

硕 士 研 究 生 读 书 报 告



题目 Hyperledger Fabric 的版本创新及其应用前景

作者姓名 张岩

作者学号 22051197

指导教师 李启雷

学科专业 电子信息

所在学院 软件学院

提交日期 2021 年 1 月

目录

[1、背景 3](#_Toc62748909)

[1.1 区块链简介 3](#_Toc62748910)

[1.2 区块链特点 3](#_Toc62748911)

[2、Hyperldger Fabric 3](#_Toc62748912)

[2.1 超级账本的发展历程及简介 3](#_Toc62748913)

[2.2 Hyperledger Fabric的系统逻辑架构图 4](#_Toc62748914)

[2.3 超级账本各个模块及其基本功能 4](#_Toc62748915)

[2.4区块链技术平台的比较 5](#_Toc62748916)

[2.4.1 共识算法 5](#_Toc62748917)

[2.4.2 智能合约 6](#_Toc62748918)

[2.5 Fabric1.0采用的新框架 6](#_Toc62748919)

[2.6 交易流程 7](#_Toc62748920)

[2.6.1 交易中的节点 7](#_Toc62748921)

[2.6.2交易过程详细流程 7](#_Toc62748922)

[2.7 Fabric 1.0 的Evaluation 8](#_Toc62748923)

[3、Hyperledger Fabric的优势 10](#_Toc62748924)

[3.1 Hyperledger Fabric的安全保障 10](#_Toc62748925)

[3.2模块化设计，可插拔架构 10](#_Toc62748926)

[3.3高性能和可扩展 10](#_Toc62748927)

[3.4提供丰富的查询功能 10](#_Toc62748928)

# 1、背景

## 1.1 区块链简介

区块链在比特币系统中是作为一个分布式共享账本的形式存在，同时也是比特币的底层技术，在其中发挥连接沟通的作用，使得网络中所有节点之间形成稳定的信任关系。区块链实质上是一种以块链形式数据结构存储和验证数据、以分布式共识算法生成和更新数据、以密码学方式加密数据、保障传输、同时以自动化脚本代码进行数据运算和系统运转的分布式构架。

区块链是一种去中心化的数据库，去除了传统第三方支付平台中的中央数据库，继而由网络中千千万万个节点来共同承担数据库的作用，储存和维护发生在网络中的每一笔交易信息，因此，每个节点既扮演数据库维护者的角色，也发挥数据共享者的作用。然而，在区块链系统中，仅仅做到去中心化还不能完全保障数据安全，还需将网络中各个区块之间进行链接，共同记录和监管所有的交易数据。在区块链中，各区块之间是一种共生的关系， 即下一区块的内容由上一区块的内容决定，区块之间环环相扣，若要更改其中一个区块的内容需要获取其他全部区块的认可，因此难度极大，继而确保了数据的安全性 。

## 1.2 区块链特点

1、去中心化。区块链的核算和存储技术是分布式的，相比与传统数据结构，去除了中央数据库，网络中各节点具有相等的权利和义务，由全体共同负责数据的维和和存储。

2、自治性。区块链中所有节点的数据交互遵循一套既定的协议和规范，任何人为的干预行为都将被拒绝，因此整个区块链节点都能在自由安全的环境下交换数据，从而确保交易活动的安全可靠。

3、不可篡改性。数据信息一旦通过各节点验证写入区块链系统，就将被各节点共识并封装，在单个节点篡改数据信息不能达成共识，因而无效，从而极大程度地确保了区块链信息的安全性。

4、匿名性。整个区块链都遵循同一套协议和规范，因此网络中任意两个节点之间无需建立信任即可进行数据交互，从而确保了数据信息的匿名性 。

目前，全球有数个区块链技术平台，如比特币（Bitcoin）、以太坊（Ethereum）和超级账本（Hyperledger Fabric）等。

# 2、Hyperldger Fabric

## 2.1 超级账本的发展历程及简介

超级账本（Hyperledger）是Linux基金会的区块链项目，目的是发展商用区块链平台技术。从创立初期，超级账本就吸引了很多行业独角兽，覆盖了互联网行业、金融业、银行、运输业等。发展至今，Hyperledger Fabric拥有100多名成员，包括Cisco、IBM、Intel、J.P.Morgan、荷兰银行等。基于区块链技术、智能合约及其他相关技术，其希望能建立新一代的分布式账本交易应用平台，从而在简化商业流程和法律事务的同时，建立起商业信任、透明、审查能力。旗下的Hyperledger Fabric子项目是以IBM早期捐献出的Open Blockchain为主体搭建而成，其中 44000行开源代码由IBM贡献。

HyperLedger Fabric是一个带有可插入各种功能模块架构的区块链实施方案，目标是打造成一个由全社会共同维护的开源超级账本。

Fabric的核心开发语言是Go，其更适合于联盟链。在2016年IBM宣布，计划提供开源代码并持续向超级账本项目（Hyperledger Project）贡献区块链代码。IBM将提供经过IBM测试与认证的超级账本区块链代码，以及在多种技术平台上进行安装的方法，以便开发者可以在容器（Container）内执行超级账本的代码，并开始快速构建商品溯源、贸易融资、信用证、供应链以及企业贷款等区块链网络。

Hyperledger是对传统区块链模型的革新，在某种程度上是允许创建授权和非授权的区块链。Hyperledger还通过提供一个针对身份识别、可审计、隐私安全和健壮的模型，使得缩短计算周期、提高规模效率和响应各个行业的应用需求成为可能。利用超级账本平台，用户可以轻松地搭建起企业级的区块链网络。在这个网络中，每名成员都可以访问实时更新、加密过的账本，并能查询及发起交易。一旦交易经过共识流程的验证，它就会立即加人到网络中所有的账本中，并且不能更改。交易结果迅速、私有、保密且易于审计。另外，早期的超级账本还定义了协议规范：Open Blockchain Protocol Specification，并以此建立了区块链平台Hyperledger Fabric，并可以用于一系列B2B和B2C交易相关的行业案例中。

## 2.2 Hyperledger Fabric的系统逻辑架构图

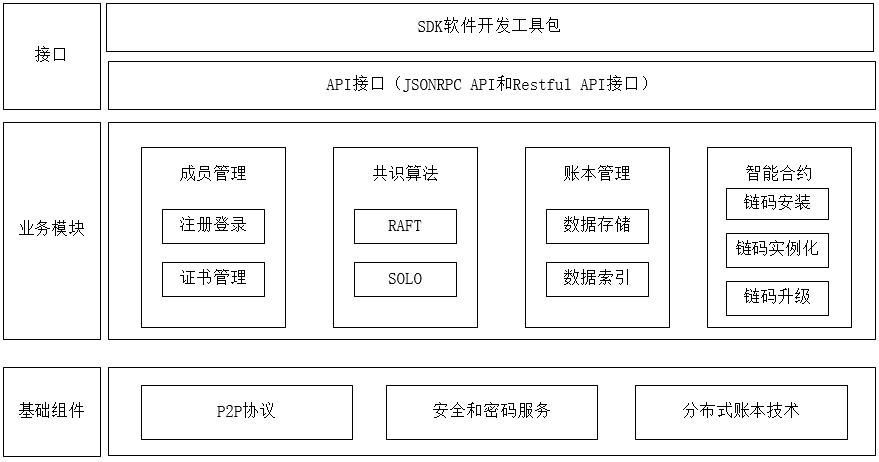


图2-1 Hyperledger Fabric 的系统逻辑架构图

## 2.3 超级账本各个模块及其基本功能

Hyperledger Fabric 功能模块大致分为共识排序模块、智能合约模块、账本管理模块、客户端管理模块、成员管理模块。

共识排序模块负责保证系统的一致性和安全性。基本功能有对接收到的交易进行背书、排序、验证，并打包生成区块，保证各记账节点的账本状态一致， Leader选举、节点主动恢复、动态增删节点等。

智能合约模块负责对交易进行验证和执行。实现的基本功能有链码的打包、链码的安装、链码的实例化、链码的升级等。

账本管理模块负责对系统数据的管理。基本功能有使用文件系统存储账本数据时能够提交区块到账本、获取区块信息、获取区块数据等，使用区块索引时能够将区块索引存储在leveldb中，根据区块编号、哈希等方便快速定位区块在文件中的位置，使用状态数据库时使用leveldb存储所有曾经在交易中出现的键值对的最新值。

客户端管理模块负责向系统中发送控制信息，并返回执行结果。基本功能有创建新的通道、将通道信息发送给节点用于节点加入、在节点上安装链码、提交交易、查询链码状态、其他查询（通过哈希查询区块，高度查询，通过ID查询交易，查询节点安装的所有链码）等。

成员管理管理联盟链平台的成员信息。在基本功能有注册初始化管理用户、登记新用户、注册Peer节点、获取CA证书链、重新获取用户的注册证书、用户注销等。

## 2.4区块链技术平台的比较

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 名称 | 共识算法 | 适用场景 | 开发语言 | 智能合约 |
| 比特币 | PoW | 公有链 | C++ | 否 |
| 以太坊 | PoW/PoS | 公有链/联盟链 | Go | 是 |
| Hyperledger Fabric | PBFT为主 | 联盟链 | Go | 是 |

### 2.4.1 共识算法

工作量证明，PoW（Proof of Work）可以简单理解为一份证明，用来确认你做了一定量的工作。工作量证明机制是比特币、莱特币等所采用的共识机制，矿工通过付出算力来挖矿进而获得相应的区块奖励。

权益证明，PoS（ Proof of Stake），最早在 2013 年被提出，最早在 Peercoin 系统中被实现，类似现实生活中的股东机制，拥有股份越多的人越容易获取记账权（ 同时越倾向于维护网络的正常工作）。典型的过程是通过保证金（ 代币、资产、名声等具备价值属性的物品即可） 来对赌一个合法的块成为新的区块，收益为抵押资本的利息和交易服务费。提供证明的保证金（ 例如通过转账货币记录） 越多，则获得记账权的概率就越大。合法记账者可以获得收益。

实用拜占庭容错，PBFT（Practical Byzantine Fault Tolerance）共识算法可以在少数节点作恶（如伪造消息）的场景中让分布式系统能够达成共识，它采用签名、签名验证、哈希等密码学算法确保消息传递过程中的防篡改性、防伪造性、不可抵赖性，并优化了BFT算法，将其算法复杂度从指数级降低到多项式级别。在一个由（3f+1）个节点（f代表系统中拜占庭节点的数量）构成的分布式系统中，只要有不少于（2f+1）个非拜占庭节点正常工作，该系统就能达成一致性。

### 2.4.2 智能合约

1995年，“智能合约”（Smart contract）由密码学家尼克，萨博（Nick Szabo）首次提出。在智能合约中，当一个预先编好的条件被触发时，对应的合同条款就会被执行。从本质上讲，这些智能合约的工作原理类似于其他计算机程序的if-then语句，智能合约只是以这种方式与真实世界的资产进行交互。而随着区块链技术的发展，以智能合约为核心的区块链平台如Hyperledger Fabric和Ethereum越来越受到重视。

### 2.5 Fabric1.0采用的新框架

大部分区块链所采用的是order-execute框架，如图2-2所示：已有的智能合约区块链实现了主动复制，它就是一个共识协议或原子传播，一、对交易排序并传播给所有节点；二、每个结点按序执行交易。每个结点都执行每笔交易，并且交易是确定的。order-execute框架存在于现有的所有区块链系统，如Ethereum、 Tendermint、Chain、Quorum等。

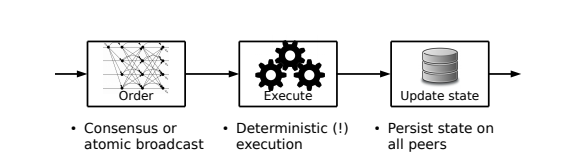


图2-2 order-execute框架

在此之前的许可链（私有链）存在许多缺陷，它来源于它未许可的关系或order-execute框架。（1）共识机制被硬编码到平台中；（2）交易验证的信任模型需要共识机制确认，并且不能适应智能合约的要求；（3）智能合约被不标准或特定场景的语言编写，阻碍了它的广泛适用性；（4）所有对等方按序执行交易限制了性能，采取复杂的操作阻止平台的DOS攻击；（5）每个智能合约运行在所有对等点，这与机密性不符。

Fabric的结构是一个新型的范式，可以在不信任环境中去中心化的执行不信任代码。它将交易流分为三步，运行在系统的不同实体（1）执行一个交易并检查它的正确性，从而确定他（对应于其他区块链中的交易验证）；（2）通过一个共识机制排序，而不管交易本身；（3）根据每一个特定应用的信任假设来进行交易验证，并且可以阻止由于并发导致的竞争。

这个设计与order-execute范式不同，Fabric在达成最终订单协议之前执行交易，他有两种复制方式：被动和主动。一、Fabric使用被动或主备复制的方式，这在分布式数据库中很常见，但是具有基于中间件的非对称更新处理，并移植到具有拜占庭错误的不受信任的环境。二、Fabric结合主动复制，即交易对账本状态的影响只有在他们总的顺序达成共识后才被写入，每一个对等方单独执行确定的验证步骤。总的来说，这个复制设计在拜占庭模式中混合了被动和主动复制，execute-order-validate范式，代表了Fabric框架中的主要创新，这些解决了前面提出的问题。Fabric v0.6在2016年九月发布，当时的Fabric和其他联盟链没有太大区别，采用PBFT共识。v1.0 Fabric，从节点架构上来看，取消了原来的Validating和Non-Validating节点，取而代之的是Endorser节点、Committer节点和全新的Orderer模块。

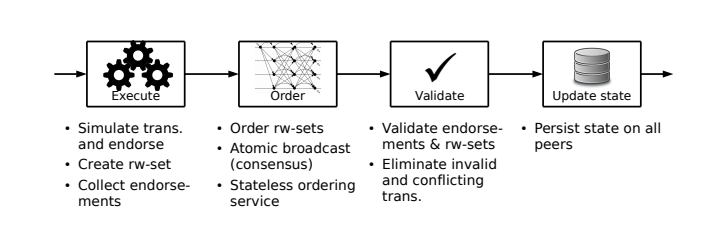


图2-3 execute-order-validate框架

## 2.6 交易流程

### 2.6.1 交易中的节点

节点是区块链的通信主体，Hyperledger Fabric中有多种类型的节点：CA节点、Peer节点、排序节点和客户端节点。

1、 CA节点。CA节点是Hyperledger Fabric的证书颁发机构，接收客户端的用户注册申请，返回注册密码用于登陆和获取身份证书，而在区块链网络上的所有操作都会验证用户的身份证书。

2、 Peer节点。所有的Peer节点都是记账节点，负责验证排序服务节点区块里的交易，维护状态数据和账本的副本。部分节点会执行交易并对结果进行签名背书，充当背书节点。背书节点是动态的，与具体链码绑定。

3、 排序节点。排序节点接收包含背书签名的交易后，对未打包的交易进行排序生成区块，广播给Peer节点。

4、 客户端节点。客户端想背书节点提交交易提案，当收集到足够背书后，向排序服务广播交易，进行排序，生成区块。

### 2.6.2交易过程详细流程

1、应用程序客户端通过SDK调用证书服务（CA）服务，进行注册和登记，并获取身份证书；

2、应用程序客户端通过SDK向区块链网络发起一个交易提案（Proposal），交易提案把带有本次交易要调用的合约标识、合约方法和参数信息以及客户端签名等信息发送给背书（Endorser）节点。

3、背书（Endorser）节点收到交易提案（Proposal）后，验证交易提案的格式是否正确，交易是否被提交过，交易签名是否有效（通过MSP）并确定提交者是否有权执行操作，同时根据背书策略模拟执行智能合约，并生成读写集，将结果及其各自的CA证书签名发还给应用程序客户端。

4、应用程序客户端收到背书（Endorser）节点返回的信息后，先对背书节点签名进行验证，判断提案结果是否一致，以及是否参照指定的背书策略执行，如果没有足够的背书，则中止处理；否则，应用程序客户端把数据打包到一起组成一个交易并签名，发送给Orderers。

5、 排序节点（Orderers）对接收到的交易进行共识排序，然后按照区块生成策略，将一批交易打包到一起，生成新的区块，发送给提交（Committer）节点；

6、提交（Committer）节点收到区块后，会对区块中的每笔交易进行校验，检查交易依赖的输入输出是否符合当前区块链的状态，完成后将区块追加到本地的区块链，并修改世界状态。交易流程如图2-4所示。

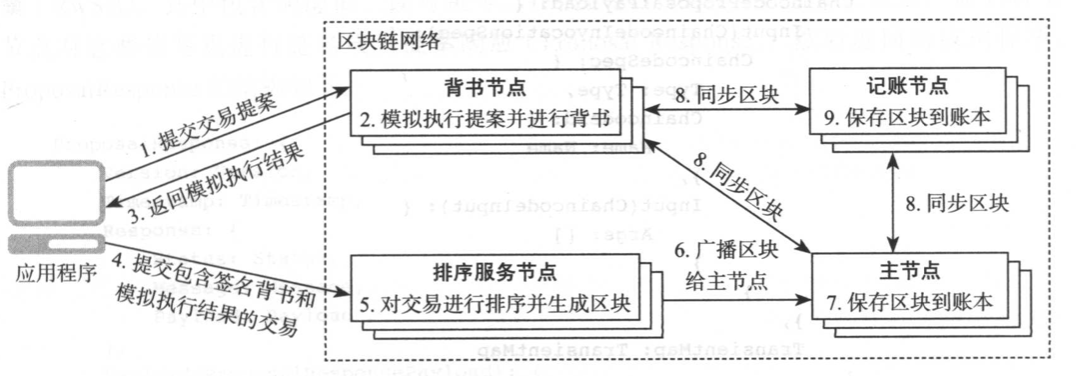


图2-4 交易流程图

## 2.7 Fabric 1.0 的Evaluation

为了测试，Fabric设计了一种UTXO模型的代币，简称Fabcoin。通过一个chaincode不断产生SPEND和MINT transactions，分别模拟Fabcoin的产生和销毁。

实验 1：选择区块大小。影响吞吐量和延迟的关键结构配置参数是区块大小。为了调整后续实验的区块大小，并评估区块大小对性能的影响，我们进行了区块大小从 0.5MB 到 4MB的实验。结果描述如下图所示，显示对等体测量的峰值吞吐量以及与端到端 （e2e） 延迟的平均值。

我们可以观察到，吞吐量在block size超过2MB后没有显著改善，但延迟会变得更糟。因此，我们将 2MB 作为后续实验的区块大小，目的是最大限度地提高测量吞吐量，假设可接受大约 500ms 的端到端延迟。

交易记录的大小。在实验中，我们还观察了Mint 和Spend Transaction的大小。特别是，2MB的区块包含 473 Mint Transactions或670 Spend Transactions，即 Spend Transaction大小为 3.06kB，Mint Transaction大小为 4.33kB。在Fabric的一般交易比较大，因为它们带有证书信息。此外，Mint Transaction 比 Spend Transaction大，因为它们带有 CB 证书。

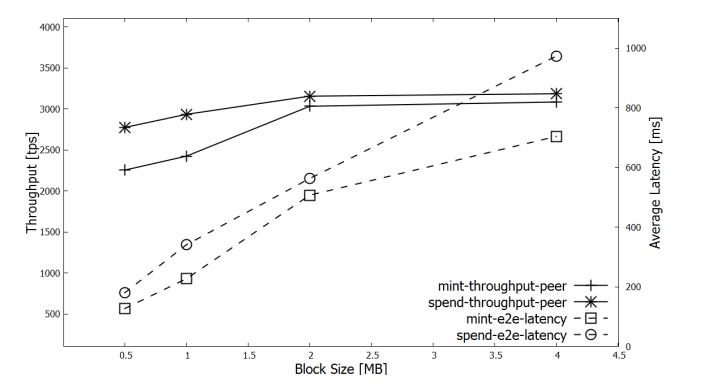
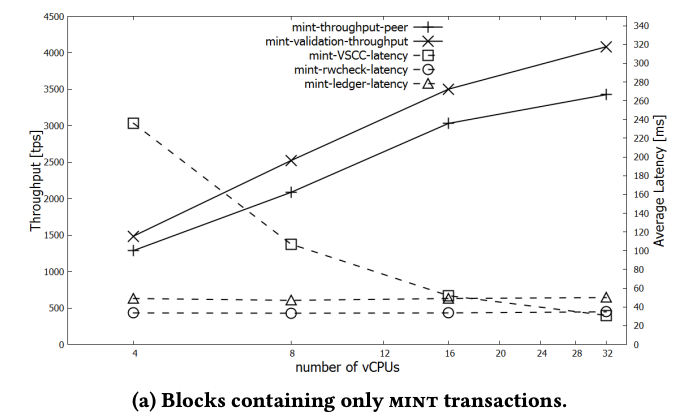
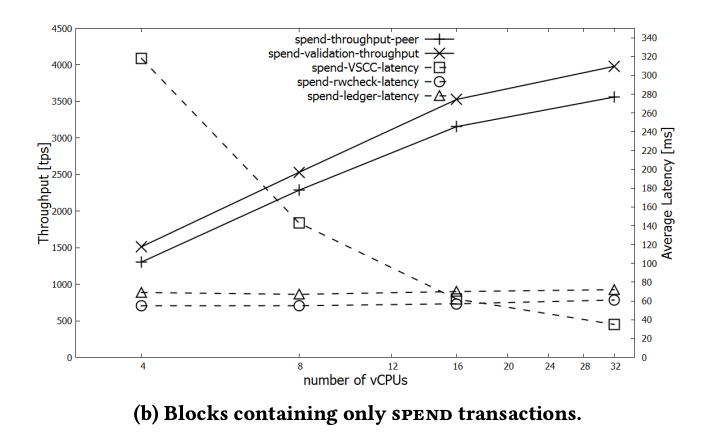


图2-5 block size – Throughput

实验2:性能测试。Validation Phase 是主要瓶颈，但随着vCPU增加得到了缓解，但是由于endorsement很难并行因此提升有限。





# 3、Hyperledger Fabric的优势

## 3.1 Hyperledger Fabric的安全保障

Fabric采用X.509数字证书验证使用者身份和角色。成员必须被许可才能加入网络，通过证书，加密，签名等手段保证安全。通过多通道功能，保证只有参与交易的节点能访问到数据，其他的节点看不到。满足数据保护方面的法律法规要求。

## 3.2模块化设计，可插拔架构

Hyperledger Fabric的成员管理模块可以采用自己的。共识机制和加密算法也可以根据实际情况选择替换。

## 3.3高性能和可扩展

Fabric采用模块化架构把交易处理划分为3个阶段：通过Chaincode进行分布式业务逻辑处理和协商；交易排序；交易的验证和提交。不同的阶段由不同的节点参与，不需要全网的节点都参与。网络的性能和扩展性得到优化。Peer节点和Orderder节点可以独立扩展，并可以动态增加。

## 3.4提供丰富的查询功能

可以在Level DB上进行按key查询，按复合key查询，按key的范围查询。如果采用Couch DB，Couch DB是文档数据库，数据是JSON格式的。除了支持按key查询，按复合key查询，按key的范围查询外，还支持全文搜索。

**参考文献：**

[1]黄宗敏,张大伟.Hyperledger Fabric中基于层级结构的公钥广播加密方案[J/OL].计算机应用研究:1-9[2021-01-28].https://doi.org/10.19734/j.issn.1001-3695.2020.06.0159.

[2]Stamatellis Charalampos,Papadopoulos Pavlos,Pitropakis Nikolaos,Katsikas Sokratis,Buchanan William J. A Privacy-Preserving Healthcare Framework Using Hyperledger Fabric.[J]. Sensors (Basel, Switzerland),2020,20(22).

[3]Lu Xu,Wei Chen,Zhixu Li,Jiajie Xu,An Liu,Lei Zhao. Solutions for concurrency conflict problem on Hyperledger Fabric[J]. World Wide Web,2020(prepublish).

[4]高云,严悍.Hyperledger Fabric区块链软件架构中的中间件设计[J].计算机与数字工程,2020,48(09):2195-2200+2274.

[5]Christian Gorenflo,Stephen Lee,Lukasz Golab,Srinivasan Keshav. FastFabric: Scaling hyperledger fabric to 20 000 transactions per second[J]. International Journal of Network Management,2020,30(5).

[6]刘镇江,戚湧,严悍.Fabric区块链SDK连接配置方法研究[J].计算机应用研究,2020,37(S1):215-217+220.