区块链技术与应用

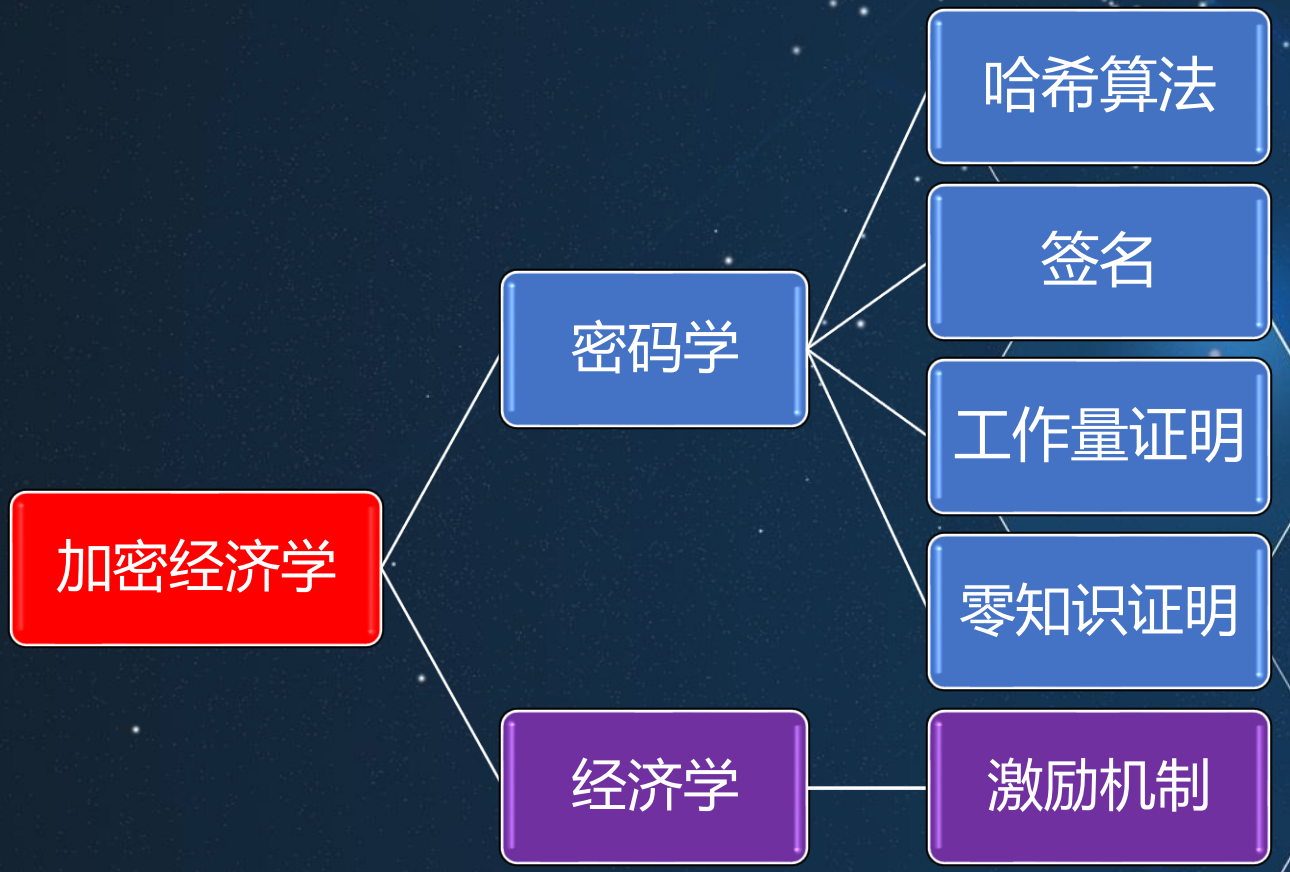
（2022年春季）

计算机科学与技术学院　李京

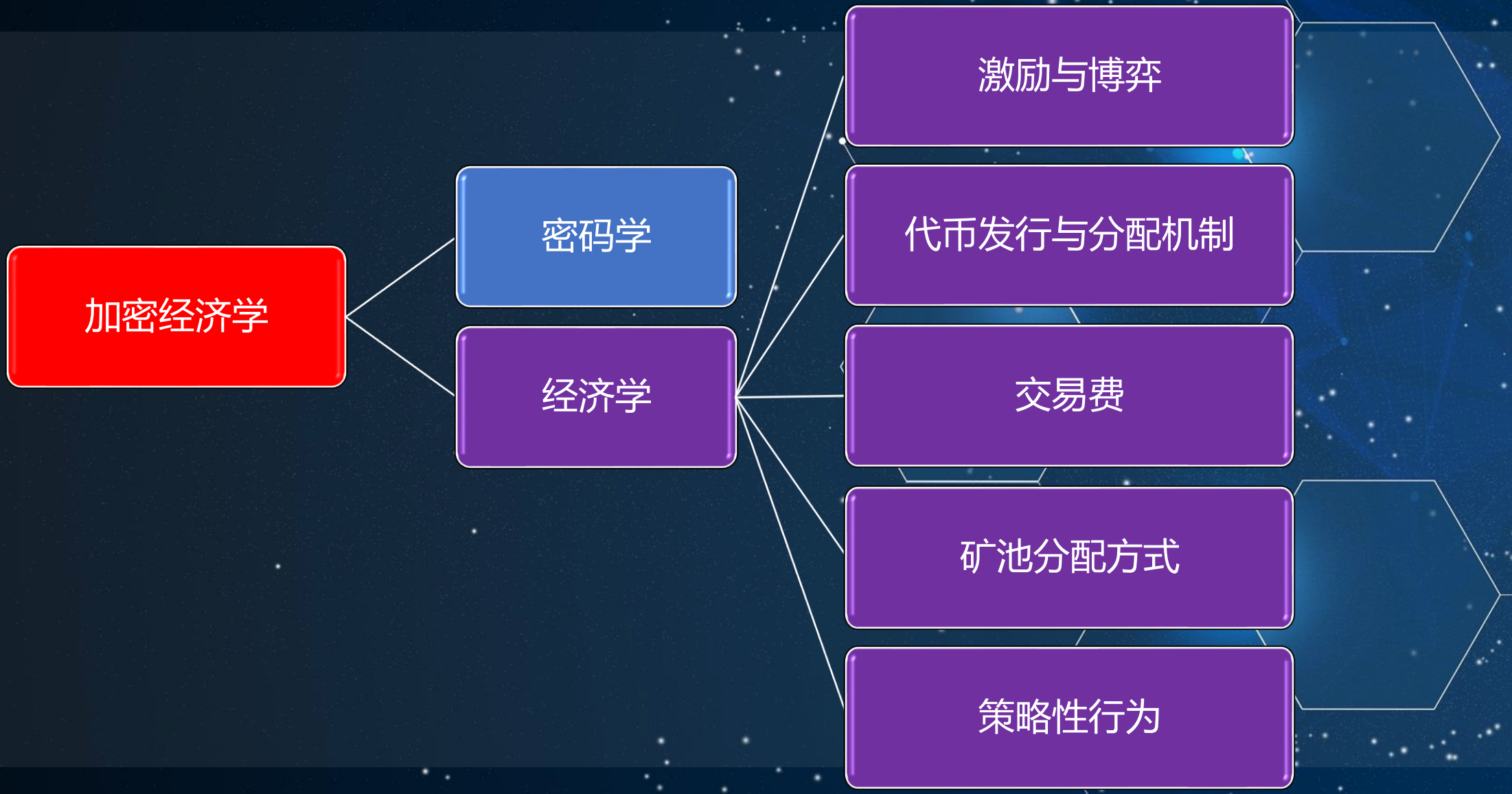
05章 区块链激励机制

- 区块链不仅是一种全新的分布式计算技术，同时也是一类新兴的交易模式和成功的商业逻辑。区块链系统的核心驱动力之一是经济激励。本节课简要探讨区块链技术所面临的各类行为与激励相关问题，重点介绍区块链生态系统的激励机制以及参与者的各类策略性行为。
- 区块链经济学亦称加密经济学(Crypto-economics)：是利用激励和密码学来设计的新型的系统、应用程序和网络。

加密经济学



加密经济学

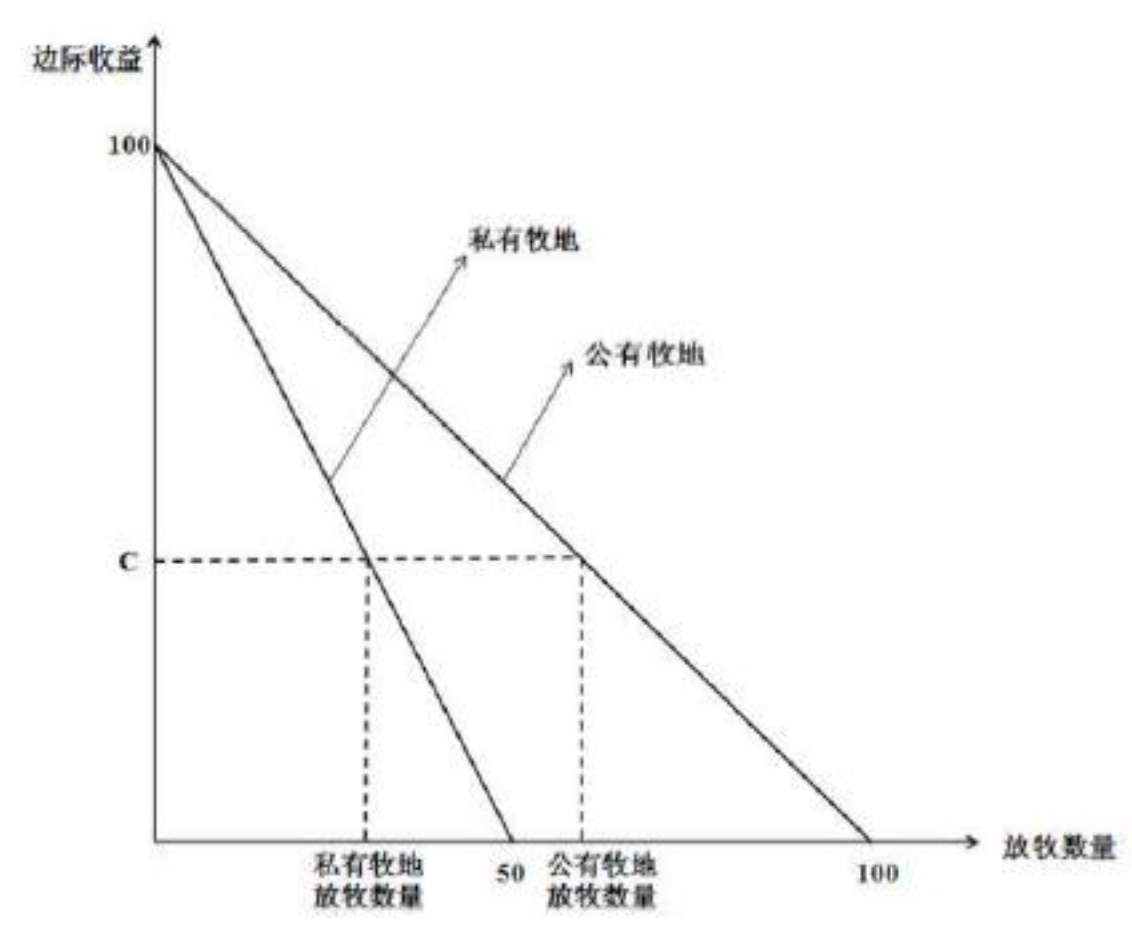


目 录

5.1激励与博弈-区块链中的博弈论

- 区块链系统的参与者众多，每个矿工都是一个节点，他们通过贡献自己的算力进行竞争性挖矿，即通过不断地进行哈希运算来求解密码学难题。当找到一个完整的解随机数（称为全解）时，挖矿成功，矿工可以获得打包交易的记账权，并可以获得区块奖励和该区块内部交易附带的所有交易费。
- 区块链挖矿的过程是一个完全竞争博弈的过程。在这个过程中，海量分散、无组织的节点之间进行不断的竞争，由于挖矿过程中需要消耗大量电力资源，经济激励是保证他们持续贡献算力来挖矿的根本动力。
- 在区块链经济中，每个节点都是经济理性人，他们都会有自利性，总是试图通过采用一些策略性挖矿行为来提高自身的挖矿奖励。由于个体节点只考虑自身的收益最大化，而忽略整个区块链系统的效益最大化，当个体节点的微观目标与整个系统的宏观目标不一致时，个体节点收益的最大化必然会损害其他节点乃至整个系统的利益，从而形成区块链生态系统的“公共地悲剧”。

公共地悲剧



- “公共地悲剧”是1968 年由英国经济学家盖瑞特·哈丁（Garrit Hadin）提出的，是指当任何人都有权使用有限的公共资源，并且使用时不受任何限制时，必然会由于人的自利性而导致公共资源的过度使用，最终使每个人的利益受损。
- 例如，由于公有牧地对所有牧民都是开放的，每个牧民都想通过增加放牧数量来提高收益，当公有牧场都达到饱和时，再增加放牧数量就会导致边际收益降低。随着放牧数量的不断增加，公有牧场会因被过度利用而退化，从而使每个牧民的收益受损，这就是“公共地悲剧”。
- 实际上，与私有牧场相比，在公有牧场上更容易出现过度放牧的现象。因此，当牧民在公有牧场上放牧时，为了获得与在私有牧场上放牧相同的收益，往往需要更多的放牧数量。

5.2 代币发行机制

- 代币（Token）是区块链经济激励的典型载体和表现形式，也有学者译为通证。区块链系统内生代币的发行机制决定了区块链资产的分配机制，对区块链项目未来走向和发展前景具有举足轻重的意义。
- 发行代币的区块链项目一般可以分为公链和去中心化应用（DApp）两类，公链中往往包含多种属性的Token，如股份、货币或商品等；应用型Token的设计通常采用积分+股份相结合的方式，这类Token往往代表了项目的所有权。
- 代币发行将公司发行股份和中央银行发行货币相结合，形成了区块链项目中单Token 和双Token 两种代币发行机制。

单Token 发行机制

- 单Token 发行机制就是区块链项目在发行过程中只发行一种Token。
  - 总量有上限
  - 总量无上限
  - 总量有上限与总量无上限相结合

单Token 发行机制：总量有上限

- 在总量有上限的Token 发行机制中，必须首先设定一个Token 发行总量的上限。
- 这些Token 中分成三部分，一部分留给项目团队，一部分用于ICO 或私募，剩下的一部分奖励给矿工。
- 在总量有上限的应用型Token 中，一方面，Token 具有积分的特性，可以换取某种服务或抵扣某种费用如交易手续费等，还可以通过某种活动的方式来免费发放，从而提升社区活跃度。另一方面，Token 具有股份的特性，Token 持有者可以通过Token 分红、Token 回购销毁等方式来获得项目发展的红利。
- Token 总量有上限的区块链项目也具有一定的风险。由于此类项目早期具有较高的奖励，可以快速吸引大量矿工的参与，而后期随着奖励的逐渐减少，则可能无法继续吸引矿工，使得矿工大量离开，从而使项目消亡。此外，当区块奖励耗尽时，矿工主要靠交易费获利，如果无法激励用户付较高的交易费，则可能导致挖矿的“公地悲剧”。

单Token 发行机制：总量无上限

- 在总量无上限的Token 发行机制中，每个区块的奖励会设置一定的通胀率，因此，Token数并不是固定的，随着区块的不断挖出而逐渐增加。目前主流的公链体系，如ETH 和EOS等，都采用该发行机制。
- 在PoW 共识机制下，矿工通过挖矿的区块奖励不断获得新发行的Token，而普通持币人由于不参与挖矿无法获得新发行的Token。因此，随着挖矿的持续进行，Token 数量越来越多，普通持币人所持有的Token 数量占比逐渐减少，使得他们的权利逐渐弱化。
- 在PoS 或DPoS 共识机制下，每个持币人都能不断获得新发行的Token，从而保证持币人Token 数量占比的稳定性。
- 在PoW 和PoS 共识机制下，新发行的Token 完全基于代码进行分发，是客观的，而在DpoS 共识机制下，被普通持币人授权的矿工 / 代表人拥有分配新发行Token 的权利，具有一定的主观性。
- 应用型总量无上限的Token 的提出主要是为了解决区块链项目可能会面临的配股、增发或发行可转债等需求，应用型Token 往往基于公链创建，而由于公链的功能有限，因此这类Token 的特性也会受到一定的限制。

单Token 发行机制：总量有上限与总量无上限相结合

- 在总量有上限+总量无上限相结合的Token发行机制中，主要采用混合挖矿方式来发行新Token，并奖励给矿工或Token持有人。例如，点点币（Peercoin）采用PoW+PoS共识机制，是最为典型的混合挖矿方式发行的Token。
- 在混合挖矿体系下，新发行Token来自两部分，一部分是总量有上限的Token，这部分由于Token总量有限，因此随着区块高度的逐渐增加，新发行的Token数不断减少，直至到达上限。另一部分是总量无上限的Token，这部分Token 随着区块的不断挖出逐渐增加，即具有一定的通胀率。例如，点点币根据用户的持币量和币龄将挖矿奖励设置为1%，即在PoS 机制下的这部分Token每年有1%的通胀率。

双Token 发行机制

- 部分公链项目发行了两类Token
  - 一类代表区块链系统所有权并且具备激励特性
  - 一类是价格稳定的Token 作为生态内的“货币”来使用
- 为了实现Token的稳定性，可以采用发行借据锚定美元等稳定资产、以其它Token作为基础资产抵押和算法央行这三种方式来发行Token。
  - Tether
  - SteemDollars（SBD）
- 由于Token+稳定币的双Token发行方式发行的Token类似于“股份+货币”，因此比单纯采用总量有上限的单币发行方式更具优势，有利于生态体系的建立。Token 的分配机制需要权衡各方利益，从而激励各利益群体参与项目的积极性。

代币分配机制

- 新发行Token 的分配方式取决于其所在链上的共识算法：
  - 采用PoW 共识算法的区块链项目，往往会把新产生的Token全部分配给矿工。
  - 采用工作量证明+服务量证明混合模式的项目DASH 区块链，把区块奖励在矿工、主节点和基金会这三者之间进行分配，其比例分别为45%、45%和10%
  - 采用DPoS 共识机制的项目Steem 区块链，将新发行的Token 分配给潜在消费者（即代币持有者）和矿工，其比例分别为90%和10%

EOS 代币分配机制

- EOS 代币分配是运行在以太坊区块链上，总共耗时341 天。在此期间，EOS 总共分配10亿个ERC-20 兼容代币，这10 亿EOS 代币分为三部分：
  - 第一部分为总量的20%即2亿个EOS 代币，在前五天内分配
  - 第二部分为总量的70%即7 亿个EOS 代币，从第六天开始，以每23 小时200 万增量的形式分配。
  - 第三部分为总量的10%即1 亿个EOS 代币，这部分会留给项目开发者，并且在整个分配期间都不能在以太坊网络上进行交易或转移。
- EOS 代币分配类似拍卖，每个人的价格都相同，该价格等于所有人愿意并能够在特定时间段内支付的最高价格。在前两部分的分配期结束时，一定数量的EOS 代币将根据每个时期筹集的以太币（“ETH”）总量按照比例分配给所有授权购买者。
- EOS 代币分配按照逻辑一致性原则，即没有人可以不劳而获、每个人都应该获得市场决定的价格、每个人都应该享有平等的参与机会、开发人员奖励应该一致、不能购买超过50%的分配量、最小化交易成本（采矿、手续费等）。EOS 代币分配机制可以保证广泛接受性、逻辑一致性和公平性。

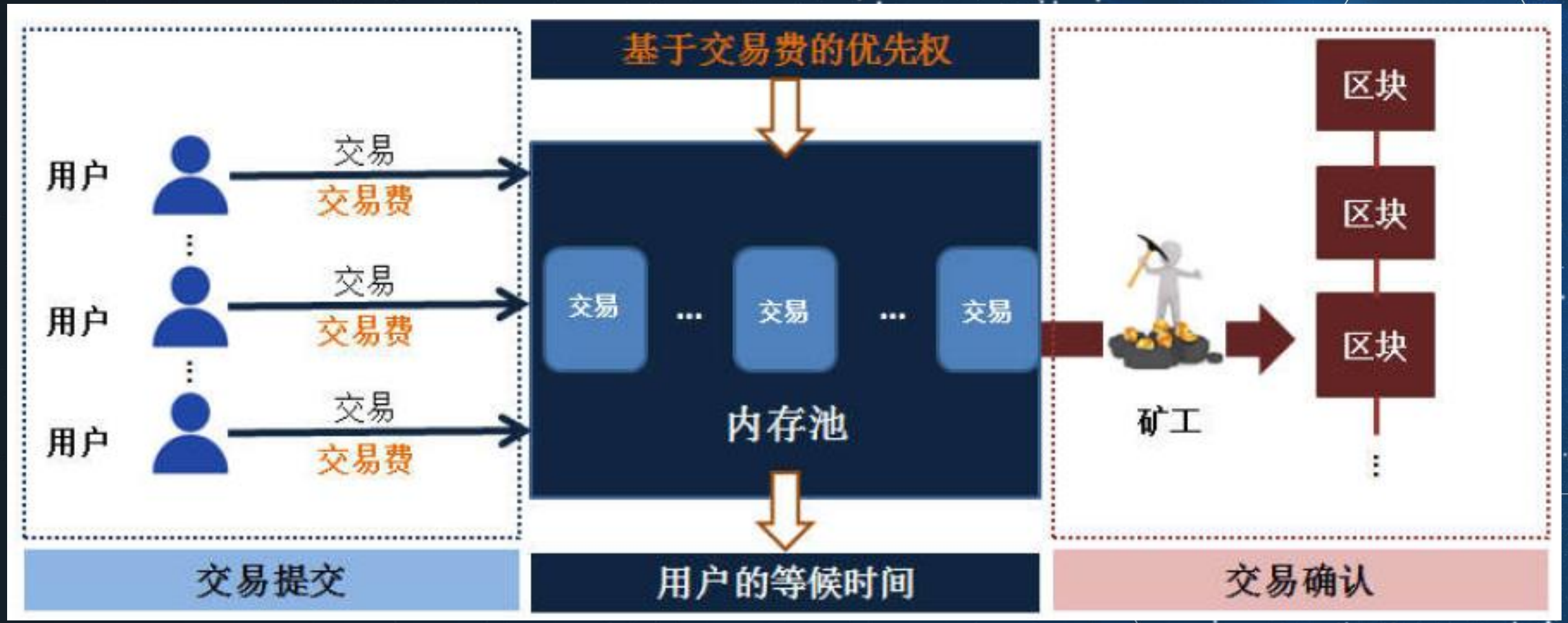
Filecoin代币FIL的分配机制

- 在Filecoin系统的代币FIL分配机制中，代币按四部分进行分配：
  - 70%的代币分发给矿工，这部分以区块奖励的形式根据挖矿进度进行分配，并且6 年分发一半。
  - 15%作为研发费用留给协议实验室，并且采用线性释放的方式在6 年的时间逐步解禁。
  - 10%通过ICO（包括公募和私募）进行募集，并且根据挖矿进度逐步解禁。
  - 5%用于设立Filecoin基金会，作为长期社区建设和管理等费用，并且通过线性释放的方式利用6年的时间进行逐步解禁。
- Filecoin的Token分配方式采用线性释放，即随着每个区块的挖出，逐步分发Token，这样的分配过程可以确保代币的发放过程平滑，可以有效避免突然间的大量代币解禁而对币价造成波动的情况。

5.3 交易费

- 在区块链生态系统中，矿工通过提供算力获取报酬，主要包括基础区块奖励和交易费两部分。其中，交易费是由用户提供的，他们在提交交易确认请求的同时，需要提交其所愿意支付的手续费金额，该费用一般是非强制的，一旦提交，不可修改不可撤销。在挖矿过程中，矿工与矿池首先需要从“内存池”（即待确认交易池）中抽取一定数量的“待确认交易”进行排序和封装，以最大化其收益。只有成功挖到新区块的矿工封装的交易会被最终确认，而他们将获得相应的交易费收益。

交易费


基于交易费的优先权
用户
交易
交易费
用户
交易
交易费
用户
交易
交易费
交易
交易
交易
内存池
矿工
区块
区块
区块
交易提交
用户的等候时间
交易确认

5.4 矿池与分配方式

- Solo挖矿：矿工利用其自身算力进行独立挖矿的过程。对于个体挖矿的矿工来说，如果矿工成功挖到一个区块，将会获得该区块的所有奖励，如果在很长时间内挖矿一直不成功，则不会获得任何区块奖励。

区块链挖矿方式

年份	年初算力	年末算力	增长
2009	0.5 MH/sec	8 MH/sec	16倍
2010	8 MH/sec	116 GH/sec	14500倍
2011	116 GH/sec	9 TH/sec	78倍
2012	9 TH/sec	23 TH/sec	2.5倍
2013	23 TH/sec	10 PH/sec	450倍
2014	10 PH/sec	300 PH/sec	30倍
2015	300 PH/sec	800 PH/sec	2.66倍
2016	800 PH/sec	2.5 EH/sec	3.12倍
2017	2.5 EH/sec	13.8EH/sec	5.5倍
2018	13.8EH/sec	24.8EH/sec	

比特币全网算力表

H为算力单位：即每秒进行的Hash数运算次数，1H=每秒运行1次Hash计算

1KH/s = 每秒1,000次哈希计算

1MH/s = 1000KH，每秒1,000,000次哈希。

1GH/s = 1000MH，每秒1,000,000,000次哈希

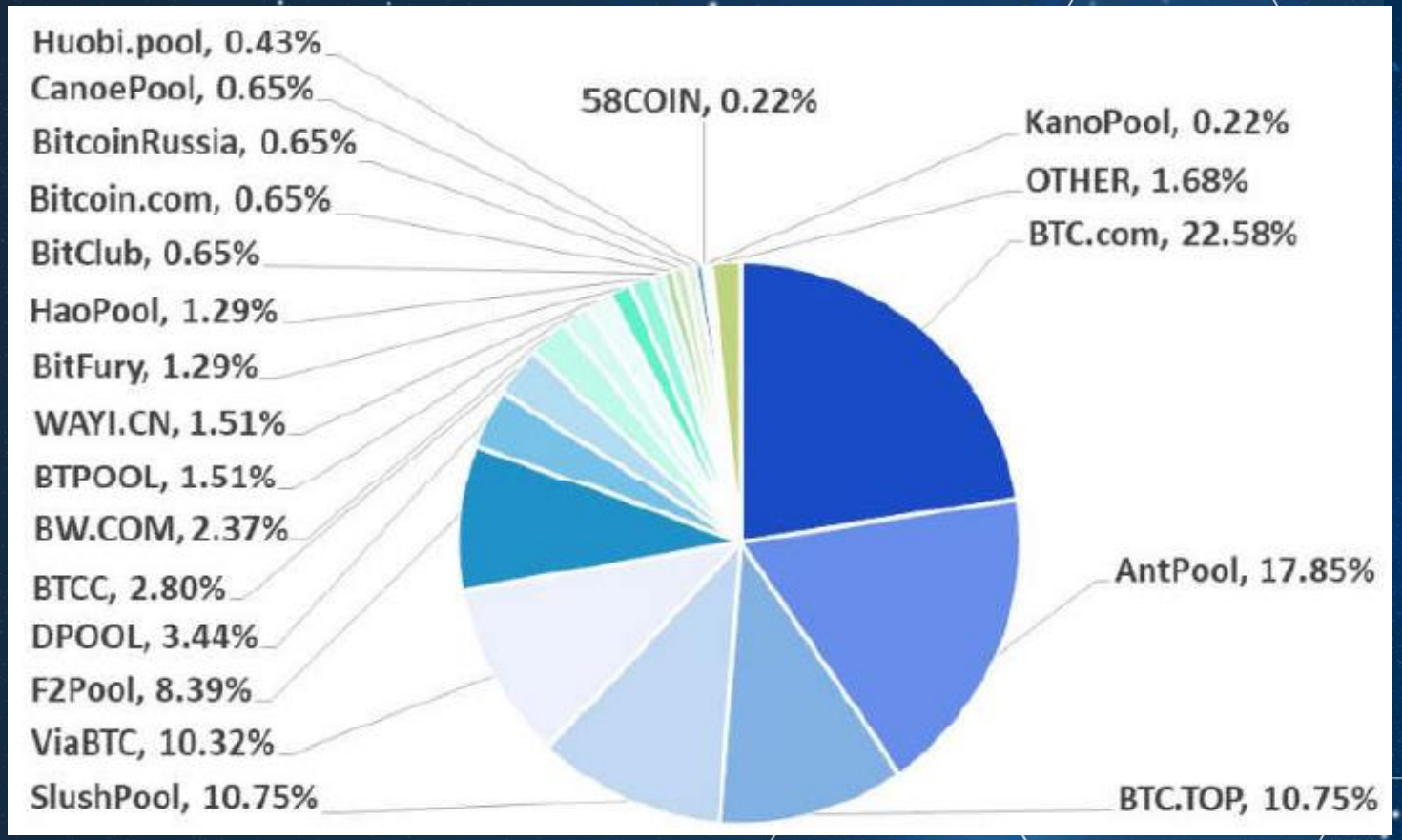
1TH/s = 1000GH，每秒1,000,000,000,000次哈希

1PH/s = 1000TH，每秒1,000,000,000,000,000次哈希

1EH/s = 1000PH，每秒1,000,000,000,000,000,000,000次哈希

矿池与分配方式

- 矿池挖矿：矿池根据区块链网络中的挖矿难度给矿工分配适当难度的任务，通过收集矿工提交的满足该难度的解来统计矿工的工作量，并根据矿工的工作量分配奖励。



比特币矿池份额

矿池分配方式-按比例分配（Proportional）

按比例分配是矿池进行奖励分配的最简单的方法，也是最能体现矿池挖矿原理的分配方式。在按比例分配的矿池中，矿池在每一轮挖矿成功之后，都会将奖励按矿工在该轮挖矿过程中所提交的部分解所占的比例分配给矿工，其中一轮是指成功挖到两个区块的时间间隔。同样地，也正是因为只有矿池成功挖到区块之后，矿工才能分到奖励，因此矿工的收益具有不稳定性。此外，由于挖矿的随机性，该模式下每一轮的挖矿时间也不一样，这就使得每个部分解的收益不同。因此，在这种模式下，矿工可能采取一些策略性行为，如跳矿，来获得高于其自身算力的收益，所以按比例分配模式是激励不相容的。这里所谓跳矿是指矿工可以策略性地选择何时为矿池挖矿以及何时将算力转移到其他矿池，从而获得高于其实际算力的收益，这将损害在同一个矿池中连续进行挖矿的矿工的收益。

矿池分配方式-PPS（Pay Per Share）

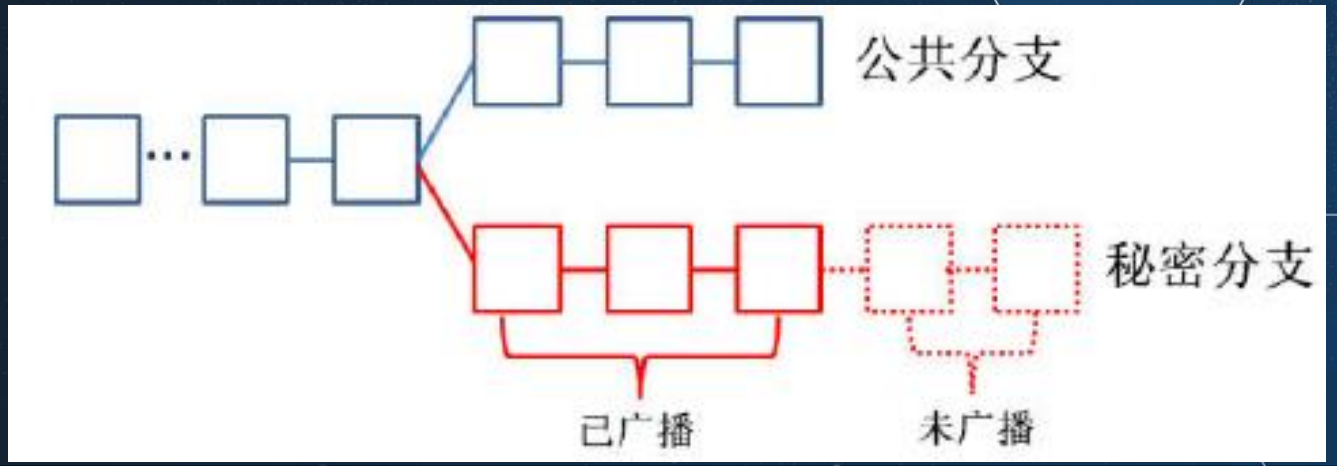
- 在PPS模式下，矿池管理者首先根据其所有矿工的总算力在整个区块链网络中的比例估算矿池每天可以成功挖到的区块数量，并根据矿工的总算力估算出矿池每天可以收到的部分解的数量，进而计算出每个部分解所对应的奖励期望值，并且该值是固定的，与矿池当天实际成功挖到的区块数量无关。当矿工提交一个部分解时，矿池立刻就将一个部分解的平均奖励分配给矿工。通过这种方式，PPS模式将按比例分配模式中矿工所面临的风险转移到矿池，从而使矿工可以获得稳定的收益。
- 该模式对于矿工来说具有以下优点：
  - 可以将矿工每个部分解的奖励风险降为零，当矿工提交部分解时可以立刻获得奖励，而不需要等到矿池成功挖到一个区块之后再获得奖励。
  - 矿工可以精确地知道其应获得的奖励数量，并且可以很容易地验证是否获得了应得的奖励，而不会因为矿池管理员的不诚实或其他矿工的策略性行为导致奖励的损失。
  - 矿工也不会因为发生跳矿行为而损失奖励。
- 对于矿池来说具有以下缺点：
  - PPS模式对于矿池来说风险非常大，所有矿工面临的风险都被转移到矿池。

矿池分配方式-PPLNS（Pay Per Last N Shares）

- 在PPLNS模式下，矿池管理员会选择一个时间段，无论在该时间段挖到多少个区块，都将在该时间段挖到的所有区块奖励分配给那些提交最后N个部分解的矿工，即只有所提交的部分解位于最后N个部分解之中的矿工才会收到奖励。
- 在PPLNS矿池中，运气成分很重要，如果矿池一天可以成功挖到很多个区块，那么矿工将会获得很多奖励；反之，如果矿池一天成功挖到的区块很少，则矿工获得的奖励也会随之减少。
- PPLNS模式具有一定的滞后性，即矿工在PPLNS 矿池挖矿的奖励会有一定的延迟。
- PPLNS模式是激励不相容的，矿工可以通过一些策略性行为如延迟汇报等来提高其收益。

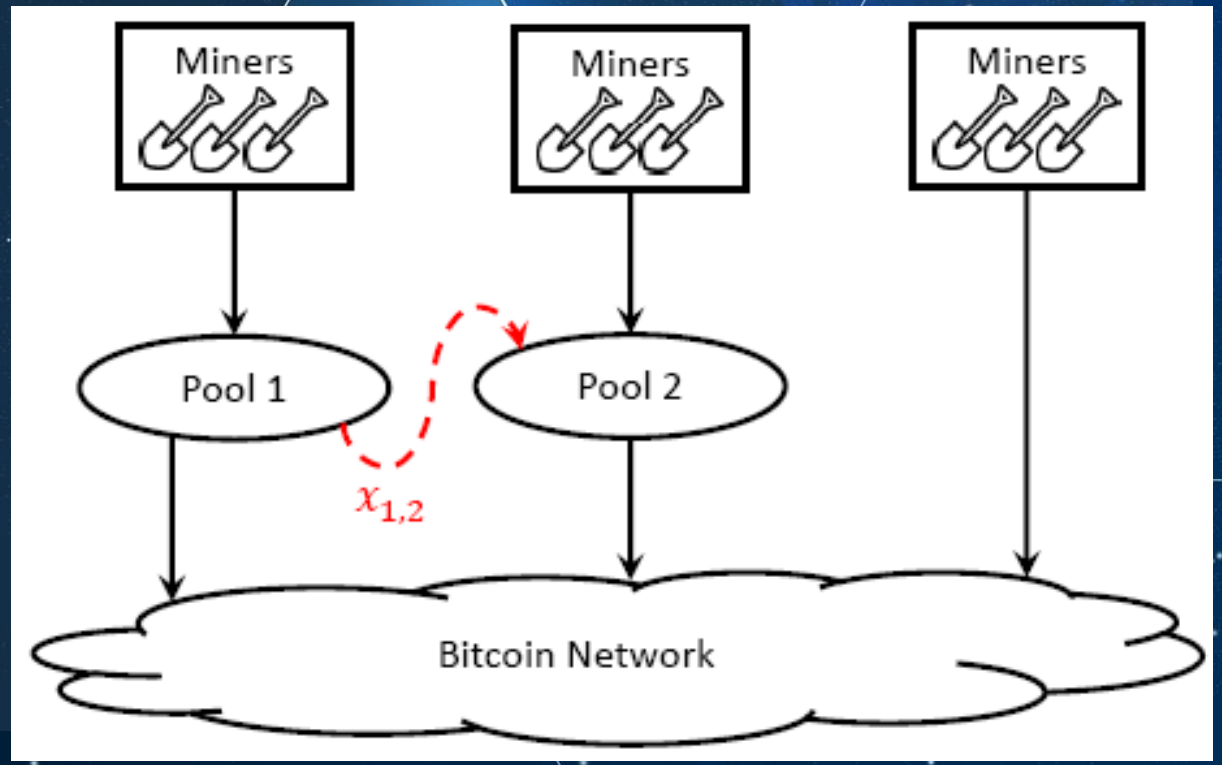
5.5策略性行为-自私挖矿

- 自私挖矿的概念最初是在2012 年BitcoinTalk论坛上提出的。
- 自私挖矿主要由矿池发起，矿池在某一时间段内扣留新挖到的区块暂不公开，并等待合适的时机广播其全部区块。
- 这种行为的目的不是破坏加密货币的区块链网络，而是获得更大利润。
- 自私挖矿是由于区块链共识机制的激励不相容性导致的矿池的策略性行为。



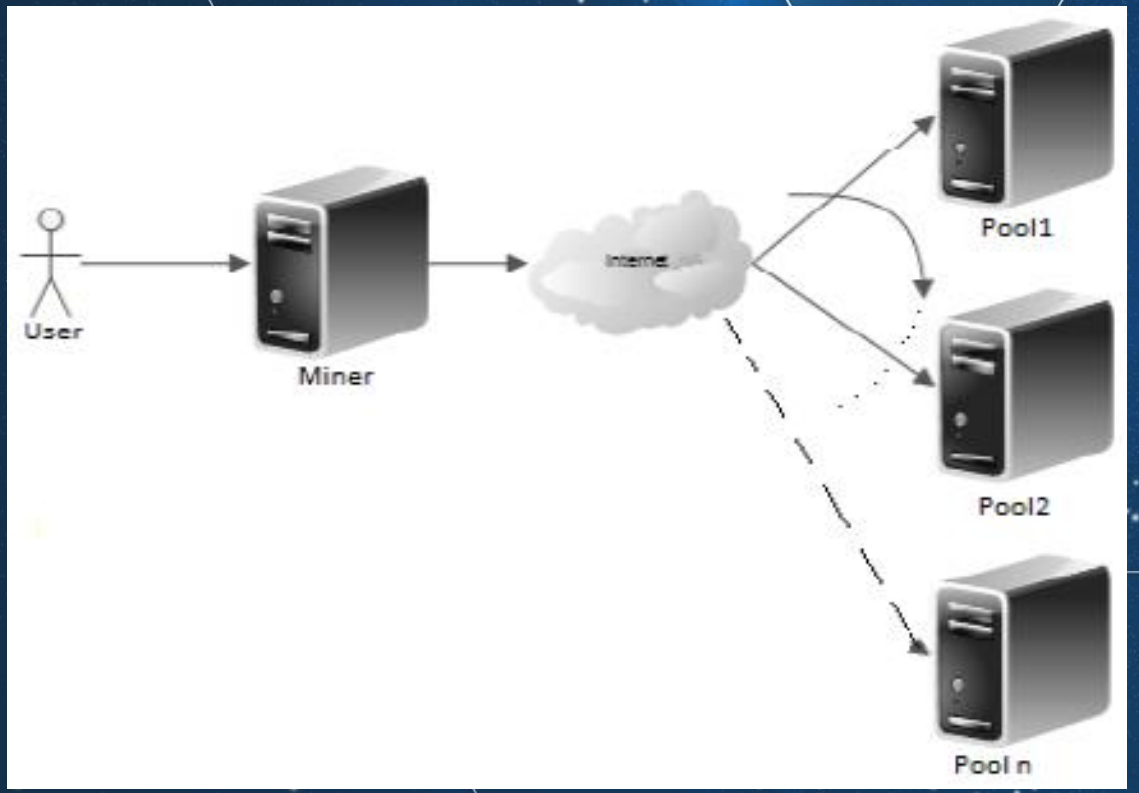
策略性行为-扣块攻击

- 扣块攻击是指攻击者在矿池中进行挖矿时，只向矿池汇报部分解，而不汇报全解，从而降低矿池及矿池中每个矿工的收益。由于扣块攻击的矿工挖到全解时会抛弃，这就降低了矿池挖矿成功的概率。
- 扣块攻击也是矿池攻击其他矿池的一种手段。扣块攻击的矿池可以将自身的一部分算力潜入到对手矿池进行扣块攻击来浪费对手矿池的算力，并从对手矿池获取一定的收益，从而降低对手矿池中矿工的奖励。



策略性行为-跨链套利和跨矿池套利

- 跨链套利和跨矿池套利是矿工提高收益的主要策略性行为，是指矿工为了获得更高的收益，不是一直保持在同一条链或在同一个矿池中进行挖矿，而是根据各链或矿池的当前收益进行切换，不断转到收益较高的分叉链或矿池中进行挖矿，以获取更高收益.
- 由于矿池奖励分配机制的不同、或者是同源分叉链（例如比特币BTC 和比特币现金BCC）难度调整机制和代币发行机制的不同，同一矿工在不同的矿池和分叉链挖矿时可能具有不同的获胜概率。因此，为最大化其收益，理性的矿工通常选择加入具有较高获胜概率的矿池或分叉链，而暂时离开具有较低获胜概率的矿池或分叉链。
- 跨链套利或跨矿池套利的策略性行为可使得矿工获得高于其实际算力的收益，并损害诚实矿工的收益和矿池的稳定性。



策略性行为-挖空块

- 在区块链中，每一个区块包含一个区块头和一个区块体，其中区块头用来保存元数据，区块体则保存打包的交易。当一个新区块中只包含区块头，而区块体为空时，我们称其为空块，矿池（或矿工）生成空块的行为称为挖空块。当矿池挖空块时，由于没有验证交易，只能获得coinbase 奖励，而无法获得交易费奖励。

数据项	描述	长度
Magic no（魔法数）	总是0xD9B4BEF9	4字节
Blocksize（区块大小）	到区块结束的字节长度	4字节
Blockheader（区块头）	包含6个数据项	80字节
Transaction counter（交易数量）	正整数VI=VarInt	1-9字节
Transactions（交易）	交易列表（非空）	<Transaction counter>-许多交易

策略性行为-挖空块

- 在获得当前区块的区块体时就开始挖掘下一个区块，为了使得下一个区块体填充交易与当前区块体的填充交易不重合，他们选择不在下一个区块体填充交易，而是直接挖掘空的区块。该策略性行为缩短了验证区块和组装区块的时间，使得矿工可以抢先开始挖矿，以期更早地挖出新区块，以获得基础区块奖励。
- 矿池挖空块的原因是他们无法在H 高度区块得到确认之前获得其包含的交易信息，因此，解决挖空块的思路就是提前获得这些交易信息。BTC 和BCH 网络中通常采用布隆过滤器和致密区块或瘦区块这两个技术来解决这个问题，但无法真正解决挖空块的问题。
- 要想彻底解决挖空块的问题，矿池需要找到一些不可能在H 高度块中包含的交易，如将用户在交易所发起的提现交易、交易所给矿池提交的保密交易等。

策略性行为-AsicBoost挖矿

- AsicBoost挖矿是一种利用比特币PoW算法漏洞来提升挖矿效率的方法，使用该算法的矿工可以利用一个输入过程中的算力去执行另一个输入过程，并可以降低哈希计算的功耗，从而提升大约20%的挖矿速度。在AsicBoost算法中，相同类型的运算会分配给相同的矿机，这样每个矿机就可以专注于同一类型的运算，从而使得在单次运算上需要消耗掉的功耗降低。
- 由于AsicBoost挖矿被申请了专利，只有专利拥有者才能采用该技术进行挖矿，从而使专利拥有者在挖矿中占据有利地位，然而这却破坏了挖矿的公平性。为了阻止AsicBoost被滥用，比特币核心开发者提出基于Segwit（隔离见证）的解决方法。然而，AsicBoost区块探索者（Block Explorer）显示，蚂蚁矿池已经启用AsicBoost算法，其挖掘出来的第540032号区块就是使用该算法挖出的，因此，采用Segwit来阻止AsicBoost并不一定有效。

小结

- 区块链不仅是一种全新的分布式计算技术，同时也是一类新兴的交易模式和成功的商业逻辑。区块链系统的核心驱动力之一是经济激励。
- 加密经济学在区块链体系中占据核心地位，是保证区块链生态系统自洽运行的先决条件。加密经济学的核心要素是保证项目参与方价值分配的合理性和激励相容性，通过这种价值分配方式，实现各参与方的利益最大化，并能够有效激励更多个人和组织不断加入。
- 在区块链经济系统中，经济激励是保证各参与方进行分布式协作挖矿的重要前提，也是维护区块链挖矿可持续性的重要保证。区块链技术中所蕴含的经济激励使区块链技术具有巨大的发展和应用潜力。

谢谢!

致谢：本节PPT修改自“中国自动化学会区块链专委会、中国人工智能学会社会计算与社会智能专委会、中国管理现代化学会平行管理专委会、青岛市人工智能学会 区块链讲习班”PPT”（由清华大学出版社提供）