企业级区块链综述

郭壮 22151198 软件工程 2102 软件学院

**摘要**：区块链是由节点参与的分布式数据库系统，它的特点是不可更改，不可伪造，也可以将其理解为账簿系统。常见的公有区块链具有一个重要的性质，即节点可以随意地进入或者退出其所在的区块链，且为了应对这种场景下带来的不可信和恶意行为，往往使用工作量证明来进行交易共识，使用挖矿的方式来对参与方进行激励，这种方法性能较低，交易成本高且资源消耗巨大这种性质显然是不能满足许多企业对建立区块链的最低标准，因此出现了企业级区块链，本文对三个主要的企业级区块链进行描述，总结了三种企业级区块链之间的异同。

###### 1.企业级区块链简述

区块链是由节点参与的分布式数据库系统，它的特点是不可更改，不可伪造，也可以将其理解为账簿系统。它是比特币的一个重要概念，完整比特币区块链的副本，记录了其代币的每一笔交易。通过这些信息，我们可以找到每一个地址，在历史上任何一点所拥有的价值。区块链是由一串使用密码学方法产生的数据块组成的，每一个区块都包含了上一个区块的哈希值，从创始区块开始连接到当前区块，形成块链。每一个区块都确保按照时间顺序在上一个区块之后产生，否则前一个区块的哈希值是未知的。 这些特征使得比特币的双花非常困难。区块链是比特币的核心创新。常见的公有区块链具有一个重要的性质，即节点可以随意地进入或者退出其所在的区块链，且为了应对这种场景下带来的不可信和恶意行为，往往使用工作量证明来进行交易共识，使用挖矿的方式来对参与方进行激励，这种方法性能较低，交易成本高且资源消耗巨大这种性质显然是不能满足许多企业对建立区块链的最低标准，因此出现了企业级区块链，绝大多数企业级区块链都是“许可型区块链”，也就是说企业可以直接控制这些区块链。例如，企业可以在执法部门的要求下拦截不符合规则的交易。这就是许可型区块链与比特币之类的公链最大的区别之一，企业级区块链只有特定的联盟成员或者获得一定数量的联盟成员许可的机构或组织可以加入，且所有的交易只在联盟成员之间发生，主要区别见表1。

**表1。公有链与企业级区块链对比**



###### 2.主要的企业级区块链

在过去几年中，数十亿美元的公司已经开始投入到试验、试点和整合区块链技术。然而，企业使用DLT和区块链的趋势早在2014年就已经出现。公司开始试验Multichain、Hyperledger和Corda，它们是银行巨头的流行许可解决方案，如汇丰银行、ING、渣打银行、瑞银、法国巴黎银行；以及保险公司、领先的石油加工商和食品加工商，仅举几例。事实上，截至2021年9月，前100家上市公司中有81家正在使用区块链技术，其中Hyperledger 是最受欢迎的解决方案，其中26%的公司将其作为首选解决方案。其次是以太坊（18%）、Quorum（11%）和Corda（8%）。

2.1Hyperledger Fabric

Hyperledger Fabric是一个开源的企业级授权分布式账本技术(DLT)平台，专为在企业环境中使用而设计，与其他流行的分布式账本或区块链平台相比，它提供了一些关键的区别能力。一个关键的区别是Hyperledger是在Linux基金会的支持下建立的，该基金会本身有一个很长的和非常成功的历史，在开放的治理下培育开放源码项目，使社区和生态系统发展壮大。Hyperledger由一个不同的技术指导委员会管理，Hyperledger Fabric项目由来自多个组织的不同维护人员组成。它的开发社区已经发展到超过35个组织和近200名开发人员，从它最早的提交开始。

Fabric具有高度模块化和可配置的架构，能够为广泛的行业用例(包括银行、金融、保险、医疗保健、人力资源、供应链，甚至数字音乐传输)提供创新、多功能性和优化。Fabric是第一个支持用Java、Go和Node。js等通用编程语言而不是受约束的特定领域语言(DSL)编写的智能合约的分布式分类帐平台。这意味着大多数企业已经拥有开发智能合约所需的技能集，不需要额外的培训来学习新的语言或DSL。Fabric平台也是联盟链平台，Fabric节点中的MSP(membership service provider)模块负责身份管理，主要完成数字证书验证、签名与验证、私钥管理等功能。Fabric 网络的各类节点(背书/提交节点、排序节点、客户端)由X。509数字证书表示其身份。

平台最重要的区别之一是它支持可插入的共识协议，这使得平台能够更有效地定制，以适应特定的用例和信任模型。例如，当在单个企业中部署时，或者由受信任的机构操作时，完全复杂的容错共识可能被认为是不必要的，并且会过度拖累性能和吞吐量。在这种情况下，崩溃容错(CFT)共识协议可能就足够了，而在多方、去中心化的用例中，可能需要更传统的拜占庭容错(BFT)共识协议。这些不同的设计特性的结合使Fabric成为当今交易处理和交易确认延迟方面性能更好的平台之一，它支持交易和实现这些交易的智能合约(Fabric称之为“链码”)的私密性和保密性。Fabric在网络层采用了基于gRPC的Gossip协议，且支持 TLS加密通信，在数据层，Fabric是基于账户模型的，其采用区块链来组织交易数据，为了实现基于哈希的快速检索，选用了健值数据库 LevelDB，并且还支持CouchDB数据库。

Fabric交易流程如下：

(1) 客户端对新的交易数据签名并发送到一至多个背书节点;

(2) 背书节点以交易数据为输入执行智能合约并生成读写集(readset，writeset);

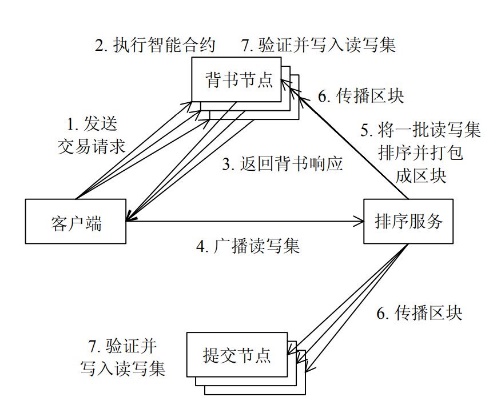
(3) 背书节点对读写集进行签名并返回至客户端;

(4) 客户端收集读写集，验证符合背书策略(endorsement policy)后将其广播至排序服务;

(5) 排序服务基于共识机制对多笔交易的读写集排序并将其打包成区块;

(6) 排序服务将区块传播至提交节点;

(7) 提交节点对从排序服务收到的区块中的读写集进行背书策略验证和读集(readset)版本验证，验证通过后，将区块追加至区块链，并将写集(writeset)写入状态数据库。



2.2 Corda

Corda是一个编写“CorDapps”的平台，“CorDapps”是一种应用程序，可以用新的功能扩展全球数据库。这类应用程序定义了新的数据类型、新的节点间协议流和允许更改的“智能合约”。Corda使用UTXO模型，因此它的交易在结构上与比特币交易相似:它们有输入、输出和签名。与比特币不同，Corda数据库行可以包含任意数据，而不仅仅是值字段。因为事务消耗和添加的数据不一定是一组键/值对，所以我们不讨论行，而是讨论状态。像比特币一样，Corda状态与字节码程序相关联，这些程序必须接受交易才能使交易有效，但与比特币不同的是，交易必须同时满足程序的输入和输出状态。发行交易可以在不消耗任何现有状态的情况下向数据库添加新的状态，但与比特币不同的是，这些交易并不特殊，可以由任何人在任何时候创建。

与比特币和以太坊不同，Corda不使用区块链进行交易，也就是说不使用矿工或工作量证明。相反，每个状态指向一个公证人，公证人是一种服务，它保证只有在所有输入状态都没有被使用的情况下才会签署事务。一个交易不允许消耗由多个公证人控制的状态，因此不需要公证人之间的两阶段提交。在网络层，Corda采用了AMQP1。0协议，且支持TLS加密通信，在共识层。Corda提供了高信任场景下的单节点 Notary服务，为了实现分布式的Notary 服务，还提供基于Raft的Copycat和基于PBFT的BFT-SMaRt分布式共识，类似于 Fabric，Corda的共识也是在交易层面达成的，仅涉及交易的各方。交易取决于共识是满足交易合法性，还是交易唯一性。交易合法性通过运行与交易相关联的智能合约代码（智能合约将在下文给出详细介绍），检查需要的所有签名，并确保所引用的任何交易也是有效的。交易唯一性涉及交易的输入状态。具体而言，必须确保有疑问的交易是所有输入状态的唯一消费者。换句话说，不存在任何消耗同一状态的其它交易。这是为了避免产生双重支付。实现交易唯一性的共识，是在称为“公证人”的参与节点中达成的。其中使用的算法和Fabric一样，是“可插拔的”。因此，我们同样可以使用BFT算法。

Corda交易流程如下：

(1) 发送者创建交易并签名;

(2) 发送者发送交易数据及签名至接收者;

(3) 接收者验证交易数据及发送者签名无误，就附加上接收者签名;

(4) 接收者发送交易数据及交易双方签名至 Notary 共识服务;

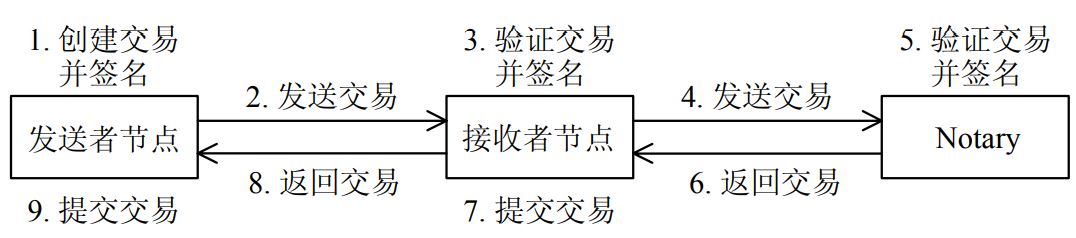
(5) Notary 验证交易数据及交易双方签名无误，就附加上 Notary 签名;

(6) Notary 返回交易数据至接收者;

(7) 接收者核对 Notary 签名无误后提交交易;

(8) 接收者返回交易数据至发送者;

(9) 发送者核对接收者及 Notary 签名无误后提交交易。



2.3 Quorum

Quorum，是一个企业级分布式账本和智能合约平台，可看作企业版的以太坊（以太坊，是第二代公有区块链智能合约平台）。Quorum通过一套区块链架构，提供私有智能合约执行方案，并满足企业级的性能要求。适用于任何需要高速和高吞吐量处理联盟许可间进行私有交易的应用程序，解决了区块链技术在金融及其他行业应用的特殊挑战。Quorum，是基于以太坊分布式账本协议开发而成，为金融服务行业提供以太坊许可链方案，以便支持交易与合约的隐私性。Quorum的主要特点及其基于以太坊公有链的扩展功能，具体如下：交易与合约的隐私性；多种基于投票的共识机制；网络/节点的许可管理；更高性能。

Quorum，基于以太坊协议官方Go方案开发而成，支持私有链和联盟许可链，它使用基于投票的共识算法，通过介绍一个新的私有交易识别器来实现数据隐私。Quorum的设计目标之一，就是尽可能复用更多的已有技术，最大限度地减少对现有以太网的改造，以减少与以太坊未来版本保持代码一致性所需要的工作量。Quorum的本质，是使用密码学技术来防止交易方以外的人看到敏感数据。该解决方案，需要一个单独的共享区块链，和一个智能合约框架与以太坊原始代码的修改组合；其中智能合约框架对隐私数据进行了隔离。对go-ethereum代码库进行的修改，包括区块提案和验证过程的修改。区块验证过程，是通过执行交易合约代码来进行的，比如所有节点都对公开交易、和与交易方相关的私有交易进行验证；对于其他私有交易，节点将会忽略合约代码的执行过程。在网络层，Quorum分别采用以太坊P2P协议和HTTPS协议传输公有交易和私用交易。在数据层，Quorum为了实现基于哈希的快速检索，选用了健值数据库LevelDB。

Quorum交易流程如下：

(1) 客户端发送私有交易到 Quorum 节点，并在交易中直接指明每个接收者的公钥;

(2) Quorum 节点将私有交易传送至对应的 Constellation 进行加密;

(3) Constellation 生成一个对称秘钥，先用该对称秘钥加密私有交易负载(payload)，再分别用每个接收者

的公钥分别加密该对称秘钥，最后还要基于私有交易的加密负载计算其哈希值;

(4) Constellation 将私有交易的加密负载、私有交易的加密负载的哈希值、加密后的对称秘钥分别点对

点的传播至每个交易接收方的 Constellation;

(5) 数据传播成功后，Constellation 将私有交易的加密负载的哈希值返回至对应的 Quorum 节点;

(6) Quorum 节点将私有交易的加密负载的哈希值打包为一个以太坊交易，经以太坊 P2P 协议广播至所有

Quorum 节点;

(7) 该以太坊交易经过共识被打包进 Quorum 区块。当每个 Quorum 节点执行该以太坊交易时，需要基于该

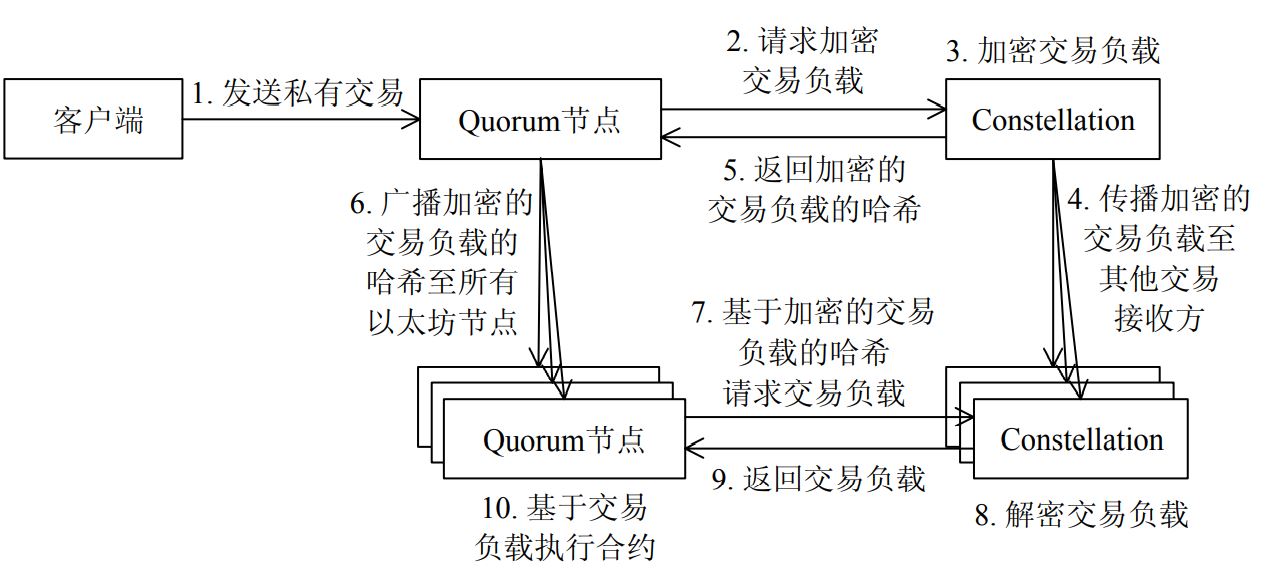
以太坊交易的负载(即私有交易加密负载的哈希值)向对应的 Constellation 请求原始的私有交易负载;

(8) 根据 Quorum 节点的请求，各个交易接收方的 Constellation 基于自己的私钥、公钥加密的对称秘钥、

对称秘钥加密的私有交易负载解密出原始的私有交易负载;

(9) 交易接收方的 Constellation 将原始的私有交易负载返回至对应的 Quorum 节点。非交易接收方的Constellation没有接收过加密的私有交易负载，其向Quorum节点返回的是“NotARecipient”消息;

(10) 交易涉及的每个 Quorum 节点将私有交易提交至智能合约运行，智能合约会将执行私有交易时生成的状态数据存储至私有状态数据库



###### 3.总结

关系数据库基于关系模型、事务处理、查询优化等技术，解决了以银行为代表的金融机构内部记账的业务需求。区块链技术通过集成 P2P 协议、块链结构、共识机制、智能合约等技术，解决了多个互不信任机构间一致性记账的业务需求，减少了跨机构业务流程中的摩擦，缩短了对账周期、降低了运营成本、提升了协作效率。目前，Hyperledger Fabric，Corda 和 Quorum 等企业级区块链平台在以金融机构为代表的众多企业应用实施时，还主要以概念验证(proof of concept，简称 POC)为主。与发展了近 40 年的传统数据库相比，企业级区块链技术仍处于技术路线的初期阶段，从系统架构到开发范式都尚未形成统一标准，在诸多方面还存在许多问题。为了解决这些问题，未来的还需更多的研究工作。

**参考文献**

[1]邵奇峰,张召,朱燕超,周傲英.企业级区块链技术综述[J].软件学报,2019,30(09):2571-2592.DOI:10.13328/j.cnki.jos.005775.

[2]张海宁. 超级账本:助力企业级区块链应用与开发[C]//《IMI研究动态》2017年上半年合辑.,2017:565-570.

[3]邵奇峰,金澈清,张召,钱卫宁,周傲英.区块链技术:架构及进展[J].计算机学报,2018,41(05):969-988.

[4]黄晓艳.区块链技术的应用场景与发展战略——专访IBM全球企业咨询服务部大中华区银行业总经理范斌[J].高科技与产业化,2017(07):68-73.

[5]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.

[6]何蒲,于戈,张岩峰,鲍玉斌.区块链技术与应用前瞻综述[J].计算机科学,2017,44(04):1-7+15.

[7]钱卫宁,邵奇峰,朱燕超,金澈清,周傲英.区块链与可信数据管理:问题与方法[J].软件学报,2018,29(01):150-159.DOI:10.13328/j.cnki.jos.005434.

[8]王赫彬.区块链技术与应用前瞻综述[J].科技创新导报,2020,17(14):126-127.DOI:10.16660/j.cnki.1674-098X.2020.14.126.

[9]朱立,俞欢,詹士潇,邱炜伟,李启雷.高性能联盟区块链技术研究[J].软件学报,2019,30(06):1577-1593.DOI:10.13328/j.cnki.jos.005737.

[10]贺海武,延安,陈泽华.基于区块链的智能合约技术与应用综述[J].计算机研究与发展,2018,55(11):2452-2466.