**区块链进阶调研**

任务：了解实际工程领域的区块链技术，扩展本实验中区块链的分布式、安全性等能力。

# 一、实际工程中的区块链技术

Localhost:5000/chain

## 1.1 区块链技术的原理

当下区块链技术涉及四大技术领域，分布式账本技术、非对称加密技术、共识机制技术和智能合约技术。

分布式账本（Distributed ledger）是一种在网络成员之间共享、复制和同步的数据库。分布式账本一起记录参与者间的数据行为（如交易、资产交换行为等）， 而共享机制降低了“因调解不同账本” 所产生的时间和成本。

非对称加密技术即存储在区块链上的交易信息是公开的，但每个账户的身份信息是高度加密的。单个账户只有在拥有者授权的情况下才能访问到，从而保证数据的安全和个人隐私。

共识机制技术即开发者必须首先考虑用怎样的技术可以使更多人对一种规则达成共识，同时还要考虑通过多少个特殊节点的确认，才能在很短的时间内实现对数据行为的验证， 从而完成一笔交易。一般而言，区块链技术需要若干利益不相干的节点对一笔交易进行确认，如果确认就认为达成共识，认为全网对此也能达成共识，这样才算完成一笔交易。

智能合约技术指基于大量可信的、不可篡改的数据，可以自动化地执行一些预先定义好的规则和条款，比如彼此间定期、定息、定额的借贷行为。

其中共识算法和分布式存储为区块链的核心。[1]

### 1.1.1 区块链共识算法

#### (1) 区块链共识过程的基本流程

区块链建立在P2P网络之上，全体节点集合记作P分为生茶 数据或者交易的普通节点，以及负责堆普通节点生成的数据或者交易进行验证、打包、更新尚联登挖矿操作的“矿工”节点集合（M），两类节点可能会有交集；矿工节点通常全体参与共识竞争过程，在特定算法中也会选举特定的代表节点、代替他们参加共识过程并竞争记账权（D）；通过共识过程选定的记账节点记作A，共识过程按照轮次重复执行，每一轮共识过程一般重新选择该轮的记账节点。

共识过程的核心是选主和记账两部分，具体操作中每一轮可以分为：选主（Leader election）、造块（Block generation）、验证（Data validation）和上链（Chain updation,即记账）四个阶段。共识过程的输入是数据节点生成和验证后的交易或数据，输出则是封装好的数据区块以及更新后的区块链。四个阶段循环往复执行，每一轮都会生成一个新的区块。

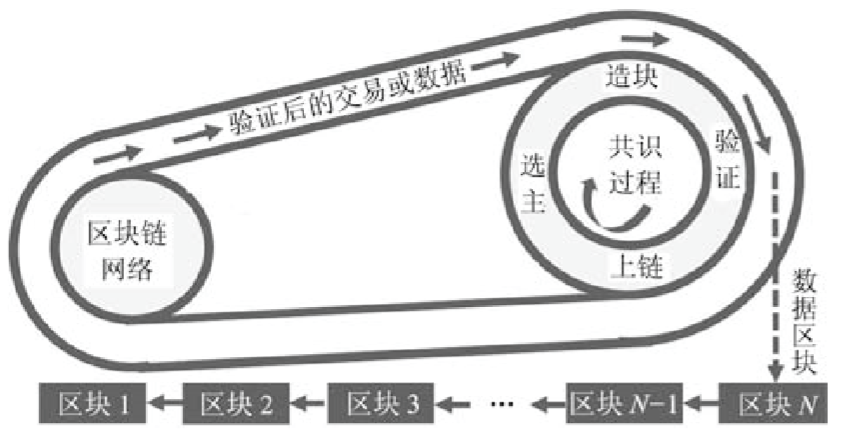


图1.1-1 区块共识过程基础流程

1）选主：选主是共识过程的核心，从全体矿工节点集M中选出记账节点A的过程：

F(M)🡪A ( |A|=1)

最终选择唯一的矿工节点来记账。

2）造块：第一阶段选出的记账节点A根据特定策略将前段时间内全体节点P生成的交易或者数据打包到一个区块中，并将生成的新区块广播给全体矿工节点M或其代表节点D。交易通常考虑综合因素进行排序依次打包进入新区快。造块策略是区块链系统新能的关键因素，也是贪婪交易打包、自私挖矿等矿工策略性行为的集中体现。

3）验证：矿工节点M或者代表节点D收到广播的新区块后，将各自验证区块内封装的交易或者数据的正确性和合理性。如果得到大多数验证或代表节点的认可，该区块将作为下一区块更新到区块链。

4）上链：记账节点将新区块添加到主链，形成一条从创世区块到最新区块的完整的、更长的链条。如果主链存在多个分叉链，则根据共识算法规定的主链判别标准来选择其中恰当的分支作为主链。[2]

#### (2) 共识算法分类

共识算法有多种分类方法，可以根据其容错类型、部署方 式和一致性程度等多个维度加以分类. 例如, 根据容 错类型, 可以将区块链共识算法分为拜占庭容错和 非拜占庭容错两类; 根据部署方式, 可以将区块链共 识算法分为公有链共识、联盟链共识和私有链共识 三类; 根据一致性程度, 还可以将区块链共识算法分 为强一致性共识和弱 (最终) 一致性共识等。一下是根据选主策略对共识算法进行的划分。

1）选举类共识：矿工在每一轮共识过程通过“投票选举”的方式选出当前轮次的记账节点，首先获得半数以上选票的矿工节点将会获得记票权。多见于产痛分布式的一致性算法，如Paxos和Raft等。

2）证明类共识：也称“Proof of X”类共识，即矿工节点在每一轮共识过程必须证明自己具有某种特定的能力，证明方式通常是在竞争性的完成某项难以解决但易于验证的任务，在竞争中胜出的矿工节点将获得记账权；例如PoW和PoS等共识算法是基于矿工的算力或者权益来完成随机数搜索任务，一次竞争记账权。

3）随机类共识：矿工节点根据某种随机方式直接确定每一轮的记账节点，例如Algorand 和PoET共识算法等。

4）联盟类共识：矿工节点基于某种特定方式首先举出一组代表性节点，而后代表节点以轮流或者选举的方式一次取得记账权。这是一种“代议制”为特点的共识算法，例如DPos等。

5）混合类共识：矿工节点采取多种共识算法的混合体来选择记账节点，如PoW+PoS混合共识、DPoS +BFT共识等。[2]

### 1.1.2 区块链去中心化存储

区块链去中心化存储技术，即分布式账本技术。首先，区块链被看作是一个点对点网络（P2P Network），没有中心节点，所有参与计算的节点是对等的，都保存了区块链的副本，节点之间通过区块头信息保证了区块链副本的一致性。区块通过哈希值与前一区块相连，可以防止被恶意修改，即如果想修改某个区块，必须重新计算所有前驱区块的哈希值，增加了计算复杂性。这些特点使得区块链非常适合构建安全的存储系统，同时添加了区块链的分布式存储系统可以有效地防止单点故障问题，即如果中心节点发生故障或宕机，分布式存储系统可以使用区块链来恢复关键数据，如元数据等。此外，区块链的防篡改特点，可以保证存 储在区块链中的数据完整性，这同样是安全存储系统所必需的。[4]

## 1.2 区块链技术的应用

区块链在经济、金融、能源、农业等多个方面都有应用。其主要应用场景为以下七个方面。

第一，信息共享，区块链各个节点信息一直，自带信息共享功能，而且P2P技术让信息的实时性得以实现，而区块链的不可篡改和共识机制保障了信息的安全可靠。

第二，版权保护，区块链应用到鉴证证明后，登记和查询都比较方便，无需奔走于各个部门之间。其去中心化存储保证了数据不能被任意一家机构篡改。

第三，物流链。由于区块链开放透明，任何人都可以公开查询，伪造数据被发现的概率增加；其数据的不可篡改性让每个产品信息被永久记录，无法通过简单复制防伪信息蒙混过关，实现第二次销售；这也让每一个商品都有迹可循，让消费者了解商品的前世今生。

第四，供应链金融，传统供应链的中小微企业，由于银行和中小企业之间缺乏一个有效的信任机制，融资比较困难。假如供应链的所有节点上链，通过区块链的私钥签名技术保证了核心企业等的数据可靠性；而合同、票据等上链，是对自残的数字化便于流通，实现了价值传递。

第五，跨境支付，区块链的引入，能够解决跨境支付信息不对称的问题，并建立一定程度的信任机制，提高了效率，降低了费用。比如Ripple, Circle、招商银行等。

第六，资产数字化。使用区块链实现资产数字化后，易于分割，流通方便，交易成本贬低，比如腾讯的微黄金应用。

第七，代币，即使用区块链来存储交易信息，例如比特币。

## 1.3 区块链面临的问题

### 1.3.1 存储空间的相对稀缺性

假如有一项服务有 1000 万人在使用，理论上区块链应该建立1000万个节点，如果 A 给 B 转了 100 元钱,以前服务器只改变一个或几个服务器信息，现在需要 1000 万次信息修改和存储，存储空间、存储时间、能源消费提升 了1000万倍，耗费了巨大的社会资 源和时间。地球资源是短缺的，时间是不可逆的，因此这个缺陷在短期内看是灾难性的。目前，比特币的钱包已经需要占用几百 G 的存储空间，一般的手机都无法使用，普通台式机也够呛，进行一次比特币转账，根本没有办法实时到账，必须长时间对大量节点进行存储才能完成。因此，无论是改变世界的能力,还是区块链本身的能力，作为存储方式和信息传递的 一种模式，区块链在短期内和互联网的发明、存储材料硅的发明、人工智能技术的发明相比都还有较大的距离,都不足以和这些划时代意义的技术相抗衡。[1]

### 1.3.2 效率问题

在区块链中，客户端发起的每笔交易或合约状态变更等，只要是放入区块链账本的数据，都要经过节点的验证。区块链应用巨大的数据量会导致数据的验证速度变慢，从而降低区块链网络的处理效率。

解决方案，一是区块数据的压缩，也就是剔除掉区块链账本中的那些完全老旧的交易事务，其二就是同样使用区块链技术来实现一个去中心分布式的自治存储系统。[5]

### 1.3.3 安全问题

区块链网络层包含的多种网络技术本身的安全问题必然会对区块链网络层带来安全风险，包括P2P网络缺少身份认证、数据验证、网络安全管理机制，节点的网络拓扑结构也会为攻击者实施攻击创造便利，而网络传输用户IP地址之间的关联性，也能被监听追踪。

共识层是区块链架构的核心，根据采用的基础协议不同，可以划分为5大系列，包括PoW、PoS、拜占庭容错、分片技术、可信硬件，区块链上的共识机制发展尚不完善，普遍存在安全性证明不完备、安全性假设不可靠、扩展性差、一致性不稳定、初始化和重构难等问题，不同类型的共识机制还面临不同的攻击威胁。

区块链的激励层与共识层相互依存，共同维护区块链系统的安全性与稳定性，激励层需要解决的主要问题是经济学上的激励不相容，指参与维护的矿工不会实施危害安全性的恶意攻击，但是会以自身利益最大化来指导自己的挖矿策略，这种策略与区块链整体利益形成冲突，破坏区块链系统效率和稳定性，包括自私挖矿攻击、Nothing at stake攻击、扣块攻击和激励不可持续问题。

智能合约是合约层的核心，最早由Nick Szabo提出，后经以太坊重新定义，但由于智能合约代码开源、涉及数字资产转移，一旦代码漏洞被利用，会造成不可逆转的损失。除智能合约创建者在设计业务逻辑时的文本安全问题以外，合约层还面临智能合约代码漏洞、外部数据源调用、缺乏形式化验证、难实现隐私保护等问题。

应用层是指区块链技术在金融、供应链、能源等多领域具有广泛的应用场景，作为直接与用户交互的区块链层级，在架构设计上一般需要具备API接口、跨链异构和监管技术，而目前看来面临跨链操作难、监管技术缺失和应用层攻击等问题。

**参考文献：**

[1]黄奇帆.“区块链”有三个问题无法回避[J].中国经济周刊,2019(22):101-104.

[2]袁勇,倪晓春,曾帅,王飞跃.区块链共识算法的发展现状与展望[J].自动化学报,2018,44(11):2011-2022.

[3]张桐.数据治理的变革：来自区块链技术的支持与想象[J].宁夏社会科学,2019(06):76-82.

[4]郝琨,信俊昌,黄达,王国仁.去中心化的分布式存储模型[J].计算机工程与应用,2017,53(24):1-7+22.

[5]蒋勇.《白话区块链》