

**区块链的架构研究综述**

学生姓名： 刘鹏

学号：22151195

课程：企业级区块链系统设计

年级与专业：2021级软件工程

所在学院：软件学院

浙江大学

2022年1月

# 摘 要

区块链作为一种去中心化、不可篡改、可追溯、多方共同维护的分布式数据库, 可在互不信任的多方间建立可靠的信任, 在没有第三方中介机构的协调下, 实现了可信的数据共享和点对点的价值传输。它提供了一套安全、稳定、透明、可审计且高效的交易数据记录和信息交互的架构，是未来社会发展中解决信任危机的一种革命性技术。区块链技术的快速发展引起了政府部门、金融机构、科技企业和资本市场的广泛关注。区块链技术有望像互联网一样彻底重塑人类社会活动形态, 并实现从目前的信息互联网向价值互联网的转变.

本文主要从系统架构的角度出发，分析区块链系统对于吞吐量提升的解决方案。首先，本文介绍了区块链的基础架构模型。其次分别按照节点准入机制和网络拓扑结构两个层面对区块链系统进行了分类，接着介绍了区块链与物联网、云计算的融合架构与应用。最后，从链的扩展性的角度，介绍了区块链技术在分片、跨链技术的相关研究。

**关键词：**区块链、区块链架构、区块链拓扑结构、吞吐量、扩展性

**目 录**

[第一章 绪论](#_Toc619475557_WPSOffice_Level1) [3](#_Toc619475557_WPSOffice_Level1)

[第二章 区块链架构分类](#_Toc1713460937_WPSOffice_Level1) [4](#_Toc1713460937_WPSOffice_Level1)

[2.1 区块链的基础架构](#_Toc1713460937_WPSOffice_Level2) [4](#_Toc1713460937_WPSOffice_Level2)

[图2.1 区块链的基础架构模型](#_Toc1713460937_WPSOffice_Level3) [4](#_Toc1713460937_WPSOffice_Level3)

[2.2 区块链的分类](#_Toc382261889_WPSOffice_Level2) [4](#_Toc382261889_WPSOffice_Level2)

[表2.1 非许可链与许可链的对比](#_Toc382261889_WPSOffice_Level3) [5](#_Toc382261889_WPSOffice_Level3)

[2.3 区块链的拓扑架构](#_Toc1551980246_WPSOffice_Level2) [5](#_Toc1551980246_WPSOffice_Level2)

[2.3.1 链式结构](#_Toc1551980246_WPSOffice_Level3) [5](#_Toc1551980246_WPSOffice_Level3)

[2.3.2 DAG](#_Toc795618060_WPSOffice_Level3) [5](#_Toc795618060_WPSOffice_Level3)

[2.3.3 树图](#_Toc1719548198_WPSOffice_Level3) [5](#_Toc1719548198_WPSOffice_Level3)

[图2.2 三种区块链的拓扑结构](#_Toc1759126107_WPSOffice_Level3) [6](#_Toc1759126107_WPSOffice_Level3)

[2.4 区块链与其它技术的融合](#_Toc795618060_WPSOffice_Level2) [6](#_Toc795618060_WPSOffice_Level2)

[2.4.1 区块链与云计算](#_Toc1225112100_WPSOffice_Level3) [6](#_Toc1225112100_WPSOffice_Level3)

[图2.3 区块链与云计算的融合架构](#_Toc385857264_WPSOffice_Level3) [7](#_Toc385857264_WPSOffice_Level3)

[2.4.2 区块链与物联网](#_Toc1849905755_WPSOffice_Level3) [7](#_Toc1849905755_WPSOffice_Level3)

[图2.4 区块链与物联网的融合架构](#_Toc97783019_WPSOffice_Level3) [8](#_Toc97783019_WPSOffice_Level3)

[第三章 区块链的架构发展趋势](#_Toc382261889_WPSOffice_Level1) [9](#_Toc382261889_WPSOffice_Level1)

[3.1 分片](#_Toc1719548198_WPSOffice_Level2) [9](#_Toc1719548198_WPSOffice_Level2)

[图3.1 以太坊分片架构](#_Toc614210378_WPSOffice_Level3) [9](#_Toc614210378_WPSOffice_Level3)

[3.2 跨链](#_Toc1759126107_WPSOffice_Level2) [9](#_Toc1759126107_WPSOffice_Level2)

[3.2.1 Polkadot](#_Toc79931917_WPSOffice_Level3) [9](#_Toc79931917_WPSOffice_Level3)

[图3.2 Polkadot架构示意图](#_Toc1238449644_WPSOffice_Level3) [10](#_Toc1238449644_WPSOffice_Level3)

[3.2.2 BitXHub](#_Toc1211659984_WPSOffice_Level3) [10](#_Toc1211659984_WPSOffice_Level3)

[图3.3 BitXHub中继链架构图](#_Toc1929410234_WPSOffice_Level3) [10](#_Toc1929410234_WPSOffice_Level3)

[第四章 总结](#_Toc1551980246_WPSOffice_Level1) [12](#_Toc1551980246_WPSOffice_Level1)

[参考文献](#_Toc795618060_WPSOffice_Level1) [13](#_Toc795618060_WPSOffice_Level1)

# 绪论

2008年，Nakamoto提出了比特币[1]，区块链技术开始进入到公众的视野。区块链技术是一种不同节点能在没有可信第三方存在的分布式网络环境中依靠共识算法使公共账本达成数据一致的技术[2]。区块链一般主要有以下几个特点: 第一是去中心化。去中心化是指节点之间没有具有公信力的第三方中心机构作为背书，可直接建立起点对点的可信价值传递；第二是不可篡改。区块链中的数据经过各节点的某种特定的共识算法确认后，将被写入区块中，数据一旦上链之后便可认为被篡改的可能性极低；第三是可追溯性。在区块链中，节点能随时获得整个网络中的区块链数据，任何一笔交易都是可以追溯的；第四是匿名性。区块链通过采用零知识证明、混币机制等加密技术, 使交易数据在共享的时候还能有效保护用户隐私。

随着比特币近年来的快速发展与普及, 区块链技术的研究与应用也呈现出爆发式增长态势, 被认为是继大型机、个人电脑、互联网、移动/社交网络之后计算范式的第五次颠覆式创新, 是人类信用进化史上继血亲信用、贵金属信用、央行纸币信用之后的第四个里程碑[3]，同时，最近大火的元宇宙，更是集合了区块链、交互技术、电子游戏技术、人工智能技术、网络及运算技术和物联网技术共六大技术。区块链技术，整合了分布式存储、点对点数据传输、共识机制等特性，解决了数据的可靠和隐私问题，能为元宇宙打造可靠的基础设施。

区块链的发展同时会给云计算、物联网、元宇宙等领域的发展带来更多的想象空间。所以区块链不仅仅是一种新型分布式技术，也是一场互联网价值革命，将会给众多行业带来深远影响。

区块链作为近年来兴起发展的新技术，面临各种制约其发展的问题和障碍。其中，系统的吞吐量，即每秒处理交易数（Transactions Per Second, 简称TPS），尤为突出。比特币目前每秒处理7笔交易，以太坊每秒约处理30笔交易，而VISA每秒最多可以处理10000笔交易[3]，极大的限制了区块链的应用场景。而围绕着TPS这一问题，有学者从共识算法层面进行研究[2]，本文主要从架构的角度，对许多区块链项目进行了介绍，分析并且比较了不同项目对区块链系统的改进。

第二章 区块链架构分类

## 2.1 区块链的基础架构

区块链技术的基础架构模型如图2.1所示. 一般说来, 区块链系统由数据层、网络层、共识层、激励层、合约层和应用层组成[4]。其中, 数据层封装了底层数据区块以及相关的数据加密和时间戳等技术; 网络层则包括分布式组网机制、数据传播机制和数据验证机制等; 共识层主要封装网络节点的各类共识算法，如PoW[1]，PoS[5]，PBFT[6]，Raft[7]等，各节点通过共识算法达成账本一致; 激励层将经济因素融合到区块链技术体系中, 主要包括代币的发行机制和分配机制等，如出块奖励，Gas手续费等。适度的激励可以使节点更加愿意参与挖矿，从而维护区块链系统的稳定；合约层主要封装各类脚本、算法和智能合约, 是区块链可编程特性的基础；应用层是基于区块链的各种具体应用，如“区块链+货币”，“区块链+司法”，“区块链+教育”等。

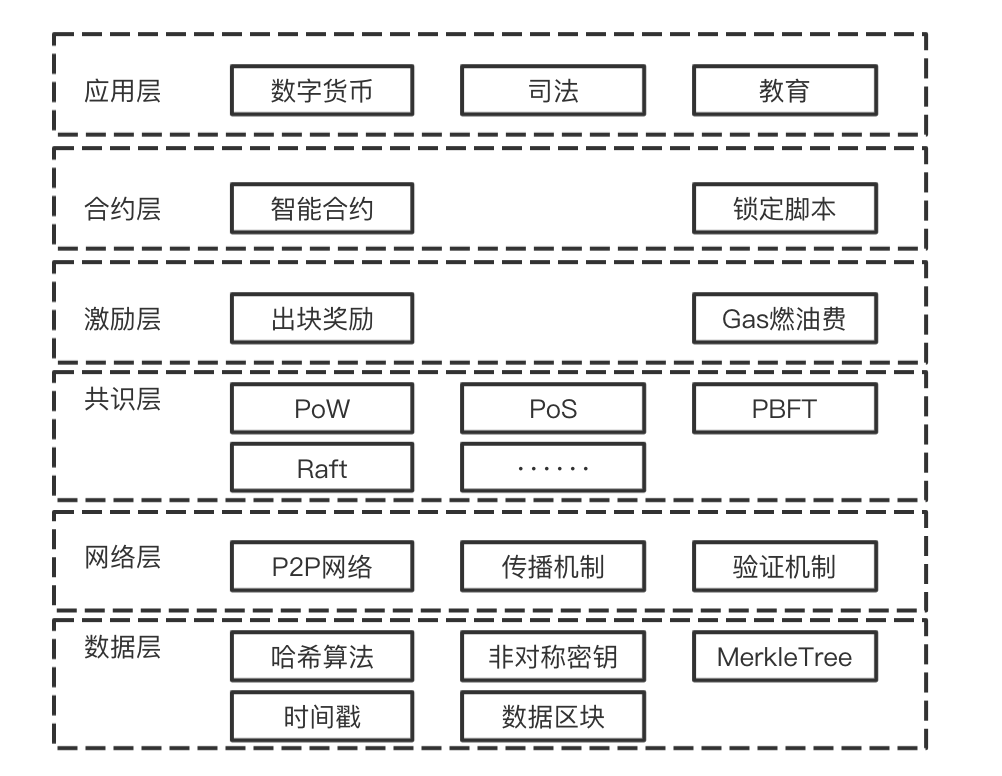


图2.1 区块链的基础架构模型

## 2.2 区块链的分类

按节点准入机制，区块链系统分为非许可链(permissionless blockchain)和许可链(permissioned blockchain)两类[8]。非许可链系统中没有许可机构对节点进行身份审查，节点以匿名形式任意加入或退出系统，因此非许可链又被称为公有链(public blockchain)。针对不同应用场景，许可链又分为联盟链(consortium blockchain)和私有链(private blockchain)[8]。联盟链通常由具有相同行业背景的多家不同机构组成，共识节点来自联盟内各个机构，区块链数据在联盟机构内部共享。私有链通常部署在单个机构内部，共识节点来自机构内部，类似于传统的分布式数据集群。

将非许可链和许可链共识协议的不同特征总结见表2.1。针对准入机制，非许可链允许节点自由准入，许可链共识协议要求节点审查准入。非许可链共识协议一般具有较高的网络规模，许可链共识协议的网络规模相对较低。通常情况下，分布式系统网络规模越大，达成共识的难度越高，因而非许可链吞吐量通常较低，许可链较高。在一致性方面：非许可链共识协议通常以一定概率确保数据一致，实现弱一致性；许可链通常采用确定性方式确保数据一致，实现强一致性。

表2.1 非许可链与许可链的对比

|  |  |  |
| --- | --- | --- |
|  | 非许可链 | 许可链 |
| 应用场景 | 公有链 | 联盟链、私有链 |
| 准入机制 | 公开，随时加入或退出 | 需要审核才可加入 |
| 网络规模 | 高 | 低 |
| 一致性 | 概率一致性 | 确定性 |
| 吞吐量 | 低 | 高 |

## 2.3 区块链的拓扑架构

区块链技术在发展的过程中，形成了多种拓扑结构，主要包括链式结构、有向无环图（Directed Acyclic Graph，DAG）结构、树图（Tree-Graph）结构。

### 2.3.1 链式结构

目前绝大多数区块链系统都是采用链式结构，如图2.2（a）所示。每一个区块（除了创世区块）通过哈希指针指向上一个区块，任何一个后继区块经过哈希指针都能追溯到创世区块。系统每次只能出一个块，如果多个节点同时出块，会产生分叉的情况，比特币中首先提出了最长合法链[1]的概念，系统选择最长的合法链作为主链，丢弃其它分叉链。丢弃分叉链这一方案存在出块效率低和算力浪费的问题，还会降低诚实节点所占算力比重，影响整个系统的安全性。

### 2.3.2 DAG

为了提高区块链系统的吞吐量，IOTA[9]和Byteball[10]改变了原有的链式结构，采用了有向无环图作为系统的拓扑结构。如图2.2（b）所示，区块链不再是由区块构成，而是由交易构成，将共识粒度从区块细化到交易，省去了打包交易出块的环节。DAG图中每笔交易都包含着对之前交易的验证，而一笔交易在被若干个交易验证后即视为有效。由于DAG结构具有天然的偏序关系，不同节点的交易先后顺序可能会有偏差，随着系统的运行，节点之间运行的数据可能会出现偏差，因此，DAG无法支持数据的强一致性。

### 2.3.3 树图

由于DAG的偏序问题，DAG无法支持需要确定交易顺序的智能合约。为了提升吞吐量以及实现系统的全序，Conflux[11]提出了树图(Tree-Graph)的概念，Conflux基于有向无环图计算区块内交易的全局顺序，剔除冲突交易，使得分叉所有交易得到利用，提高系统的吞吐量。如图2.2（c）所示，Conflux中使用了两类指针：一类指针指向父亲区块，与图2.2 a的链式结构相似。系统通过该类指针构成了一颗树；另一类指针指向引用区块，表达了不同区块的先后（happen-before）关系，系统通过该类指针构成了有向无环图。Conflux首先通过Ghost协议选出主链，然后利用引用两类指针实现区块的全局排序。

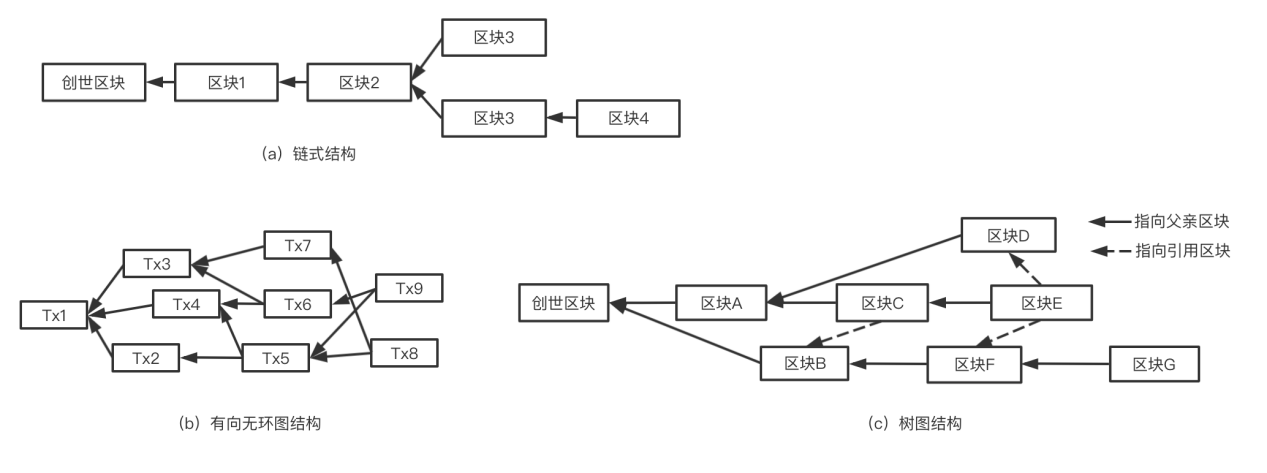


图2.2 三种区块链的拓扑结构

## 2.4 区块链与其它技术的融合

### 2.4.1 区块链与云计算

云计算让传统信息行业变得前所未有的便捷。利用云计算所提供的服务，只需要简单的开发工作，便可以完成需要大量研发和运营时间成本的任务。过去几年已经出现了很多云服务架构，典型的应用架构有基础设施即服务(IaaS)、平台即服务(PaaS)、软件即服务(SaaS)。用户可以利用PaaS方便地在线管理开发应用；可以利用SaaS使用网络软件，比本地软件更方便迅捷；利用IaaS，可以从完善的计算机基础设施获得服务。

区块链技术具有最普适的底层技术框架，可以为诸如金融、医疗、公共设施领域带来深刻变革。但由于学术研究的相对滞后，区块链技术还远不能达到传统分布式技术的性能。为促进区块链的更快发展，首先需要把这项技术带进工业界和商务领域，而云计算平台则提供了最好的服务传递方式，利用云服务平台的应用可以减少企业区块链开发的大量后端工作[12]。

文献[12]提出了区块链即服务的由基础设施层、中间层、服务层的通用架构模型。如图2.3所示，第1层是基础设施层，封装了数据存储的底层细节，对外提供统一的API接口；第2层是中间层，实现了基础设施层之上的通信协议，以及区块链与区块链外界交互信息的相关协议；第3层是服务层，根据具体应用需求，提供了用户开发需要的相关接口。

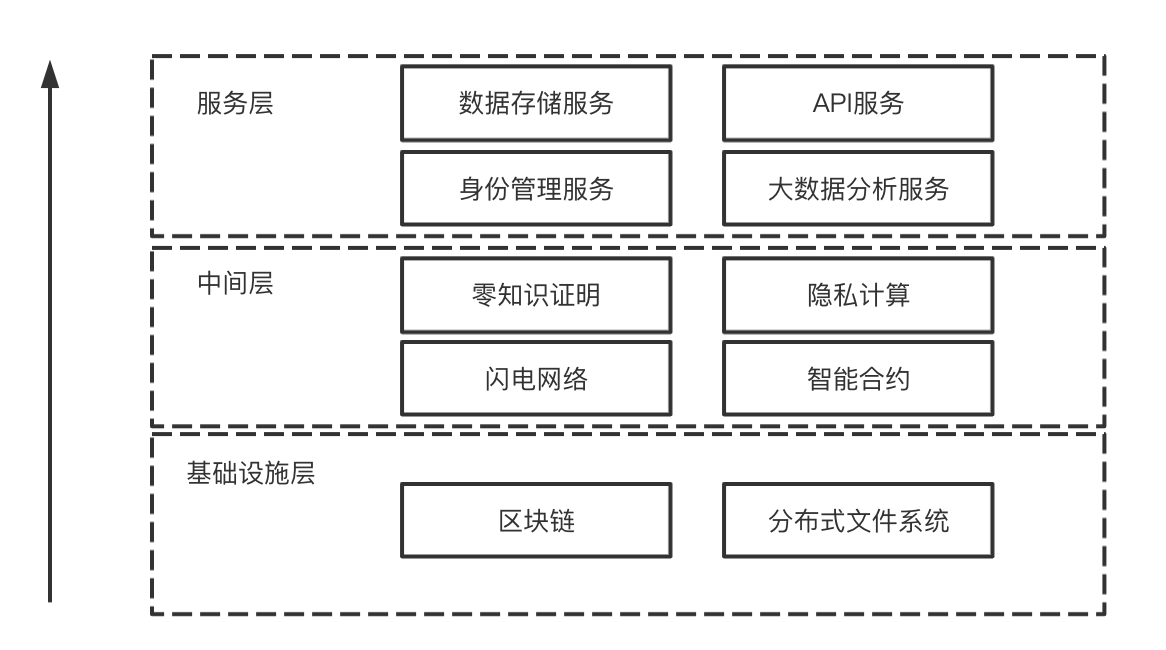


图2.3 区块链与云计算的融合架构

针对区块链的云服务形态，IBM和微软正尝试定义一个新的区块链即服务(BaaS)市场。不同于之前的软件即服务、平台即服务与基础设施即服务，区块链即服务是基于区块链向客户提供特定云服务。微软在2015年11月推出了自己的BaaS平台，IBM也相继在2016年2月发布了IBM区块链服务。同时，微软和IBM还各自推行独立的开源项目。IBM在2015年12月发起超级账本项目(hyperledger project)[13]，Hyperledger分别提出了Fabric，Sawtooth，Burrow和Indy等多个企业级区块链平台，以适应不同的需求和场景。Hyperledger Fabric 应用最为广泛。该微软也在同年6月发布Bletchley计划[14]。可见，未来区块链的发展主要会集中于对BaaS的研究，通过云服务基础设施将区块链技术普适化，变革如今的互联网架构。

### 2.4.2 区块链与物联网

物联网（Internet of Things, IoT）的出现使得异构和轻量的智能设备能协同为人们提供服务。随着基于IoT的智能应用的出现，高度互联的智能设备以及其产生的大量的交易数据引发了人们对安全和隐私的关注。传统的安全策略面临性能瓶颈或者单点故障问题，不能有效地解决物联网系统中的性能问题和安全问题。区块链技术适用于物联网对于数据安全性和隐私性的要求。

区块链与物联网的融合架构主要分为以下四层：数据层，网络层，共识层，应用层[15]。如图2.4所示。数据层从IoT设备收集数据，网络层负责数据安全可靠的传输，数据经过共识层达到一致后，便不可篡改，然后由应用层的具体应用为用户提供服务。

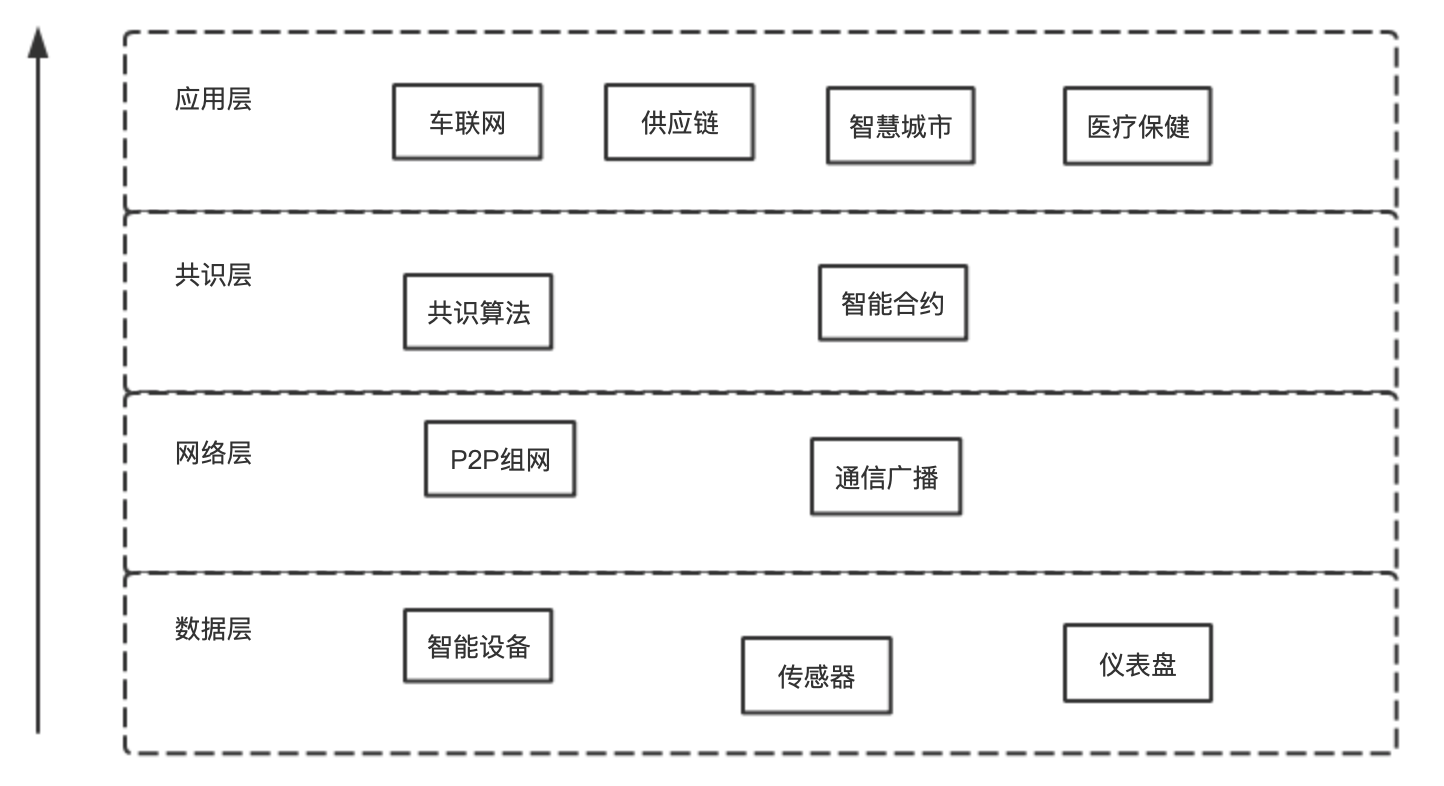


图2.4 区块链与物联网的融合架构

值得一提的是，区块链应用于物联网存在很多问题。例如，在目前的区块链技术中大多系统使用吞吐量比较低的PoW、PoS和类PoS的共识机制，不足以满足物联网设备高并发的数据特征，并且物联网节点计算资源受限，处理数据的能力偏低，无法提供足够的算力进行挖矿，为此，有学者[16]将Tangle共识算法（基于2.3.2小节提到的DAG技术）应用于物联网从而提高吞吐量。

# 第三章 区块链的架构发展趋势

在传统分布式系统中，分布式数据库的总体性能随着服务器集群节点数量增加而线性增加。但在区块链系统中，网络中的每个共识节点需要处理全部的数据。因此，在共识算法的影响下，随着节点数量增加，系统反而可能会性能下降。为了提高系统的扩展性以及吞吐量，出现了分片技术和跨链技术，这使得区块链系统能够并发处理交易，提升系统的整体性能。

## 3.1 分片

为了解决以太坊的吞吐量问题，以太坊创始人Vitalik Buterin率先提出了分片处理交易的解决方案[17]。在以太坊的2.0版本中，以太坊依据账户地址将全网划分为多个相对独立的分片, 每个分片内维护一条独立子链, 并且新增了信标链（Beacon Chain）负责不同分片之间的协调，用户可自行选择在哪个分片执行自己的交易, 每个节点根据自身的计算和存储能力选择加入一到多个分片, 并处理和存储这些分片上的交易。每条分片链处理不同的业务，每个节点只需维护最少一条分片链的一个节点。

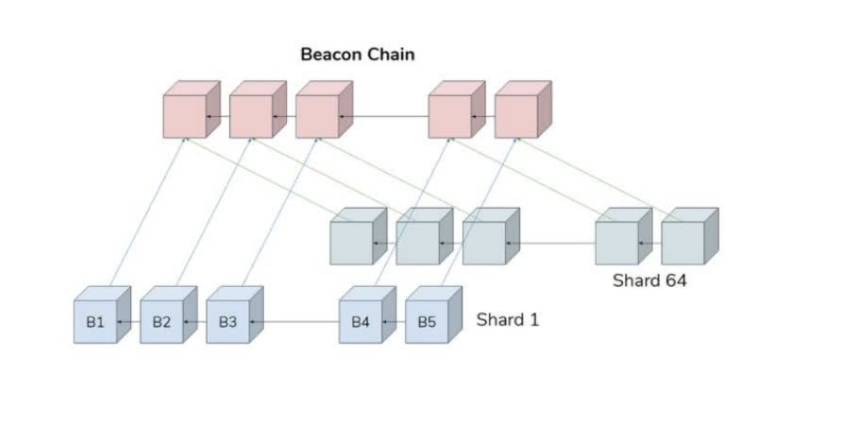


图3.1 以太坊分片架构

## 3.2 跨链

在区块链的应用发展过程中，各种应用平台互不兼容，衍生出多种类型的区块链，各大公司专注搭建自己的区块链平台，久而久之各个链之间就变成信息孤岛、价值孤岛。为了实现链与链之间的价值互通，出现了跨链技术。文献[18]分析了跨链技术的需求和面临的技术难点，并总结了24种主流的跨链技术的原理和实现思路。目前主流的区块链跨链技术⽅案的实现⽅式主要有：公证⼈机制(notary schemes)、哈希锁定（Hash-locking）、侧链/中继链（relay-chain）。公证人机制引入了可信第三方作为中介，哈希锁定主要通过智能合约实现跨链功能。侧链/中继链技术则提出了一种新的架构，接下来3.2.1和3.2.2将对侧链/中继链技术进行介绍，分别选取了国外的Polkadot项目和国内的Bitxhub项目进行分析。

### 3.2.1 Polkadot

Polkadot[19]是由以太坊前任CTO Gavin Wood在2016年提出的跨链项目。如图3.2所示，Polkadot主要由以下几个部分构成：中继链（Relay Chain）、平行链（Parachain）、转接桥（Bridge）。中继链为整个网络提供了统一的共识和安全性保障，平行链会负责具体业务场景的实现，转接桥是一种连接，允许从一个网络转移到另一个网络的任意数据。

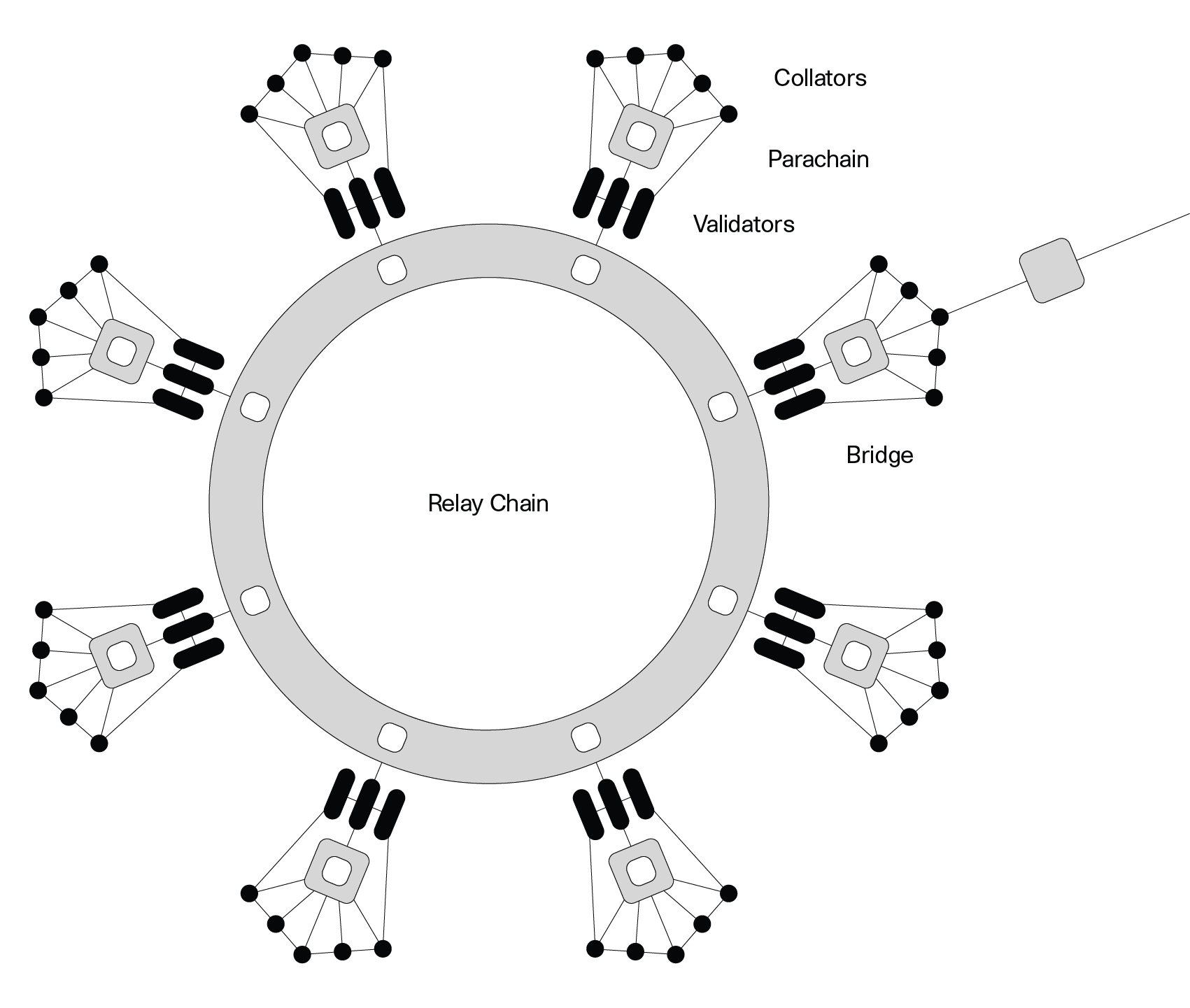


图3.2 Polkadot架构示意图

### 3.2.2 BitXHub

BitXHub[20]是国内趣联科技提出的跨链技术。如图3.3所示，BitXHub平台是一种由中继链、跨链网关和应用链所构建的跨层级链间互操作服务平台，其主要组成部分包括：中继链、跨链网关、应用链。BitXHub设计了一种类似TCP/IP的跨链传输协议：IBTP（Inter-Blockchain Transfer Protocol），该协议能够支持不同异构区块链之间的交易分发和验证。

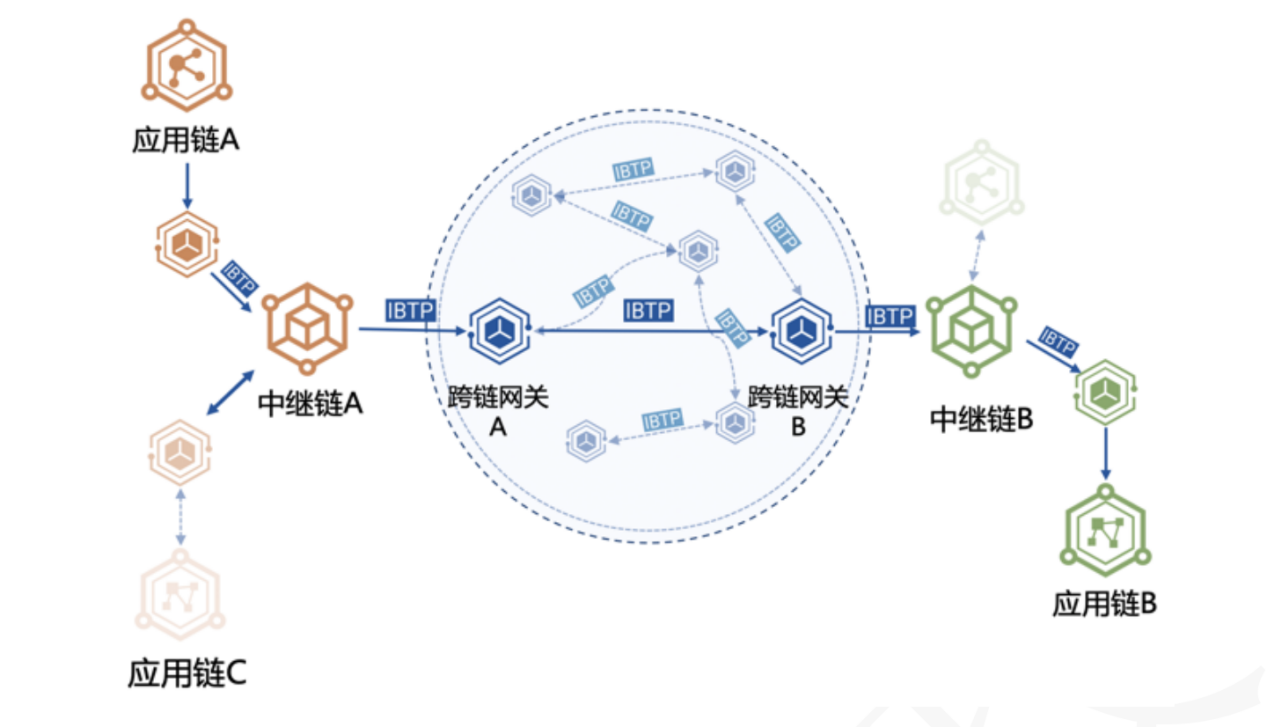


图3.3 BitXHub中继链架构图

可以看出，Polkadot和BitXHub在架构设计上有很多异曲同工之妙，相同点如下：

都采用了“中继链+应用链/平行链+跨链网关/桥”的思想，即由中继链负责共识，应用链负责具体业务，跨链网关负责交易的转发；（2）中继链的共识模块采用插件形式，灵活可插拔，耦合性低，可以根据具体需求更换共识算法；（3）中继链架构可以通过跨链网关相连实现进一步的网络扩展

在具体的实现上，两者对于跨链消息协议的设计有着一定的区别。除此之外，由于Polkadot是公有链，与国内的联盟链BitXHub也有着不同的地方：Polkadot有经济激励机制，而BitXHub没有任何代币奖励。

第四章 总结

区块链具有去信任化、不可篡改、可追溯性、匿名性等特点，使其在数字加密货币、金融和社会系统中有广泛的应用前景。并且，区块链的发展同时会给云计算、物联网、大数据等行业的发展带来更多的想象空间。所以区块链不仅仅是一种新型分布式技术，也是一场互联网价值革命，将会给众多行业带来深远影响。与此同时，围绕着区块链的安全、吞吐量和扩展性等问题，本文主要从系统架构角度探讨了现有的一些解决方案，但仍需结合具体层次（数据层、网络层、共识层等）进一步研究，但由于区块链技术涉及到的知识面较广，再加上本人知识的不足，本篇综述亟待深入分析。

# 参考文献

1. NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system [EB/OL］. [Online]．Availble:https: //bitcoin.org/bitcoin.pdf.
2. 刘懿中,刘建伟,张宗洋,徐同阁,喻辉.区块链共识机制研究综述[J].密码学报,2019,6(04):395-432.
3. Swan M. Blockchain: Blueprint for a New Economy. USA:O’Reilly Media Inc., 2015.
4. 袁勇,王飞跃.区块链技术发展现状与展望[J].自动化学报,2016,42(04):481-494.DOI:10.16383/j.aas.2016.c160158.
5. Larimer B D . Transactions as Proof-of-Stake!.
6. Castro M, Liskov B. Practical byzantine fault tolerance[C]//OSDI. 1999, 99(1999): 173-186.
7. Ongaro D, Ousterhout J. In search of an understandable consensus algorithm[C]//2014 {USENIX} Annual Technical Conference ({USENIX}{ATC} 14). 2014: 305-319.
8. Bitfury Group. Public versus private blockchains. White Paper, 2015.
9. Popov S. The tangle[J]. White paper, 2018, 1(3).
10. Churyumov A. Byteball: A decentralized system for storage and transfer of value[J]. URL https://byteball. org/Byteball. pdf, 2016.
11. Li C, Li P, Zhou D, et al. A decentralized blockchain with high throughput and fast confirmation[C]//2020 {USENIX} Annual Technical Conference ({USENIX}{ATC} 20). 2020: 515-528.
12. 朱昱锦, 姚建国, 管海兵. 区块链即服务: 下一个云服务前沿[J]. Journal of Software, 2020, 31(1).
13. The Linux Foundation. IBM’s hyperledger project. 2016. <https://github.com/hyperledger/fabric>
14. Gray M. Microsoft’s bletchley project. 2016. <https://github.com/Azure/azure-blockchain-projects/blob/master/bletchley>
15. 史慧洋,刘玲,张玉清.物链网综述:区块链在物联网中的应用[J].信息安全学报,2019,4(05):76-91.
16. Zou J, Dong Z, Shao A, et al. 3d-dag: A high performance dag network with eventual consistency and finality[C]//2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN). IEEE, 2018: 262-263.
17. Buterin V.Ethereum mauve paper.White Paper.2016
18. 李芳,李卓然,赵赫.区块链跨链技术进展研究[J].软件学报,2019,30(06):1649-1660.
19. Wood G. Polkadot: Vision for a heterogeneous multi-chain framework. <https://github.com/polkadot-io/polkadotpaper/raw/master/PolkaDotPaper.pdf>
20. 叶少杰, 汪小益, 徐才巢, 等. BitXHub: 基于侧链中继的异构区块链互操作平台[J]. 计算机科学, 2020, 47(6): 294-302.