

关于联盟链和联盟链可以为金融行业和企业提供技术解决方案的问题，很多小伙伴都是不知道，接下来和Dadaqq.Com小编往下看联盟链的具体解答吧。

Fabric 是超级账本联盟推出的核心区块链框架，它适合在复杂的企业内和企业间搭建联盟链。根据超级账本联盟的目标，Fabric 被建设为一个模块化的、支持可插拔组件的基础联盟链框架。；

与以太坊系的Quorum不同，Fabric从一开始就只考虑企业间的应用。其独有的channel概念，将企业根据业务目的不同以不同的子网连接起来，每一个子网对应一个channel，而每个channel有自己独立的区块链。而Quorum很显然是只有一个公网（所有企业节点都加入进去），企业与企业间的私有业务是通过Private Manager 完成的。

理解channel的最简单方法就是，将它类比为一条消息服务提供的Topic，实际上Fabric最早就是基于Kafka?的分布式消息服务来实现。

???在Fabric网络中，一个企业可以有一个或多个节点加入整个联盟链；一个企业可以加入1个或者多个Channel（子网）；一个节点可以加入1个或者多个channel。每个channel构成一个子网，所以Fabric是一种由子网组成的网络。

那么Fabric是怎么实现智能合约的执行和完成业务上链（将事务结果记录在区块链里）的呢？

与其它框架不同，Fabric 将整个过程分成了三个阶段：

业务背书阶段： 客户的请求发送的背书节点，通过智能合约完成业务的计算（但不更新状态），并完成背书；将背书结果返回个客户端。

业务的排序阶段： 客户端将背书结果通过Channel被发送到排序节点（orderer），在排序节点完成事务的排序，并打包到block里，最后下发给所有连接到channel的节点。

业务验证并写入账本阶段： 通过Gossip 网络，所有Channel的节点都会接收到新的block，节点会验证block中的每一个事务，确定是否有效：有效地将会跟新world state，无效的将会标志为“无效”，不会更新World state，但整个block会被完整的加入到帐本中（包括无效的事务）。

根据上述文章内容的描述，Fabric 节点实际可以分为？，普通节点和Order节点：

?Peer, 普通节点, 完成背书 (包括只能合约的执行) 和验证。

orderer,? 排序节点, 完成排序。

加入orderer节点的Fabric网络可以被描述如下：

每一个Channel, 都定义了所有属于channel的节点, 但是并不需要所有节点都连接到Orderer 节点 (节点间可以通过gossip 协议通讯来传播私有数据或事务)。

???在区块链中, 共识是区块链的基础。与公有链不同, 联盟链的共识要求所有加入账本的事务是确定的、最终的, 也就是不可以有分叉, 区块与区块间的顺序是一定的, 只存在唯一一条链。在Fabric 中, 这个客观需求正是由排序实现的, 所有的事务将被提交给orderer节点获得确定的顺序, 并最终打包成block进入帐本。Fabric 从1.4.1开始支持基于Raft实现排序服务,? 可以认为基于Raft实现共识。

基于RAFT的排序服务相对于早期的Kafka 具有更好的分布性, 配置更加简单, 是联盟链里常用的一个常用的达成共识的算法, Quorum就默认使用RAFT作为共识层。简单的说, RAFT是一个leader和follower的模式, 所有加入RAFT网络的节点, 任意时候都有一个leader,? 只有这个leader有权决定事务的顺序, 并打包成Block, 其它节点只能作为follower提交事务和同步block。

基于FAFT网络, 每个企业可以有一个或多个节点参与到Orderer中去。在Frabric中企业间的网络连接可以变化成如下形式：

???区块链的使用用户在以太网中被称作EOA (External of Account), EOA的载体是钱包。我们沿用这个概念, 来看看Fabric是如何实现用户和发起事务的。Fabric中EOA是一个CA中心发布的certificate (x.509), 一个Certificate代表一个Identity (这与以太坊还是有很大区别的, 以太坊中一个EOA其实是一个hash地址), EOA能够参与的channel以及被授权的操作是有channel的MSP (Membership Service Provider) 决定的 (如下图)。

注：certificate 是一种密码学上验证身份的通用做法；certificate包含了个人的信息, 公钥以及发布这个certificate的CA的签名。验证方只需要拥有这个CA的证书 (包含CA的公钥), 就可以验证这个签名是否正确, certificate的内容是否有篡改。简单的说, 通过CA和Certificate, 我们可以获得一个可验证的身份和信任链。

??? 如上图, fabric中通要使用Wallet作为EOA的载体, 一个Wallet中可以包含多个Identity (x.509 certificate)。Identity 通过 CA提供的信任链来验证正确性。

? 验证了身份之后，Fabric 通过MSP在区块链网络中解决该身份是否代表组织的成员和在组织内具有什么角色。例如，channel首先会验证当前用户Identity是否是有效地身份，然后通过MSP查看其所处的企业和具有的角色，最终确定该用户是否有权执行操作。

可以说，Fabric的访问控制是通过MSP来完成的。在每一个需要访问控制的地方都需要定义一个MSP。? 例如，每个channel都定义一个MSP，这个MSP规定了在channel范围内资源的访问权限。MSP是Fabric里一个晦涩难懂的概念，也是其赋予企业间安全访问的基础。

前文提到，Fabric 将业务处理和上账分成了三个部分，背书，排序，验证后加入账本。

其中背书是Fabric执行智能合约的阶段。以太坊中，智能合约是在EVM中执行的，有多种语言支持。在Fabric，智能合约被称为chaincode：一个chaincode可以理解为是智能合约的容器，可以包含一个或多个智能合约，不用于EVM，chaincode是在 JVM 或NodeJS中执行。

客户应用程序通过智能合约来访问账本，每一个可访问的智能合约都被安装在客户端可以访问的节点上，并被定义在channel里。（有只能合约的节点被称为背书节点，没有只能合约的节点被称未提交节点，提交节点只维护账本）

客户应用提交一个交易请求，请求到达背书节点，背书节点首先会验证客户的签名，确保客户的身份有权执行本次交易，接着执行交易提及的智能合约（chaincode），并生成一个背书响应（或者叫做交易提案，transaction proposal）。这个背书响应中通常包含World state 的读集合，写集合，以及节点对本次交易的签名。这里与以太坊系联盟链最主要的不同是：背书阶段只模拟交易，并不真正更新交易结果。而真正更新交易在第三阶段完成。背书节点最后将生成的背书响应fanhui给客户端，智能合约部分的执行就结束了。

通常一个交易的执行需要多方的签名，所以客户端需要将一个交易发送给多个背书节点，这些背书节点的选择需要满足背书策略的要求。

下图是一个包含有客户、背书节点，提交节点的网络示意图。

根据Fabric官方的参考文档，客户交易的正果过程可使用下图描述。

如上图，从1到3，为背书阶段，4为排序阶段，4.1,4.2, 5为验证提交阶段。参考Frabric的节点 概念，可以了解更多在交易细节的概念。

总的来看，Fabric 更专注于企业间，通过上文，可以让大家对Fabric的基本构成与概念有一个总的了解。Fabric本身并不神秘，都是使用的现有的企业间的技术。要更好的了解，建议参考阅读分布式消息系统和企业的安全基础设施（CA相关）的支持。与以太坊系联盟链实现比较，Fabric 的子网更概念对于复杂企业间应用适应更强，但是其复杂的安全考量，使得运营成本很高，另外，Fabric 使用Certificate做为用户身份，有很大的局限性，在新的2.0里，Fabric对于此处将有所改变。

下一篇，我们将来看看Sawtooth?，由Inter 提供的区块链框架。

区块链之联盟链(一) 认识以太坊

区块链之联盟链(二) 认识Quotum

区块链之联盟链(三) 认识Fabric

区块链之联盟链(四) 认识Sawtooth

随着区块链技术的发展，越来越的个人及企业也开始关注区块链，而和区块链联系最为紧密的，恐怕就是金融行业了。

然而虽然比特币区块链大受热捧，但毕竟比特币区块链是属于公有区块链，公有区块链有着其不可编辑，不可篡改的特点，这就使得公有链并不适合企业使用了，毕竟如果某金融企业开发出一个区块链，无法受其主观控制，那对于他的意义就不大了。

因此私有链就应运而生了，但私有链虽然能够解决上述文章内容的问题，如果仅仅只是各个企业自己单独建立，那么还将是一个个孤岛。

如果能够联合起来开发私有区块链，最好不过了。

这就是今天要讲的主题：联盟链。

联盟链本质上仍然属于一种私有链

联盟链本质上仍然是一种私有链，只不过它比单个小组织开发的私有链更大，却没有公有链这么大的规模，可以理解为它是介于私有链和公有链之间的一种区块链。

联盟区块链是指其共识过程受到预选节点控制的区块链；例如，不妨想象一个有15

个金融机构组成的共同体，每个机构都运行着一个节点，而且为了使每个区块生效需要获得其中10个机构的确认（2/3确认）。区块链或许允许每个人都可读取，或者只受限于参与者，或走混合型路线，例如区块的根哈希及其API（应用程序接口）对外公开，API可允许外界用来作有限次数的查询和获取区块链状态的信息。这些区块链可视为“部分去中心化”。

联盟链的特点

1.部分去中心化

与公有链不一样，联盟链在某种程度上只属于联盟内部的成员所有，且很容易达成共识，因为毕竟联盟链的节点数是非常有限的。

2.可控性较强

公有链是一旦区块链形成，将不可篡改，这主要源于公有链的节点一般是海量的，比如比特币节点太多，想要篡改区块数据，几乎不可能，而联盟链，只要所有机构中的大部分达成共识，即可将区块数据进行更改；

3.数据不会默认公开

不同于公有链，联盟链的数据只限于联盟里的机构及其用户才有权限进行访问。

4.交易速度很快

跟私有链一样，联盟链本质上还是私有链，因此由于其节点不多的原因，达成共识容易，交易速度自然也就快很多。

联盟链的应用

目前已经有了很多的联盟链，比较知名的有：

1.R3区块链联盟

R3区块链联盟于2015年9月份成立，目前已经有大约40多家国际银行组织加入，成员几乎遍布全球。其主要致力于为银行提供探索区块链技术的渠道以及建立区块链概念性产品。该联盟成立之后，召开了一系列的研讨会。R3表示，其允许银行加入的“初始窗口”已经关闭，2016年，该联盟将寻求与非银行金融机构和团体合作。R3使用以太坊和微软Azure技术，将11家银行连接至分布式账本。R3公司对于自己

正在做的事情非常肯定，它说，区块链技术受到了世界各地银行的欢迎，已经有一些银行不仅在跟R3合作探索区块链技术，还自己开展区块链技术的调查研究。2016年4月，R3CEV与微软正式建立合作关系，研究实验区块链应用。

R3CEV是一个知名的联盟链

2.超级账本 (Hyperledger)

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，加入成员包括：荷兰银行 (ABN AMRO)、埃森哲 (Accenture) 等十几个不同利益体，目标是让成员共同合作，共建开放平台，满足来自多个不同行业各种用户案例，并简化业务流程。由于点对点网络的特性，分布式账本技术是完全共享、透明和去中心化的，故非常适合于在金融行业的应用，以及其他的例如制造、银行、保险、物联网等无数个其他行业。通过创建分布式账本的公开标准，实现虚拟和数字形式的价值交换，例如资产合约、能源交易、结婚证书、能够安全和高效低成本的进行追踪和交易。据相关资料显示，目前已经有北京AiYi数字金融科技公司、Belink (数贝荷包)、BitSE和Onchain共4家中国公司加入。

3.俄罗斯区块链联盟 (俄罗斯版R3)

这个私链联盟正式成立于2016年7月1日，其成员包括支付公司QIWI、BN银行、汉特-曼西斯克银行 (Khanty-Mansiysk Otkritie Bank)、盛宝银行 (Tinkoff Bank)、莫斯科商业世界银行 (MDM Bank) 以及埃森哲咨询公司 (Accenture)。这个被称为“俄罗斯版R3”的区块链联盟于第25届俄罗斯国际金融会议上正式宣告成立，该次会议的主办方为俄罗斯央行。这个区块链联盟的主要目标是发展区块链概念验证；进行合作研究和政策宣传；创建区块链技术的共同标准。同时，他们公开宣布将积极建立与国内监管部门和政府的合作。

公有链联盟链的基本特征主要有部分去中心化；可控性较强；数据不会默认公开；交易速度很快。

公有链是完全去中心化的一种区块链，比特币就属于这种公有链，是完全去中心化的。任何人既可以进行交易也可以读取信息。任何人都可以参与链上的交易确认和共识机制。各个节点可以随时假如节点也可以随时退出节点。

联盟链由多个中心控制，系统由几个权威的机构共同分布式记账，这些节点再根据共识机制协调工作。这是部分去中心化的区块链，民众可以进行查阅和交易，不过验证交易的话就需要联盟内部决定。

公有链与联盟链各有特点：

公有链有三个主要特点。公有链中用户权益可以得到很好保护，公有链中的程序开发者不能干涉用户；开放性更强，任何用户都可以在其上开发自己的应用，并且产生效应；数据完全公开透明，每个参与者都能看到所有账户交易活动，不过由于匿名性，参与者可以很好地隐藏自己的真实现实生活中的身份。

联盟链的一个最显著的特点就是各个节点都对应一个实体机构，任何实体机构节点想要加入联盟连，需要得到联盟的许可。这些机构共同维护系统的稳定发展。

旅游联盟链是正规平台。

旅游联盟链是正规的，而且也还是比较安全的。可以放心使用呢。【旅游联盟链】是《重庆市蚁丛科技有限公司》倾力打造的新型旅游模式，将移动互联网和传统旅游相结合，将线上和线下相结合，其商业模式与运营思路，独具创新性，更具颠覆性。

【旅游联盟链】APP2020年9月24日上线运营，至今广受市场欢迎，2021年8月在国家相关部门的要求指导下进行区块链改革。并响应国家号召与国内部分景区一起进行区块链改革，形成一个旅游联盟，共同构建链上旅游生态。

是真的。游戏联盟链是介于公有链和私有链之间，具备部分去中心化的特性。联盟链是由若干机构联合发起，由盟友共同来维护，它只针对特定某个群体的成员和有限的第三方开放。

区别如下：

分布式系统：分布式数据库所采用的共识算法一般都是基于 Paxos 所衍生出来的一系列算法。这些算法的安全性仰赖于中心化的假设，即所有的节点由一个可信赖的中心管理。

在这个假设下，所有节点都被认为是“诚实”的，也就是说，所有节点都竭尽全力去传递消息，并且消息不会被篡改。如果有少部分节点宕机，或者失联也不会影响协议的安全性。

联盟链：对节点准入进行限制，只允许特定节点参与的区块链，联盟链的共识模型移除了代币系统，其维护共识稳定的基石实际上为参与节点的信用背书。

区块链带来的另一项革新就是链式的结构。每个区块都通过哈希跟前面的区块链接

在一起，一直追溯到初始区块，形成一条绵延不绝的链。这个结构带来的一个好处就是当一个节点确认一个区块的时候，意味着同时确认了这个区块所在链上之前的所有区块。

基于这种链式的结构，区块链中很容易采用一种「最长链」原则发布新的区块。比如在比特币中，由于网络问题和恶意攻击的存在，一个矿工可能会看到多条链，但矿工总是倾向于在最长的一条链上挖矿。即使挖矿挖到一半发现了一条比所在的链更长的链出现，也要切换到更长的链。

最长链原则并不一定是非遵守不可，它并不会对协议安全造成严重影响，但当所有矿工都遵守这一原则的时候，每个矿工所能期望获得的收益最大。当然，也有例外，当一个矿工占有比较多的资源的时候（少于50%），可以采取一种「自私挖矿」（selfish mining）[4] 的策略，通过违背最长链原则，谋求更高的收益。

区块链的链式结构也给研究传统 BFT 的研究者带来很大启发，很多为区块链量身定做的 BFT 协议开始涌现。这其中最著名的要数 Facebook 所采用的 LibraBFT [5] 共识协议。

LibraBFT 基于 HotStuff [6]，由来自 VMware 的研究者在 2019 年的 PODC 上提出。HotStuff 通过采用区块链的链式结构改进了传统 BFT 的性能，使得协议能够部署在具有上百个节点的网络中。

上述文章内容就是“联盟链”和“联盟链可以为金融行业和企业提供技术解决方案”的详细内容了，希望对您有帮助，更多内容查看Dadaqq.Com百科网。