交易平台不同，区块链技术通过共识机制达成一致，因此其性能效率问题一直是研究的关注点。比特币系统每秒最多处理7笔交易，远远无法支持现有的业务量。

4 **资源消耗**。即在达成共识的过程中，系统所要耗费的计算资源大小，包括CPU、内存等。区块链上的共识机制借助计算资源或者网络通信资源达成共识。以比特币系统为例，基于工作量证明机制的共识需要消耗大量计算资源进行挖矿提供信任证明完成共识。

囚徒困境和博弈论

代炜琦

wqdai@hust.edu.cn

华中科技大学

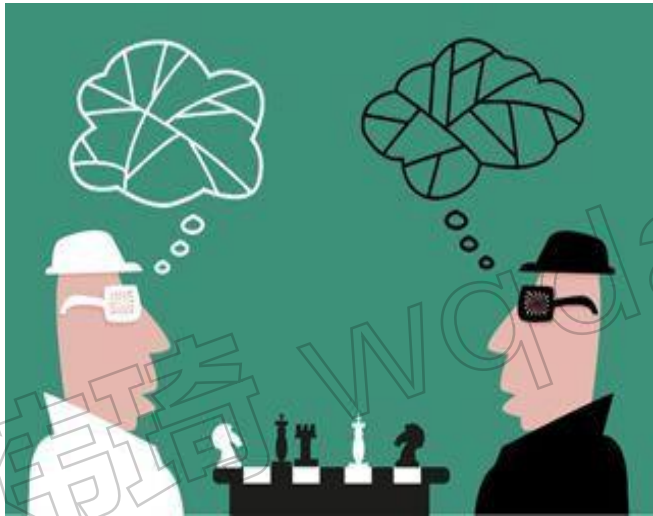
Huazhong University of Science and Technology

做个小游戏

- 每人给出一个从0到100之间的数字。把所有人的数字求算术平均值。谁选的数字最接近这个算术平均值的 $\frac{2}{3}$ ，谁就赢得整场游戏。

什么是博弈论？

博弈论是研究多个个体之间的收益与奖励，以及如何使用它们来分析一次性和持续性游戏中的激励因素。它应用到区块链的核心就是共识机制，让链上所有参与者就同一问题达成统一意见。这里涉及到最关键的两个博弈论概念是：**纳什均衡**和**谢林点**。

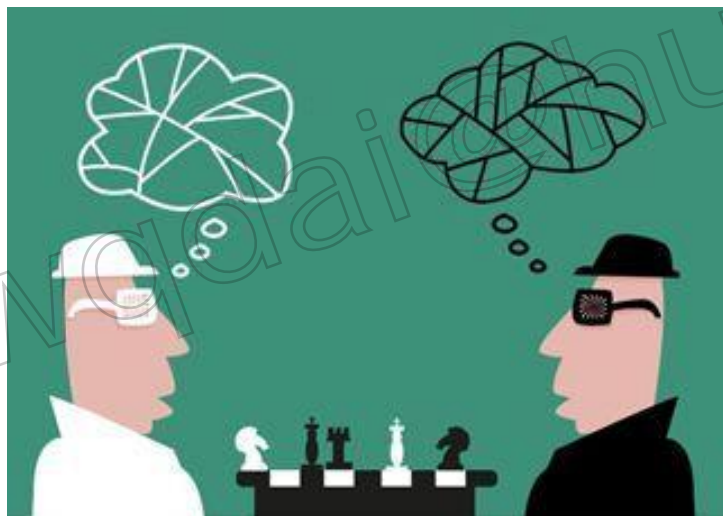


什么是博弈论？

博弈论是研究战略决策的理论。由冯·诺依曼和奥斯卡·摩根斯坦于1944年提出。从那时起，博弈论在各种领域和技术上得到了广泛的应用。

一个博弈论模型至少有三个组成部分：

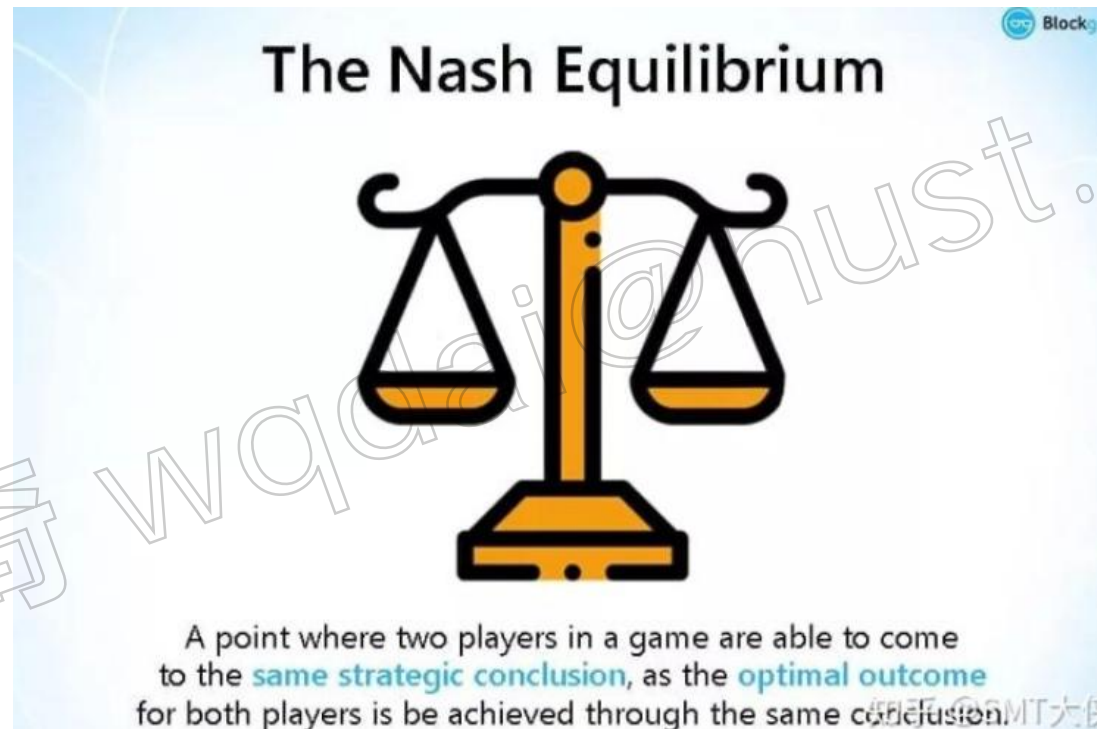
- 1、决策者，例如公司董事长；
- 2、战略，为了推动公司发展而做出的决定；
- 3、回报，策略的结果。



在博弈论中，有两种类型：1、**零和游戏**：一种以牺牲另一个玩家为代价换取一个玩家的收益的游戏；**非零和游戏**：一个玩家的收益不以另一个玩家的损失为代价的游戏。

什么是纳什均衡点？

纳什均衡是博弈论的一个解决方案。假设每个参与者都知道其他参与者的策略的情况下，没有参与者可以通过改变自身策略使自身受益时的一个概念。它是由约翰·纳什制定的，对于像区块链这样的分布式计算机系统有着巨大的影响。



事实上，区块链是“无欺骗”的，因为整个共识机制是处于一个纳什均衡点上。

区块链未被认知的潜力：从囚徒困境到合作博弈

囚徒困境



囚徒困境

假设甲和乙因为偷盗商铺被发现，在调查过程中，发现他们两人过去都犯过更严重的罪行，比如抢劫银行。警察审问了他们两个，并提出了一个建议。

提议 1、如果你们两个都不认罪，那么你们两个会被判 2 年监禁；

提议 2、如果你们中的一个出卖了另一个，那么认罪的人会被判 0 年，而另一个会被判 8 年；

提议 3、如果你们两个都认罪，那么你们两个会被判 4 年监禁。



囚徒困境

现在我们来分析一下

	乙认罪	乙不认罪
甲认罪	(4, 4)	(0, 8)
甲不认罪	(8, 0)	(2, 2)

如果他们都不认罪，那么回报矩阵表示结果是 (2, 2)，是最好的结果他们每人会被判 2 年。然而，他们知道有一个更好的提议摆在桌面上。如果他们真的出卖了对方，那么他们将有 0 年的刑期。在这种情况下，当他们两个都认罪的时候，甲和乙达到他们的最佳解决方案 (4, 4)，纳什均衡点就发生了。

囚徒困境

如果存在这样一种情景，即两个参与者的最佳解决方案对社会产生不良影响，该怎么办？想想甲和乙正在计划抢劫银行，让我们做一个矩阵的正收益表格，将得到以下情况：

	乙不抢银行	乙抢银行
甲不抢银行	(3, 3)	(0, 6)
甲抢银行	(6, 0)	(7, 7)

正如你所看到的，在这个假设的场景中，最好的策略是甲和乙都抢银行。虽然这对他们两人都有好处，但对社会来说却不是一个好的方案。这也是“惩罚”的意义所在。

什么是惩罚？

假设上面囚徒困境的例子中，我们有这样一个惩罚策略：每一个被认为对社会“不利”的行为都会得到 -7 的惩罚，而社会成本只有 0.5。社会成本的丧失可以是金钱、时间或任何东西，另一方面，犯罪的人也会受到可怕的惩罚。

我们总是把这融入到日常生活中，加上惩罚策略，减少了“坏”行为的回报，并像下面这样改变了矩阵：

	乙不抢银行	乙抢银行
甲不抢银行	(3,3)	(0,-1)
甲抢银行	(-1,0)	(0,0)

看看这个“坏”行为的回报是如何推导出来的？正如你所看到的，通过加入惩罚策略，纳什均衡点从对社会有害的东西变成了对社会有益的东西。最优策略从甲和乙一起抢劫银行变为不抢银行。

谢林点

伟大的经济学家约翰·托马斯·谢林做了一个实验，让一群学生回答一个简单的问题：“明天你要去纽约见一个陌生人，会和他约定何时何地见面呢？”他发现最常见的回答是：“中午在中央车站。”之所以会发生这种情况，是因为中央车站对于纽约人来说是一个自然的焦点，焦点也被称为“谢林点”。



“谢林点”也是博弈论的一个解决方案，是指人们在没有沟通的情况下的选择倾向，做出这一选择可能因为它看起来自然、特别、或者与选择者有关。

谢林点

假设有两个囚犯被关在两个不同的房间里，他们被给予一个随机的数字序列。然后他们被要求猜测另一个囚犯会猜测的数字，而这两个囚犯之间没有任何联系。如果他们猜错了数字，那么他们就会被杀死(只是为了增加赌注)。

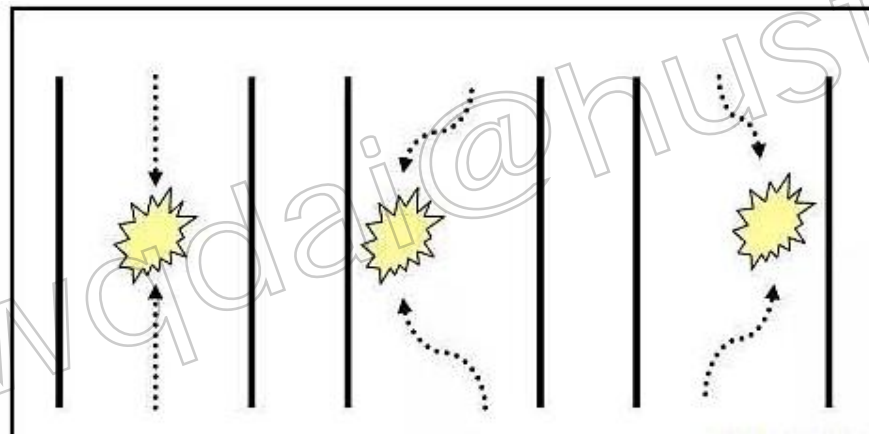
- 给出的数字是：7816239、676716313、100000000、871823719

答案是 100000000

- 为什么？因为与其他数字相比，它是不同和特殊的，它就是谢林点。

谢林点

一个非常著名的谢林点游戏，称为“胆小鬼博弈”。游戏中两个人相对驱车而行。如果都拒绝转弯，任由两车相撞，最终两人都会死于车祸；但如果有一方转弯，而另一方没有，那么转弯的一方会被耻笑为“胆小鬼”，另一方则胜出。如何解决这个难题呢？



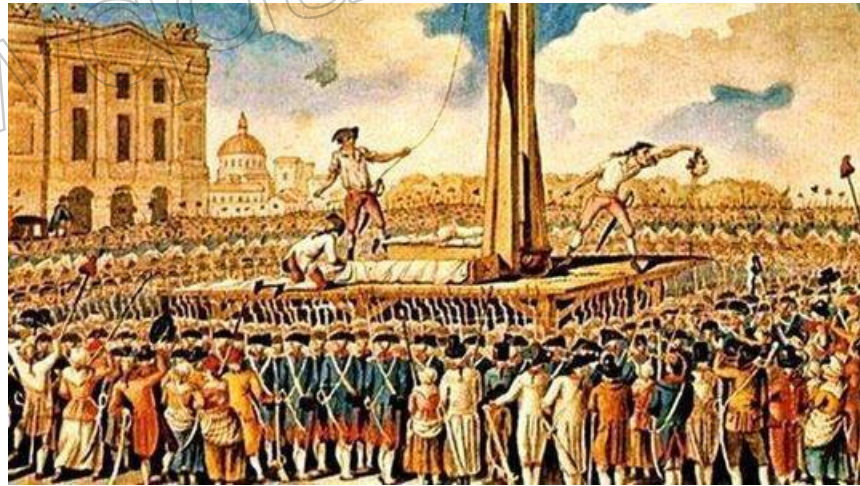
谢林使用焦点的概念来解决问题。这个游戏的最佳解决方案是不要直视对方的眼睛，即切断与对方的沟通，专注于自己的本能。因为在美国，人们习惯靠右行驶，如果我们让直觉控制自己的行为，就会自动驱车驶向右边，这就是谢林的观点所在。

冷酷触发策略

为了理解冷酷触发策略是如何起作用的？

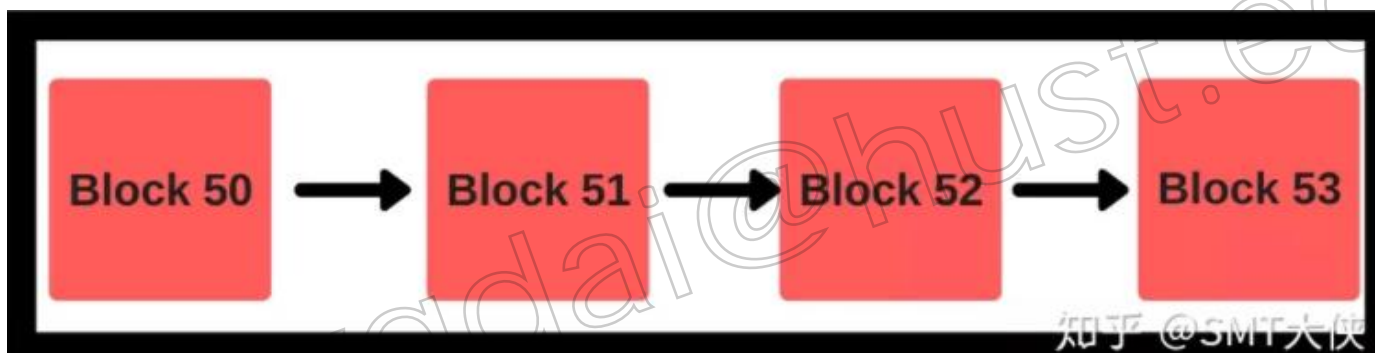
我们需要考虑一个场景，想象一个君主制的社会，人们相信国王的统治是因为上帝赋予他们的神圣权利。然而，如果国王被杀，那么神权法则就会自动消失，因为每个人都会明白，国王不是神，可以被杀死。

现在每个人都清楚国王是可以被杀的，这将开始一个无休止的血腥循环，没有什么可以阻止后来的国王被谋杀。停止这种恶性循环的唯一办法是首先不杀死国王，并保持“神权”的概念。这就是所谓的冷酷触发策略。把它想象成一种状态，在这种状态中，如果你偏离了哪怕一点点，你就会导致一个无休止的恶性循环。



区块链与加密货币的博弈理论

区块链是由一个个区块以链条（有序列表）的形式构成。其中每一个区块是由区块头（head）和区块体（body）两部分组成的数据结构容器。



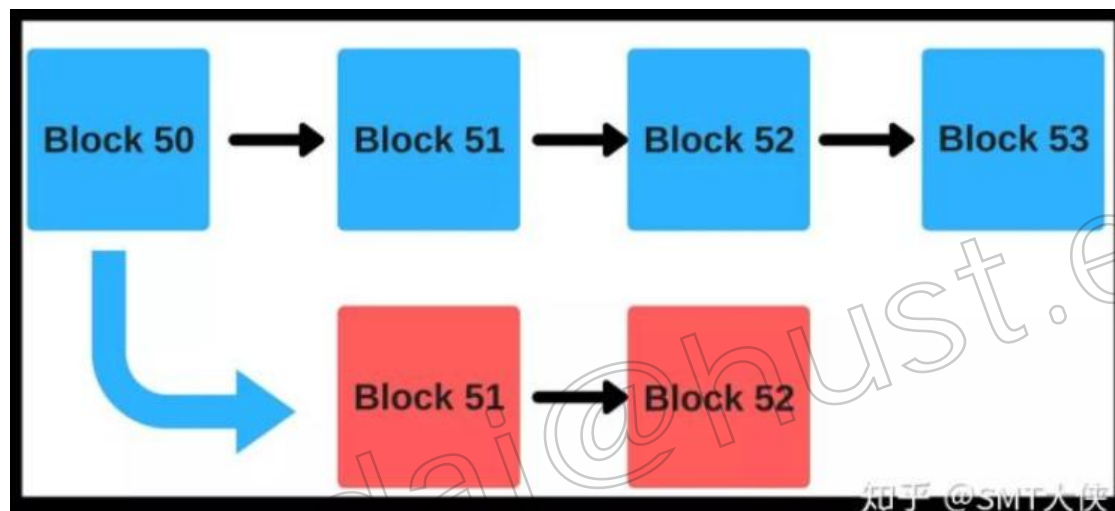
基于区块链的比特币系统中，一般有两个参与者：用户和矿工。比特币的用户使用两种功能：接受或发送比特币。为了做到这一点，用户需要两个密钥：公钥和私钥。矿工所做的是通过挖矿来验证交易，挖矿是指如何发现新的区块并添加到区块链上。

区块开采

通过一系列的哈希计算，矿工找到一个新块，并将其添加到链上。目前在比特币中，挖矿奖励是 25 比特币。如果矿工为了个人利益选择“欺骗”网络，会破坏区块链的系统。为了让矿工诚实，区块链使用了博弈论来保护系统。

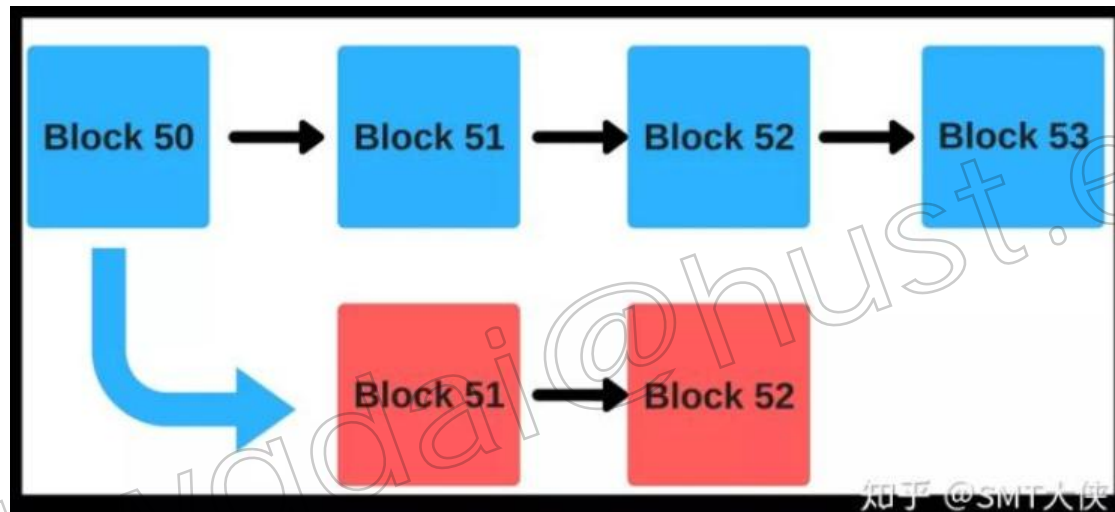


矿工如何作弊？



如图所示，蓝色的区块是主链。假设有一个矿工，在蓝色区块 51 时用 10 BTC 交换得到 500 Litecoin（假设）。现在又创建一个带有新块 51 (红色)的并行链，但不执行之前的交易，将新的并行链作为主链继续挖矿，他就同时获得了 10BTC 和 500Litecoin。这被称为“双重支付”。

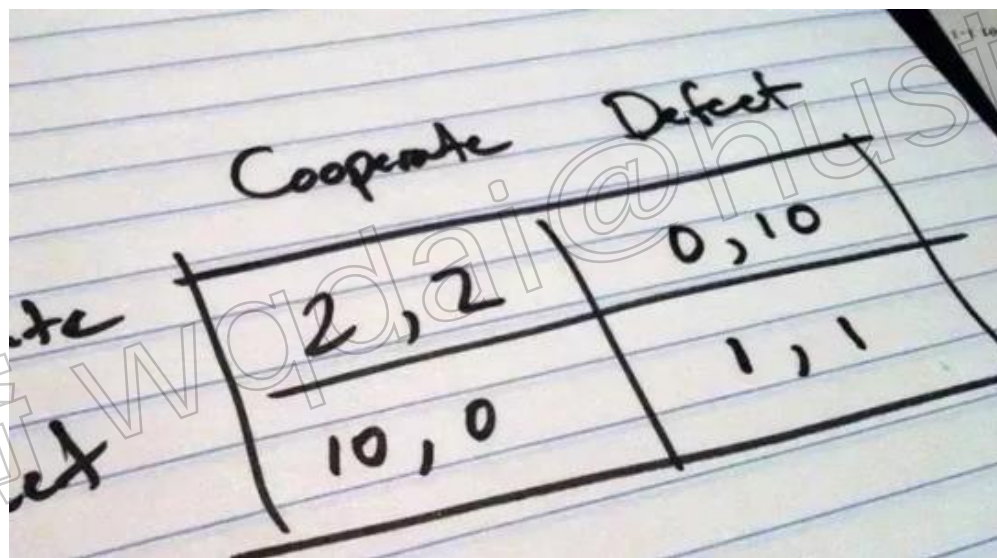
挖矿的纳什均衡点



如果一个矿工创建了一个无效的块，那么其他人就不会在它上面挖矿，因为一个规则已经被定义在惩罚策略上。任何在无效块顶部挖掘的块都会变成无效块。因此，矿工将直接忽略无效块，并继续在主链(即图中的蓝色链)的顶部进行挖掘。

博弈论和以太坊

最大的智能合约平台——以太坊就是一个不会被收买、无处不在的外部监督者。用于执行和监督利益相关者之间的协议。这意味着在理论上，以太坊可以将任何非合作博弈变成合作博弈。在智能合约机制的引入下，此前的利益格局会被打破。



A handwritten payoff matrix for a Prisoner's Dilemma game is shown on lined paper. The columns are labeled 'Cooperate' and 'Defect'. The rows are labeled 'Cooperate' and 'Defect'. The payoffs are as follows:

	Cooperate	Defect
Cooperate	2, 2	0, 10
Defect	10, 0	1, 1

以太坊和智能合约并非改变博弈的必要条件。但在此之前，我们很难找到普适、可信的第三方工具。当然要智能合约与现实博弈相结合，我们必须找到合适的机制让博弈的关键操作与链上合约绑定。