区块链技术研究报告

1.背景

近年来，加密货币引起了工业界和学术界的广泛关注。经常被称为第一种加密货币的比特币取得了巨大成功，2016 年资本市场达到 100 亿美元。区块链是比特币的核心机制。区块链于 2008 年首次提出，2009 年被实施。区块链可以看作是一个公共分类账本，其中所有提交的交易都存储在一个区块链中。当新的块被添加到该链时，该链不断增长。区块链技术具有关键特征，如分散性、持久性、匿名性和可审计性。区块链可以在分散的环境中工作，这是通过集成密码哈希、数字签名(基于非对称密码)和分布式共识机制等几项核心技术来实现的。有了区块链技术，交易可以以分散的方式进行。因此，区块链可以大大节约成本，提高效率。

虽然比特币是区块链应用中最著名的应用，但区块链可以应用到远远超出加密货币的各种应用中。由于区块链允许在没有任何银行或中介的情况下完成支付，因此它可以用于各种金融服务，如数字资产、汇款和在线支付。此外，技术正在成为下一代互联网交互系统最有前途的技术之一，如智能合同、公共服务、物联网、信誉系统和安全服务。

2. 国内外研究现状和趋势

2.1 经典区块链应用

以比特币为代表的第一代区块链系统，主要解决货币产生以及交易的去中心化问题。以以太坊为代表的第二代区块链系统，其将智能合约技术引入到区块链中。以 Hyperledger 为代表的第三代区块链系统，致力于解决区块链平台的可扩展性。

2008 年全球金融危机爆发后，一个名为“中本聪”的学者设计出了一种名为比特币的网络虚拟货币。比特币是基于密码编码，通过复杂算法所产生的，其通过电子签名来实现流通，通过分布式记账的方式来保证交易的安全与可靠。比特币九年的稳定运行，充分验证了其底层区块链技术的可行性与安全性。

受比特币的启发，2013 年底，程序员 VitalikButerin 提出了以太坊公共区块链平台。以太坊提供了一套图灵完备的脚本语言 EVM 来编写去中心化的应用程序，并首次将智能合约引入到区块链中，目前已有多个成熟的基于以太坊所创建的项目或应用场景。

Hyperledger 是 2015 年由 linux 基金发起的一个区块链项目，该项目的目的是打造一个公开、透明、去中心化的超级账本，建立区块链技术的开源规范与标准，使更多的应用轻松地建立的区块链技术之上。目前，全球有 200 多家的企业与机构已经加入到 Hyperledger 项目。

Hyperledger 目前已有多个相对比较成熟的项目，例如 Burrow、Fabric、Iroha、Sawtooth、Indy 等。其中，Burrow 提供了一个模块化的区块链客户端，可以看做是一个支持许可的智能合约机；Faric 是专门针对企业级的区块链应用而设计的，其采用模块化的架构作为开发区块链程序的基础，支持身份识别与权限控制，支持多种编程语言，支持共识算法及成员服务的即插即用；Sawtooth 是一个创建、部署和运行分布式账本的模块化平台；Indy 是为去中心化的身份而建立的一种分布式账本。

2.2 BAT 布局区块链

由于区块链能够减少交易成本，提高经济效率，助力经济发展，越来越多的企业将区块链作为转型方向，截至 2018 年 3 月底，我国以区块链业务为主营业务的区块链公司数量已经达到了 456 家。截止到 6 月份以区块链概念上市的公司就已经达到了 67 家，区块链产业已经初步形成规模。国内众多互联网公司积极布局区块链，百度、阿里巴巴、腾讯、京东、网易、苏宁等都已经展开了对区块链的研究，并取得了初步的成效。腾讯区块链主要提供共享账本与数字资产服务，于 2017 年 6 月发布企业级区块链数据库——TrustSQL，次年 5 月份发布首款基于该平台的区块链游戏。TrustSQL 有两个优点：一是支持 SQL 接口访问，用户可以沿用以前的开发习惯；二是独创内置智能合约，执行起来更加的安全、高效。百度 2017 年 7 月推出了商业级区块链开放平台 BaaS；2018 年 3 月发布图腾项目解决版权保护问题；2018 年 6 月份发布新一代区块链网络操作系统—超级链。阿里巴巴 2016 年 7 月将区块链技术引入到支付宝爱心捐助平台，实现捐款信息可溯源；之后又将区块链技术引入到商品溯源中，实现对物品的跟踪，防止造假。

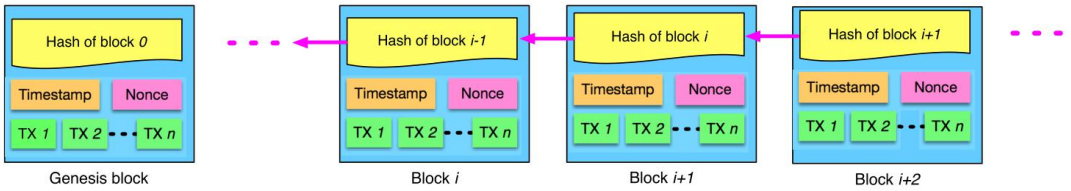
2.3 学术研究情况

在计算机科学中，近年来围绕区块链发表了各种论文，例如，Eyal 和 Sirer 等人于 2014 年分析了共识算法，Kosba 等人于 2016 年提出了解决智能合同隐私问题的新概念。然而，除了许多关于区块链的行业白皮书，区块链信息系统的学术论文目前主要集中在加密货币上。除了显著的好处，也有缺点和潜在的风险，这些都在这一系列的文献中讨论过。Barber 等人(2012 年)强调了比特币的几个弱点，如比特币被盗或丢失(恶意软件攻击、意外丢失)、可扩展性问题(如延迟交易确认、数据保留和通信故障)以及结构性问题(如通缩螺旋)。与此同时，巴伯等人(2012)提出了改进现有比特币技术的解决方案。例如，“公平交换协议”可以提高用户的匿名性。其他作者也讨论了比特币的隐私含义。在现在的比特币世界里，隐私只能用假名来保护。作为比特币的扩展，迈尔斯等人在 2013 年因此开发了零币，允许完全匿名地交易加密货币。2016 年，零币的继承者 Zcash 上线。如果数据块以高速率添加到网络中，则生成新数据块的过程意味着性能问题。作为现有区块链结构的替代方案，勒文伯格等人于 2015 年引入了“包容性区块链协议”，以提高交易速度。观察这种新技术是否能克服性能问题将是很有趣的。克罗曼等人于 2016 年提供了一份关于比特币可扩展性的分析。

3. 相关理论概述

3.1 区块链简介

区块链是一个区块序列，它拥有一个完整的交易记录列表，就像传统的公共分类账一样。图 1 展示了一个区块链的例子。每个块通过一个引用指向前一个块，该引用本质上是前一个块的哈希值，称为父块。区块链的第一个区块叫做创世纪区块，它没有母区块。



3.2 区块链的主要特点

区块链有以下主要特点：

(1) **去中心化**。在传统的集中式交易系统中，每笔交易都需要通过中央可信机构(例如中央银行)进行验证，这不可避免地导致中央服务器的成本和性能瓶颈。不同的是，区块链网络中的交易可以在任何两个对等体(P2P)之间进行，而无需中央机构的认证。通过这种方式，区块链可以显著降低服务器成本(包括开发成本和运营成本)，并缓解中央服务器的性能瓶颈。

(2) **不可篡改**。由于跨网络传播的每个事务都需要在分布于整个网络的块中进行确认和记录，因此几乎不可能篡改。此外，每个广播块将由其他节点验证，并检查事务。所以任何伪造都很容易被发现。而且只有掌握整个系统 51%节点，才能对区块链信息进行篡改，而这几乎不可能实现。

(3) **可追溯**。区块链本身是一个块链式数据结构，链上的信息依据时间顺序环环相扣，这就使得区块链具有可追溯性。运用到生活上，就是产品的种植、生产、运输、销售、监管等所有信息均被记录在区块链上。一旦发生任何问题，就可以往前追溯，检测每个环节，以确保产品的安全性。

(4) **开放性**。由于区块链是去中心化的，所有网络节点都可以参与区块链网络数据的记录维护。这要求区块链网络必须是开放的。区块链网络只有开放了，才能保证所有人都可以参与进来，才能保证数据的安全性。

区块链数据记录和运行规则可以被全网节点审查、追溯,具有很高的透明度区块链公有链就是充分展示区块链开放透明的例子。

(5)**匿名性**。如果说去中心化是很多人了解区块链的动力，那么匿名性则是很多人选择区块链的重要原因。区块链运用哈希运算、非对称加密、私钥公钥等密码学手段，在实现数据完全开放的前提下，保护个人交易隐私。

区块链的匿名性目前也屡受质疑，原因是部分不法分子利用区块链开展洗钱、资产盗取等非法行为，但由于区块链具备匿名性，仅通过地址无法获知不法分子相关身份信息，导致不法分子可以不被发现、逍遥法外，引发监管难题。目前各大项目均通过加强技术防范，降低甚至避免不法行为的发生。

3.3 区块链核心技术

3.3.1 共识机制

区块链系统是一个去中心化的分布式系统，节点分散在各处，为了保证节点愿意主动去记账，区块链形成了一个重要的共识机制，这种共识机制也被称为区块链的灵魂。简单来说，共识机制是区块链节点就区块信息达成全网一致共识的机制，可以保证最新区块被准确添加至区块链、节点存储的区块链信息一致不分叉，甚至可以抵御恶意攻击。实践中要达到这样的效果需要满足两方面条件：一是选择一个独特的节点来产生一个区块，二是使分布式数据记录不可逆。

当前主流的共识机制包括：工作量证明/POW（ProofofWork）、权益证明/POS（ProofofStake）、股份授权证明/DPOS（DelegatedProof-of-Stake）、实用拜占庭容错（PBFT）、瑞波共识协议等。这里简单介绍一下 POW。POW 是最初的一种共识机制，就是一份证明，用来确认做过一定量的工作。通过数学运算，计算出一个满足规则的随机数，随后发出本轮需要记录的数据，全网其它节点验证后一起存储。同时其他节点对该节点的区块结果进行验证，通过后则接受这个区块。由于可以互相验证，也保证了数据的可靠性。工作量证明是目前最流行的算法，应用于大多数加密货币的共识机制上。

3.3.2 密码学原理

密码学技术是区块链的核心技术之一，目前的区块链应用中采用了很多现代密码学的经典算法，主要包括：哈希算法、对称加密、非对称加密、数字签名等。其中非对称加密技术是保障安全的重要部分。其需要两个密钥：公钥和私钥。公钥与私钥是一对，如果用公钥对数据进行加密，只有用对应的私钥才能解密；如果用私钥对数据进行加密，那么只有用对应的公钥才能解密。

其实现机密信息交换的基本过程是：甲方生成一对密钥并将其中的一把作为公钥向其它方公开；得到该公钥的乙方使用该密钥对机密信息进行加密后再发送给甲方；甲方再用自己保存的另一把专用密钥对加密后的信息进行解密。

3.3.3 分布式存储

区块链最吸引人的是其分布式存储的机制，即去中心化的思想。区块链中每一个区块上的信息记录，都是由参与记账的每一个电脑，即节点竞争记录的。去中心化的分布式存储数据可以说是区块链的特点之一，它可以在所有节点上实现分布式的数据存储，并完整保存下来。

区块链分布式存储可以很好地解决传统的集中式存储存在数据安全性和可靠性的问题，（分布式存储把一个完整的文件给切开，分成 N 片，我们称它为切片，然后把这 N 个切片加密数据存储到各个不同的硬盘上，每个硬盘只保存这个文件的一小部分。同时，有关切片文件的存储信息会被记录到区块链上，以防止信息被篡改。）

在区块链领域，分布式存储可以应用在很多场景中。例如沃尔玛早已就使用区块链平台保存支付数据提出了两项专利申请，涉及到供应商支付共享系统，并创建一个能够代表客户指定交易的网络，为供应商存储付款数据，同时也将确保付款数据安全。

3.3.4 智能合约

智能合约是一种用计算机语言取代法律语言去记录条款的合约。智能合约是在区块链数据库上运行的计算机程序，可以在满足其源代码中写入的条件时自行执行。智能合约有三个技术特性：

(1) **数据透明**

智能合约的数据处理是公开透明的，运行时任何一方都可以查看其代码和数据。

(2) **不可篡改**

部署在区块链上的智能合约代码以及运行产生的数据输出是不可篡改的，运行智能合约的节点不必担心其他节点恶意修改代码与数据。

(3) **永久运行**

支撑区块链网络的节点往往达到数百甚至上千，部分节点的失效并不会导致智能合约的停止，其可靠性理论上接近于永久运行，这样就保证了智能合约能像纸质合同一样每时每刻都有效。

下面介绍一下智能合约的工作原理。

开发人员会为智能合约撰写代码，该代码包含一些会触发合约自动执行的条件，一旦编码完成，智能合约就会被上传到区块链网络上，即它们被发送到所有连接到网络的设备上。一旦将数据上传到所有设备上，用户就可以与执行程序代码的结果达成协议。然后更新数据库以记录合约的执行情况，并监督合约的条款以检查合规性。单独的一方无法操纵合约，因为对智能合约执行的控制权不在任何单独一方的手中。

智能合约在各个领域都有很广泛的应用，比如，与房屋租金协议相关的智能合约只有当业主收到租金才会触发自动执行，并将公寓的安全密钥发送给租户。这个合约可以确保租金的定期支付，并且每个月重启。

3.4 区块链体系

区块链通用层次化技术结构，自下而上分别为网络层、数据层、共识层、控制层和应用层。其中，网络层是区块链信息交互的基础，承载节点间的共识过程和数据传输，主要包括建立在基础网络之上的对等网络及其安全机制；数据层包括区块链基本数据结构及其原理；共识层保证节点数据的一致性，封装各类共识算法和驱动节点共识行为的奖惩机制；控制层包括沙盒环境、自动化脚本、智能合约和权限管理等，提供区块链可编程特性，实现对区块数据、业务数据、组织结构的控制；应用层包括区块链的相关应用场景和实践案例，通过调用控制合约提供的接口进行数据交互。

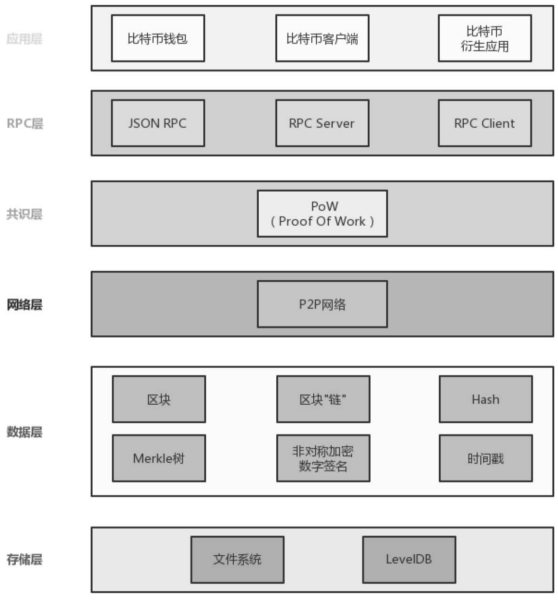
4.技术选型分析

区别于其他技术，区块链发展过程中最显著的特点是与产业界紧密结合，伴随着加密货币和分布式应用的兴起，业界出现了许多区块链项目。这些项目是区块链技术的具体实现，既有相似之处又各具特点，本节将根据前文所述层次化结构对比特币、以太坊、超级账本项目进行分析。

4.1 比特币

4.1.1 体系结构

如图所示，比特币系统分为 6 层，由下至上依次是存储层、数据层、网络层、共识层、RPC 层、应用层。



其中，**存储层**主要用于存储比特币系统运行中的日志数据及区块链元数据，存储技术主要使用文件系统和 LevelDB。

数据层主要用于处理比特币交易中的各类数据，如将数据打包成区块，将区块维护成链式结构，区块中内容的加密与哈希计算，区块内容的数字签名及增加时间戳印记，将交易数据构建成 Merkle 树，并计算 Merkle 树根节点的哈希值等。

区块构成的链有可能分叉，在比特币系统中，节点始终都将最长的链条视为正确的链条，并持续在其后增加新的区块。

网络层用于构建比特币底层的 P2P 网络，支持多节点动态加入和离开，对网络连接进行有效管理，为比特币数据传输和共识达成提供基础网络支持服务。

共识层主要采用了 PoW(ProofOfWork)共识算

法。在比特币系统中，每个节点都不断地计算一个随机数(Nonce)，直到找到符合要求的随机数为止。在一定的时间段内，第一个找到符合条件的随机数将得到打包区块的权利，这构建了一个工作量证明机制。从 PoW 的角度，是不是发现 PoW 和分布式锁有异曲同工之妙呢?

RPC 层实现了 RPC 服务，并提供 JSONAPI 供客户端访问区块链底层服务。

应用层主要承载各种比特币的应用，如比特币开源代码中提供了 bitcoinclient。该层主要是作为 RPC 客户端，通过 JSONAPI 与 bitcoin 底层交互。除此之外，比特币钱包及衍生应用都架设在应用层上。

4.1.2 比特币脚本语言存在的限制

（1）缺少图灵完备性

这就是说，尽管比特币脚本语言可以支持多种计算，但是它不能支持所有的计算。最主要的缺失是循环语句。不支持循环语句的目的是避免交易确认时出现无限循环。理论上，对于脚本程序员来说，这是可以克服的障碍，因为任何循环都可以用多次重复 if 语句的方式来模拟，但是这样做会导致脚本空间利用上的低效率，例如，实施一个替代的椭圆曲线签名算法可能将需要 256 次重复的乘法，而每次都需要单独编码。

（3）价值盲（Value-blindness）

UTXO 脚本不能为账户的取款额度提供精细的控制。例如，预言机合约（oraclecontract）的一个强大应用是对冲合约，A 和 B 各自向对冲合约中发送价值 1000 美元的比特币，30 天以后，脚本向 A 发送价值 1000 美元的比特币，向 B 发送剩余的比特币。虽然实现对冲合约需要一个预言机（oracle）决定一比特币值多少美元，但是与现在完全中心化的解决方案相比，这一机制已经在减少信任和基础设施方面有了巨大的进步。然而，因为 UTXO 是不可分割的，为实现此合约，唯一的方法是非常低效地采用许多有不同面值的 UTXO（例如对应于最大为 30 的每个 k，有一个 2^k 的 UTXO)并使预言机挑出正确的 UTXO 发送给 A 和 B。

（4）缺少状态

UTXO 只能是已花费或者未花费状态，这就没有给需要任何其它内部状态的多阶段合约或者脚本留出生存空间。这使得实现多阶段期权合约、去中心化的交换要约或者两阶段加密承诺协议（对确保计算奖励非常必要）非常困难。这也意味着 UTXO 只能用于建立简单的、一次性的合约，而不是例如去中心化组织这样的有着更加复杂的状态的合约，使得元协议难以实现。二元状态与价值盲结合在一起意味着另一个重要的应用-取款限额-是不可能实现的。

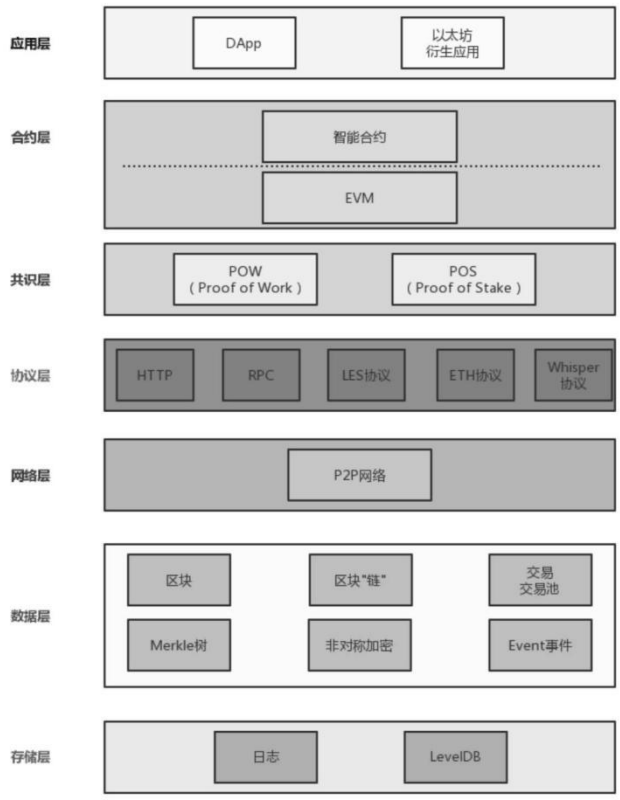
（5）区块链盲（Blockchain-blindness）

UTXO 看不到区块链的数据，例如随机数和上一个区块的哈希。这一缺陷剥夺了脚本语言所拥有的基于随机性的潜在价值，严重地限制了博彩等其它领域应用。

4.2 以太坊

4.2.1 系统架构

如图所示，以太坊架构分为 7 层，由下至上依次是存储层、数据层、网络层、协议层、共识层、合约层、应用层。



其中**存储层**主要用于存储以太坊系统运行中的日志数据及区块链元数据，存储技术主要使用文件系统和 LevelDB。

数据层主要用于处理以太坊交易中的各类数据，如将数据打包成区块，将区块维护成链式结构，区块中内容的加密与哈希计算，区块内容的数字签名及增加时间戳印记，将交易数据构建成 Merkle 树，并计算 Merkle 树根节点的 hash 值等。

与比特币的不同之处在于以太坊引入了交易和交易池的概念。交易指的是一个账户向另一个账户发送被签名的数据包的过程。而交易池则存放通过节点验证的交易，这些交易会放在矿工挖出的新区块里。

以太坊的 Event(事件)指的是和以太坊虚拟机提供的日志接口，当事件被调用时，对应的日志信息被保存在日志文件中。

与比特币一样，以太坊的系统也是基于 **P2P 网络**的，在网络中每个节点既有客户端角色，又有服务端角色。

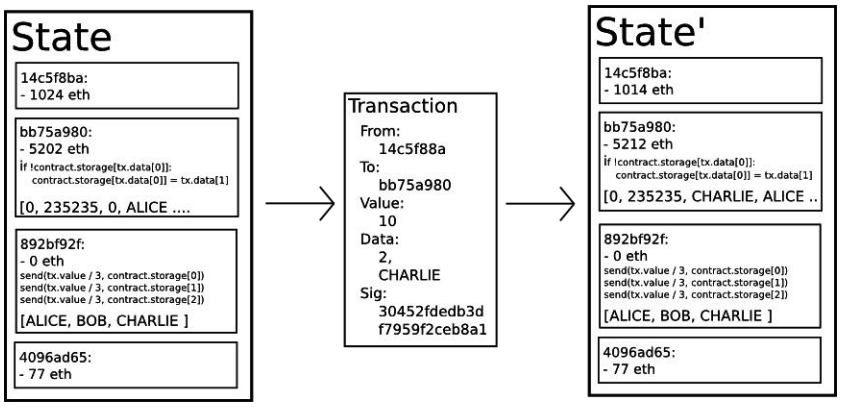
协议层是以太坊提供的供系统各模块相互调用的协议支持，主要有 HTTP、RPC 协议、LES、ETH 协议、Whipser 协议等。以太坊基于 HTTPClient 实现了对 HTTP 的支持，实现了 GET、POST 等 HTTP 方法。外部程序通过 JSONRPC 调用以太坊的 API 时需通过 RPC(远程过程调用)协议。Whisper 协议用于 DApp 间通信。LES 的全称是轻量级以太坊子协议(LightEthereumSub-protocol)，允许以太坊节点同步获取区块时仅下载区块的头部，在需要时再获取区块的其他部分。

共识层在以太坊系统中有 PoW(ProofofWork)和 PoS(ProofofStake)两种共识算法。

合约层分为两层，底层是 EVM(EthereumVirtualMachine，即以太坊虚拟机)，上层的智能合约运行在 EVM 中。智能合约是运行在以太坊上的代码的统称，一个智能合约往往包含数据和代码两部分。智能合约系统将约定或合同代码化，由特定事件驱动触发执行。因此，在原理上适用于对安全性、信任性、长期性的约定或合同场景。在以太坊系统中，智能合约的默认编程语言是 Solidity，一般学过 JavaScript 语言的读者很容易上手 Solidity。

应用层有 DApp(DecentralizedApplication，分布式应用)、以太坊钱包等多种衍生应用，是目前开发者最活跃的一层。

4.2.2 以太坊状态转换函数



以太坊的状态转换函数：APPLY(S,TX)->S’，可以定义如下：

（1）检查交易的格式是否正确（即有正确数值）、签名是否有效和随机数是否与发送者账户的随机数匹配。如否，返回错误。
（2）计算交易费用:fee=STARTGAS*GASPRICE，并从签名中确定发送者的地址。从发送者的账户中减去交易费用和增加发送者的随机数。如果账户余额不足，返回错误。
（3）设定初值 GAS=STARTGAS，并根据交易中的字节数减去一定量的燃料值。
（4）从发送者的账户转移价值到接收者账户。如果接收账户还不存在，创建此账户。如果接收账户是一个合约，运行合约的代码，直到代码运行结束或者燃料用完。
（5）如果因为发送者账户没有足够的钱或者代码执行耗尽燃料导致价值转移失败，恢复原来的状态，但是还需要支付交易费用，交易费用加至矿工账户。
（6）否则，将所有剩余的燃料归还给发送者，消耗掉的燃料作为交易费用发送给矿工。

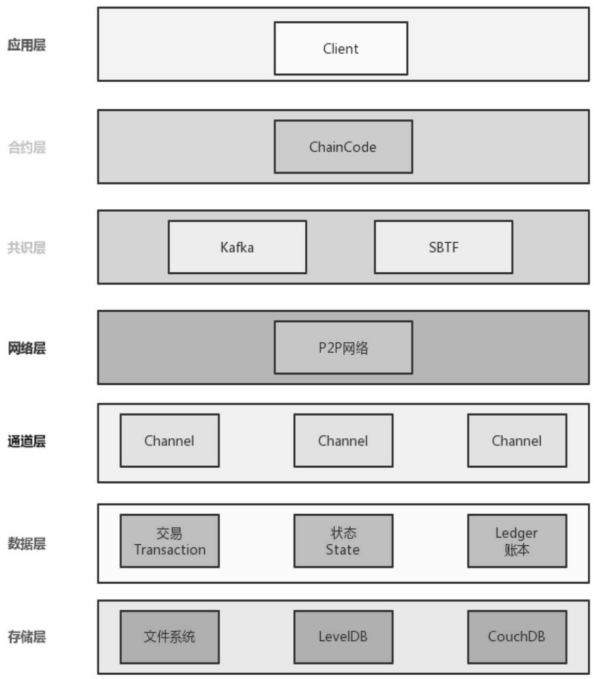
4.3 Hyperledger 架构

超级账本(Hyperledger)是Linux基金会于2015年发起的推进区块链数字技术和交易验证的开源项目，该项目的目标是推进区块链及分布式记账系统的跨行业发展与协作。

目前该项目最著名的子项目是 Fabric，由 IBM 主导开发。按官方网站描述，HyperledgerFabric 是分布式记账解决方案的平台，以模块化体系结构为基础，提供高度的弹性、灵活性和可扩展性。它旨在支持不同组件的可插拔实现，并适应整个经济生态系统中存在的复杂性。

4.3.1 体系结构

HyperledgerFabric 可以分为 7 层，分别是存储层、数据层、通道层、网络层、共识层、合约层、应用层。



其中**存储层**主要对账本和交易状态进行存储。账本状态存储在数据库中，存储的内容是所有交易过程中出现的键值对信息。比如，在交易处理过程中，调用链码执行交易可以改变状态数据。状态存储的数据库可以使用 LevelDB 或者 CouchDB。LevelDB 是系统默认的内置的数据库，CouchDB 是可选的第三方数据库。区块链的账本则在文件系统中保存。

数据层主要由交易(Transaction)、状态(State 和账本(Ledger)三部分组成。

其中，交易有两种类型：

（1）部署交易：以程序作为参数来创建新的交易。部署交易成功执行后,链码就被安装到区块链上。

（2）调用交易：在上一步部署好的链码上执行操作。链码执行特定的函数，这个函数可能会修改状态数据，并返回结果。

状态对应了交易数据的变化。在 HyperledgerFabric 中，区块链的状态是版本化的，用 key/valuestore(KVS)表示。其中 key 是名字，value 是任意的文本内容，版本号标识这条记录的版本。这些数据内容由链码通过 PUT 和 GET 操作来管理。如存储层的描述，状态是持久化存储到数据库的，对状态的更新是被文件系统记录的。

账本提供了所有成功状态数据的改变及不成功的尝试改变的历史。账本是由 OrderingService 构建的一个完全有序的交易块组成的区块哈希链(HashChain)。账本既可以存储在所有的 peers 节点上，又可以选择存储在几个 orderers 节点上。此外，账本允许重做所有交易的历史记录，并且重建状态数据。

通道层指的是通道(Channel)，通道是一种 HyperledgerFabric 数据隔离机制，用于保证交易信息只有交易参与方可见。每个通道都是一个独立的区块链，因此多个用户可以共用同一个区块链系统，而不用担心信息泄漏问题。

网络层用于给区块链网络中各个通信节点提供 P2P 网络支持，是保障区块链账本一致性的基础服务之一。

在 HyperledgerFabric 中，Node 是区块链的通信实体。Node 仅仅是一个逻辑上的功能，多个不同类型的 Node 可以运行在同一个物理服务器中。Node 有三种类型，分别是客户端、peers 节点和 OrderingService。其中，客户端用于把用户的交易请求发送到区块链网络中。peers 节点负责维护区块链账本，peers 节点可以分为 endoringpeers 和 committingpeers 两种。endoringpeers 为交易作认证，认证的逻辑包含验证交易的有效性，并对交易进行签名；committingpeers 接收打包好的区块，并写入区块链中。与 Node 类似，peers 节点也是逻辑概念，endoringpeers 和 committingpeers 可以同时部署在一台物理机上。OrderingService 会接收交易信息，并将其排序后打包成区块，然后，写入区块链中，最后将结果返回给 committingpeers。

共识层基于 Kafka、SBTF 等共识算法实现。HyperledgerFabric 利用 Kafka 对交易信息进行排序处理，提供高吞吐、低延时的处理能力，并且在集群内部支持节点故障容错。相比于 Kafka，SBFT(简单拜占庭算法)能提供更加可靠的排序算法，包括容忍节点故障以及一定数量的恶意节

点。

合约层是 HyperledgerFabric 的智能合约层 Blockchain，Blockchain 默认由 Go 语言实现。Blockchain 运行的程序叫作链码，持有状态和账本数据，并负责执行交易。在 HyperledgerFabric 中，只有被认可的交易才能被提交。而交易是对链码上的操作的调用，因此链码是核心内容。同时还有一类称之为系统链码的特殊链码，用于管理函数和参数。

应用层是 HyperledgerFabric 的各个应用程序。

此外，既然是联盟链，在 HyperledgerFabric 中还有一个模块专门用于对联盟内的成员进行管理，即 MembershipServiceProvider(MSP)，MSP 用于管理成员认证信息，为客户端和 peers 节点提供成员授权服务。

5. 区块链技术的潜在问题与风险

（一）安全性

以比特币为例，由于比特币采用的 PoW 共识认证机制，理论上任一拥有 51％及以上算力的节点具有操纵整个比特币区块链的能力 f1 目，即存在“51％攻击”问题。为解决 PoW 共识机制的。51％攻击”问题，业内工程师发明了 PoS 共识机制，即将以算力主导的工作量证明机制，改为持有相关区块链权益数量对应的投票权证明机制，从而解决算力操纵和计算资源浪费的问题。

（二）缺乏统一标准

由于不同企业、机构都倾向于研发自己的区块链系统，区块链技术所代表的分布式记账技术(DLT)有可能标准林立而各自为政。目前全行业亟需建立统一标准规范。

（三）用户保护

用户私钥保管及维护是区块链技术无法回避的问题。在现有区块链技术规则下，用户的私钥等价于个人身份信息，遗失后却无法追索，增加了用户身份被窃取盗用的风险，未来需要在安全性、便利性方面进行平衡。

（四）对金融系统的风险

区块链本质上是一种虚拟基础设施，其主要风险将集中于操作风险或是监管风险。以比特币为例，由于比特币的区块链网络是一项由数千个分布在全球各地的节点所维护，具有明显的匿名性和去中心化特征，因此一旦出现技术漏洞，这种管理机制将变得极其脆弱甚至会陷入混乱凹。

6. 结论

区块链基于多类技术研究的成果，以低成本解决了多组织参与的复杂生产环境中的信任构建和隐私保护等问题，在金融、教育、娱乐、版权保护等场景得到了较多应用，成为学术界的研究热点。比特币的出现重塑了人们对价值的定义，伴随着产业界的呼声，区块链技术得到了快速发展，而遵循区块链层次化分析方法，能够直观地区别各项目的技术路线和特点，为优化区块链技术提供不同观察视角，并为场景应用的深度融合创造条件，促进后续研究。未来的发展中，区块链将成为更为基础的信任支撑技术，在产业互联网等更广阔的领域健康、有序地发展。