北京師範大學
BEIJING NORMAL UNIVERSITY

区块链与数字资产

姓名 宋圣洁　　院系 湾区国际商学院

2024 年 6 月 18 日

目录

1 区块链概论

1.1 区块链的含义

区块链是一种的布式信息基础架构与网络计算机制，内涵是：

- 利用块链式数据结构验证和存储数据，
- 利用分布式节点共识算法生成和更新数据
- 利用密码学保证数据传输和访问安全
- 利用自动化脚本代码组成的智能合约编程和操作应用功能

外延是：区块链可以延展为共识，信任，共享等价值观带来的全新社会思潮，是技术，理念，模式，运营的深刻变革创造区块链经济的新模式。

比特币与区块链是产品与技术的关系

1.2 主要特点

- 去中心化：每个节点高度自治，彼此可以自由连接，都可能成为阶段性的中心又不具备强制性的中心控制功能。节点网络而形成非线性因果关系，是开放式、扁平化、平等性的系统现象或结构
- 不可篡改，可追溯：每一笔交易通过密码学与相邻两个区块串联，单个甚至多个节点对数据库的修改无法影响其他节点的数据库，除非控制超过 51%
- 交易透明，双方匿名：运行规则公开透明，数据信息公开，每一笔交易所有节点可见；节点之间无需公开身份。
- 开放、共识：节点间基于共识机制，竞争计算共同维护整个区块链。任一节点失效，其余节点仍能正常工作。

1.3 区块链的分类

- 公有链：没有官方组织和中心服务器，参与节点按照系统规则自由接入，节点基于共识机制开展工作；优点是公开透明，每个人都可以竞争记账；缺点是效率低、大规模耗电、验证时间长；特点是高度去中心化、无法篡改；适用于对安全可信要求高，对交易速度要求不高的场景。
- 联盟链：特点是去中心化，与其他机构合作，公开程度仅限联盟内成员，记账规则按照联盟规则运行，节点只有读写权限；缺点是公开透明性降低；适用于机构之间交易结算。

- 私有链：特点是在企业内部，仅限少数节点读取，保留真实性和部分去中心化特性，具有私密性；优点是交易速度快、成本低，隐瞒篡改可以追踪来源，更好保护隐私；适合公司内部访问修改数据的场景。

1.4 分层架构

- 数据层：
  - 数据存储和交易安全
    - 数据区块：记录交易，区块主体记录前一段时间所有交易信息，功能优区块头实现
    - 数据区块 + 链：哈希指针互联和相互验证，可以定位数据块位置和根据哈希值判断是否被篡改
  - 连续分布式存储
    - Merkle 树：归纳所有交易信息生成统一的哈希值，哈希二叉树可以快速校验大规模数据，任何改变 Merkle 树都会改变。
  - 交易安全
    - Hash 函数：任意长资料 Hash 转变为定长代码，单向哈希函数容易被验证不易被破解，特点是：输入任意长，降低分布式存储压力；同输入同输出；稍有变化大不相同；正向容易，逆向困难
    - 加密算法：公钥加密、私钥解密，私钥签名、公钥验证。
- 网络层：
  - 采用网络标准协议和 P2P 传输技术，实现节点数据交换
    - P2P 技术：点对点技术，没有中心服务器、依靠网络用户群交换信息的互联网体系，每个用户既是节点也是服务器。特点是：去中心化，资源服务分散在各个节点上实现传输和服务，无需中心化服务器介入；健壮性：耐攻击、高容错，部分结点遭到破坏对其他节点影响小。
- 共识层：
  - 负责节点间网络一致性保障，封装共识算法。
    - 共识机制：达成共识记录有效性，作用是认定和防止篡改，有 PoW 和 PoS 共识机制等。
- 激励层：
  - 发行激励机制：交易输出小于输入的差额作为交易费激励，既定数量电子货币进入流通时，激励机制可以完全依靠交易费而不必发行新的货币。

  - 智能合约：情景应对型的程序化规则和逻辑，通过区块链上的去中心化、可信共享的脚本实现；程序代码形式附在区块链数据上，P2P 验证后计入区块链中；封装了预定义的规则场景行动；实时监控智能合约状态并在满足触发条件后激活执行合约。

- 应用层：
  - 可编程货币：发行分配调节机制
  - 可编程金融：跨境支付、数字票据、资产证券化、保险，减少中间环节、提升数据安全性
  - 可编程社会：身份认证、健康管理、人工智能、投票、公证见证、供应链、去中心化

2 区块链技术原理

2.1 加密算法

2.1.1 密码学简介

- 古典密码学：保存、传递、破译
- 现代密码学：信息完整性、不可抵赖性、防攻击的安全性与机密性、认证性

2.1.2 哈希算法

- 哈希函数：有限合理时间，把任意长消息压缩为定长输出，不可逆。
- 特点：正向快速；逆向困难；输入敏感；冲突避免（防碰撞，抗匹配、替换攻击）。
- 算法设计：不哈希则有存在性伪造攻击
- 种类：MD4 不安全，MD5、SHA 不抗强碰撞攻击，一般推荐至少 SHA2-256 或更安全算法
- 应用：数字签名可认证性；加密算法保密及隐私

2.1.3 加解密算法

- 算法不变、公开可见，密钥需要保存和特殊硬件保护，随机生成，长度越长强度越大

- 分类：根据密钥是否相同，对称加密-加解密密钥相同，计算效率和强度高，但需要提前共享、易泄露，如 DES、3DES；非对称加密-加解密密钥不相同，无需提前共享，但计算效率低、存在中间人攻击，比如 RSA。根据密钥使用方法，可以分为对称密码和公钥密码。
- 对称加密算法：AES
  - 特点：最简单、最快速、同密钥、效率高、广泛用；密钥小，速度快，空间占用小，强度高；需要提前持有密钥
  - 分类：分组密码将明文分为定长数据块作为基本加密单位；序列密码每次只对一个字节或字符进行加密处理，密码不断变化，仅用于特定领域
  - 举例：DES/AES；序列密码，每次用与明文登场的随机密钥串对明文加密处理，通过伪随机数生成器来生成伪随机密钥串
  - 场景：适用于大量数据的加解密过程，如比特币钱包文件
- 非对称加密算法：RSA
  - 特点：解决对称加密的提前分发密钥问题，公钥公开、私钥私人持有；优点是公私钥分开，不安全通道也可以使用；缺点是处理速度慢两三个数量级，强度低；主要基于大数质因子分解、离散对数、椭圆曲线等
  - 算法种类：RSA
  - 场景：适用于签名场景或密钥协商，商用场景下密钥至少 2048 位
- 比特币中的应用：采用椭圆曲线数字签名算法，公钥加密，私钥签名，另一个人公钥解密，哈希验证

2.2 共识机制

2.2.1 共识机制含义

- 含义：在不可靠的异步网络中定义容错协议，确保各主机达成安全可靠的状态共识，实现状态复制。
- 关键问题：定义一个规则来在网络中选择记账节点，保障账本数据在全网中达成正确、一致的共识。
- 地位：区块链技术的基础和核心
- 分类：经典分布式共识机制和区块链共识机制
- 流程：选举出块者（PoW 和 PoS 防止女巫攻击）、生成区块、节点验证更新区块链

2.2.2 评价标准

1. 安全性：抵御敌手操纵网络资源和其他资源情况下的攻击
2. 交易吞吐量：每秒钟处理交易的数量为交易处理速度，受到区块产生间隔、区块大小和网络延时影响
3. 可扩展性：网络处理交易性能能够随节点增多而增强
4. 交易确认时间：交易从被提交至共识网络到完全被确认所需要的时间。交易被确认是区块被写入且大概率不被篡改；确定性共识中，区块链一般不分叉，确认时间降低。
5. 去中心化：共识机制中没有可信第三方存在
6. 资源占用：通信复杂度和计算复杂度

2.2.3 典型方案

1. 经典分布式共识机制：
   - 在授权网络中完成状态机复制，实现一致性和活性
   - 网络模型是部分同步网络，容错协议采用拜占庭协议，容忍恶意和崩溃节点
   - 部分同步：收集部分的来验证上传；异步：每一轮取一些加密；同步：法定人数
   - 适用：分布式数据库系统
2. 授权共识机制：
   - 联盟链中，节点经过身份认证后，通过分布式一致性算法完成区块的生成和维护
   - 节点分工明确化、数据处理模块化可以提高交易吞吐量
3. 基于工作量证明的共识机制
   - 含义：节点利用自身算力通过寻找哈希函数原像完成出块者选举
   - 弊端：巨大能源消耗，安全隐患：日蚀攻击（提前攻占链接地址）、双花攻击（最长链原则）、自私挖矿（不公布）
   - 技术原理：工作量证明函数和区块数据：80 个字节定长区块头是输入字符串，根哈希值存到区块头，交易信息哈希为 Merkle 树，加上指针，形成区块链；挖矿难度：需要多少次哈希运算产生一个合法的区块，新难度值 = 旧难度值 ×（过去 2016 个区块花费时长/20160 分钟），目标值 = 最大目标值/难度值，

比特币工作量证明的达成就是矿工计算出来的区块哈希值必须小于目标值。: 节点获取挖矿难度、交易信息，自由加入、无需注册，最长链选取 → 寻找工作量证明，挖矿，迭代 nonce 值直到满足 → 新区块的广播和验证，通过后新区块继续挖矿，基础奖励 + 交易费

4. 基于权益证明的共识机制

   - 含义：根据持币量和时间，获得利息。币龄 = 量 × 时间，反映某刻用户所拥有的货币数量。首富权力更大，有可能支配记账权。
   - 应用：点点币，每签名一个区块，币龄清零，30 天后才能签下一个，寻找下一区块最大概率在 90 天后达到最大值，防止大权益、减少计算能力。

5. 混合共识机制

   - 含义：经典分布式 + 区块链共识，PoW 和 PoS 选举委员会，委员会生成区块
   - 流程：选举委员会成员（PoW-设定挖矿难度 PoS-根据币数量随机选，防止女巫攻击），选举委员会领导者（随机数、投票，防止不作为或恶意行为），运行委员会内分布一致性算法（PBFT，实现拜占庭容错，生成维护区块链），广播区块（更新），重配置委员会（每个时期更新，防止敌手腐化）
   - 问题：协议启动问题（创世区块，初始化配置）、委员会重配置问题（更新期间的诚实用户比例，交替时持续处理，防止敌手加入）、新节点加入问题（快速自启，识别敌手虚假信息）、委员会内分布一致性算法（交易能够快速响应，提高效率，实现并行提议）
   - 分类：
     - 单一委员会的混合共识机制
     - 多委员会的混合共识机制：处理网络中不同分片交易，实现可扩展性：通信分片（划分全网片区）、计算分片（交易 ID 末号 i，则由 i 委员会负责）、存储分片（交易区块链来存储，降低节点存储负担）
     - 区别：单一 VS 多委员会；委员会成员分配（防止敌手）；需要考虑跨片交易处理（防止双花攻击）；存储分片中不存在全局的区块链

2.3 智能合约

2.3.1 什么是智能合约

- 智能合约是将合约内容通过算法和程序编写为代码并在区块链上部署，满足条件自动执行无需人为操作。可以根据规则和承诺转移数字资产和实现特定功能。

- 性质：自治（自动运行）、自足（提供服务或发行资产来获取资金，需要时使用资金）、去中心化（分布式网络节点运行）
- 特点：基于区块链技术实现，合约触发执行合并为一次原子操作，无须第三方机构介入

智能合约和传统合约的区别：（自主成时惩）

1. 自动化：自动、人为
2. 主客观：客观、主观
3. 成本：低、高
4. 执行时间：事前预定预防执行、事后追溯
5. 违约惩罚：数字化属性抵押资产、实物抵押资产

2.3.2 智能合约的运行

比特币智能合约：价值传递、创建合约、调用合约函数
以太坊：把调用的信息放入交易中，对其签名并发送到以太坊网络中执行

2.3.3 主要类型

1. 智能法律合约：涉及严格法律追索权的合同，以防当事人不履行交易目的
2. 去中心化自治组织：区块链上的社区，用一系列规则来定义，任务是程序中断时可以执行获得追索权，协同监管和监督参与者
3. 应用逻辑合约：物联网领域和其他设备通信合作，可以和区块链上其他智能合约和程序一起工作

2.3.4 优点与缺点

- 优点：
    1. 速度效率精确度：满足条件可以立即执行；无需处理文书工作；避免手动填写文档导致的错误
    2. 安全：加密难破解；分布式账本前后关联，改变整个链才能改单个记录
    3. 节约成本：避免中介机构处理交易，消除时延和费用
- 缺点：

1. 图灵完整，理论上可以做任何事，但不适合繁重工作，合约计算越多，成本越高
2. 合约越复杂，越可能出现安全漏洞，具有不可篡改特性
3. 无法感知外部信息，需要输入后才能裁决

3 区块链应用场景

3.1 供应链金融

3.1.1 什么是供应链金融

- 产生背景
  1. 产业组织：产业模式从纵向一体化向网链式组织发展；竞争方式从单个企业到供应链；金融服务从传统金融服务到供应链金融服务
  2. 解决融资难问题（自身严重问题、外部环境支持、上下游制约）
  3. 银行：深化核心企业优质客户关系；业务派生存款；短期特定全流程，提高风险管理水平；低风险集群式开发中小企业市场
  4. 多方共赢：增值服务，企业融资管理、物流利润、银行风险客户多，社会产业链升级
- 含义
  1. 供应链：围绕核心企业的信息流、物流、资金流，从产品服务设计、原材料采购、制造包装到支付给最终用户的全过程
  2. 融资：货币资金的融通
  3. 供应链金融：供应链各环节企业提供贸易资金、新型贷款，以核心客户为依托、以真实贸易背景为基础，自偿性贸易融资方式
- 对比：供应链金融 vs 非供应链金融
  1. 主体范围质押：单个多个企业、单个企业本身；动产质押、核心资产质押
  2. 风险：较小、较大
  3. 服务品种、效率、内容、作用：品种多样、及时解决、信贷支持、持续竞争；品种较少、手续繁琐、一时需求、资金困境
- 特点：
  1. 目的是融资，特点是科学、个性化、针对性强，操作是流动性差但资金流确定的资产作为还款来源、借助中介企业协调降低金融服务成本

2. 以供应链真实贸易背景为基础
3. 闭合式资金运作，逐笔审核放款
4. 个性化服务方案，提高经营管理能力
5. 流动性差的资产为目标，前提是自偿性好

3.1.2 传统供应链的问题

困境：缺乏战略信任机制；信息资源整合利用能力低、共享协作之后；企业规模扩大、多元化、市场覆盖度扩大；信息追溯能力不足，虚假套利；链上真实完整的数据

挑战：核心企业、上下游企业信用风险；贸易背景真实性风险；业务操作、物流监管、抵押资产风险

3.1.3 区块链如何赋能

1. 多主体合作：分布式账本提供共享平台，降低风险，信息追溯无法篡改，实时同步对账
2. 多层信用传递：区块链打通各层交易关系，构建扁平化点对点信用网络，将信用纳入供应链金融服务范畴
3. 资产数字化：流动性、份额化，获得现金流支持，降低负债率
4. 流程智能化：控制供应链流程，减少人为干预，实时监控

传统供应链和供应链金融对比：

1. 融资审批时间：不掌握信息时间长，掌握真实情况缩短时间
2. 融资成本：融资手续费高，降低手续成本
3. 工作效率：逐笔审核效率低，实时操作自动简便
4. 信息验证：人工验证表单繁琐，保存各层交易过程
5. 交易透明化：不透明信用风险；无法篡改可追溯
6. 风险：难确权风险高；核心企业资信风险低

3.2 数字票据

3.2.1 从票据到数字票据

- 票据：出票人委托付款人（银行、商业信用）一定金额（支付）流动性好（融资）有价证券（金融产品）

- 特点：一经开立，重要信息不得更改；已完成的交易不可撤销；银行承兑汇票比商业承兑汇票数量和流通量大；单个银行风控影响其他参与者
- 分类：本票、支票、汇票
- 业务模式
  1. 银行承兑汇票：企业申请，银行承兑，核心真实贸易；有保证金、收费收益（利润来源）
  2. 贴现：企业申请，银行贴现，第三方可代理申请贴现，非银行支付贴现利息；贴现利息（主要盈利模式）
  3. 转贴现：银行申请，人民银行再贴现，货币政策、控制信贷
- 作用：信用（诚信自律、债权债务关系）、企业融资产业转型、利率传导实体经济抗风险
- 形态发展：纸质（需要印章）、电子（接入 ECDS 系统办理）、数字（区块链、智能合约等）

3.2.2 数字票据

- 内涵：大数据、区块链技术对票据资源优化配置和创新，服务经济金融；数字票据：具备电子票据功能优点，又融合进区块链技术的优势
- 特点：
  1. 科技赋能：新技术赋能业务处理分析
  2. 高度透明：主体、信息、效率、全方位
  3. 嵌套式监管：大数据分析参与者业务行为、人工智能干预违规交易、票据监管嵌入日常行为
  4. 标准统一：规则、口径、要求
  5. 交易创新：票据业务、票据数据资产化
  6. 服务创新：重构传统票据资源，释放数据生产要素价值，创新服务模式
- 核心优势：
  1. 不需要中心服务器和中心级应用：降低开发、系统维护优化成本，减少中心化带来的黑客攻击、节点出错带来的风险，减少数据被反复记录保存成本
  2. 完整透明时间戳：降低违约信用风险，法律追诉，防止重复抵押合伙作案
  3. 可编程和可控制：自动赎回买断；不需要线下合同避免违约

3.2.3 区块链如何赋能

区块链如何解决传统票据存在问题：

1. 贸易背景造假-分布式共享总账-数据完整信息透明
2. 一票多卖-多中心化共识机制-去中心化真实可靠
3. 背书不连续-智能合约-可视化
4. 审核困难成本高-时间戳不可更改-全流程可审计

区块链在数字票据中的价值：

1. 去中介-解决价值在无形传递中点对点问题，票据中介重新定位
2. 改系统-原本集中式登记和数据交换通道；区块链多中心，时间戳追溯产生到消亡
3. 防风险：道德-时间戳和全网公开防赖账、操作-非对称加密和高容错防人为失误、信用-所有参与者信用搜集评估控制、市场-可编程性可资产负债平衡，数据透明，资金需求真实）
4. 降成本：编程控制价值流转方向、规则全覆盖硬控制，时间戳保透明，货币政策定点约束智能投放

区块链在数字票据中的应用场景：

流程：开票验证授信生成区块、流转买卖公私钥记录交易信息，编程控制托收规则

1. 承兑：非中心化出票、减少网银中介、时间戳解决信任问题、信息安全
2. 流转：免去到中心化系统信息流转、点对点区中心、智能合约防风险、交易公平价格真实
3. 托收：价值交换直接完成、账实相符

4 数字资产

4.1 数字资产的内涵

- 数字是用来表示数的书写符号，数字资产的特征是可交换的价值是以数字化方式呈现的
- 数据是事实或观察的结果，是对客观事物的逻辑归纳，是用于表示客观事物未经加工的原始素材，是重要的经济战略资源

- 资产是法人或自然人拥有的各种财权和债权及其他各种权利的资金表现形式，具有经济价值、价值可计量、所有权要素，是经济主体控制的、预期带来收益的、过去事项形成的。

- 数字资产是企业或个人拥有或控制的，以电子数据形式存在的，在日常生活中持有以备出售或处于生产过程中的非货币资产。以二进制形式储存在设备中，密码学保证资产安全，具有数据权属的数据集。

数据资产和数字资产的区别：

- （定义和本质）数据资产是能够创造价值的数据资源，包含结构化和非结构化数据，恰当利用后为企业创造价值；数字资产是数字形式存在的可以交易的虚拟资产，包括加密货币等，本质是表示所有权和价值的一串代码。

- （价值体现）数据资产可以通过对数据的挖掘，为企业带来新的增长机会，间接为企业创造价值；数字资产直接蕴含所有权和货币价值，价值取决于市场供需和投资者预期。

- （形态和交易方式）数据资产以结构化和非结构化形式存在于企业内部，交易转移在企业内部或特定场景进行；数字资产以密码学原理构建加密代码或 NFT 形式存在于区块链上，可在互联网上点对点交易，通过去中心化的数字交易所或钱包转移实现。

- （管理和控制权）数据资产管理控制权在企业内部，数字资产由于去中心化、不可篡改特性，管理控制权在个人投资者手里，可以任意审查。

- 联系：深度融合——数字资产化、资产数字化

数字资产和数字货币区别和联系：

- 货币本质是所有权和市场关于交换的契约，法定货币不代表实质商品，依靠法令合法通货；电子货币是法币的电子化；虚拟货币是无形的，是非法币的电子化；数字货币具有分布式记账、独特加密技术、去中心化结算特点，要成为法币需要获得国家信用。

- 区别：加密货币受到投资者关注形成规模后，就是数字资产，是数字化的金融资产而不是数字货币；法定货币和数字网络技术结合后形成数字化法定货币；数字货币可能取代有形货币，数字资产只是数字经济一部分。

- 联系：价值取决于供求关系

4.2 特点

广义上：商无保增长要权（简记）

- 具有市场商品基本属性：具有价值和使用价值，市场交易使用才能实现价值
- 属于无形资产管理范畴：存在安全风险隐患
- 具有资产保值增值功能：必须不断赋予新的内涵保值增值
- 具有可以长期重复使用的价值：永远存续，链越长，价值越大
- 属于新型的生产要素：劳动者，技术，资本等传统生产要素之外的新生产要素
- 具有所有权以及使用权（经营权和管理权）：临时让渡

狭义上：比人未扩（简记）

- 比特结构形式：是以比特结构形式存在的数字代币
- 无需人为处理的智能交易：实质是代码间的交换，无需人为处理
- 权属确认未定：数字资产在确权方面没有定论
- 概念内涵外扩：传统资产数字化

4.3 类别

- 根据数字资产内容不同，可以划分为虚拟货币、娱乐消遣类等
- 根据数字资产形式不同，可以划分为标准化数字资产和非标准化数字资产等

4.4 数字资产交易模式

4.4.1 基于区块链

- 主链注册，辅链交易：采用二维平面模型架构模式，将数字资产的登记与交易进行合并，能够同时在两个维度上同时记录不同类型的数据。区块主链负责记录不同作品的登记信息，进行资产注册，区块辅链记录每个数字资产的交易信息。
- 数字资产登记区块链：区块主链是由作者、登记平台和底层区块链三种不同的角色共同参与，通过注册流程机制对用户提交的数字资产进行注册。再设立一个独立于用户和登记平台的第三方 CA 证书机构，这个机构向参与到注册过程的用户和平台颁发密钥并负责日常密钥的维护工作，保证用户提供信息的安全性和避免后续操作过程中发生用户抵赖。

- 数字资产交易区块链：卖方是资产的提供者，买方是数字资产的交易目标对象，交易平台是一个信息化的市场，为买卖双方提供信息交换渠道，方便卖方发布资产信息，为买方提供了更大的选择范围，底层架构是所有交易信息都需要转换为区块节点形式记录在交易区块链（易用性、便捷性、安全性）

4.4.2 基于托管

托管是主要模式，原因：目前区块链技术还在发展过程中，其交易方式还不太成熟。数字资产拥有者将其数字资产在数字资产交易平台进行托管，经托管后的数字资产可以由购买方认购，这也为数字资产第三方交易模式。一旦托管的行为发生，数字资产的拥有者将无权管理且无法知道该笔交易的具体内容，其获利行为为一次性产生。

4.5 数字资产的未来机遇与挑战

4.5.1 机遇

- （投资）随着数字资产市场规模和影响力扩大，数字资产将成为重要的新型投资标的/资产配置选项，提供新的投资机会。
- （就业）新型数据资产和数字资产相关岗位需求增加

4.5.2 挑战

- 合规性：产业监管政策法规亟需出台健全
- 安全性：技术向恶难监管（数据安全和反洗钱）
- 专业性：无先例可依（规范和抑制创新的权衡）

5 数字货币

5.1 数字货币概览

5.1.1 数字货币的内涵

含义、范畴、对比、发展历程

- 含义：使用分布式账本技术发行的数字工具。
- 不包括法定形式数字货币，属于非实物货币
- 和电子货币、虚拟货币这两种非实物货币对比，区别是：主范数储流，价信安成环

- 发展历程：萌芽-盲签名的密码协议，具有匿名性和不可追踪性，中心化交易；中心化-E-gold 锚定黄金，1：1 兑换，仍需中心化机构；去中心化-有货币重复支付和货币生成难题；山寨币大爆发

5.1.2 数字货币的特征

简记：去追主名量

- 去中心化：点对点交易，无需媒介
- 可追溯：已发生过的全部交易可追溯，无需授权认证
- 超主权：与主权脱钩，不属于任何国家
- 匿名性：不需要实名认证，交易双方不知道对手信息
- 总量有限：数字货币总量有限，不是无限增发

5.1.3 数字货币的运行系统：发行

根据数字货币特征与优势，设计发行目的、依据、机制，提高发行成功率。随着数字货币发行总量的不断攀升，发行的成功率开始下降。

ICO 影响因素：

1. 主体提供的“白皮书”是信息披露的主要途径，包含项目信息、技术源代码以及社交媒体宣传。但可能导致信号传递中的道德风险，造成投资者的失望情绪和数字货币贬值，影响成功率，因此 ICO 适用于高收益和高风险的融资项目。
2. 发行者个体特征、CEO 负面情绪、开发团队知识能力对 ICO 成功率和 ICO 抑价都有影响。
3. 宏观因素的监管政策不仅影响本国的 ICO，也影响全球企业家创新精神。

分类：依据国家信用发行的法定数字货币；依据有价资产发行的资产数字货币；依据程序算法发行的算法数字货币。

特点：

- 流通货币职能。
    1. 是一种弱货币，使得劳动和知识交换成为可能，有利于缩小贫富差距。
    2. 能够补充传统货币体系，具有交易便捷、低手续费、防止货币超发。
    3. 受到蒙代尔不可能三角制约，难以全球流通。

4. 受金融包容和金融摩擦影响，现金功能方面，降低市场对实体货币需求，央行需要增加货币需求来保持币值稳定，确保成功发行；存款方面，挤出银行存款，加剧与传统银行竞争。

- 资金融通职能。

1. 因其具有收益风险性、可交易性、等额均分性，因而可以作为一种去中心化的融资方式。
2. 本质是众筹，高流动性可以提高众筹项目效率.
3. 主要受到监管、需求、产品利润影响，可能成为主流融资途径。

5.1.4 数字货币的运行系统：价格

特性、宏观、微观、安全、非法、锚定、预测

- 定价特性：流动性强，可以 24 小时连续交易，是良好的金融资产。
- 宏观：受到传统资产和经济因素影响小，价格波动主要由交易动量和投资者关注来解释，包含：资本管控、监管措施；股市波动、经济政策不确定性；民族文化、社交媒体信息。
- 微观：工作量证明机制下，受制于硬件和能源成本，价格波动主要由铸造成本决定；随着向权益证明机制转换，铸造成本降低，价格也会减弱。
- 安全：安全性是数字货币价值主要来源，共识机制转换会使得安全性能降低，造成价格下降。
- 非法活动：计算机病毒和网络勒索曾一度影响比特币价格。
- 锚定效应：数字货币锚定比特币等主流数字货币时，价格走势受创始人持有量和平台经营状况影响。
- 价格预测：自回归滞后分布模型、神经网络、深度学习

5.1.5 数字货币的运行系统：交易

- 数字货币运行主要依靠特定共识机制，PoW 共识机制本质通过加密运算提高系统安全性能，算力越高越有可能获得记账权和比特币奖励。随着比特币价格升高和硬件设备升级，挖矿消耗资源越来越多，会限制数字货币稳定发展。解决路径是调整为 POS 共识机制，长期来看不会造成代币的垄断效应。

- 分布式信息存储要求区块容量较小，但交易流量也不高，即使有隔离见证扩大流量，也无法满足交易需求。可以通过改变交易排序、区块间隔和区块容量来缓解拥堵问题，也可以提高交易费，但考虑交易时效性时，转向 PoS 共识机制是更好的选择。

- 突然发生的非法活动和网络勒索会提高交易量，造成网络拥堵；交易费不仅是矿工收入和挖矿激励，也是定价的因素，类似重复性拍卖。

5.2 比特币

5.2.1 比特币含义

基于**开源算法**产生，依托 **P2P 网络交易**，结合**点对点技术**和**密码学技术**的匿名数字货币。

特点是**去中心化**，不依靠特定机构发行，拥有**数量不限的分布式节点**，**总量限制**在 2100 万枚，可以**兑换成大多数国家的货币**。

比特币有三重含义，比特币区块链是底层技术和去中心化总账，比特币协议和用户是交易软件，比特币还是一种数字货币。

5.2.2 发行机制

本质是复杂算法的特解，产出是基于网络开源程序、解决特定数学问题的过程，是一种基于竞争记账的发行模式。

比特币系统每隔 10 分钟产生一个随机数，节点基于 PoW 算力竞争记账权和比特币奖励。这种激励机制将竞争记账和货币发行结合，解决了去中心化货币系统的发展难题，而且防止通胀。

5.2.3 交易机制

比特币钱包存放公钥和私钥，用公钥生成地址。A 公钥加密，私钥签名，B 用 A 公钥解密，计算 data 的哈希值和原来的是否一样，一样则说明没有被修改。

比特币没有单独的货币单元来表示，而是通过交易单来体现。

5.3 以太币

5.3.1 什么是以太币

以太币是一个基于交易的状态机，读取一系列输入转换成一个新的状态，从创世纪状态开始，当交易被执行后转换成最终状态，最终状态代表以太坊当前的状态。

区块结构的全局状态是由账户地址和账户状态组成的一个映射，映射保存在 Merkle Patricia 树中；以太坊每个块都有一个头，头中保存了三个 Merkle 树，分别是：状态树、交易树、收据树。

以太坊状态有百万个交易，一个区块包含一系列交易，证实新区块会得到以太币奖赏。

5.3.2 发行机制

除了开发以太坊软件外，还要发布新的加密货币和区块链，通过预售筹募资金，也催生了几个法律实体。

5.3.3 交易机制

以太坊每个账户都有状态和地址，有外部拥有账户和合约账户两种，包括 nonce、balance 拥有 Wei 的数量、StorageRoot、codeHash。外部拥有账户的 nonce 是账户地址发送的交易序号，合约账户的 nonce 值代表此账户创建的合约序号，而且由 codeHash 保存。合约账户被合约代码控制且有代码与之关联，外部拥有账户则没有。

燃烧和费用：gas Price 是愿意支付 gas 上 Ether 的数量；gas Limit 是最大数量。

交易变量包含：nonce/gas Price/gas Limit/to/value/init/data

交易过程：就是指外部拥有账户生成的加密签名的一段指令，序列化后提交给区块链。首先，需要正确的格式化 RLP 和有效的签名、序号；gas Limit 要大于使用的 intrinsic gas，包含交易预定费用、随交易发送的数据的 gas 费用、合约创建交易；发送账户还要有足够的 Ether 来支付前期的费用，包含 gas Limit × gas Price 和从发送方到接收方的总值。然后，从发送者账户余额中扣除前期费用、nonce++、交易总 gas 减去 intrinsic gas。接着，创建自毁集、日志系列、退款余额，更新子状态；最后，交易完成后，gas 的 Ether 实现传递、gas 添加到区块计数中、自毁集删除。

交易的两种形式：交易是外部世界和以太坊内部状态连接的桥梁，交易发送时，代码被执行。

- 合约创建：目的是创建一个新的合约账户，nonce 初始化为 0，账户余额为 value，存储设置为 0，codeHash 为空字符串的 Hash 值。交易不允许使用的 gas 超过剩余的 gas，否则会异常退出，状态恢复到开始前的一个点，已经花费的 gas 无法退回。初始化代码完成之后，创建的花费才会被支付。

- 消息通信：不含 initcode，包含输入和输出数据。如果 gas 不足导致交易无效，已经使用的和未被使用的 gas 都无法退回，状态恢复到开始前的一个点，并且没有办法终止。

5.4 稳定币

5.4.1 什么是稳定币

含义：私人机构发行的数字货币，通过锚定一定比例货币或资产以维持价格稳定（是法币和数字货币的桥梁）

作用：币种结余（避险、中介、结算、晴雨表）

- 资金避险：预判未来大跌趋势时，可以通过套利保值、将数字货币兑换成 UDST，以备抄底之需。
- 交易中介：两个波动性高的加密货币的交换媒介，找到价格共识和减少交易时间和成本。
- 支付结算：价格相对稳定而作为资金支付的硬通货和计价单位。
- 加密市场晴雨表：总供应量的变化代表加密市场的状态

稳定币 VS 央行数字货币（国家记账单位的数字支付工具，是央行直接负债）：发行人、安全性（主体信用）、价格波动、使用场景、离线支付（部分钱包、可以离线）、交易费用（有、无）

5.4.2 分类和机制

- 以法币为抵押的稳定币——泰达币（USDT）：全球首个以法币为抵押的稳定币；每发行 1 个 USDT，其银行账户都会有 1 美元的资金保障发行和流通。产生方式是中心化实体背书和法比抵押；特征是中心化 + 交易对手风险 + 受管制 + 高流动性 + 易锚定。
- 以商品为抵押的稳定币：产生方式是商品支持；特征是中心化 + 交易对手风险 + 受管制 + 高流动性 + 易锚定
- 以加密货币为抵押的稳定币——Dai：部署在以太坊上的去中心化组织 MakerDAO 发布，1DAI 兑 1 美元，每枚 Dai 币背后有超额 ETH 以及 ERC-20 代币担保 (如 USDC)，存放在智能合约。与 USDT 相比，Dai 除了公开审计、完全透明、去中心化之外，还给了用户和机构新的价值 (如抵押贷款，dAPP 默认使用的稳定支付手段)。价值高于 1 美元，鼓励生成更多 Dai，套利获利润，价值回归。产生方式是：以一个或一篮子加密货币为抵押。特征是：发行流通、利息费用去中心化 + 智能合约风险、无交易对手风险 + 流动性低 + 价格波动，受锚定货币价格影响
- 弹性供应的稳定币——TerraUSD（UST）：通过所在区块链上的两个代币（Luna 和 UST）相互转化和套利的智能合约（Terra 协议）来维持与美元的“挂钩”，确保稳定性。LUNA 是 Terra 公链的原生代币，价格并不稳定；UST 则是 Terra 公

链的算法稳定币，是 Terra 生态的 “法币”。维护价格稳定的机制：Luna 代币以及市场上的套利动机，通过网站上的用例和 Terra 母公司背书。UST 的初始价格与美元挂钩，1UST=1USD，UST 需求量 > 供应量，UST 价格超过 1 美元，LUNA 持有人以 1 美元汇率兑换成 UST 并出售，LUNA 被销毁，UST 被铸造，UST 供给上升，价值回归。UST 价格高于 1 美元时，不断有人购买 LUNA 来套利，UST 的供给持续上升。产生方式是锚定机制完全通过算法和智能合约调整稳定币供应量，特征是：去中心化 + 智能合约风险、无交易对手风险 + 抗审查性 + 价格不太稳定

5.4.3 风险

面临三元悖论，安全、效率和去中心化不可兼得，安全效率-中心化加密货币，去中心化效率-算法稳定币，安全去中心化-超额抵押稳定币。影响是：（商鞅稳检体校，商行、央行、稳定、监管、货币体系、消费者）

- 商业银行（存贷跨）：分流零售存款，降低资金来源稳定性；削弱乃至取代跨境支付；贷款业务削弱金融中介职能
- 央行货币政策传导（替金）：稳定币对法定货币的替代可能造成银行存款总量和结构变化，降低货币需求稳定性，影响货币乘数，削弱政策传到效率和效果；金融资产属性为持有者带来收益，削弱货币政策利率传导渠道有效性
- 国际货币体系（主权遏私结）：冲击一国货币主权；变相美元化，遏制多极化；使国家受制于私营公司的货币立场；稳定币结算会削弱法币影响
- 金融稳定（根跨挤）：币值稳定是不稳定的根源；削弱资本管制的效果，冲击跨境资本流动；遭遇挤兑时，为偿付赎回而清算资产冲击全球金融体系
- 金融监管：逃避汇率和资本管制，非法活动盛行。
- 消费者保护：数据隐私保护引发网络安全等问题；消费者可能无法完全理解稳定币的风险

5.5 数字藏品和 NFT

5.5.1 什么是 NFT

- 本质：区块链技术对非同质化数字资产形成映射的数字凭证。数字藏品区块链可以记录 NFT 的铸造和交易过程，保证交易公开和安全稳定。
- 作用：由于其不可拆分性、唯一性、可交易性，有利于理清虚拟世界权属关系；由于其稀缺性，有利于交易。

- 定义：基于区块链技术和 NFT 技术（技术）对各类作品、艺术品及有价值实体或虚拟物品（对象）生成的加密数字权益凭证（内涵），具有独一无二、不可替代、不可分割、不可篡改等特性（特点），可监管、真实可信、可追溯，能够实现数字化发行、交易、收藏和展示等功能（功能）。
- 国内与国外本质区别在于，国内：数字藏品只能通过人民币或数字人民币购买，与虚拟货币彻底划清界限，不具备资金及流通属性。

5.5.2 特征：唯一、透明、可验、不可分篡

- 唯一性：以智能合约形式发行，记录独一无二的 TokenID、资源存储地址、各项信息
- 可验证性：区块链的存储功能可以对元数据和所有权信息溯源、公开验证
- 透明性：可在链上公开查询，每个 NFT 包含最新所有权信息
- 不可篡改性：交易记录持续储存，一旦交易被确认不能被操纵或篡改
- 不可分割性：NFT 数据通过智能合约存储在区块链上，每个 NFT 都拥有固定的信息，不可随意分割

无所有权的数字藏品 vs 游戏道具：

- 所有权：自主打开欣赏使用展示 vs 中心化机构（运营方）可以随意掌控或者夺走，跑路则无法观看
- 永久性：一旦铸造永远存证 vs 会员过期得续费才能用
- 可查验：依托区块链分布式存储、防篡改特性，认购藏家可以查验信息 vs 中心化平台内数据可以篡改，无法确认是否是盗版

数字藏品与 NFT 的弱货币属性：

- 加密货币：链下资产同质化，可以无限等额分割，只需关注代币数量，无需关注质地；
- NFT：无法等额分割，需要单独评估每一份 NFT 的价值才能确定兑换比率，弱化了支付手段、价值尺度等货币属性

交易的本质：交易的不是作品而是 NFT 本身，只是一个字符串；NFT 出现使得增加数字作品交易维度，仅交易复制件（唯一性），类似于实体书买卖

- 线上使用权：仅供个人使用，同作品发布多份，获得所有权而不是版权
- 线上使用编辑权：处于个人使用目的可以利用、复制、改编
- 所有权：版权页随之转让，限量一份、单价较高

5.5.3 营销模式

- 艺术家头部 IP 合作，行业合作、活动举办，平台推广，社区自治，用户奖励，实物 + 数字藏品捆绑，社交裂变

5.5.4 铸造机制

国外以太坊公链的 NFT 铸造方式：NFT 初始化铸造者和日期，记录流转信息，数字作品 NFT 化，将作品确权和唯一化、不可替代环节：

- 获得作品的元数据：（实体作品 → 计算机存储 →）数字作品 → 元数据记录属性 → 存储到分布式文件系统、中心化服务器
- 将元数据映射上链：作品 → 哈希值（ID）→ 智能合约存储在区块链上得到作品 Token ID→ 浏览器读取 Token URL 可以看听

发行模式：

- PGC（专业生产内容）：专业知识团队或个人（艺术家、博物馆）
- UGC（用户生产内容）：普通用户

5.5.5 交易机制

- 国外 NFT：海外公链铸造、流转，采用公链支付体系，具有匿名性；也可以在交易平台交易，因强稀缺性而具有金融属性
- 国内数字藏品：联盟链、法币购买、实名交易、限制二次流转
- 交易方式：
  - 依托公链直接交易
  - 交易平台间接交易：第一类是自运营的发行平台，采取 B2C 的交易模式：平台只能购买不能交易，平台有所有权或被授予发行权；第二类是第三方交易平台，采取的交易模式主要是 C2C：可以上传或流转，其他用户可以购买，平台有服务费（gas）

5.5.6 风险：权钱市能安　漏洞缺唯一

- 剽窃发行导致的侵权风险
- 场外交易滋生的洗钱风险
- 加密货币涨跌引发的市场风险

- 过度发行导致的能耗风险
- 黑客攻击导致的安全风险
- 智能合约漏洞风险
- 数字作品 NFT 跨链不唯一的风险
- 监管、救济措施缺位风险

6　一文读懂区块链与数字资产　by 宋圣洁

区块链是计算范式变革的里程碑。提起区块链，最先想到的是比特币，那比特币又是什么？和区块链又有什么关系呢？比特币产生的价值是什么？会代替日常流通的法定货币吗？首先要明确的一点是，区块链不等同于比特币，前者是技术，后者是产品，好比工业革命电和灯泡一样，不是先有区块链后有比特币，而且为了造比特币发现了区块链，然后区块链又能用到其它地方去。

区块链从名字上看，就是数据结构的链表，也有 data 和指针。data 承载的信息是交易信息，也就是区块体，这个交易信息会记录从产生到“目前”所有的交易过程，用一个完全二叉树实现。也就是说，你拥有的这个比特币，其实只是交易信息的一个字符，并不是真的有货币，毕竟都是链上的代码，但必须用私钥签名后才能“花掉”它，从而保证确实在你拥有的情况下花掉，这棵树的 root 会在区块头记录。接着是指针，也就是区块头，要记录上一节点和本节点的哈希值，哈希值就是 ID，或者说是索引；也记录了挖矿随机数，就是一个函数映射后的 y，但需要你找到 x，在你不知道函数是什么情况下，只能暴力求解，你花了多少算力去求解就是干了多少活，也就是工作量的证明；区块头还记录了时间戳，就是区块产生的时间，就是什么时候被挖出来的，即这个随机数什么时候被解出来的；当然，如果我找到了窍门，不小心一下子解除了四五个怎么办？于是还会记录一个难度，通过调节这个难度（或者说这个映射）来确保它不会贬值，你没法走捷径。这就是区块链记录的东西。我们后面都要用到这个区块链架构来分析。

听起来好像也不难，因为咱们只了解了数据结构，了解它的本质得从产生背景开始。比特币产生是基于一个想法：为什么货币发行和交易要通过银行？有没有一种货币不需要银行，还能被大家认可，并且保证安全可信呢？于是区块链天然就富有四重责任：去中心化，就是链中的每个节点高度自治，自由连接，每个节点都能成为阶段化的中心但又不能控制（必须承认中心化的好处，去中心化不等于否定中心化）；不可篡改，可追溯，由于没有中心化机构，自己控制的节点可以修改但不能修改别人的，但其他人的节点中也保存着你的信息，要想修改就要控制 51% 以上的节点，但这很难发生；交易透明，双方匿名，你可以看到别人的交易信息但不知道是谁，信息公开又保密；开放，共识，没有门槛，大家都可以来，但要承认一套规则制度，使得都有动力来维护这个区块链，有节点不想干了，也不影响其他人的工作。由此，区块链的定义就呼之欲出了，区

块链就是一个用链式数据结构验证和存储数据，通过共识机制来维护和更新数据，通过密码学来保证安全，利用一系列代码来自治的大型计算机制。不过区块链现在也延伸出了一系列代名词，象征着共识、信任、共享等。从区块链等同于货币，到开放式平台，再到赋能实体经济，提供的去中心化方案正在走入每个人的生活视野。

正如新能源汽车不一定要全油，也不一定全电一样，前面说的区块链只是一个基础信息架构，它的优点可以拆开来使用，这就产生了区块链的分类。当我想使用区块链的全部优点，如去中心化、公开、透明、各节点自由平等参与、无法篡改、基于共识，就产生了公有链。放松假设，放弃一些自由平等参与、公开透明，就是联盟链，它的公开程度有限，仅限联盟内部，并且读写和修改权限分开。再放松一下，就是私有链，可以只在公司内部使用，强调私密性，不可篡改但可追溯，比如财务数据，编辑仅限于某些人，但都可以读取。当然，由于解一个数难度很大，因此公有链的计算效率很低，随着公开程度减弱，计算效率也在加快、成本变低。

6.1　区块链的分层架构

区块链是一门技术，在实践中不单单是一个链表那么简单，就好比电不是九年级学的电流电压那么简单，而是一个复杂的系统，包括了数据层、网络层、共识层、激励层、合约层、应用层。

数据层就是储存数据的，也要保证数据的安全。存储通过链表实现，前面说了，区块头存哈希值和上下区块链接，但是哈希值是可以变的，本区块有内容更新，哈希值也会更新，上下区块都会更新，这样只要看哈希值就能知道是否被篡改，区块体存储了交易信息，这个二叉树也是哈希的，通过判断哈希值可以快速校验大规模数据的完整性。安全通过哈希函数和密码实现，哈希函数说白了就是把不定长的东西转化为一串定长的数，来唯一指代这个东西，只需要验证哈希值就可以判断是否被篡改，而且这个哈希值很难被破解，因为只有完全相同的输入才会产生完全相同的输出，否则有一点不一样，整个哈希值就不一样。传统上，我们自定义一个密码去传播数据，但是缺点是需要提前告诉别人这个密码是什么，否则别人解不开，而区块链应用的是非对称加密，也就是有公钥和私钥一对密钥，分别是公开的（不是都知道，而是可以告诉别人的）和自己知道的，公钥加密私钥解密，获取数据价值，私钥签名公钥验证，确保数据没被篡改。

数据有了，怎么传输传播呢？区块链并没有给出一个创新的模式，应用的还是传统网络标准协议，比如 TCP/IP 或者 UDP 协议，采用 P2P 传输技术，实现节点之间的数据交换。因为这个技术已经满足了区块链的要求，就是没有中心服务器，每个节点既可充当节点，又可充当服务器，资源分布在所有节点上，传输直接在节点之间运行，而且 P2P 天然耐攻击、高容错，即使一个节点被攻击，其他节点也能够正常工作。

前面的想法很美好，像一个大同社会，但难免会出现一些问题，比如怎么保证每个人都有动力去记录信息呢，如果断网了如何确认数据，再比如自己写代码去攻击呢？这就涉及到了共识层和激励层。共识层就是在出现一些问题的情况下，网络各节点还能达成共识，里面封装了一些算法去认定哪些数据有效，防止冲突和篡改。激励层说白了就

是给钱，除了新挖出来的区块链直接给你外，如果你不想要了想用这个币做交换，手续费也是可以进行流通的。这个是封装在智能合约（合约层）里面，智能合约可以拆分为智能和合约两个方面，智能就是自动执行，合约就是规则，智能合约可以识别场景、根据提前定义好的规则去触发激活，通过一系列代码实现，这些代码也存在于去中心化的脚本上，通过 P2P 分发到各个节点上。

最后就是应用层了。我们最先想到的是比特币，我们后面会讲到数字货币的发行、分配、调节机制，以及基于比特币的基础设施、交易平台、ICO 融资和综合服务。区块链和金融结合，可以降低交易成本，提高交易效率，更重要的是能够提高数据安全，比如跨境交易中往往要借助第三方支付公司，如果使用区块链的话就没有这么多麻烦。再比如保险，可以根据个人健康状况进行信息识别判定，降低核保成本。到了社会层面，应用就更多了，比如病人自己掌管病例，拿着这个信息直接跨医院就医，解决文化娱乐的产权保护问题，公益税收服务中追踪回溯，等等。

6.2　区块链技术原理

区块链底层原理架构主要是三部分，加密算法保证安全性，共识机制保证状态以致，智能合约让区块链更有活力。这三部分组成金三角，就是区块链的特殊技术。

密码是为了让传输的东西中间不被第三者破译，发现里面的内容，现代密码学有了更深一步的要求，不仅要求数据是安全的防攻击，还要求完整性可以验证（数字签名可以实现），而且不可抵赖，这催生了哈希算法和加解密算法。哈希算法前面已经讲述过，特点就是根据一组输入生成一个哈希值很快速，但是给一个哈希值倒推原像很困难，并且任何输入改变哈希值都会产生很大的变化，很难找到两段内容不同的数据使得哈希值一致，也就是找到假的消息去匹配或者替换都很困难，原数据加密后拆开只能是原数据，可以认证，相当于一个数字指纹，一一对应。现在著名的在用算法有 SHA 系列哈希函数，具备比较强的安全性。另一种就是加密解密算法，这个算法是不变的，而且公开可见，变的是密钥，需要妥善保存，每次密钥都需要重新生成。传统加密算法要求提前共享密钥，加密解密用的密码是一样的，好处是比较快，而且加密强度可以很高，而且密钥一般小于 256bit，空间占用也比较小；相对应的，非对称加密就是加解密密码不同，这意味着加密就要分为公钥、私钥，公钥随机数算法生成，比较安全的算法有椭圆曲线、质因数分解、离散对数问题，私钥一般其他人不能获取，这样解决了加密提前分发密钥的问题，但是处理速度比较慢，处理流程简单来说就是公钥加密，私钥签名，公钥解密验证。对称加密通常用于大量数据的加解密，非对称加密用于签名场景。

共识机制说白了就是要达成共识。这是一个很复杂的事情，区块链是一个分布式架构，多个主机之间通信存在错位，需要进行状态复制才能达成共识，就是说网速不一样，同一时刻接收到的信息是有些许差别的，但连上网之后所有的状态应该是一样的。这需要定义一种容错机制，每个人都不吃亏，或者是达成安全可靠的共识，让自己的账本和别人的达成一致。那为什么说这个是区块链的独有问题呢？仔细分析这个问题，就会发现，问题出现在不知道找谁作为基准，最终的复制状态听谁的，而在传统上，你如果断

网了，一系列操作应该是无效的，连上网就直接向中心化服务器看齐就行了，人家是啥你这里就是啥。所以要解决的问题就是：听谁的，如何保证听谁的。问题再进一步转化，就是怎么筛选出这个人。平常在选三好学生会筛选学习成绩、综合品格之类的标准，那么区块链这里就是也要选一些标准，比如谁挖矿挖的多也就是谁更有钱，比如你干了多少活也就是工作量证明等等。综合上述，共识机制就是在有故障节点、遭到恶意攻击、恶意节点多等可能造成状态不一致情况下，定义一种容错机制，筛选出安全可靠的节点，来让分布式账本达成一致。共识机制分为两种，一种是授权共识机制，必须通过密码认证身份后才能参与；另一种是非授权共识，节点可以随时进退，数量动态也不可以预测，主要是通过特定算法选出出块者（就是可以更新这个区块链的人）并验证更新。工作流程是选出出块者，生成这个新的区块，再广播给区块链其他人。

先来解释几个概念。状态机复制就是所有节点维护一个线性增长的日志并且一致，具有一致性和活性；公共账本就是任何人都能读取的公告牌，也具有持续性和活性；网络模型分为三种，同步网络就是大家进度都一样，部分同步也是常用的网络，就是某些情况一样，异步网络就是恶意节点可以拖延但是最终信息能够达到，腐化模型又分为三种，静态敌手是在协议前就选定目标，把这个目标变成敌手，协议运行期间敌手能够控制的节点数量不变，t 温和敌手意味着腐化需要时间 t，这个时间段内节点还是诚实的，但之后就变成恶意的了，适应性敌手最强大，随时动态腐化；区块链还会设置敌手模型，当敌手控制过一半多节点就可以操纵了，但这样计算量比较大，一般三分之一或者四分之一的模型设置，防止敌手达到控制这么多节点。那接下来就看几种机制如何做到共识的。先来明确几个评价的标准，首要的是安全性，在敌手存在并且操纵一定资源情况下，诚实节点仍能够达成一致；交易吞吐量，就是单位时间能够进行的交易操作，受到区块大小、区块间隔、网络延时问题；可扩展性，就是当节点增多时处理能够也应该相应增长；交易确认时间，就是从交易发出到共识网络，到最终确认所需要的时间，需要保证这个过程中信息不会被篡改或者分叉；去中心化，不能借助于可信的第三方或者少数几个节点，权力要分散化；资源占用，就是时间复杂度和空间复杂度不能太高。

第一种是经典分布式共识机制，主要是在授权网络中实现状态机复制，保证安全性和活性，最典型的是部分同步网络，采用拜占庭容错协议不但能容忍崩溃节点，黑能容忍敌手控制的恶意节点，因此主要面向分布式数据库系统。这又可以分为三种情况，在部分同步网络中，主要是达成共识和试图转换，先选一些节点来提交交易信息，如果相同信息达到节点数量一半以上，就达成共识广播出去，否则继续加入直至达成节点要求，为了降低储存成本，检验完的相同数据会删除保留数据和一致的节点数量，还有消息验证码保证安全；在异步网络中，不是对一系列交易信息一起看有多少节点是一样的，而是每次挑一部分数据来看哪些数据是可以达成共识的，不断迭代直到整个交易数据信息是可信的；同步网络中就是直接投票选择。

第二种是授权共识机制。主要用于企业组织联盟中，能够实现较高的交易吞吐量，由于是大数据之间的存储，需要考虑智能合约的处理问题。说白了就是三个阶段，执行、排序、验证，加入到授权网络中的节点先汇总信息给选好的背书节点，通过拜占庭容错

后再交给排序节点，进而广播给区块链。

第三种是工作量证明的共识机制。这也是比特币比较明显的一个特征，就是根据你的工作量多少，也就是每个节点的计算能力来竞争记账，PoW 就是做过一定工作量工作的证明，也就是解函数值的一个过程，要素包括工作量证明函数、区块和难度值，分别决定了计算方法、输入数据和计算量。这个区块怎么算出来的呢，就是 merkle 树的每个数据先哈希，父节点把子节点的哈希值累加再哈希，迭代得到根节点的哈希值；难度会调整，保持在 10 分钟产生一个新的区块，目标值和难度值成反比，因此工作量证明的寻找的哈希值要小于目标值。这个计算过程显然要消耗很大的算力，会带来很大的能源消耗；还存在三种攻击，日蚀攻击（攻击者先占据目标节点的网络地址，把这个地址换成其他东西，这个地址重启后很大概率变成敌手控制的节点）、双花攻击就是代币持有者在交易完成后分叉一条更长新链，使得原来包含这个交易信息的链作废，拿回自己的代币、自私挖矿就是发现了一个区块之后先不公布，等到别人发现再公布时候把自己挖到的这个拿出来，由于自己的链一般会更长，另一条就失效，浪费诚实用户算力。

第四种是基于权益证明的共识机制。就是谁有钱，谁记账，但也不代表首富垄断，好比存银行会有利息，如果把余额拿来签名的话就会清除掉币龄，等到 30 天后才能签另一个区块，并且挖到下一个区块最大概率在 90 天之后。

第五种和第六种是混合共识机制，把经典分布式和区块链的共识机制结合，选出委员会来达成共识。单一委员会就是根据工作量或者权益证明只选一个委员会，然后选出领导者，运行分布式一致算法和拜占庭容错协议，再广播区块，一段时间之后要重配置委员会。这也产生了一些问题，比如创世的第一个区块怎么办？重配置过程中如何确保安全？新节点加入和分布式一致性算法如何确保运算效率？这就产生了三种分片方法，一种是根据通信分片，直接瓜分全网；一种是计算分片，看 id 末位是多少就分配给第几个委员会；再就是存储分片，用专属的交易链来运行。这样产生的多委员会机制和单一委员会机制的区别就在于，可以防止敌手影响成员分配，跨片交易时防止双花攻击，广播区块时不存在全局的区块链。

智能合约就是一堆代码，能把提前约定好的规则在满足条件的情况下自动而不需人为执行。它可以自动一次性触发和执行，里面封装的代码很强大，可以发行资产也可以花掉这些钱，并且不需要依赖某个服务器可以分布式执行。可以看出，它的最大特点就是自动化，但也有缺点，并不是所有条件都可以写成代码的，所以智能合约更适应客观性请求并且成本较低，并且可以用数字资产。比如说，以太坊上的智能合约就是一个特殊账户，比普通账户多了代码和状态，一般的账户只有谁收钱、谁汇钱、多少钱，而以太坊的特殊账户除了价值传递之外，还可以创建合约、调用合约，本质就是调用 if…then…。智能合约的应用范围很广，比如法律追索，为了防止参与的当事人不履行，可以设置智能法律合约；应用在区块链社区治理上，可以通过代码来约定规则，即使程序中断也能执行获得追索权，这实际上成为了一个去中心化自治组织，可以协同监管；广泛的社会层面，你可能听说过物联网，其实就是区块链的智能合约代码赋能，与设备通信并验证。智能合约的优势很明显，由于无需处理文书，根据状态自动填写因此速度效

率精确度都比较高，加密算法还有分布式账本使得安全性也比较高，去中心化没有中介机构还节约了成本。当然，正如前面的比较，智能合约由于太安全而不能篡改，这也导致如果有安全漏洞也很难修复，并且一些主观性的场景如果没有外部的很多信息来量化的话，也很难实现，当计算复杂度上升时，效率也会降低。

6.3　区块链的应用

这一部分来讲两个区块链的应用，让区块链活起来。

第一个是供应链金融。传统的供应链包括从采购原材料，加工，包装到卖给用户的全过程，是涉及资金流、信息流、物流的复杂系统。随着社会的发展，产业模式走向网链化，各个企业你中有我我中有你，而中小企业对资金有着更迫切的要求，按照传统投资理论，这种企业面临的风险高，因而要求的投资回报率就很高，借贷利率高，于是迫切需要一种金融模式，能够把企业的现金流运用起来融资，这样银行也能够丰富产品，把握更多的客户并且资产证券化中提升风险管理水平，物流管理上也能够增添增值业务，于企业于银行于社会都有利。我们说金融主要考虑风险和收益，那供应链上哪些东西可以证券化，谁来承担这些风险呢？我们发现供应链涉及的是上下游交易，那就有欠钱和还钱，把这些应付账款和应收账款给用起来，这条链上总有一个大企业，可以支撑起整条链上的信用，就可以利用核心客户来保障。金融赋能实体经济无非就是借钱和还钱，供应链用的这些账款还有实际贸易保障，未来极大概率还本付息，实现自偿。应用区块链的供应链金融，可以针对性服务单个企业，但风险评级可以参考整个供应链，不一定用核心资产质押，银行承担风险更小，可以设计更多的产品，提供持续的信贷支持和持续竞争，降低供应链的运作成本。区块链如何应用到供应链金融之上呢？回到区块链的特异功能上，就是去中心，多节点，可追溯。所以可以实现多主体合作，提供了平等协作平台，降低风险和成本，链上信息可追踪不可篡改，可以实时同步对账。另外，本来供应链上智能对应自己直接相关的企业，现在间接的企业也可以对接了，相当于扩大了点对点服务范畴。前面也说了，可以把账款数字化为证券，然后这些证券可以分割以提高流动性，获得现金流支持，降低企业负债率。整个流程区块链实时监管，减少人为操纵，确保信用强链接和实时监控。

另一个应用是数字票据。我们先来回顾一下什么是票据，票据就是凭证，由于在金融领域讲到这个东西，就要带有流动性可融资的特点，也就是本身给钱 + 金融流通双重功能，而且往往是企业和银行信用比较好的。由于其本身的支付功能，就意味着票据一旦签订，重要信息不能更改，又由流通功能，转让之后也不能撤回。票据主要是银行承兑汇票，银行独立风控，当然也会影响其他主体。票据的流通转让主要有：本身汇票能够由企业申请，银行承兑，依赖真实贸易背景，银行可以通过手续费赚钱；进一步，票据可以提前贴现，利息由第三方支付或者自己支付都可以，这个利息率就是控制贴现的；银行手头有了票据之后，可以去央行换钱或者央行直接买，投放流动性释放资金，是货币政策工具，可以调控货币和信用。票据是信用的浓缩，可以融资来配合产业政策，也是利率传导工具之一，推动实体经济发展和控制风险。

前面说了票据是支付 + 流通，数字票据就再加上数字，这里数字可以是大数据，也可以是区块链，对票据资源配置创新，实现信息识别、选择、过滤等。于是我们总结一下数字票据的特点，十二个字，科技透明监管、标准交易服务。科技是用新技术手段赋能业务处理分析、客户认知和风险识别；透明的是交易主体、信息、效率，是全方位的信息；监管是全流程的监管，分析市场参与者业务行为和人工智能干预违规。标准涉及业务规则、数据统计、信息采集加工传输共享，交易创新可以是资产证券化、资产合理定价和交易创新，服务创新就是模式上重构传统票据业务，释放生产要素价值。

与电子票据相比，数字票据不需要中心化服务器，也不需要中心级应用，可以降低开发、维护优化成本，也能减少系统中心化的风险和反复被记录保存的成本；时间戳也可以保证数据的完整性、透明性，有利于形成信用和降低违约后无人知悉的可能性，也更容易对票据流转进行展示和控制，防止重复抵押和合伙做案。区块链可编程和可控制也可以根据使用者灵活设置买入买断和避免违约。

传统票据有贸易背景造假、一票多卖、背书不连续、审核成本高等问题，区块链可以去中心化，不需要隐藏的第三方来确保数据安全可靠，也不需要第三方来监督和验证，解决点对点问题，票据中介会以参与者身份重新定位；区块链会改变电子商业系统结构，不需要通过央行的存储和资源交互平台，时间戳可以进行追溯历史；防范市场风险上，由于不可篡改的时间戳和全网公开特性，可以防止赖账，防止道德风险，区块链的加密算法可以降低操作风险，实时监控和信用评估可以降低信用风险，区块链可编程性可以控制资产负债平衡，准确反映需求，降低市场风险；另外，通过编程控制价值流转方向，实现货币政策对点投放和不可篡改的时间戳，可以降低监管成本，规范市场秩序。

应用场景上，承兑环节实现了非中心化出票，减少网银中介，解决参与者的信任问题和保证信息安全；在流转环节，免去了中心化系统的信息流转，实现了点对点交易，也可以有效避免各类风险，保证交易公平和价格真实；在托收环节可以直接完成价值交换，确保账实相符。

6.4　数字资产

还是先来破题，什么是数字，什么是资产？数字就是一堆符号，也是一种表现形式，数字资产就是资产的数字化。数字资产又和数据资产不同，数据是一堆信息，可以加工为各种有用的分析材料，是一种生产要素，也是一种资产，但数据本身是客观的逻辑归纳、是观察的结果。资产是一种权利，预期这种东西可以取得收益，这种东西还必须是你所有，在过去取得而不是预期会取得。综上，数字资产就是私人拥有的，电子形式存在的，持有以备出售或者在生产中的非货币资产。数字形式简单来说就是二进制形式，密码学保证，价值可以计量。

数字资产和数据资产的区别可以从一下几个角度区分。从定义上，数据资产是创造价值的数据资源，数字资产是可以交易的虚拟资产；从价值上，数据资产是间接价值，数字资产是直接价值；从形态上，数据资产可以内部交易，有结构化和非结构化两种形式，数字资产是可以任意去中心化交易的；从管理和控制权上，数据资产可以内部管理，

数字资产可以任意审查。当然，数字资产也可以是链上的数据资产，实现更广阔的价值。

数字资产和数字货币区别在于，数字货币流通后、具有投融资功能后，可以转化为数字资产，数字货币可以取代有形货币，但数字资产只是经济体的一部分。货币发行完全取决于当局，而数字资产取决于供求。

数字资产的特点是，它是一种商品，有使用价值和价值；是一种无形资产，存在安全风险；可以保值增值，被赋予新的内涵；可以长期重复利用，永远存续；是一种生产要素，具有所有权和使用权。从内涵来看，它以比特形式呈现，是一种数字代笔，不需要认为处理，实现去中介的点对点交易，内涵也在不断扩展，但也存在权属未定的问题。它的分类主要有内容和形式两种区分，内容就看用在什么地方，形式分为结构化和非结构化。

数字资产是如何交易的呢？两种，一种是基于区块链，一种是托管。区块链的交易方式主要是主链注册，辅链交易：采用二维平面模型架构模式，将数字资产的登记与交易进行合并，能够同时在两个维度上同时记录不同类型的数据。区块主链负责记录不同作品的登记信息，进行资产注册，区块辅链记录每个数字资产的交易信息。区块主链是由作者、登记平台和底层区块链三种不同的角色共同参与，通过注册流程机制对用户提交的数字资产进行注册。再设立一个独立于用户和登记平台的第三方 CA 证书机构，这个机构向参与到注册过程的用户和平台颁发密钥并负责日常密钥的维护工作，保证用户提供信息的安全性和避免后续操作过程中发生用户抵赖。数字资产交易区块链：卖方是资产的提供者，买方是数字资产的交易目标对象，交易平台是一个信息化的市场，为买卖双方提供信息交换渠道，方便卖方发布资产信息，为买方提供了更大的选择范围，底层架构是所有交易信息都需要转换为区块节点形式记录在交易区块链。另一种托管方式，经托管后的数字资产可以由购买方认购，一经确认卖者无权知道买者是谁。

数字资产未来发展趋势，可以成为一种新的金融投机资产，也可以提供各种就业岗位。但由于是新型的东西，它的合规性、安全性、专业性受到挑战，没法给一个与时俱进的法律，又怕根据现有的去约束会制约创造性，缺乏交易规则，这就给利用去中心化、匿名跨国的洗钱和恐怖主义融资提供了可能。

6.5　数字货币

最后终于来到了压轴的数字货币，这是区块链和数字资产结合的产物，前面我们说了，区块链是数字货币应用技术，当数字货币融通的时候就成了数字资产。所以我们可以说数字货币就是用分布式账本技术实现的非实物货币。

数字货币不是电子货币，也不是虚拟货币。它的发行主体和适用范围都是不限的，理论上任何人都可以发行数字货币，但是是否受到认可就是另一回事了。而且它的发行数量是一定的，一般可以通过某个通项公式求出来，那你可能会问这不就和古代的石头和黄金一样，如果不够用了咋办？前面我们讲激励层的时候说过，除了货币奖励还有手续费，手续费就是当货币一定时，仍然可以让经济体循环起来的工具。另外，数字货币和其他货币不同在于它是数字形式呈现的，交易安全性笔记较高，成本比较低，运行网

络依赖于 P2P。

数字货币的发展也经历了一个过程，从单一中心化到多中心化，再到去中心化，从锚定黄金发行到解决货币重复支付难题，从比特币到山寨币。那到底是数字货币哪些迷人的特征使得它受人们追捧呢？除了区块链去中心化、可追溯、匿名性的技术特点外，这种数字货币还有超主权和总量一定的特点，这就给炒作带来了机会。

数字货币具有流通货币和资金融通的功能。流通货币主要强调的支付功能，数字货币是一种弱货币，能够使劳动和知识交换成为可能，可以缩小贫富差距，但也会对实体货币市场冲击，比如降低对实体货币需求以致于央行要多发货币来保证币值稳定，也会对商业银行的存贷款冲击，挤出存款。资金融通属性主要强调它的风险和收益，有的数字货币的发行本质是众筹，就是先攒钱再发行，这受到监管水平的影响，避免成为泡沫。

任何货币的运行都要考虑如何发行、如何定价、如何交易的问题。数字货币的发行也就是诞生，类似于股票发行，称之为 ICO，要想提高发行成功率也得路演，主要是依靠白皮书，也可以理解为一个说明书，会披露项目的主要信息和源代码，但这种传递也会带来信息不对称问题，造成投资者的失望情绪和数字货币贬值。在中国限制数字货币运行，这种宏观政策不仅影响本国还影响外国的发行积极性。发行者自身的特征也会影响发行成功率。总结一下，就是这个货币机制公开的全不全，发行者自己好不好，宏观环境允许否都会影响发行。因此，发行可以依靠国家信用、依靠算法、依靠资产，总要锚定点什么，而不是画大饼。

定价上，主要考虑哪些因素能够影响价格。除了最基本的供求外，还要考虑宏观微观因素，宏观主要是资本管控、相关资产的波动、人民接受程度和社交媒体传播；微观主要是投资者关注和交易动量，以及工作量和权益证明机制的影响效率。货币的安全性、受到非法活动影响的程度有多大，还有锚定的资产价格都会影响数字货币的价格。和其他资产一样，它的价格也可以通过机器学习、深度学习等算法进行预测。

交易的设计上，非常依赖共识机制。在工作量证明共识机制下，谁算力大，谁解题效率高，谁就拥有记账权，随着比特币炒作价值越来越高，算力不断攀升，消耗的人力物力财力资源也越来越多，这种机制是不可持续的，于是有人提出权益证明，就是谁有钱谁记账，但“谁”会更换，研究证明由于投机者最优决策，不会造成代币的垄断。另外一个问题是交易费过低，会导致某一段时间内交易过于密集，造成系统拥堵，即使改进交易排序和缩短区块间隔也很难优化。所以提高交易费就是一个比较可行的路径，交易费不仅是一项激励矿工的收入，还是可以对记账权进行定价，相当于一种拍卖，谁给的交易费高，谁有权争取上链，博弈这个交易费过程，可以改善交易机制。

我们将通过比特币、以太币、稳定币、稳定币、数字藏品四个例子来说明数字货币。

比特币是一种数字货币，具有去中心化、点对点交、、分布式节点、密码学保证安全、匿名、开源、数量一定的特点，甚至可以兑换成大多数国家的货币。比特币是一种货币，也是一种技术、协议，描述数字资产的转移过程。从发行机制来看，就是解一堆算法的特解来竞争记账，获得比特币奖励，奖励每四年一个半衰期，从 50 枚到 25 枚，依次递减，使得比特币数量一定，防止通胀。交易机制就不说了，前面讲过很多次了，A

公钥加密私钥签名，B 用 A 公钥解密验证哈希是否相同，相同则说明信息没有被破坏而且价值转移有效。比特币虽然是数字货币，但又没有给你发一个凭证或者票据，而是通过区块上的记账单呈现的，交易账单上有你的交易就说明你有多少货币。

以太币本质是一个基于交易的状态机，代表着读取新的输入后的最新状态，相当于用代码去更新账户。以太币也是区块链的应用，所以也是区块相连，只不过这个区块有地址可以索引，有状态可以查看，这些状态封装在 Merkle 树中，区块头包含了三个 Merkle 树的节点，分别是状态树、交易树和收据树。以太坊有百万个交易，这些交易由智能合约产生并封装在区块中，每被证实一个区块，就会得到以太币作为奖励。也就是说，以太坊是发现动态出现的块后奖以太币，比特币是答对题给比特币，以太坊是平台，以太币是一个衍生品，这意味着设计其他机制也可以在以太坊上诞生其他数字货币。从发行来看，以太坊通过公募来募集资金，也催生了一系列法律来支持开发。

从交易来看，以太坊全局状态由很多账户组成，通过消息传递来交互，每个账户对应一个地址索引和一个状态来识别。账户分为两种，一种是合约账户，一种是外部拥有的账户，账户的 nonce 值中，前者创建合约序号，后者发送交易序号；balance 是拥有的 Wei 的数量；StorageRoot 是根节点的哈希值，codeHash 是以太坊虚拟机的哈希值，合约账户有代码关联，外部拥有账户是空值。每次的交易费由 gas price 和 gas limit 构成，price 可以理解为每个 gas 的愿意花费，limit 是愿意支付多少个 gas，乘起来就是交易费用。交易过程首先要进行验证，先认证身份，也就是验证签名，还有交易序号格式是否合法，然后验证你的 gas limit 是不是比内在价值要大，内在价值包括交易预定费用、创建合约费用和 gas 费用，前两者是固定的，第三个是可变的，账户的发起方必须拥有足够的以太币来支付 gas 费用，除了交易费用外，还有 value 也就是发给对方的价值，毕竟我们是在交易。验证完成后，首先从发送者中扣除交易费用，nonce 值增加 1，然后执行交易，以太坊会生成一个自毁集（交易完成后自动销毁）和一个日志系列、退款余额（以太坊的存储也要付费，发送者清理了内存就会有退款），交易完成后，退款给发送者，value 给接收者，交易的 gas 添加到区块中，自毁集删除。

交易总是由外部世界触发，这不意味着内部世界无法传递价值，而是会通过触发合约来进行。交易的目的是为了创建一个新的合约账户被称为合约创建，先对账户的 nonce、value、存储、codeHash 进行初始化并设置为 0，使用 init code 作为序号就创建了一个账户，交易不允许使用的 gas 超过剩余 gas，否则就会异常退出，异常退出花费的 gas 不会退还，但是发送的以太币 value 会退还，如果初始化完成合约就会创建，存储成本和创建花费就会被支付。另一种交易是消息通信，不包含 initcode，但是包含输入输出数据，同样的，过程中交易无效或者 gas 不足的已经支出部分不退还，毕竟程序运行了，但状态会恢复到余额转移前的点，而且没有办法在程序开始执行后中止它。

稳定币是通过锚定某种资产来维持价格几乎不怎么波动的一种数字货币。由于不波动，可以用来支付、避险、作为价值交换的中介，它的供应量变化也可以作为加密货币市场的晴雨表。它和央行数字货币相比，范围上仅适用于加密货币，部分情况支持离线支付并且易受冲击。目前，市场上有以法币、商品、加密货币抵押的，还有算法稳定币，

它们的中心化、管制和流动性风险不同，价格波动也不同。

USDT 以法币为抵押，1 美元 =1USDT，用户将美元存入发行者 Tether 公司账户，然后 Tether 会为用户开户并存入相应的 USDT，用户可以自由交易，也可以赎回法币。简单来说，就是受限不同的美元。

Dai 以加密货币抵押，背后以 ETH 和 ERC-20 代币作为担保，除了公开审计、公开透明、去中心化外，还可以用于抵押贷款，当 ETH 价值下降时，也会销毁一些 Dai 来保证币值稳定。Dai 可以自由兑换美元，当 Dai 价值高于或低于 1 美元时，会有很多人套利，使 Dai 价值回归 1 美元。用户将担保代币存入智能合约后，可以创建和提取 Dai，但不是 1：1，而是可能 1.5：1，比如存入 1ETH，价值 100 美元，就给你 100+100/1.5=166Dai，多的这 66Dai 跟借钱一样，要缴纳利息。MKR 是这个项目的治理代币，当贷款者没有清偿就会以潜在贴现率清算抵押品。MKR 用于利息和清算，当缺乏抵押品时，合约就发一个 MKR 折价出售，激励用户投票 MKR 的抵押率、清算率等然后购买或者赎回 Dai，清算完成后燃烧 MKR，由于 MKR 产生和消亡会影响 Dai 价格，而用户们随时面临抵押不够而自己拥有的代币价值下降的风险，因此系统中每个主体都有激励来保证系统稳定。

UST 是算法稳定币，它和 Terra 链上的 Luna 共同维持价格稳定。1UST=1USD，当 UST 供大于求的时候，UST 价值会小于 1 美元，UST 持有者可以以 1 美元价值铸造回 LUNA 出售获利，反之，套利机制使得 UST 稳定。从加密货币设计来看，存在安全、效率、去中心化三元悖论，比如算法稳定币，去中心化发行并且效率高，但很难抵御投机，难以达到安全目的，一旦市场信心崩溃，价值会大跌。

这些货币当然会影响商业银行存款、贷款和跨境支付主导地位，也会影响央行存款和货币乘数，影响金融系统稳定，削弱国际货币体系中法币的作用，冲击货币主权，造成系统性金融风险。

最后来看一下数字藏品，为什么说这也是一种数字货币呢？它不就是一个数字化的艺术品吗？先从数字藏品的分类说起。有的藏品是有限复制，买到的是线上使用展示权，还有买到的是基于个人使用目的的线上使用编辑权，很少是直接买到这个设计的所有权。区块链可以保证交易的安全性，对产品进行追溯确权，也就是说，其实买到的是一串字符，而不是作品，区块链可以保证唯一性，将数字作品复制件的所有权交易。而数字藏品有性状，每个藏品价值不同、不同时刻价值也不同，也就是非同质化的，因此在价值确认时面临每次用 NFT 交易都要重新确认价值，而且价值不可分割的问题。综上，数字藏品是用区块链技术对虚拟物品的一种凭证，独一无二、不可篡改、不可分割，可以验证、公开透明。

数字藏品和其他虚拟道具有什么区别呢？比如视频网站会员，只是拥有一段时间的使用观看权，而且随时出个公告说版权问题下架或者延期更新你也没有什么办法，或者给你看盗版，而数字藏品则满足可查验、永久性和所有权。

从发行铸造看，需要将作品映射到联盟链上，目的是使得数字作品唯一化，需要对作品的元数据进行中心化存储，然后生成哈希值来保证唯一性，这个哈希值就是作品的

ID。有的发行平台会邀请创作者生产，也有的会鼓励用户生产。从交易来看，使用公链的支付体系因而具有匿名性，由于数字藏品具有唯一性因而也具备金融属性。我国国内只能允许人民币购买，限制流通且实名购买，因此在我国不具备货币属性。交易可以通过公链直接交易，也可以通过平台间接交易，但会收取手续费，也有智能买不能卖的，这实际上是著作权人借助平台进行发行出售。相关风险主要有，把别人作品上链的侵权风险、用来圈钱洗钱、价格波动剧烈的市场风险、过度发行的能耗风险和黑客攻击的安全风险，也存在漏洞和监管缺位风险。

以上就是区块链与数字资产的几乎所有底层逻辑和核心内容，由于是一门新的技术必然存在不完善的地方，我们期待区块链成为价值物联、信用去中心化的关键工具。

参考书籍：

- 《区块链：从数字货币到信用社会》
- 《链接未来：迎接区块链与数字资产的新时代》
- 《区块链：通往资产数字化之路》