7. 区块链经济学

宫汝凯
gong.rukai@dhu.edu.cn
2025.05.20-27

区块链产业快速发展

- 根据《2023年中国区块链年度发展白皮书》的有关数据，2021年我国区块链产业规模为65亿元，较2019年的10.7亿元增加了5倍左右，区块链应用的落地项目具体包括政务服务、金融、数据共享和隐私计算领域。
- 以区块链技术为基础的经济模式的迅速发展引发待思考问题：区块链技术是什么？区块链为何能够在经济活动中得到广泛应用？区块链产业发展背后的风险是什么？
- 理解这些问题，不仅需要了解区块链技术本身，还需要从经济学理论视角对区块链及其应用展开分析。

主要内容

- 区块链
- 区块链应用
- 区块链的局限性和规制困境

1. 区块链与交易

- 传统互联网交易几乎都不可避免地需要借助第三方金融机构作为中介来促成交易，而基于第三方信用的中心化(centralization)机制往往存在着诸多弊端。
  - 交易中介存在：增加交易成本+对实际可行的最小交易规模产生限制；
  - 中介机构本身存在道德风险（moral hazard）和效率问题。
- 区块链是一种基于互联网的加密分布式记账技术，通过特定的共识与认证机制将一系列数据区块(Block)按照时间戳(Time stamp)依次相连，构成完整的链式数据结构。
  - 单独修改链上的某个区块，从被篡改的区块链开始所有的区块均无效，使得篡改区块链的可行性极低；
  - 区块链的链式数据结构使得账户上每一笔收入和支出都可以很容易地追溯到来源。

区块链与交易

- 采用非对称密码学保证交易信息的安全性。
  - 每一笔新发布到比特币网络的加密交易首先被加入到结算池中，要成功记录在区块链上（即“上链”），还需要经过记账人的审核与结算；
  - 每隔一段时间，一个被选中的记账人从结算池中选取若干交易记录打包形成区块，向全网络公布；
  - 在其他记账人验证该区块并达成共识后，此区块成功上链，即加入被全体用户认可的公共账本。

2. 区块链运行的经济学原理

- 分布式共识机制与博弈论分析
- 区块链运行的市场均衡分析
- 区块链网络的扩散与分叉

2.1分布式共识机制与博弈论分析

- 区块链作为一种分布式记账技术，存在多个用户节点对区块交易信息共同记录。
  - 根据记账人组织结构与服务对象的不同，区块链主要分为公有链(Public Blockchain)、私有链(Private Blockchain)、联盟链(Consortium Blockchain)三种形式：
  - 公有链：全网络所有人都有权限读取、参与交易并参与记账与共识过程的区块链。特点：访问门槛低、用户节点免受开发者影响、交易数据公开透明、去中心化程度高；如比特币、以太坊(Ethereum)等；
  - 私有链：由中心组织或机构控制记账权，仅对授权节点开放的区块链。特点：交易速度快、交易成本低、中心化程度高；主要应用场景：大型企业内部的办公审批、财务审计等；
  - 联盟链：由联盟内成员共同维护、只针对联盟成员开放部分功能的区块链，性质介于公有链与私有链之间，由多个组织或机构共同管理链条，具有部分去中心化的特点。

分布式共识机制与博弈论分析

- 两个关键问题需要重点关注：
  - ✓ 如何确定新的记账人打包区块并完成上链过程；
  - ✓ 如何保证全网络各个节点记录的账本信息是一致的。
    - 在公有链与联盟链中，记账权难以直接决定，往往分散在多个记账人手里，需要竞争机制来确定。这些记账人通常被称为“矿工”(Miner)；
    - 为了保持区块链的运行和更新，该共识机制需要包含合理的内置激励机制。在激励机制下，矿工之间争夺记账权的过程被称为“挖矿”(Mining)。
- 1. 区块链的内置激励机制
  - 区块链采取的激励模式主要包括：交易费与新区块奖励；
  - 对于挖矿成功的矿工：收获该区块中买卖双方所支付的交易费+系统代币奖励；当新区块奖励降为零后，矿工激励将完全来自于交易者所提交的交易费用。

分布式共识机制与博弈论分析

- 2. 区块链的主要共识机制1
  - 工作量证明机制(PoW: Proof-of-Work)：首位找到答案的矿工即可获得新区块的打包与记账权。
  - ✓ 合理性：
    - PoW机制下破坏系统需要投入极大的成本，系统安全性较高；
    - 多劳多得、按劳分配：确保区块链记账权分派的公平性，有利于维持系统的去中心化水平。
  - ✓ 弊端：
    - 像一场“军备竞赛”：矿工们源源不断地投入更多资源以提高计算能力，提高获取记账权的能力；
    - 区块生成速度受到限制，系统吞吐量有限，造成交易记录上链的拥堵问题。*Q1:* 拥堵可能导致哪些问题？
      - 拥堵促使交易者提供更高额的交易费，激励更多的矿工加入网络挖矿，有利于提高区块链系统的可信度；
      - 拥堵导致交易效率下降。

分布式共识机制与博弈论分析

- 2. 区块链的主要共识机制2
  - 权益证明机制(PoS: Proof-of-Stake)
    - PoS类似于现实市场中的股份制，节点权益主要由其持币数量、持币时长等因素决定。
    - 区块链系统按照“权益越大，获得记账权概率越大”的分配原则，每隔一段时间随机选择一名记账人。
    - ✓ 合理性：
    - 权益越大的实体越乐意维护系统的安全性与一致性。
    - 记账权由系统随机指定，矿工不需要通过算力竞争来争夺记账权，PoS消耗的能源大幅降低，交易效率提升。
    - 弊端：以权益分配记账权的方式容易造成寡头优势，且时间越长，马太效应越明显。若最终产生权益超过50%的节点，则区块链将被动演化为非预期的中心化结果。

分布式共识机制与博弈论分析

- 2. 区块链的主要共识机制3
  - 股份授权证明机制(DPoS: Delegated-Proof-of-Stake)
    - 在PoS的基础上改进，解决PoS中可能的记账权寡头问题。
    - DPoS类似于人民代表大会制度或董事会选举制度，持币人将其持有的代币权益作为选票，投票选取一定数量的节点作为代表，代表对区块链网络的运行及新区块的验证、记账负责；
    - DPoS延续了PoS效率高、能耗低的优点，更为去中心化的运作方式一定程度上削减了寡头优势产生的负面效应，使得记账权分配更加民主化；
    - 但是，DPoS仍存在中心化风险，且在运行过程中，大多数普通投资者节点的投票积极性往往不高。

分布式共识机制与博弈论分析

- 3. 区块链运行的博弈论分析(*选学)
  - 挖矿策略博弈
    - 实际运作中，矿工可以不遵守上述机制，采取策略性行为以实现个体效用最大化；
      - ✓ 中本聪在设计比特币时提出了最长链规则(Longest Chain Rule)：节点总是认为最长的链是正确的并持续致力于延长。
      - ✓ 然而，在最长链规则下，矿工仍然存在偏离策略。该策略在应用中能否受益实际受到多方面因素影响，如矿工算力情况、区块大小等。
    - 矿池(Mining Pool)：PoW下常见的博弈策略。矿池通过聚合大量用户节点的算力，大幅提升了奖励概率，而参与矿池的矿工个体无论算力水平如何，可以根据对矿池算力的贡献获得少量比特币奖励。由于矿池作为整体代表全体参与矿工进行决策，有利于各节点一致共识的达成。
      - 降低了矿工的收益风险；
      - 有利于整合大量节点形成最长链共识。矿池中矿工所面临的挖矿博弈实际上对应到博弈论中经典的囚徒困境问题。

分布式共识机制与博弈论分析

- 3. 区块链运行的博弈论分析
  - 攻击策略博弈
    - 比特币网络的最长链规则有利于防止区块链信息篡改、保证交易信息可信。然而，最长链规则仍然存在部分局限。例如，其理论上无法抵御“51%攻击”(51% Attack)；
    - 算力成本是攻击者考虑是否实施51%攻击时的核心关注点。若攻击者耗费的算力成本过高，则最终很有可能得不偿失，这也是现实生活中51%攻击较少出现的主要原因。

2.2 区块链运行的市场均衡分析

- 消费端：交易者的消费动机主要来自记账服务的稀缺性。
  - 由于区块大小有限，每次写入的交易信息有限，无法第一时间将所有新交易记录到新区块中；
  - 区块服务的提供者——矿工为了最大化挖矿收益，优先选择将结算池中交易费更高的交易记录打包记入区块中。具有不同等待成本的交易者自愿支付交易费用，以获得打包服务的优先权。
- 生产端：生产者的生产动机主要来自各类共识机制及交易费的激励。
  - 考虑自由竞争市场情形下的均衡变动：随着科技水平提升，矿工的算力成本下降，边际收益将大于边际成本，吸引更多矿工加入网络，使得算力竞争更为严重，矿工需要投入更多的成本以争夺记账权。

区块链运行的市场均衡分析

- 在生产者与消费者的竞争均衡问题上，矿池以及其他类似的集中化力量的崛起，引发了人们对区块链系统能否在长期内保持去中心化的担忧。
  - Cong等(2021)研究认为，占主导地位的矿池对新矿工加入往往收取更多费用，吸引的矿工数量更少，增长速度更为缓慢，因此，矿池总量增长并不会伴随着矿池过度集中，与比特币网络的实际情况相一致；
  - Huberman等(2021)对区块链中的寡头势力展开研究，认为，虽然大型矿商可以影响交易者对交易费用的选择，但是交易费用的增加会吸引新的矿工加入，导致网络竞争加剧，将反过来降低大型矿商试图通过提高交易费用带来的利润。

2.3 区块链网络的扩散与分叉

- 代币对区块链网络的扩散过程起着至关重要的作用
  - 在区块链网络建立初期，网络通过发放代币作为激励快速吸引矿工加入网络，促进网络扩散；
  - 新加入的矿工可以使用挖矿奖励的代币参与交易，为网络发展进一步提供资源；
  - 在网络不断扩散的过程中，随着使用者的增多，代币价值逐渐提高，又进一步吸引更多的使用者与矿工加入，实现网络发展的良性循环。
- 区块链网络在扩散过程中面临着分裂的阻力
  - 如果遇到超出既定规则解释范围内的冲突，可能因无法达成共识而产生永久性分叉；
  - 若分叉后区块链仍能向前兼容，且旧节点能够就新区块达成共识，则称其为软分叉(Soft Fork)；反之，若分叉后区块链不再向前兼容，且旧节点不再接受新区块，则称其为硬分叉(Hard Fork)。

2. 区块链应用

- 区块链的重要特征
- 区块链的应用
- 代币的应用
- 区块链的发展及展望

区块链的核心特征

- 去中心化：体现在共识形成+共识信息的分发和存储方式(Chen等, 2020)；
  - 各个节点都具有区块链状态的完整、准确和可信的信息，区块链中不再存在绝对意义上的中心节点。
- 不可篡改：区块链上的共识信息难以被篡改；
  - 去中心化特征意味着区块链没有一个中心化的机构有能力修改共识信息；
  - 去中心化共识机制保证上链信息不可篡改。
- 可追溯性：能够观察到区块链从开始到最后的所有状态数据，能够对链上信息实现追溯；
  - 区块链采用带有时间戳的链式区块结构存储数据，为数据增加了时间维度，使得区块链数据具有很强的可验证性和可追溯性。

区块链的衍生特征

- 去信任化：区块链的共识机制能够保证参与人对信息的客观信任，而不需要由信任实体背书；
- 信息透明：区块链中的用户能够获得区块链上的信息，数据信息和数据操作行为高度透明，主要是由区块链的去中心化特征和可追溯性所致；
- 信息保护：区块链不要求交易主体之间公开真实身份，从而让用户的信息得到良好的保证，即匿名性。

区块链应用

- 1. 提高信息质量
  - 去中心化使得区块链中能够有多个节点具有区块链状态的完整、准确、可信的信息；部分去中心化程度较高的企业允许区块链各个节点拥有并记录节点信息；
  - 共识信息不可篡改性进一步提高了信息质量；
  - 区块链能够通过提高信息质量而被应用于司法、公共管理和实时会计等方面。
    - ✓ 司法：区块链能够通过提高信息质量，满足信任构建、信息共享、多主体协作的需求；
    - ✓ 公共管理：区块链上的高质量信息能够协助完成公共预警、身份认证、政务处理、电子证照等任务；
    - ✓ 实时会计：确保信息质量意味着可以将公司的日常会计数据永久地、不可更改地记录在区块链上。

区块链应用

- 2. 减少信息不对称
  - ✓ 促进企业信息披露，提高企业透明度和治理水平。
  - 在公有链上市的企业的所有权透明度较高，股东和其他利益相关方能够随时观察到企业所有权的变动情况并及时调整策略，提高投资积极性；
  - 透明度更高的企业对于外部投资者有更强的吸引力，从而不同企业之间会形成信息披露的竞争，有助于整体提高企业的透明度和公司治理水平。
  - ✓ 在透明度更高的区块链上市会降低公司被恶意收购的概率；
  - 隐藏持有的股票头寸是投资者减少收购成本的一个重要方法，透明度更高的区块链削弱了积极投资者和蓄意收购者的交易活动的私密性，提升了收购公司的难度。

区块链应用

- 2. 减少信息不对称con.
  - ✓ 股票在区块链上交易能够提高对管理者相对绩效评估的有效性。
  - 区块链增强公司所有权的透明度将使得管理者持有竞争对手头寸的行为更容易被观察到，因此降低了管理者利用该方法进行对冲的可能，从而提高相对绩效评估的效果。
  - ✓ 所有权透明度提升进一步对市场价格的传播机制带来影响。
  - 在所有权透明的情况下，知情者的身份更容易被识别出来，使得判断知情抛售行为更加简单，使得股价能更快地反应出不利消息；
  - 所有权透明使得股票出售方的其他股票的持有情况能够被观察到，从而更加准确地识别到这笔交易是由于流动型冲击还是不利信息引起的，提高了价格的有效性；
  - 外部交易者具有更大的激励获取企业相关信息，从而优化资源配置。

区块链应用

- 3. 避免集中化的结构
  - ✓ 影响公司选举，避免权力集中。
  - 基于区块链的选举投票速度快、透明度高，有助于在投票中避免不清晰的结果，降低了管理层操纵结果的能力；
  - 使用区块链能够有效防止空投票权(empty voting)，空投票权是指投资者在没有购买股票的情况下通过借入股份或一定的衍生证券组合暂时获得投票权。
  - ✓ 避免集中化结构、提高效率的作用在公司治理上有所体现。
  - 区块链能减少证券交易的成本和时间，显著提高证券的流动型，扩大了对证券的需求。
  - 由于不需要经过中间商就能完成交易，因此也能够减少佣金和价格磋商带来的成本。

区块链应用

- 4. 支持价值交换
  - ✓ 为公司选举带来影响，避免权力集中。
  - 基于去信任化、不可篡改、可追溯的技术特性，区块链能够有效支撑碳足迹全生命周期的可信记录和碳排放全要素的可信流转，提供了更安全、高效、经济的碳交易市场环境，以及可视、可信、可靠的监管环境，为碳排放领域的价值交换提供了技术支持。
- 5. 智能合约
  - ✓ 智能合约：一套以数字形式指定的承诺，包括合约参与方执行这些承诺的协议；
  - ✓ 智能合约可用来向区块链中的一方保证其交易对象将确定性的履行承诺，从而可以克服策略性违约等道德风险问题，并且可以大幅降低验证和执行成本等代理成本。

代币的应用

- 代币融资
  - 代币融资(ICO, Initial Coin Offerings)：企业通过出售加密代币、并保证未来产品仅能够使用该代币进行交易的方式实现融资；
  - 对于传统的股权融资而言，企业股票的价格取决于企业未来利润的贴现总和，而ICO发行代币在未来的货币价格则更多地由未来的收入流情况决定。
- 代币融资主要存在着如下问题：
  - 道德风险问题；
  - 在ICO结束之后，企业以代币计价的均衡价格等同于消费者在没有代币的情况下支付的货币计价价格，企业在事前并没有承诺特定价格的激励，难以吸引融资；
  - 企业需要在代币标价的稳定性和能够通过ICO筹集金额之间权衡；

代币的应用

- 代币融资
  - ✓ 代币融资主要存在着如下问题con.：
  - 在部分情况下，企业需要保留部分代币，减轻未来可能存在的以代币计价的价格上涨和产品供应不足的风险；
  - 成功实现代币融资的两个重要承诺：限制代币供应、强制将代币作为唯一媒介来交易产品。
  - 通过ICO融资的企业的后续融资面临着约束，部分原本可以通过传统渠道筹集到足够资金的企业却可能无法通过ICO筹集到足够资本(Catalini等, 2018)。
  - ✓ 虽然代币融资存在上述缺点，但是区块链降低交易成本、便利协调经济活动等特点将显著降低企业融资摩擦(Catalini等，2018)；
  - ✓ ICO投资者从项目的销售收入获得收益，而不从利润获得收益，将促使企业管理者采取努力以节约成本，使得ICO融资能够产生比传统融资方式更高的净现值(Garratt等，2022)。

区块链数字货币

- 传统货币的职能
  - ✓ 交易媒介：货币在市场交易中被作为流通工具来购买和出售产品和服务。
    - 比特币的交易功能是比特币作为一种货币形式的重要体现。大规模利用比特币交易面临着如下困难：较长的确认时间；参与方风险；错误转账和诈骗难以被追回；可能面临分叉、双花等技术性问题。
  - ✓ 记账单位：比特币能够作为经济社会中价值衡量的手段。
    - 比特币价格波动意味着比特币的记账单位功能具有新的表现形式。
  - ✓ 价值贮藏：对购买力的跨越时间段的贮藏，即可以把购买力以货币形式从获得收入之日储蓄到支出之日。
    - 比特币的发行数目是固定的，作为货币的比特币能够发挥价值贮藏职能，而不用担心货币政策导致的信用货币价值波动；事实上，大部分的比特币持有者并不是以交易为直接目的，而是希望能够通过持有比特币实现增值。

央行数字货币

- 以区块链技术为基础的数字货币广泛发展，但存在着大量缺陷。
  - ✓ 私人数字货币的迅速发展使得大量交易脱离于法定货币，将带来两方面的担忧：
    - 虽然部分私人货币之间能够相互兑换，但是由于缺乏币值稳定、流通性强的数字资产作为货币锚，不同私人货币之间的相互兑换存在着障碍；
    - 私人数字货币的大量发行使得交易可以脱离大型货币机构和中央银行进行，交易双方制定合约的记账单位更多地基于私人数字货币而不是法定货币，损害央行通过货币政策来调整经济的能力。
  - ✓ 去中心化金融(DeFi)：Decentralized Finance, 区块链技术+智能合约代替中心化金融体系，算法信任替代用户与金融体系之间的信任。

央行数字货币

- CBDC(central bank digital currency)是克服区块链数字货币无序发展的重要方式，从两方面克服私人数字货币带来的种种担忧。
  - CBDC为各种私人数字货币提供了货币锚，有助于维持数字经济中货币的统一性，有利于消除由于不同私人数字货币之间存在的信息不对称导致的效率低下；
  - CBDC开辟了货币政策向公众传导的直接渠道，保持了央行提供的记账单位能够和数字经济保持良好的相关性。无论是否有私人数字货币存在，只要公众在某些情况下习惯于使用CBDC，CBDC就能够作为记账单位与数字经济活动产生联系，传统货币政策渠道仍会保持有效。
  - CBDC和大型数字平台之间的互操作性是确保二者成功的关键，互操作性对于联系CBDC与公众行为至关重要。

区块链发展与展望

- 区块链的历史发展阶段
  - ✓ 美国区块链科学研究所创始人梅兰妮·斯万(Melanie Swan)在《区块链：新经济蓝图及导读》中率先提出区块链1.0、区块链2.0和区块链3.0的概念来形容区块链技术应用的三个阶段，在不同阶段，区块链的技术突破和应用场景都有所不同。
  - 区块链1.0：主要指区块链作为数字货币的应用，这一阶段构建了去中心化的数字支付体系，并支持快捷的跨国货币交易。代表：比特币、莱特币等数字货币。
  - 区块链2.0：引入了智能合约的应用；智能合约的出现允许用户不需要借助中介即可自动触发支付和执行的条款程序，使得区块链在股票、证券、期货、贷款、清算结算等商业合同和交易的应用方面得到进一步发展。智能合约使得区块链的主要应用领域由此前的货币金融支付体系扩展到了货币之外的数字金融资产转移和交易，应用场景更加广泛。以太坊(Ethereum)被视为区块链2.0时代的标志。

区块链发展与展望

- 区块链的历史发展阶段
  - ✓ 美国区块链科学研究所创始人梅兰妮·斯万(Melanie Swan)在《区块链：新经济蓝图及导读》中率先提出区块链1.0、区块链2.0和区块链3.0的概念来形容区块链技术应用的三个阶段，在不同阶段，区块链的技术突破和应用场景都有所不同。
    - 区块链3.0(可编程社会)：进一步全面拓宽区块链的应用：区块链将超越数字货币和数字金融等只在网络上实现的经济行为，而将直接赋能实体经济；
    - 区块链技术有望成为“万物互联”的一种最底层的协议，逐渐应用在身份认证、公证、仲裁、审计、域名、物流、医疗、邮件、签证、投票等多个领域，将应用范围扩大到整个社会；
    - 代表性项目：EOS、Cosmos等。

区块链发展与展望

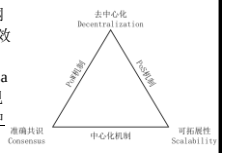
- 区块链产业的未来展望
  - ✓ 标准和监管更加完善。
    - 进一步完善区块链产业标准，并实现对区块链产业的更加合理的监管是我国未来区块链产业发展的一个重要趋势；
    - 中国早在2016年10月就开启了区块链和分布式记账技术领域的标准化工作。然而，当前我国对区块链技术标准的研究仍主要集中在基础设施方面，亟需开展针对区块链应用和服务标准的研究；
  - ✓ 成为国际竞争新赛道。
    - 越来越多的国家将区块链产业上升到国家战略层面，并出台相关措施鼓励区块链产业发展，显示出区块链越来越成为国际竞争的新赛道。
  - ✓ 可信数字化进程加速。
    - 可信数字化：利用区块链等信息技术手段在多方主体之间建立和维护信任，从而为企业带来巨大的竞争优势；
    - 由于区块链具有去信任化的特点，能够将契约机制转化为由参与者共同维护的共识机制，自动化地生产人对数据的客观信任，区块链技术在可信数字化发展的过程中扮演着极为重要的角色，加速可信数字化进程也是区块链产业的未来重点发展方向之一。

区块链发展与展望

- 区块链产业的未来展望con.
  - ✓ 开启共享经济新时代。
    - 区块链技术与共享经济有着内在的一致性，区块链能够满足共享经济逐渐由实体演变为非实体形式的需求，并进一步体现出共享经济“去中心化”的特点：
      - 从构建信任机制角度来看，随着共享经济模式的发展，共享目标逐渐开始从实体物品向非实体物品转变；
      - 共享经济强调所有参与者都能够平等高效地使用体系内的资源，而不存在一个绝对的权力主体。
  - ✓ 助力数字中国全面建设。
    - 助力全面建设数字中国是区块链的未来发展趋势之一；
    - 区块链技术具有去中心化、去信任化和可编程性等关键特征，能够构建互通互信的新型互联网生态系统，促进人、机、物安全协作。能够与金融、工业、农业、司法、政府管理等领域相结合，构建出广泛的“区块链+社会”的形式。

区块链的局限性与规制困境

- 区块链的局限：不可能三角
  - ✓ 区块链技术的一个核心目标：实现更高程度的去中心化；
  - ✓ 但若想区块链真正得到广泛的接受与应用，必须确保其共识形成的准确性与技术服务的可拓展性（泛在性）。实际上，区块链机制和传统的中心化机制共同面临着不可能三角(*Impossibility Triangle*，Chen等, 2020)。
    - 比特币PoW机制：去中心化程度+准确的网络节点共识，但受到资源耗费量大、交易效率低下等因素限制，难以实现可拓展性；
    - 传统的中心化金融支付技术：如银联、Visa和Mastercard等，依靠中心机构背书，实现准确的共识+较强的可拓展性，但缺乏去中心化。
    - 以太坊PoS机制：去中心化+可拓展性，但难以达成准确共识。

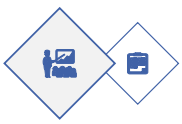


区块链的局限性与规制困境

- PoW机制下的资源耗散与低效率
  - ✓ 区块链系统中PoW机制所引发的能源影响：
    - 根据剑桥大学替代金融研究中心的估算，目前比特币挖矿年均消耗电量已经达到90TWh，该数值超过了芬兰、希腊等国家2020年的总耗电量。
  - ✓ 区块链系统中PoW机制所引发的低效率：
    - Benetton等（2019）研究表明，比特币的开采活动挤占其他经济活动，可能导致净福利损失。通过使用中国和美国各个城市的数据，作者发现挖矿行为对当地经济产生了很大的负外部性，如对当地工资和电价的扭曲；
    - O'Dwyer和Malone（2014）研究表明，若将所使用的能源部署到其他地方，可能会产生更大的社会效益。

区块链的局限性与规制困境

- PoS机制下的攻击与分叉



- **无利害关系（Nothing At Stake）攻击是PoS经常面临的安全隐患**
  - 当攻击者恶意发起攻击并制造分叉时，对于各节点而言，无需判断哪个分支最终会胜出，**最佳的策略是在多个分叉上同时进行挖矿**，如此，则持币节点最终都能获益，但这同时也大幅增加了恶意分叉主链成功的可能性。
  - 一旦攻击成功，随着时间的推移，系统中链条的分叉将越来越多，造成混乱，且全体节点一致共识的达成面临困难。
- **无利害关系攻击成功概率较大的原因**
  - 无利害关系攻击在PoS机制下成功概率较大的原因关键在于：**节点制造新区块不需要付出任何多余成本。**
  - 因此，当面临分叉攻击，记账节点总可以在不受多余损失的情况下同时为多条链制造区块，从而有可能获得全部收益

区块链的局限性与规制困境

- 过度集中

➢ POW机制：尽管PoW机制下过度集中现象的产生会在一定程度上削弱系统的去中心化程度，但其无法使区块链彻底沦为中心化系统。

- 不同矿池的多样化和矿池的产业组织形态自然地缓和了采矿力量的过度集中。
- 较大的矿池拥有更多的市场力量，因为它提供的风险分担程度更大。因此，这类矿池所有者将收取更高的费用，将导致矿池规模的增长速度更慢。最终，没有任何矿池能够发展到拥有挖矿的绝对控制权，这与现实情况相一致。

➢ POS机制

- 权利容易被少数几个大节点掌握，进而产生寡头优势，引发马太效应。
- 与PoW不同，由于PoS下大节点必然代表系统中的绝大多数利益，因此即便假设最终演化出中心节点，也没有必要作恶，因为这是与其利益相悖的。在这种意义上PoS机制不存在所谓的中心化安全问题。

区块链的局限性与规制困境

- 无法替代现实治理

➢ 尽管区块链可以采用多种分布式共识机制解决交易信息的信任问题，但其无法确保从信息数据到对应实体的关键一跃的安全性，从而无法完全替代现实治理。

- 例如，在物流业的供应链管理中，利用区块链分布式账本信息透明、不可篡改的特点来对各个实体的交互进行记录，从而大幅减少供应链各环节涉及到的信息成本，并有效地提高供应链的可追溯性与透明度。
- 仅依靠区块链无法完全替代现实治理，区块链技术需要依赖法律法规及相应部门的监督监管才能发挥最大效用。

区块链的法律风险与规制困境

- 区块链的法律风险

➢ **由区块链的匿名性、去中心化等特性及数字货币所引发的法律风险层出不穷。**

- **1. 区块链的匿名性引发的法律风险**
  - 在区块链网络如比特币中，各节点用户只通过特定的地址传递信息，用户依赖区块链获得匿名性。正因如此，给不法分子冒用他人身份或使用虚假身份进行违法交易行为提供了可乘之机。
- **2. 区块链的去中心化引发的法律风险**
  - ✓ 区块链巧妙地利用各类分布式共识机制构建全节点信任与共识，从而实现较好的去中心化水平。
  - 在公有链中，交易者可以利用区块链机制自证，不需要第三方中心机构的信任背书便可直接参与交易。
  - 然而，在区块链技术的去中心化推动下，许多现存的法律法规似乎已经失去必要。
  - 去中心化的机制一旦推行大规模应用，将对当前政府相关管理部门的职权地位造成巨大挑战，其引发的私权自治与公权力之间的抗衡是目前无法回避的重要问题。

区块链的法律风险与规制困境

- 区块链的法律风险

➢ **由区块链的匿名性、去中心化等特性及数字货币所引发的法律风险层出不穷。**

- 3. **区块链的数字货币引发的法律风险**
  - 数字货币运行的底层逻辑依托于区块链技术，同样具有去中心化和匿名性等特点，因此许多犯罪组织将其作为黑市交易、逃税、洗钱等犯罪行为的中介，大肆开展非法投机行为，构成严重的法律风险。
  - 同时，利用数字货币开展的犯罪行为将大幅增加相关监管部门维护法律的成本，对国内相关消费者造成经济损失，还可能影响公众对金融与法律的信心。
    - 例如，许多不法分子以发行ICO的方式展开新型诈骗，打着科技创新的幌子进行虚假宣传融资，欺诈公众财产。因此，2017年9月，我国央行等七部门发布《关于防范代币发行融资风险的公告》，提醒公众应当高度警惕ICO与交易的风险隐患，并全面叫停ICO。
    - 针对ICO风险问题，Bourveau等（2022）学者通过研究表明，由于新生的ICO市场缺少传统机构的监管（如银行、审计公司），公众对其自愿披露但不可核实的筹集资金用途的可信程度往往存在较大质疑；然而，即使在信息披露可验证性有限的情况下，信息披露水平较高的企业仍然拥有更强的融资能力，且来自信息中介机构的外部审查（如信用评级平台）能够加强信息披露水平和融资能力之间的正相关关系。

区块链的法律风险与规制困境

- 区块链的规制困境

➢ **区块链本身的去中心化与匿名性等特性使得犯罪隐蔽，监管难度较高。**

- 区块链本身的去中心化与匿名性等特性使得犯罪隐蔽，监管难度较高。
- 区块链系统较低的准入门槛与较大的监管与侦查难度为不法分子实施违法犯罪行为提供便利。

➢ **区块链的部分拓展内容如智能合约也存在法律困境。**

- 具体问题包括：如何确定智能合约与《合同法》的关系？智能合约是否属于《合同法》的规制对象？智能合约如果内容违法应当如何受到有效监管与控制？

➢ **区块链目前仍然缺乏国际统一的安全技术标准，且存在较大的跨境金融法律风险。**

- 包括我国在内的大部分国家，对于比特币等数字货币缺少明确的法律定位；
- 区块链资产的跨境转移不需要银行等第三方机构便可以参与境外数字货币的交易。如果一项境外金融活动违反我国的法律法规，但在境外却属于合法行为，那么其利用区块链技术向我国境内居民提供的服务是否因违反我国相关法规而需要被追究法律责任？

本讲小结

➢ 重点掌握区块链的经济学特征与应用逻辑；

➢ 了解区块链的经济学原理；

➢ 了解区块链的发展历程；

➢ 掌握区块链的局限性和规制困境。