浙 江 大 学

硕士学位论文文献综述

**(专业学位)**

文献综述题目： 联盟区块链技术综述

姓 名： 黄 宁

学 号： 21751143

专 业： 软件工程

院 别： 软件学院

导 师： 张志猛、肖俊

日期：二零一八年 十一月

目 录

[一、区块链的概述 - 1 -](#_Toc530092415)

[二、区块链的应用场景 - 2 -](#_Toc530092416)

[三、区块链的关键技术 - 4 -](#_Toc530092417)

[3.1 密码学 - 4 -](#_Toc530092418)

[3.1.1 哈希函数 - 4 -](#_Toc530092419)

[3.1.2 签名算法 - 5 -](#_Toc530092420)

[3.2 节点间共识机制 - 5 -](#_Toc530092421)

[3.3 智能合约 - 6 -](#_Toc530092422)

[3.4 隐私保护技术 - 7 -](#_Toc530092423)

[参考文献 - 8 -](#_Toc530092424)

# 一、区块链的概述

区块链(Blockchain)是一种由多方共同维护，使用密码学保证传输和访问安全，能够实现数据一致存储、难以篡改、防止抵赖的记账技术，也称为分布式账本技术(DistributedLedgerTechnology)。典型的区块链以块-链结构存储数据。作为一种在不可信的竞争环境中低成本建立信任的新型计算范式和协作模式，区块链凭借其独有的信任建立机制，正在改变诸多行业的应用场景和运行规则。

典型的区块链系统中，各参与方按照事先约定的规则共同存储信息并达成共识。为了防止共识信息被篡改，系统以区块(Block)为单位存储数据，区块之间按照时间顺序、结合密码学算法构成链式(Chain)数据结构，通过共识机制选出记录节点，由该节点决定最新区块的数据，其他节点共同参与最新区块数据的验证、存储和维护，数据一经确认，就难以删除和更改，只能进行授权查询操作。按照系统是否具有节点准入机制，区块链可分类为许可链和非许可链。许可链中节点的加入退出需要区块链系统的许可，根据拥有控制权限的主体是否集中可分为联盟链和私有链；非许可链则是完全开放的，亦可称为公有链，节点可以随时自由加入和退出。

相对于传统的分布式数据库，区块链体现了以下几个对比特征:

1. 从复式记账演进到分布式记账。传统的信息系统，每位会计各自记录，每次对账时存在多个不同账本。区块链打破了原有的复式记账，变成“全网共享”的分布式账本，参与记账的各方之间通过同步协调机制，保证数据的防篡改和一致性，规避了复杂的多方对账过程。
2. 从“增删改查”变为仅“增查”两个操作。传统的数据库具有增加、删除、修改和查询四个经典操作。对于全网账本而言，区块链技术相当于放弃了删除和修改两个选项，只留下增加和查询两个操作，通过区块和链表这样的“块链式”结构，加上相应的时间戳进行凭证固化，形成环环相扣、难以篡改的可信数据集合。
3. 从单方维护变成多方维护。针对各个主体而言，传统的数据库是一种单方维护的信息系统，不论是分布式架构，还是集中式架构，都对数据记录具有高度控制权。区块链引入了分布式账本，是一种多方共同维护、不存在单点故障的分布式信息系统，数据的写入和同步不仅仅局限在一个主体范围之内，需要通过多方验证数据、形成共识，再决定哪些数据可以写入。
4. 从外挂合约发展为内置合约。传统上，财务的资金流和商务的信息流是两个截然不同的业务流程，商务合作签订的合约，在人工审核、鉴定成果后，再通知财务进行打款，形成相应的资金流。智能合约的出现，基于事先约定的规则，通过代码运行来独立执行、协同写入，通过算法代码形成了一种将信息流和资金流整合到一起的“内置合约”。

区块链是建立在传播机制、验证机制和存储机制基础上的一个分布式系统，整个网络没有中心化的硬件或管理机构，任何节点都有机会参与总账的记录和验证，将计算结果广播发送给其他节点，且任一节点的损坏或者退出都不会影响整个系统的运作。

区块链有两类现行的共识机制，根据数据写入的先后顺序判定，从业务应用的需求看，共识算法的实现应综合考虑应用环境、性能等诸多要求。一般来说，许可链采用节点投票的共识机制，以降低安全为代价，提升系统性能。非许可链采用基于工作量、权益证明等的共识机制，主要强调系统安全性，但性能较差。为了鼓励各节点共同参与进来，维护区块链系统的安全运行，非许可链采用发行Token的方式，作为参与方的酬劳和激励机制，即通过经济平衡的手段，来防止对总账本内容进行篡改[1][2]。因此，根据运行环境和信任分级，选择适用的共识机制是区块链应用落地应当考虑的重要因素之一。

智能合约负责将区块链系统的业务逻辑以代码的形式实现、编译并部署，完成既定规则的条件触发和自动执行，最大限度的减少人工干预。智能合约的操作对象大多为数字资产[3]，数据上链后难以修改、触发条件强等特性决定了智能合约的使用具有高价值和高风险，如何规避风险并发挥价值是当前智能合约大范围应用的难点。

区块链平台的接口层主要用于完成功能模块的封装，为应用层提供简洁的调用方式。应用层通过调用RPC接口与其他节点进行通信，通过调用SDK工具包对本地账本数据进行访问、写入等操作。同时，RPC和SDK应遵守以下规则：

1. 是功能齐全，能够完成交易和维护分布式账本，有完善的干预策略和权限管理机制。
2. 可移植性好，可以用于多种环境中的多种应用，而不仅限于某些绝对的软件或硬件平台。
3. 是可扩展和兼容，应尽可能向前和向后兼容，并在设计中考虑可扩展性。
4. 是易于使用，应使用结构化设计和良好的命名方法方便开发人员使用。常见的实现技术包括调用控制和序列化对象等。而应用层作为最终呈现给用户的部分，主要作用是调用智能合约层的接口，适配区块链的各类应用场景，为用户提供各种服务和应用。

由于区块链具有数据确权属性以及价值网络特征，目前产品应用中很多工作都可以交由底层的区块链平台处理。在开发区块链应用的过程中，前期工作须非常慎重，应当合理选择去中心化的公有链、高效的联盟链或安全的私有链作为底层架构，以确保在设计阶段核心算法无致命错误问题。因此，合理封装底层区块链技术，并提供一站式区块链开发平台将是应用层发展的必然趋势。同时，跨链技术的成熟可以让应用层选择系统架构时增加一定的灵活性。

# 二、区块链的应用场景

作为一项新兴技术，区块链具有在诸多领域开展应用的潜力。然而，区块链不是万能的，技术上去中心化、难以篡改的鲜明特点，使其在限定场景中具有较高的应用价值[4]。

首先，源自于应用场景对数据库的需要。区块链本质上是一种带时间戳的新型数据库，从对数据真实、有效、不可伪造、难以篡改的组织需求角度出发，相对于传统的数据库来说，可谓是一个新的起点和新的要求。其次，需要是一个跨主体、多方写入的应用场景。多个主体各自维护账本，往往因为数据信息不共享、业务逻辑不统一等原因，导致“账对不齐”的现象。与之相反，区块链中每个主体都可以拥有一个完整的账本副本，通过即时清结算的模式，保证多个主体之间数据的一致性，规避了复杂的对账过程。再次，适合于在不可信的环境中建立基于数学的信任。区块链在技术层面保证了系统的数据可信(密码学算法、数字签名、时间戳)、结果可信(智能合约、公式算法)和历史可信(链式结构、时间戳)，因此区块链提供了一种“机器中介”，尤其适用于协作方不可信、利益不一致或缺乏权威第三方介入的行业应用。最后，根据系统控制权和交易信息公开与否进行归类。公有链允许任一节点的加入，不对信息的传播加以限制，信息对整个系统公开;联盟链只允许认证后的机构参与共识，交易信息根据共识机制进行局部公开;相比而言，私有链范围最窄，只适用于限定的机构之内。不同区块链平台在准入机制、共识算法等诸多方面均存在差异。

公有链常被形象化为“区块链世界的操作系统”，此类区块链平台允许节点自由加入网络，且所有节点均有权限查看账本信息。典型的、当前应用最为广泛的公有链平台为以太坊。以太坊供了图灵完备的编程语言，允许开发者部署智能合约，可帮助处理复杂业务流程。然而，受限于交易处理速度、可扩展性等，以上公链平台难以进行大规模商业应用落地。自2017年以来，区块链逐步成为能够构建更高效社会活动的一种社会关系，成为能够减少摩擦高效率的新范式。业界开始追求公链底层技术新的突破，探索更加普适、稳定的公链平台，并将基于该类平台的下一个时代定义为区块链3.0。目前，公链3.0平台仍处于探索阶段，大部分主网暂未上线。据各平台对外公布数据，可以预见的是，2018年将是公链3.0平台高速发展的元年，各公链主网将陆续于2018年下半年至2019年完成上线。

联盟链通常被用于政府机构、商业机构及公司之间，节点通过准入机制得到授权后方可加入，不同节点所拥有的信息查看权限不同[5]。典型的区块链联盟项目如超级账本(Hyperleger)、R3。超级账本(Hyperledger)项目由Linux基金会发起，旨在构建跨行业开源区块链商业平台，推动各行业成员协同合作、共建开放平台、简化业务流程[6]。其中，专注于供企业级区块链解决方案的IBMHyperLeger(也即Fabric)区块链平台备受关注。R3是由美国初创公司R3CEV发起的金融行业区块链联盟，目前已吸引多家国内外金融机构加盟。该项目旨在为银行业供探索区块链技术的渠道，同时开发分布式账本平台Corda。

根据实现方式和作用目的的不同，当前基于区块链技术的应用可以划分为三类场景，如表1所示：

1. 价值转移类，数字资产在不同账户之间转移，如跨境支付。
2. 是存证类，将信息记录到区块链上，但无资产转移，如电子合同。
3. 授权管理类，利用智能合约控制数据访问[7]，如数据共享。此外，随着应用需求的不断升级，还存在多类型融合的场景。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **类型** | **政府** | **金融** | **工业** | **医疗** | **法律** | **版权** |
| **价值转移** |  | 数字票据  跨境支付  应收账款  供应链金融 | 能源交易 | 医疗保险 |  |  |
| **存证** | 电子发票  电子证照  精确扶贫 | 现钞冠字号溯源  供应链金融 | 防伪溯源 | 电子病例  药品溯源 | 公证  电子存证  网络仲裁 | 版权确认 |
| **授权管理** | 政府数据共享 | 征信 |  | 健康数据共享 |  | 版权管理 |

表1 区块链应用场景分类

# 三、区块链的关键技术

## 3.1 密码学

区块链中多个环节使用密码学算法。密码库为上层组件提供基本的密码学算法支持，包括各种常用的编码算法、哈希算法、签名算法、隐私保护算法等。与此同时，密码库还涉及诸如密钥的维护和存储之类的功能。

### 3.1.1 哈希函数

哈希函数是一种数学函数，满足如下两个条件：第一，输入任何字符串可以是任意长度，对应输出字符串的长度是确定的。第二，它是可以有效计算的：对于长度为n的输入，能够用O(n)的时间计算得到输出。在安全应用中使用的哈希函数被称为密码学哈希函数，一个密码学哈希函数需要满足如下条件[8]：抗碰撞性、难题友好性和隐蔽性。

密码学哈希函数的概念最早被提出于文献[9]，它可以应用在消息认证，消息承诺，数字签名等算法中。经典的密码学哈希函数有MD系列算法、SHA系列算法、RIPEMD系列算法等[10]。比特币系统计算公钥地址时用到了密码学哈希函数RIPEMD160和SHA-256。矿工挖矿时计算的数学难题也是SHA-256，它是利用Merkle-Damgard转换[11]来实现的，由于压缩函数的输入长度是确定，因此，需要对长度不确定的输入字符串分块。

### 3.1.2 签名算法

数字签名是利用密码学技术来实现的一种电子签名。为了模拟传统的纸上签名，数字签名需要满足这些条件：首先，只有本人能够签名他人无法伪造，但是所有人都可以验证签名的正确性。其次，该签名与特定文件关联，因此不能被用于其他文件。

比特币系统使用的数字签名算法是椭圆曲线数字签名算法（ECDSA），椭圆曲线数字签名算法[12]是基于椭圆曲线上的离散对数（ECDLP）这个困难问题而设计的。本文将在后续内容中用到部分盲签名算法。部分盲签名的思想是由 Abe 等人在1996 年提出的。与传统的数字签名不同，部分盲签名具有一定的盲性：除了事先与被签名者协商好的共识消息外，签名者无法获取所签消息的信息，这在一定程度上保护了被签名者的隐私。同态加密算法是指，对若干密文进行运算得到的结果，可由对应明文进行有效运算后得到。有些加密算法对某一种运算具有同态性，比如在工程上应用比较广泛的 Paillier 加密算法[13]，它具有加法同态性。

## 3.2 节点间共识机制

共识机制本质上是一套博弈系统:共识的产生需要付出一定的代价，矿工努力工作后能获得有效的奖励，通过一奖一罚的博弈保证系统稳定实施。现存的共识机制，在应用层面比较专注于某一特定场景并存在一定程度的短板。比如PBFT比较适用于联盟网络的共享账本技术，POW能耗较高、POS存在中心恶意干涉的可能性等[14]。

在当前的技术背景下，功能过于全面的共识算法无法真正可用。在新一代区块链共识机制的设计过程中，根据实际应用场景，有的放矢的选择去中心化、节能、安全等设计原则，对一些原则支持强弱进行取舍，将一定程度上升系统的整体运行效率。因此，在新一代的区块链系统设计中，可插拔的共识机制可能是未来发展的主要方向:在区块链解决方案中，应该实现兼容多种共识算法，在实际业务落地中有选择性的使用一种最合适的共识机制，甚至整个网络具备让开发者自定义共识机制的能力。

共识机制在区块链中扮演着核心的地位，决定了谁有记账的权利，以及记账权利的选择过程和理由，因此一直是区块链技术研究的重点。常见的共识机制包括PoW、PoS、DPoS、拜占庭容错[15]等，根据适用场景的不同，也呈现出不同的优势和劣势。单一共识机制，各自有其缺陷，例如PoS依赖代币且安全性脆弱，PoW非终局且能耗较高。为提升效率，需在安全性、可靠性、开放性等方面进行取舍。区块链正呈现出根据场景切换共识机制的趋势，并且将从单一的共识机制向多类混合的共识机制演进，运行过程中支持共识机制动态可配置，或系统根据当前需要自动选择相符的共识机制。

## 3.3 智能合约

智能合约是一种可编程化的数字协议，当合约参与方满足触发条件后，合约条款将自动执行。智能合约的加入，为区块链带来了新的契机，保障部署在区块链上的合同条款可以实现自动、去中心化[16]的计算，从而为诸多领域(尤其针对流程复杂繁琐、效率低下的领域)的效率升、成本控制起到不可忽视的作用。

智能合约应用是否丰富，取决于智能合约自身及其所在区块链对于智能合约应用的支撑能力，而智能合约的开发和执行效率则取决于开发语言和执行虚拟机。在目前的生态系统中，智能合约的开发语言不够规范，为了适应智能合约，需要创造新的合约语言或为现有语言增加形式更为严格的规范和校验。智能合约在轻量级的执行环境中将实现快速的启动时间和较高的执行效率。

智能合约的发展方向包括如下几点:

1. 可插拔的执行环境架构:默认的执行环境应该不提供持久化存储，让合约默认是一种类似于微服务的无状态函数，从而直接进行并发处理。
2. 明示化的调用关系:即只提供静态调用的功能，从而使得程序的调用关系可以在运行它之前就整理清楚。
3. 可链外存储的合约代码:通过链上存储散列值、链外存储合约代码实现存储空间的扩展性。
4. 低耦合度的设计:降低合约语言、执行环境、区块链之间的耦合度，提高智能合约系统的通用性;5)完整安全的防护体系:代码定型与发布时的验证与检查，节点在执行合约中的动态验证，合约执行完毕的合理性判断，相关利益方的申诉机制与自动判决技术[17]。

智能合约根据图灵完备与否可以分为两类，即图灵完备和非图灵完备。影响实现图灵完备的常见原因包括:循环或递归受限、无法实现数组或更复杂的数据结构等。图灵完备的智能合约有较强适应性，可以对逻辑较复杂的业务操作进行编程，但有陷入死循环的可能。对比而言，图灵不完备的智能合约虽然不能进行复杂逻辑操作，但更加简单、高效和安全。

|  |  |  |
| --- | --- | --- |
| **区块链平台** | **是否图灵完备** | **开发语言** |
| **比特币** | 不完备 | Bitcoin Script |
| **以太坊** | 完备 | Solidity |
| **EOS** | 完备 | C++ |
| **Hyperledger Fabric** | 完备 | Go |
| **Hyperledger Sawtooth** | 完备 | Python |
| **R3 Corda** | 完备 | Kotlin／Java |

表2 部分区块链系统的智能合约特性

当前智能合约的应用仍处于比较初级的阶段，智能合约成为区块链安全的“重灾区”。从历次智能合约漏洞引发的安全事件看，合约编写存在较多安全漏洞，对其安全性带来了巨大挑战。目前，提升智能合约安全性一般有几个思路:一是形式化验证(FormalVerification)。通过严密的数学证明来确保合约代码所表达的逻辑符合意图。此法逻辑严密，但难度较大，一般需要委托第三方专业机构进行审计。二是智能合约加密。智能合约不能被第三方明文读取，以此减少智能合约因逻辑上的安全漏洞而被攻击。此法成本较低，但无法用于开源应用。三是严格规范合约语言的语法格式。总结智能合约优秀模式，开发标准智能合约模板，以一定标准规范智能合约的编写可以提高智能合约质量，提高智能合约安全性[18]。

## 3.4 隐私保护技术

在传统的信息系统中，隐私保护通常是指数据拥有者不愿意泄露的原始数据或者数据背后所具有的属性。而在区块链中，为了在不同节点之间达成共识，很多信息必须公开，以使各个节点之间同步。但是，另外一方面，在区块链系统中也有隐私保护的要求[19]，对于一些敏感的信息，数据拥有者需要对其进行加密或者其它处理，降低隐私泄露的风险。聚合签名[20]天然具有压缩信息的功能，在区块链系统中，尤其是在涉及多个输入与多个输出的交易中，聚合签名可以将对多个输入和输出的签名聚合成一个签名，进而压缩交易记录的存储，在不增加区块容量的前提下，增加每个区块可以容纳的交易数量。同时，通过将多个交易的签名以及多个交易信息聚合，可以隐藏每个账户的交易量，实现交易信息的隐私保护。

参考文献

1. Marc P . Blockchain Technology: Principles and Applications[J]. Social Science Electronic Publishing, 2015.
2. Lee L. New Kids on the Blockchain: How Bitcoin's Technology Could Reinvent the Stock Market[J]. Social Science Electronic Publishing, 2015.
3. 郑佩娜. 基于区块链技术的数字资产交易:案例分析视角[D].浙江大学,2018.
4. 李林. 当前比特币行业发展现状及政策研究[J]. 清华金融评论, 2015(8):96-100.
5. 黄方蕾. 联盟区块链中成员动态权限管理方法的设计与实现[D].浙江大学,2018.
6. 史文斌. 基于Hyperledger Fabric的区块链应用系统云服务化[D].浙江大学,2018.
7. 张青禾. 区块链中的身份识别和访问控制技术研究[D].北京交通大学,2018.
8. Narayanan A, Bonneau J, Felten E, et al. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction[M]. Princeton University Press, 2016.
9. Diffie W, Hellman M E. New directions in cryptography[J]. IEEE Transactions on Information Theory, 1976, 22(6):644-654.
10. Mironov I . Hash Functions: From Merkle-Damgard to[J]. Eurocrypt, 2001, 2001:166181.
11. Johnson D, Menezes A, Vanstone S. The Elliptic Curve Digital Signature Algorithm (ECDSA)[J]. International Journal of Information Security, 2001, 1(1):36-63.
12. Abe M, Fujisaki E. How to date blind signatures[M]// Advances in Cryptology — ASIACRYPT '96. Springer Berlin Heidelberg, 1996:244-251.
13. Paillier P . Public-Key Cryptosystems Based on Composite Degree Residuosity Classes[J]. Advances in Cryptology — Eurocrypt, 1999, 547(1):223--238.
14. Yang Y. LinBFT: Linear-Communication Byzantine Fault Tolerance for Public Blockchains[J]. 2018.
15. Leslie Lamport,Robert Shostak,Marshall Pease. The Byzantine Generals Problem[J]. ACM Transactions on Programming Languages and Systems (TOPLAS),1982,4(3).
16. 安庆文. 基于区块链的去中心化交易关键技术研究及应用[D]. 东华大学, 2017.
17. 张成成. 区块链安全技术的研究与应用[D].西华大学,2018.
18. 卓海振. 基于区块链的智能合约优化研究与实现[D].浙江大学,2018.
19. 苑超. 区块链隐私保护关键技术研究[D].战略支援部队信息工程大学,2018.
20. Li F , Chen Z , Guan Z , et al. An efficient certificateless aggregate signature with constant pairing computations[J]. Information Sciences, 2013, 219(10):225-235.