好风借力，直上青云

区块链平台调研与分析

EY安永
Building a better working world

FISCO金链盟
金融区块链合作联盟（深圳）

目录

序

第四次工业革命时代，随着人类在信息产生、获取和处理成本上的逐步降低，越来越多的技术可以支撑原有的商业模式向分布式进行转移，区块链便是其中之一。在著名作家凯文·凯利所著的《失控：全人类的最终命运和结局》中，他早在上世纪九十年代便预言了分布式网络：失控是一种组织形式，是指没有中央控制中心，各部分都是自己独立支配自己的行为。分布式系统有四个特点：1. 没有强制性的中心控制；2. 次级单位具有自治的特质；3. 次级单位之间彼此高度链接；4. 点对点间的影响通过网络形成了非线性因果关系。而区块链的分布式、多中心化、点对点、共识机制等特点与凯文·凯利的分布式网络高度吻合，全球逻辑一体化账本更是对其理论的完美实践。

近年来，根据我们对区块链技术和市场发展动向的观察，区块链技术在全球范围内得到了越来越广泛的认可，世界各主要经济体及重要国际组织均在对区块链技术进行积极的探索和推进。在国内，金融机构、互联网公司、IT 企业和制造企业也在积极投入区块链技术研发和应用推广，发展势头迅猛。但同时，在研究和应用区块链技术平台的过程中，随着研究的逐渐深入，区块链应用企业遇到的问题与挑战也越来越多。为了给广大区块链应用企业选取区块链技术平台提供参考和借鉴，安永联合金融区块链合作联盟（深圳）（简称金链盟），结合双方各自优势，共同针对几个极具代表性的区块链平台进行研究与分析，希望可以对处于困惑中的企业带来些许帮助。

1 概述

从 2009 年比特币诞生至今，区块链技术（有时被称作分布式账簿技术）受到了金融和 IT 界越来越广泛的关注和认可。尽管该技术仍处于发展的初期阶段，但由于其具有简化和变革业务流程、保护数据完整性以及转变商业模式的潜力，已逐渐成为金融服务业的热点话题，一些金融机构已经在开展试验性的落地工作；在非金融领域，基于区块链的应用也在被不断开发并应用到大量场景中。在政府及行业监管层面，区块链技术的研究、应用验证也得到了前所未有的关注和支持。

随着区块链受到更广泛认可，越来越多的企业开始对该技术进行应用探索及布局。为了适应不同商业场景，企业在实际应用区块链技术的过程中，往往需要在身份认证、共识机制、密钥管理、隐私保护、监管要求等方面进行个性化配置，以满足特定业务的需求。伴随区块链技术的不断改进和企业运用区块链需求的极速增长，市场上为满足各类商业需求的开源区块链技术平台不断地涌现，如以比特币、以太坊（以下简称 Ethereum）为代表的公有链技术平台；以 Hyperledger Fabric（以下简称 Fabric）、R3 Corda（以下简称 Corda）、BCOS 区块链平台（以下简称 BCOS，BCOS 是微众银行、万向区块链及矩阵元三方共同开发的区块链底层平台）等为代表的联盟链技术平台，正可谓百花齐放、百舸争流。面对如此多样的区块链技术平台，我们建议应用企业在技术平台调研过程中，应首先根据自身业务特点进行平台选型，结合各区块链平台自身特点基础上，再量身进行定制化改造。

1.1 研究目标

当前区块链技术发展迅速，区块链技术平台也愈发多样。这就导致区块链应用企业亟待解决选什么、怎么选区块链技术平台的问题，同时，应用企业往往需要花费大量时间和精力投入到区块链技术平台的选择中。另外，各区块链平台之间及后进者亦需要迅速、全面地了解区块链技术平台市场的技术现状和发展风向。

故此，在本报告中，我们通过调研分析部分有代表性的区块链技术平台，从其架构分析、核心技术组件、应用功能、技术能力、安全机制、平台适用性、开发

及工具、维护支持能力等方面进行对比，明确不同平台的特点和适用范围，协助广大区块链应用企业在其选取区块链技术平台的过程中，提供一个较综合的信息参考和借鉴，以帮助企业更加全面地了解区块技术平台发展现状和动向。同时，该研究报告的发布，亦旨在为各区块链平台的进步和完善提供参考。

1.2 研究平台范围

我们将从全球范围内选择具有广泛影响力、经过充分运营实践、具备一定技术支持能力的平台进行分析。目前主流的区块链平台主要有比特币(Bitcoin)、以太坊(Ethereum)、Fabric、Corda、BCOS 等。由于资料公开程度较高，故我们将只选择开源的区块链技术平台进行分析。

在入选研究范围内的平台方面。Ethereum 发布于 2014 年，是一个图灵完备的区块链开发平台。从发布到 2017 年 5 月，3 年多的时间内，已经有 200 多个 Ethereum 应用诞生。Ethereum 具有遍布全球的开发者社区，并且设计了明确的开发路线图。同时，Ethereum 在技术方面也在隐私保护、吞吐量及智能合约等方面进行探索，以满足各行业的需求。Hyperledger 是 Linux 基金会于 2015 年发起的开源项目，联盟主要成员来自大型金融机构、大型 IT 企业、大型咨询机构等不同的利益体。Fabric 是 Hyperledger 项目在其原有代码库被 IBM 捐赠给 Linux 基金会后的首个被孵化的项目。Fabric1.0 版本已于 2017 年 7 月正式发布，官网显示，27 个组织、159 位开发者参与并作出贡献。Corda 是世界上最主要的区块链联盟之一 R3 使用的区块链平台，其成员包括国际大型银行、科技公司和其他金融服务企业。Corda 并不是严格意义上的区块链，据其白皮书，Corda 是一个“受区块链系统启发”的技术平台，考虑到其成员主要来自于金融领域，聚焦于分布式账本技术在金融领域的应用，且 Corda 在共识、有效性、唯一性、不可更改和可认证性上与区块链高度重合，所以我们也把 Corda 列入研究范围。BCOS 是微众银行、万向区块链、矩阵元共同开发的区块链技术平台，目前 BCOS 已在联合贷款备付金管理与对账、供应链金融服务和股权登记与服务等方面进行了实际运行，作为国内率先运用于金融领域并取得商用实践成果的区块链平台，我们亦将其纳入本次研究范围之内。

在未入选研究范围内的其他平台方面。比特币(BitCoin)的概念最初由中本聪在 2009 年提出，是一种 P2P 形式的数字货币，自诞生至今已平稳运行 8 年，具备成熟的生态系统，并且拥有众多的社区及技术力量。但公有链、单一标的资产和 PoW 共识机制等特性限制了比特币在非数字货币领域的应用。因此在本报告中，我们将不会针对比特币进行深入研究。

综上，结合影响力、运营实践程度、技术能力及应用能力，本报告将围绕 Ethereum、Fabric、Corda 及 BCOS4 个区块链技术平台展开分析。

1.3 研究内容

本报告将主要从 8 个维度对研究范围内平台展开分析，这些维度将从区块链平台所需关注的技术、应用、安全、支持等重点领域进行研究分析，具体研究内容包括：

一、区块链平台架构分析。在架构分析维度，分析了研究范围内平台在架构灵活性及节点分类合理性等方面的能力表现。

二、区块链平台核心技术组件分析。分析了研究范围内平台在共识机制、通信/P2P 协议、存储效率等方面的现状。

三、区块链平台应用功能分析。在应用功能维度，从基础应用功能、扩展功能，是否支持智能合约、监管接入等方面对研究范围内各平台进行分析。

四、区块链平台技术能力分析。在技术能力维度，量化对比各平台在吞吐量、响应时间方面的表现；在可用性上，主要分析了研究范围内各平台可用性与交易的最终性之间的关系。

五、区块链平台安全机制。在安全机制维度，主要从密钥安全性、隐私保护、防“双花”等方面分析研究范围内各平台的表现。

六、区块链平台的适用性分析。在平台适用性维度，主要从各个平台支持的业务场景进行分析。

七、区块链平台开发及工具分析。在开发及工具维度，主要从研究范围内平台所支持的开发语言，以及配套开发工具和环境进行研究。

八、区块链平台维护支持能力分析。主要从研究范围内平台的升级是否平稳、安全有序等角度进行分析。

1.4 研究方法

本报告的研究遵循安永区块链平台研究方法论。一、**维度框架**。选取 8 个维度进行分析，这些维度从区块链平台所需关注的技术、应用、安全、支持等重点领域进行研究分析。这 8 个维度排序不分先后，读者应结合自身情况及关注点进行研判。我们尽可能结合各平台官方信息以及市场公开信息对不同维度进行分析，并力求分析结果的全面性和客观性。二、**分析**。每个维度中设计若干变量指标，这些指标从不同的方面描述其所在维度的实际情况，使维度的分析更加立体、深厚。三、**总结**。以前期研究的不同维度及指标为基础，从宏观视角分析各平台的实际情况，总结不同平台的特点，并从应用角度对不同平台适用场景提出客观建议，供企业在选择区块链平台时进行参考。

在撰写本报告过程中，我们遵循的研究步骤主要包括以下三个方面：背景信息研究、维度选择及指标分析。首先，我们通过搜集各区块链平台的官方白皮书、官网披露信息等材料，作为信息的研究文献输入，以保证报告信息的权威性和及时性。由于官方公开披露的资料可能无法提供足够的研究分析背景信息，因此我们还会引用其他公开的、有明确来源的信息，例如官方论坛、第三方社区、Github 等。通过上述的背景信息研究，结合国内外发展现状和应用场景，参考《分布式账本技术：超越区块链》（英国政府首席科学顾问报告）、《The future of financial infrastructure An ambitious look at how blockchain can reshape financial services》、《中国区块链技术和应用发展白皮书（2016）》等主要权威文献中所提出的区块链通用技术需求及区块链技术框架、核心关键技术、治理、安全等框架，我们逐个挑选出开源区块链平台评价的一系列维度。

其次，在维度选择的基础之上，我们细化出各个变量指标，变量指标作为分析维度的延伸，将详细描述各个平台在这些维度中的客观表现。

最后，在对不同维度进行比较分析时，我们也秉持基于事实描述的原则来描

述不同平台的实际情况，不评价好坏优劣。例如，分析核心组件时，对于共识机制，我们不对共识机制的好坏发表评价，仅对平台支持的共识机制以及目前共识机制业界普遍的认知进行客观描述。

1.5 术语和缩略词

本报告中涉及的主要术语及其定义如下表所示。

术语	定义/解释
区块链	分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式。
分布式	相对于集中式而言。分布式是区块链的典型特征之一，对应的英文是 Decentralized，完整的表达形式是不依赖于中心服务器（集群）、利用分布的计算机资源进行计算的模式。
共识机制	区块链系统中实现不同节点之间建立信任、获取权益的数学算法。
智能合约	一种用计算机语言取代法律语言去记录条款的合约。
挖矿	比特币、以太坊系统中争取记账权从而获得奖励的活动。
区块	区块链系统中，一个区块是一个数据包，其中包含零个或多个交易，前块（“父块”）的散列值，以及可选的其它数据。
分布式账本	一个可以在多个站点、不同地理位置或者多个机构组成的网络中分享的资产数据库。其中，资产可以是货币以及法律定义的、实体的或是电子的资产。
轻客户端	也叫 SPV 客户端，一个只下载一小部分区块链的客户端，使拥有低功率或低存储硬件的用户能够得到几乎相同的安全保证。
幽灵	一个协议，通过这个协议，区块可以包含不只是它们父区块的散列值，也散列父区块的父区块的其他子块（被称为叔区块）

术语	定义/解释
	的陈腐区块。这确保了陈腐区块仍然有助于区块链的安全性，并减轻了大型矿工在快速区块链上的有优势的问题，因为他们能够立即得知自己的区块，因此不太可能产生陈腐区块。
Chaincode	HyperLedger 中作为交易的一部分保存在总账上的应用级的代码（如智能合约）。链节点运行的交易可能会改变世界状态。
验证节点	HyperLedger 网络中负责达成共识、验证交易并维护总账的一个计算节点。
非验证节点	HyperLedger 网络上作为代理把交易员连接到附近验证节点的计算节点。非验证节点只验证交易但不执行它们。它还承载事件流服务和 REST 服务。
公证人	Corda 平台中的概念。公证人是一个独立的、交易双方（多方）都信任的角色，确认交易的有效性。公证人将由多个互相不信任的参与方组成，它们使用一个标准的一致性算法。
UTXO	英文 Unspent Transaction Outputs，即未花费的交易输出，它是比特币交易生成及验证的一个核心概念。交易构成了一组链式结构，所有合法的比特币交易都可以追溯到前向一个或多个交易的输出，这些链条的源头都是挖矿奖励，末尾则是当前未花费的交易输出。所有的未花费的输出即整个比特币网络的 UTXO。
图灵完备	一切可计算的问题都能计算，这样的虚拟机或者编程语言就叫图灵完备的。
双花	即二重支付，指攻击者几乎将同一笔钱用于不同交易。
Raft	一种为了管理复制日志(Replicated log)的一致性协议。

表 1 术语

本报告中涉及的主要缩略词如下表所示。

缩略词	定义/解释
PoW	工作量证明(Proof of Work)
PoS	权益证明(Proof of Stake)
DPoS	股份授权证明(Delegate Proof of Stake)
PBFT	实用拜占庭容错(Practical Byzantine Fault Tolerance)
P2P	点对点(Peer to Peer)
DApp	分布式应用(Decentralized Application)

表 2 缩略词

2 架构分析

系统架构决定了应用的适用范围、跨链及链上链下的数据整合的可行性，甚至商业变革的方向。因此，各平台架构的升级理念，无不体现平台对于区块链技术和商业模式的理解。目前，各平台对于基础架构的设计思路不一，本次研究针对传统区块链的架构进行了总结，同时结合研究范围内各平台特点，对其技术架构进行分析，并从模块化与插件化、快速构建应用、高效运营等角度，抽离出各平台在架构设计上的技术特点，为区块链应用企业从架构角度了解各技术平台提供参考。

传统区块链倾向于把架构分为数据层、网络层、共识层、激励层、合约层、应用层。

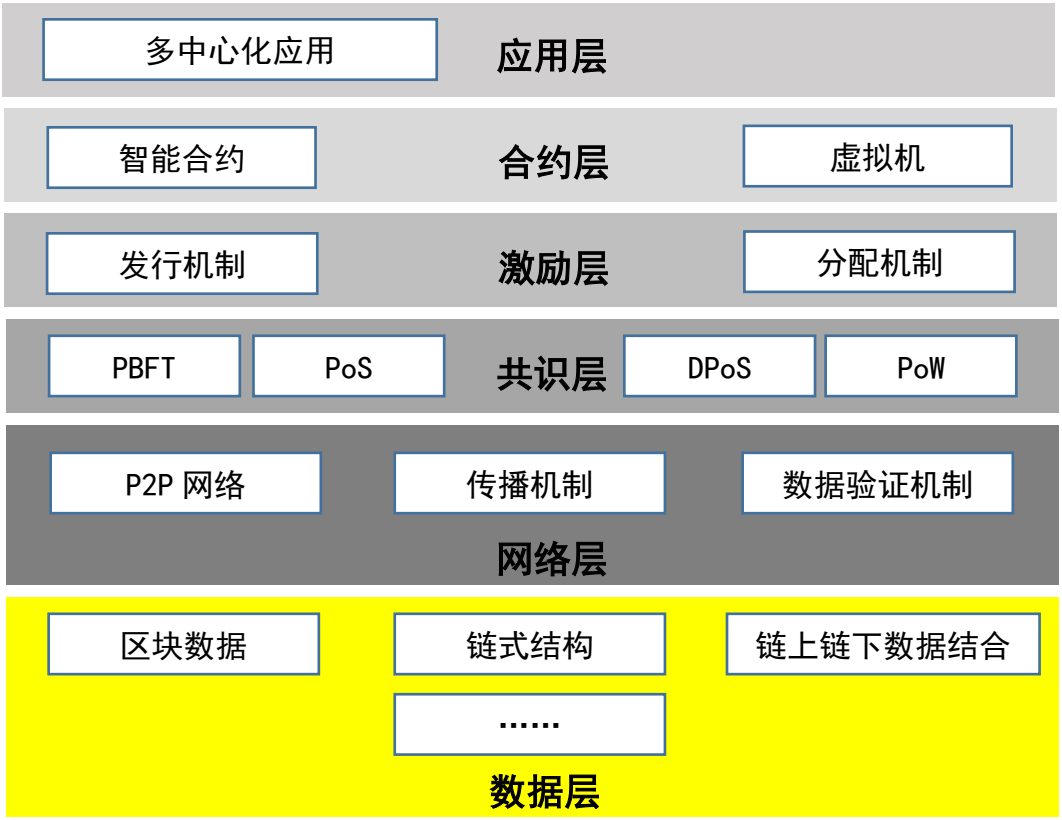


图 1 区块链平台架构示例

1、数据层

数据层是最底层的技术，封装了底层区块数据的链式结构，以及数字签名、哈希函数和非对称加密技术等多种密码学算法和技术。主要实现了数据存储、账户

和交易的实现与安全两个功能。上述大多数技术都已经在计算机领域应用多年，是相对成熟的技术。

2、网络层

网络包括 P2P 网络机制、数据传播机制和数据验证机制等，主要实现网络节点的连接和通讯。P2P 组网技术早先应用于 BT 类的 P2P 下载软件中，是一种很成熟的技术。

3、共识层

共识层主要封装网络节点的各类共识机制算法，实现全网所有节点对交易和数据达成一致，防范拜占庭攻击、女巫攻击和 51%攻击等共识攻击，其算法称为共识机制。比较常见的共识算法有工作量证明机制(PoW)、权益证明机制(PoS)、拜占庭容错算法(BFT)等。

4、激励层

激励层主要实现区块链代币的发行和分配机制，该层主要出现在公有链中，用以激励遵守规则参与记账的节点，惩罚不遵守规则的节点，促使整个系统朝着良性循环的方向发展。

5、合约层

合约层主要封装各类脚本、算法和智能合约，赋予账本可编程的特性。Ethereum、Fabric、Corda 和 BCOS 通过虚拟机的方式运行代码实现智能合约的功能，比如 Ethereum 的以太坊虚拟机(EVM)。

6、应用层

应用层封装了区块链的各种应用场景和案例，如搭建在 Ethereum 上的各类去中心化的应用(DAPP)。某些技术文档中也有人认为应用层应与合约层合为一层。

激励层、合约层和应用层不是每个区块链应用的必要组成部分。实际上，在 Fabric 和 Corda 等面向联盟链和私链的平台中一般都不设激励层。即使在公链平台上，网络层也已经开始走向跨链融合与链外资源（如 IPFS）的集成。而 Corda 在数据层没有公共账本的概念。

在架构分析维度，本次研究从架构灵活性、节点分类等方面进行分析。另外，在平台技术架构快速构建应用的能力、运营的高效性、整合分布式账本之外的技术

资源的支持能力，以及架构可配置性、可维护性、可伸缩性、可扩展性等方面也是我们在架构层面重点关注的部分，但因为缺乏有效的公开资料及信息，因此不在此论述。

（一）架构灵活性。Fabric 采用了松耦合的设计，将共识机制、身份验证等组件模块化，在应用过程中可根据应用场景选择相应模块。同时，Fabric 还可支持针对不同主体间交易的多通道结构，实现了更为灵活的业务适应性（业务隔离、安全性等方面）。Corda 在共识机制模块，设计为可插拔的独立性服务，独立服务即由一群相互无关的节点通过拜占庭容错算法组成或只是一台单独的机器，独立服务仅需要证明其状态是否被之前使用过状态的交易所使用，而不必自己证明交易的合法性。这意味着，独立性服务相比其他分布式账本和区块链设计，提高了扩展性、分账系统的兼容性和算法的敏捷性。Ethereum 计划通过分片机制提高整个网络的灵活性，分片之前整个网络的处理取决于单个节点的处理；分片后，只有同一片内的处理是同步的、一致的，不同分片之间则可以是异步的。Ethereum 分片机制尚处于研发过程中。BCOS 共识算法模块采用插件化设计实现，通过修改系统配置，实现在多个联盟链里使用不同的共识机制，参与到同一个联盟链的所有节点必须采用同一种共识配置。

（二）节点分类。对于节点的分类，就是让其在商业场景下，做最适合自己做的事情，让共识机制、多通道等方面的架构设计发挥作用。在 Fabric 中，把节点分为验证节点和非验证节点，并通过授权和证书管理节点。Corda 的节点分为普通节点、公证节点和管理节点，对于交易有效性的共识机制在公证节点处达成，另外适用于金融领域的凭证流也由公证节点运行和签发。Ethereum 正从 PoW 共识机制走向 PoS 共识机制，节点间将依据资产的多寡分配相应的记账权重，这样可以更好地利用计算资源，让处于核心地位的记账节点得到更好的资源倾斜。BCOS 将节点分为共识节点和观察节点，共识节点参与共识算法，成为链上的记账者，观察节点则不参与共识，只同步数据。

3 核心技术组件

核心技术组件是指区块链系统所依赖的基础组件、协议和算法，可进一步细分为通信、存储、安全机制、共识机制等四个方面。核心技术组件实现了区块链系统中最基础的功能，也是区块链平台的核心能力，很大程度上决定了区块链平台所具备的技术水平，是区块链应用企业在选择区块链技术平台时主要的参考标准之一。本次研究主要从共识机制、通信/P2P 技术、存储和计算效率、数据结构等方面分析各平台核心技术组件的现状。

（一）共识机制。共识机制是区块链系统中各个节点达成一致的策略和方法。目前主流的共识机制有 PoW（工作量证明机制）、PoS（权益证明机制）、DPoS（委托授权的权益证明机制）、Raft、PBFT（实用拜占庭容错算法）等，以下是选取的各个主流共识机制的对比分析：

	PoW	PoS	DPos	Raft	PBFT
场景	公链	公链、联盟链	公链、联盟链	联盟链	联盟链
去中心化程度	完全	完全	完全	半中心化	半中心化
记账节点	全网	全网	选出若干代表	选出一个 leader	动态决定
响应时间	10 分钟	1 分钟	3 秒左右	秒级	秒级
存储效率	全账本	全账本	全账本	全账本	全账本+部分账本
吞吐量	约 7TPS		约 300TPS 或更高		约 1000TPS 或更高
容错	50%	50%	50%	50%	33%

表 3 主要共识机制对比

Ethereum 当前使用 PoW 共识机制，需要全网具备较大规模算力支撑来保证网络安全性。2016 年，Ethereum 在开发路线图中提出了代号为 Casper 的 Proof of Stake（权益证明）PoS 算法，计划于 2017 年将 PoW 完全转换为 PoS，验证人数最多 250 人，并且区块一旦达到最终状态就完全不可伪造。PoS 共识机制可以解决交易的确定性问题，降低成本，也让轻客户端变得可能。2017 年 5 月初 Ethereum 公布的计划实施指南中，指出 Ethereum 将计划选择 PoW+PoS 混合机制。Hyperledger 协议下的共识运用可插入式算法，用户在配置中自行选择共识算法。Hyperledger 协议在首次发布时提供了拜占庭容错算法(BFT)，这种算法采用的是实用拜占庭容错算法(PBFT)协议。Corda 网络允许有一个或者多个公证服务，公证服务是 Corda 网络交易验证和确认的核心机制，提供交易排序和时间戳服务。它一般用 BFT 算法为公证服务，但在法规足以保证协议合规的情况下，也可以使用高性能算法（如 Raft）。在 BCOS 中，采用 PBFT、Raft 做为联盟链的共识算法，系统的共识机制采用插件化实现，通过修改系统配置，即可设定使用不同的共识机制，参与到一个联盟链的所有节点必须采用同一种共识配置。

	Ethereum	Fabric	Corda	BCOS
共识算法	PoW	主要为 PBFT	一般用 BFT	PBFT、Raft
可插拔	否	是	是	是
可扩展	否	是	是	是

表 4 研究平台共识机制对比

（二）通信/P2P 技术。区块链通常采用 P2P 技术来组织各个网络节点，每个节点通过多播实现路由、新节点识别和数据传播等功能。在通信/P2P 技术方面，Ethereum 客户端 P2P 协议是一个标准的加密货币协议，能够容易地为其它加密货

币使用，仅有的改动是引入了“幽灵”协议。Ethereum 仅采用了幽灵协议的最基础部分，即废块必须以下一个区块的叔区块的身份纳入计算。Fabric 点对点协议运用的是 Google RPC 协议，其功能包括双向流、流控制、在单一链接下执行多路复用要求等。它能与现有的网络基础设施结合，包括防火墙、代理服务器以及安全保护等。这一组合能够为对等节点采用的信息提供由点对点到多路传送的定义。Corda 的通讯协议基于 AMQP/1.0，采用 TLS 作为加密协议。Corda 内嵌了一个支持 AMQP/1.0（也支持 JMS）的全功能的消息中间件，并且适合于嵌入式应用。通过这个手段，通讯本身的功能都得到了覆盖，既包括基本的网络通讯协议的支持（Artemis 的通讯功能基于 Netty）、消息格式解析，又包括消息持久化（提升可靠性）、队列管理（简化内部消息处理流程）等特性。

（三）存储。要实现分布式账本的大规模应用，存储的开销是需要解决的关键问题之一。区块的数据结构通常只能追加记录而不能删除或者修改，以能够使新加入的节点对全网的完整交易历史进行验证，随着历史数据的增长，存储开销成了影响区块链系统扩展性的一大问题。Ethereum 和 Fabric 与比特币一样，使用 Merkle 树存放交易散列，在面临不断增长的数据时，一旦需要回收硬盘空间，可以选择将老旧的交易从 Merkle 树中剔除，但具体如何实施仍存在争议。除此之外 Ethereum 和 Fabric 还采用了状态快照的方式来节约硬盘空间，即区块头除记录当前区块所有交易的根散列外，还记录当前区块及过去所有区块中的状态根散列。所以如需节约空间，节点可以清空状态快照之前的交易历史，只保留最新区块和完整的信息状态，但这样相当于在安全性和去中心化上做出了一定妥协，因为全量历史记录有可能回退到云化甚至中心化存储。BCOS 支持分组多副本方式存储文件，并在区块链中保存文件的哈希值和相关寻址信息，提高区块链的存储和网络同步效率。BCOS 还支持分布式数据存储的方案，在综合考虑数据的容量、可维护性、安全性等方面的基础上，企业可使用现有分布式存储方法，如数据仓库、数据库集群等存储区块链数据。

（四）计算效率。若交易可以被并行验证，则可以通过简单地增加 CPU 数量来提高吞吐量。但若具备状态持久化能力的智能合约是顺序相关的，则难以并发验证。目前 Fabric 对此没有好的解决方案。Ethereum 的交易理想中可以通过分区解

决智能合约状态持久化问题，从而使得交易可以被并行验证（即将各个合约分到不同的逻辑区中，每个区中的合约都顺序执行，而不同的区之间并行执行），但该功能尚未实现。Corda 由于数据仅存放在合约执行者的节点，因此无法进行全局的持久化存储，同时 Corda 基于 UTXO（Unspent Transaction Output，即未被花费交易输出）的交易可以并行验证且任意排序，所以 Corda 的交易也可以被并行验证。BCOS 利用集群化、分片机制，使交易按一定的规则互相隔离，可被并行处理，且数据量可以通过垂直切分的方式，分布存储在不同的存储设备上，以满足性能和容量平行扩容的需求。

（五）数据结构。在区块链技术中，数据以区块的方式永久储存。区块按时间顺序逐个先后生成并连接成链，每一个区块记录了创建期间发生的所有交易信息。区块的数据结构一般分为区块头(Header)和区块体(Body)，如图 2 所示。其中，区块头用于链接到前一个区块并且通过时间戳特性保证历史数据的完整性；区块体则包含了经过验证的、区块创建过程中产生的所有交易信息。

图 2 区块链数据结构

Ethereum 的区块头中除了前一个区块的引用信息、区块号、交易信息的 Merkle 树的根哈希值和时间戳等信息外，还包含了收据（Receipts）、状态（State）的 Merkle 树的根哈希值。Fabric 的区块头内容除了前一个区块的引用信息、版本号、交易信息的 Merkle 根和时间戳等信息外，还包含了世界状态(World State)的 Merkle 树的根哈希值。Corda 中没有“区块”的概念，而是将交

易相链接，以达到数据不可逆、可追溯的特性。

4 应用功能

应用功能是指区块链平台为进行用户身份管理、实现上层应用所需的基础功能组件，应用功能是在核心技术组件基础上，提供了针对区块链应用场景的基础管理功能，一方面其允许通过使用智能合约的方式制定商业规则以管理交易，灵活操作链上资产，并辅以账户体系使区块链生态与现实商业社会更加紧密地衔接。另一方面，对于联盟链和专有链，通过应用功能中的身份认证、私钥保护等手段，强化成员管理，实现可信交易和防伪溯源。同时，通过设置节点权限，与现有商业规则中的监督体系保持一致。在应用功能维度，本报告从身份认证、账户设计、私钥保护、是否支持智能合约、监管相关功能以及特权机制等方面进行分析。

（一）身份认证。Ethereum 采取匿名身份认证体系，对线上线下的身份匹配无强制要求；Fabric、Corda 和 BCOS 均支持数字证书的身份认证形式。Fabric 提供了一个基于 PKI 的身份管理，实施交易的权限管理。首先通过 Registration Authority(RA)注册获得许可，然后通过 Enrollment Certificate Authority(ECA)获得注册安全证书(ECert)；第三步，通过 Transaction Certificate Authority(TCA)获得交易安全证书；最终只有使用以上安全证书的二者之一签名的节点才能发起交易请求。Corda 网络中，有一个负责全网身份服务的系统节点。该节点负责颁发证书、设置权限。任何想加入网络的节点都需要从身份服务节点处获得相应身份。BCOS 使用 CA 证书的准入机制，支持用户帐户管理功能，采用角色和权限模型实现联盟链参与者管理，底层平台还预置了控制交易和部署合约的权限和接口。

（二）账户设计。Ethereum 采用了余额账户机制。由于 Ethereum 是以智能合约为主要功能，而在智能合约中要处理 UTXO 的状态相当困难，相比之下，余额设计更便于程序实现。Fabric 中没有代币概念，但可以通过 Chaincode 实现本币发

行和账户功能。Corda 没有余额概念，所有余额均通过 UTXO 计算得出。Corda 采用的 UTXO 的账户机制具备私密性与可扩展性的特点。

（三）私钥保护。Ethereum采取的模式为：无人操作的挖矿/记账节点上不存储私钥，随同这些节点部署的智能合约也不使用私钥，所有私钥均部署于“端”，由用户本地存储。Fabric 的私钥由用户在本地存储。Corda 任一节点都与证书和私钥绑定，证书和私钥信息可存储在无人看管的节点机内。BCOS 加密数据的密钥采用加密机，独立密钥服务器等方式进行维护，和节点分离存储，保障密钥的安全性。

（四）支持智能合约。Ethereum 可实现“图灵完备”（一切可计算的问题都能计算，程序逻辑自洽）的智能合约功能，采取合约和共识相连。Fabric 的智能合约运行环境选择的是 Docker 容器，在容器里可以支持 Java、Go 等语言编写的智能合约，提供一些复杂业务逻辑运行。对可以执行智能合约的记账节点，每一个新部署的智能合约都将在一个独立的 Docker 中运行。为每个智能合约创建一个 Docker 是 Fabric 设计存在争议的地方。目前 Fabric 并不支持对智能合约运行 Docker 的生命周期管理。Corda 同样支持智能合约。智能合约程序代码在特定的 JVM(Java Virtual Machine)上运行。Corda 中的智能合约是一段段针对输入输出状态的验证程序，由每个交易环节按需调用，价值交换是由“交易”来承载的，所以从这一点上看 Corda 的智能合约与其他平台的智能合约有不小的差距。但是 Corda 的“流框架”（Corda 中的交易流(flow)是复杂交易的具体实现协议。现实世界中所出现的涉及多方的、多环节的、有条件的交易等复杂处理流程，需要通过交易的组合、包装来完成。Corda 有大量的内置 flow，基本覆盖了日常交易流程中所用到的功能和典型交易的过程）可以把多个交易串成流程，从而实现价值再分配的业务逻辑。所以，Corda 中的“交易”、“智能合约”和“流架构”加起来，才能达到其他分布式账本平台上通常的“智能合约”的表达能力和计算能力。BCOS 主要运用 Solidity 合约开发语言，其作为 Ethereum 的主要合约开发语言，具有图灵完备的特性。

（五）监管相关功能。Ethereum 因其公有链特征，监管可随时接入，但由于身份匿名性，监管接入的意义不大。在 Fabric 系统中，监管机构可以按照规定规则来审计全部或部分总账分录。在与参与者合作中，审计员可以通过基于时间的证

书来获得总账查看权限，连接交易来提供实际的资产操作。Fabric 利用密钥的层级可以给予审计员检查某些交易、某组交易的审计权限，只将最相关的密钥披露给审计实体以提供审计的可能性。不是系统成员的应用审计人员，可以给予被动的观察区块链数据的权限，同时保证给予他们只是为了与被审计应用程序相关的交易。Corda 支持监管接入体现在如下技术环节：（1）许可环节，可提出实名制要求、设置准入条件、通过证书和名字服务将监管要求落地；（2）运营环节，可赋予监管节点访问一切节点上本地数据库的权限，获取全部交易数据，达到“看穿式”效果。BCOS 可支持监管部门和审计部门作为特殊节点接入，即时同步数据，并对数据完整性、有效性、过程和流程的合规性进行即时的监控，从而可对异常或违规行为及时处理或给予指导意见。另外，BCOS 还可提供可监管、可审计的数据接口。

（六）特权机制的实现。目前，特权机制主要有两类：一是暂停、回滚或者取消交易；二是改正数据。在 Ethereum、Fabric 和 Corda 的公开资料中，我们均未发现与这两类特权机制相关的内容。因此，Ethereum 在受到智能合约 DAO 攻击时，只能进行硬分叉，无法进行回滚、取消交易或改正数据的处理。理论上，Ethereum、Fabric 和 Corda 都可以经过线下的组织，通过约定一定的规则，来“隐性地”实现特权机制，如有组织的硬分叉、反向交易等。具体到单个平台来讲，Corda 由于不存在公共的底层账本，只需要设计适当的凭据流，特权组织便可获得在特定节点进行应急处置操作的权利，包括但不限于暂停交易、纠正错误交易等。BCOS 可以针对特定的业务场景，制定特定的权限集合，如监管方可以是联盟链的规则制定者和实施者，通过参与准入审核，智能合约编写、部署和升级，以及事前中后的检测和干预对业务实施监管。监管方也可以选择性地参与到交易过程，例如在合约执行前或者生效前，由监管方检查合约的规则、数据，必须符合监管要求，才给出签名背书。一旦发现违规行为，监管方拥有一系列控制权限，包括但不限于对某个业务叫停、冲正某些交易、冻结某些帐户、升级合约以修改订正业务规则等。底层平台预置了控制交易和部署合约的权限和接口，通过监管工具、角色赋权等方案，让监管方可以直接实施联盟链的控制。

5 技术能力

技术能力是每个区块链技术平台的关键能力之一，也是区块链应用企业在选择区块链技术平台过程中的重要考量因素之一。区块链技术是一项新兴技术，但它所依赖的 P2P 网络协议、数字签名、非对称加密等都是较成熟的技术，这些成熟技术不同的组合所产生的技术能力也是各有长短，影响着区块链的业务场景及商业价值。在技术能力维度，本次研究主要从平台业务吞吐量、区块或交易的确认时间、区块链平台可用性等方面进行了分析。另外，平台最大支持节点数量、最大并发开发者数量、最大并发用户访问量、平台稳定性等方面也是本次研究的要素，但囿于缺乏有效的公开资料及信息，因此不在此论述。

（一）吞吐量。目前，Ethereum 网络受限于 CPU 单线程性能。早期测试网络已达到每秒实现 25 次交易（在某种优化条件下），通过优化可能会提高到 50TPS 或 100TPS。然而，在真实的应用程序负载下，Ethereum 网络当前的交易可能会被限制到 10TPS 或者更低。Fabric 在 PBFT 共识机制下，可达到 1000TPS 或更高。对于 Corda，写入操作是按需延迟复制，延迟程度跟交易复杂程度正相关，所以很难对整个网络报出一个每秒交易数。BCOS 利用 PBFT 共识机制，在 4 节点环境下，转账交易的合约调用，性能可达到数千 TPS，通过平行扩展，可以满足更高服务需求。

（二）确认时间。当前 Ethereum 协议取决于节点根据在计算上开销很高的工作量证明(PoW)算法选择用于最长链的下一区块。这种方法的缺点就是区块链每 12 秒左右才能够提交一个新的区块，确认时间也是在 12 秒左右。Ethereum 预计 2017 年推出的雷电网络解决方案(Raiden)，可以使得基于 EIP20 的 TOKEN 进行每秒 100 万笔以上的传输，传输的确认时间在毫秒级。Fabric 默认一个交易出一个块，也支持 Commit TxBatch 模式，多个交易一个块。Fabric 在 PBFT 共识机制下，需要 3-6 秒确认交易。Corda 的共识机制无需建立在批量打包成块、逐块确认的基础之上，可以对每一笔交易实时达成共识。BCOS 支持动态配置确认时间，其所采用的共识算法均可支持 1 秒出块，出块即达成共识。

（三）可用性。Ethereum采用的工作量证明机制(PoW)提供了较高的灵活性和可用性。因为每个节点都独立构造区块而不需要其他节点的参与，节点可以随时加

入或者退出网络，即使全网只剩一个节点，网络还是可以继续工作，但相应地它也失去了交易的最终性（保证交易不可撤销）。Fabric 采用的拜占庭容错机制牺牲了一定的灵活性和可用性，记账节点必须在线提供服务而不能退出网络，一旦出现三分之一的记账节点停机，网络将变得不可用，但它保证了交易的最终性（保证交易不可撤销）。在 Corda 中，由于没有统一总账，每个“节点”必须自行存储自己的交易数据。这就意味着，每个节点必须自行解决自身的网络级、系统级、应用级、数据级的容灾备份问题，否则，在需要出示单据时，上述任何一个环节出现问题，都将导致重大事故。BCOS 可支持使用 PBFT 和 Raft 两种共识机制，当使用 PBFT 时，系统可用性同 Fabric 一致，整个系统中少于等于三分之一数量的节点出现故障，均不影响共识进行；当使用 Raft 算法时，整个系统中等于或超过 1/2 数量的记账节点出现故障，网络将变得不可用。

6 安全机制

区块链在设计中采用了分布式数据存储、共识机制、数字签名、加密算法等多种安全手段和技术。这些技术保证了数据的完整性、不可篡改性和一致性，从而保证了数据从交易、共识计算、区块确认、数据存储等全生命周期的安全性。随着区块链技术受到的关注日益增强、各类数字货币的价值飞涨，导致越来越多的不法分子渴望挑战区块链的安全性。例如，51%的攻击随着矿池的兴起而逐渐具备实现的可能；区块链交易平台遭受攻击的事件频频发生。不过大部分的漏洞在于集中化的交易应用平台，而非底层技术平台的安全能力。本次研究将探讨区块链技术中各种安全机制的属性和特征，分析研究范围内平台在解决使用安全性、系统安全性、算法安全性、协议安全性等诸多挑战时所采取的策略，为区块链应用企业选择安全可靠的区块链技术平台提供参考。在安全机制维度，本次研究主要从密钥安全性、隐私保护、防“双花”、隐私保护等方面进行分析。算法和协议安全性也是区块链技术平台安全的重要考量指标，但因为缺乏足够的公开资料及信息，无法进行进一步分析。

（一）密钥生成机制。在用户账户密钥层面，各平台均利用非对称加密算法生成公私钥。Ethereum 密钥生成机制为：随机数发生器生成私钥，再经 SECP256K1（一种椭圆曲线算法）生成公钥。Fabric 提供了经过修改和未经修改的 PKCS11 来生成密钥。PKCS11 是公钥加密标准 PKCS(Public-Key Cryptography Standards)中的一份子，它为加密令牌定义了一组平台无关的 API，如硬件安全模块和智能卡。这使得在 Fabric 中可以使用 HSM（硬件安全模块）保护并管理数字密钥，以实现强身份验证。Corda 可以使用分层确定性密钥派生方案，它具有彻底分离公钥与私钥的生成从而提升安全协议的能力。

（二）密钥存储。Ethereum 密钥生成后作为文件或字符串保存在用户终端或者托管到服务器，但 Corda 的私钥可能会存储在无人看管的节点。Ethereum 和 Corda 的秘钥文件是一个 JSON 格式的文本文件。Fabric 的密钥文件可以存储在支持 PKCS11 的硬件设备中。BCOS 密钥保存在与区块链节点隔离的服务器、加密文件、USBKey、加密机等。需要使用私钥时，通过安全的内部通信接口或通过用户密码授权访问私钥。

（三）密钥使用和密钥找回。四个平台均无定期更换机制，且私钥丢失后无法找回。

（四）防“双花”。“双花”即二重支付，指攻击者几乎将同一笔钱用于不同交易。Ethereum 的防“双花”采用了余额机制：每个账户都有一个状态，状态中记录了账户当前的余额，转账的逻辑即从一个账户中减去转账的金额，并在另一个账户中加上相应的金额，减去的部分和加上的部分必须相等。Fabric 运用了状态版本的概念，如果请求节点将背书过的具有相同状态依赖的交易建议提交给共识服务两次，共识服务会分配两个序列号给这两个交易并送达各个节点，节点进行本地状态版本依赖验证时，先接受的交易由于已经 commit，本地状态已经新增了一个版本，后来的相同交易由于依赖了一个过时的版本，不会通过状态版本依赖验证，而作为非法交易被丢弃。Corda 基于公证人(notary)进行交易确认方式，在系统只有一个公证人的情况下，通过对历史交易记录进行查询的方式就可以实现。一旦系统中有多个公证人，并且出现“跨”公证人的交易活动，防止双花的职责就涉及多个公证人之间的“协同”。Corda 结合交易场景，采用了一个相对标准的方式，即

不在交易过程中让多个公证人互动，而是在交易之前必须把交易所需要的所有输入状态指定到验证该交易的公证人上，避免一个状态可以在两个公证人上进行验证的情况，从而实现了防止双花。BCOS 基于账户模型和区块高度，对交易生命周期进行检验和控制，避免交易被不正确或不合法的重放。同时，BCOS 作为联盟链平台没有内置的原生代币，不存在币的双花问题。此外，BCOS 上的数据及资产使用智能合约来定义和进行操作，智能合约图灵完备的特性，能让业务方进行有效性、合法性的判断和控制，因此能够从一定程度上保证资产交易的安全性。

（五）隐私保护。Ethereum 使用“状态旁路”方案，在这种策略下，分布式账本上可见的只是粗粒度的“批发”，而真正细粒度的双边或有限多边交易明细，则不作为“交易”记录在分布式账本上，如果需要更改旁路中资产比例，则将指令加密发送到相应智能合约之中，因此交易明细的变动对于不在合约中的其他用户而言就是不可见的，但状态旁路只能达到部分保护效果。Fabric 利用多通道(Channel)的机制保护隐私性。Channel 代表了一个私有的广播通道，保证了消息的隔离性和私密性，不同的 Chaincode 关联主体只知道自己 Chaincode 相关交易和执行交易验证，共识服务只接收相关主体的广播请求和执行对相关主体的消息送达，节点只记录与其相关的 Chaincode 的状态。另外，Chaincode 可设定为保密，系统依据部署时设定的保密级别，执行通讯消息加密。Fabric 在多通道模式下，共识节点会接收所有通道的交易数据，需要对共识节点进行适当的安全管理和技术控制，防止信息泄露。Corda 主要采用了以下两项隐私保护技术：1.抽离(Tear-off)部分敏感内容的类盲签名技术，该技术采用把敏感字段和非敏感字段分组哈希，再分层构建 Merkel 树的方式，使得去掉敏感字段后，剩余的 Merkel 树仍然具有树状结构和针对非敏感字段的验证价值，可在其基础上达到类似盲签名的效果。同时一旦发生法律纠纷，如已去除的敏感字段内容被伪造，该 Merkel 树还可用作鉴别证据真伪之用。2.复合签名技术。该技术使用感知机模型，对多个签名主体赋权，并设置加权求和阈值。一旦一个指定群体中签名的主体所占加权和超过阈值，则复合签名生效。这个模型可以实现一组签名的“与/或”逻辑组合，但在涉及“异或”这样的逻辑组合时失效。BCOS 可在部分业务场景中，引入可信的中央对手方提供信用背书，交易参与方的交易数据明细对中央对手方为全部可见，但是对联盟链为不可

见，由中央对手方对交易进行验证并提供面向全联盟链的证据。通过物理隔离，逻辑通道设计，交易明细仅发送给交易牵涉的节点以及可能存在的监管节点，从基础层面防止了隐私数据的扩散。BCOS 还可使用数据脱敏、机构间点对点通信、数据明细链下保存、高强度加密数据信封方式等方式实现隐私控制。另外，BCOS 已在客户端和智能合约上实现加法同态加密算法，例如在部分只涉及到数据加减的场景，可采用加法同态加密算法，实现对数据的隐私保护，同时不会对性能造成很大影响。BCOS 还计划增加多操作同态加密和零知识证明用于证明加密数据的正确性（如账户余额数据是否足够用于支付）。从总体上看，理想的隐私保护策略，如零知识证明、同态加密等大都基于较为复杂的密码学技术，目前在各平台实际应用中有待进一步完善并丰富应用场景。

7 平台适用性

区块链作为一项新兴技术，在优化业务流程、降低运营成本、提升协同效率等方面拥有极大的想象空间。区块链应用企业在选择技术平台过程中，应该考量企业自身的商业模式与平台应用适用性之间的契合度。随着区块链技术的不断发展，在以比特币为代表的传统区块链应用场景中遇到的技术瓶颈，如交易性能不佳、身份验证缺失、隐私无法隔离保护等方面，在 Ethereum、Fabric、Corda、BCOS 等区块链技术平台上均有所突破，由此区块链技术在各行业的应用范围也逐渐扩大。目前金融、互联网、能源、农牧、工业制造等各行各业均广泛探索区块链的应用布局。随着 PoC（Proof of Concept，概念验证）的逐步展开，区块链技术在实际应用中会不可避免地与监管、法律、社会组织有所碰撞，在治理层面将会面临很多中间状态，所以“联盟链”、“私有链”仍是目前的主要应用形态，完全的“公有链”除了比特币之外，还未看到其他成熟应用。另外，此次研究就平台适用性维度还从区块链平台支持的业务场景方面进行了分析。

Ethereum 是内置有图灵完备编程语言的区块链，该特征使得任何人都能够创建合约和多中心化应用，并在其中设立他们自由定义的所有权规则、交易方式和状

态转换函数。因为图灵完备性，Ethereum 智能合约比比特币脚本所能提供的智能合约要强大得多，因此，Ethereum 在应用场景上相较于比特币来说得到了大大的拓展。Ethereum 通过 Ethereum 社区共治的公链，体现了 Ethereum 平台对公链场景的适用性，但也可以利用 Ethereum 平台部署联盟链或私有链。Ethereum 可利用图灵完备的智能合约，适应金融应用、物联网、供应链管理、社交网络、去中心化自治组织(DAO)、预测市场等场景。

2017 年 7 月正式发布的 Fabric 1.0 在 0.6 版本的基础上，针对安全、隐私、性能、实际场景需求等方面进行了改进，尤其是验证节点(Peers)的功能分离，即将原先区块链中共识节点承担的数据维护和共识服务职责进行分离，共识服务从验证节点中完全剥离出来，独立为 Orderer 节点（共识节点）提供共识服务，验证节点只对相关的合约进行验证和背书。另外，共识节点在提供共识服务时，支持多通道消息传递，也就是说平台可以设立应用程序，在验证节点的任意子集中架设通道。子集中的验证节点组成该通道内交易的相关者集合，而且只有这些验证节点可以接收相关交易的区块，与其他交易完全隔离。例如，如下图所示，验证节点 1、2 和 N 订阅红色通道，并共同维护红色账本；验证节点 1 和 N 订阅蓝色通道并维护蓝色账本；类似地，验证节点 2 和验证节点 N 在黑色通道上并维护黑色账本。

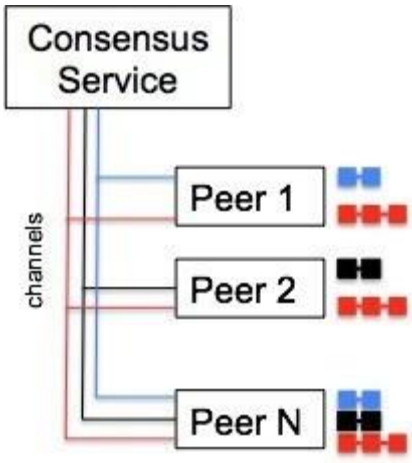


图 3 Fabric多通道架构

上述改进使得 Fabric 具备了多通道的架构设计以及共识节点的独立性，可以在保证平台上交易多方隐私性的同时，提高共识节点的效率，从而在技术上推动区

块链和分布式账本技术在跨行业应用场景中的应用，使其可满足金融服务、供应链管理、智能制造、文化娱乐、医疗健康、社会公益、教育就业等领域的应用。

Corda 由 R3 CEV 联盟组织开发，其成员主要来自于金融领域，聚焦于分布式账本技术在金融领域的应用。Corda 定位为面向非公有链的场景，其架构设计如可插拔的共识算法、灵活可配的节点权限、凭据流概念的引入，使得 Corda 更接近于受监管的金融机构的应用。

BCOS 定位为企业级应用服务的区块链技术平台，其在多链、跨链、分布式存储及隐私保护等方面上的设计，满足其在金融、健康医疗、供应链、工业、物联网、能源服务等多个领域上的适用性。另外 BCOS 可支持账号管理、资产管理、交易管理、安全控制等模块功能的配置，因此对于各多种场景下所需的功能其均能很好地实现。

另外，从区块链平台与外部数据对接的角度上看。Ethereum、Fabric、Corda 和 BCOS 在架构上均预留了身份、策略、数据、过程等应用模块，提供了区块链与链外系统对接的通道，如链外的物联网设备、支付设备、分布式云存储系统、交易系统的对接和外部用户身份的绑定等。

8 开发及工具

一个区块链技术平台能否成功，能否吸引实力强劲的开发者入驻，很大程度上取决于是否可以充分满足开发人员的需求，即其支持的编程语言是否满足主流开发人员的偏好，其开发支持文档是否详尽、易懂，接口和智能合约的开发是否简便易操作。因此，本次研究在开发及工具维度，主要从支持的开发语言、配套的开发工具、接口的完备程度及智能合约可编辑性等方面进行分析。

（一）编程语言方面。Ethereum 的客户端主要通过 Go 语言、C++语言和 Python 语言编写，再通过编译器转成 EVM 语言。Java 和 Ruby 的客户端也在开发中。Ethereum 使用四种语言进行合约编程：Serpent、Solidity、Mutan 和 LLL。其中 Solidity 是 Ethereum 的首选语言，具有图灵完备的特性，可采用分层、分模块，

以实现帐号管理、资产管理、交易管理、安全控制等金融场景所需的功能。Fabric 项目核心代码主要由 Go 编写。Fabric 采用了容器技术，将智能合约代码(Chaincode)放在 Docker 中运行，可以用 Go、Java 等语言编写智能合约。Corda 主要由 Java 和 Kotlin 开发，并在其各项功能中主要依赖 Java，如智能合约、数据访问接口等，但也支持应用使用 SQL 对其数据库进行访问。Corda 中的合约(Contract)以及分布式应用(DApp)，原则上是可以基于 JVM 上的任何语言来开发的，在应用开发者层面，一定程度上减小了 Kotlin 小众化问题的影响。BCOS 业务层支持采用如 C++、Java、Python、Javascript、Go 等语言进行开发，可使用 Ethereum 的 Solidity 作为合约开发语言。

（二）配套开发工具。Ethereum 社区是仅次于比特币的社区，主要英文技术文档都在 Github 上公布，同时也有专门的技术问答网站，中文技术文档则主要发布在 ethfans.org。Ethereum 官方提供钱包客户端 Mist，支持进行交易，同时支持直接编写和部署智能合约。由社区贡献的有网络监控、分布式应用的开发框架、智能合约分析器、智能合约管理平台等工具。微软也在其提供的 Visual Studio 集成开发环境中集成了 Solidity 语言，方便编写智能合约。Fabric 在 Github 上公布了 Fabric 项目的源码，并提供了若干 SDK 工具包、技术文档和帮助 Fabric Chaincode 开发的各个阶段的工具，如编译、测试、打包和部署等。Corda 为应用开发提供了开发模板：CorDApp-template，其可以用来作为开发一个新 App 的样板。Corda 工程中的 Samples 中提供了很多案例供开发者学习和了解，尤其是用 IDEA 开发 Corda 时，各个案例可以直接在 IDE 中快速启动。Corda 于 2016 年 11 月 30 日在 Github 上正式开源。BCOS 在 Github 上公布了源码，并为用户提供了安装说明、技术白皮书、License 以及服务邮箱等。同时，BCOS 平台提供了 SDK 工具包，在 SDK 基础上开发者可开发面向最终用户的客户端程序，在客户端上可以保存链上部分或全部的数据，也可以作为轻客户端访问链上节点。BCOS 于 2017 年 7 月 31 日在 Github 上正式开源。

（三）接口的完备程度。RPC 接口是 Ethereum 与其他 IT 系统交互的接口，Ethereum 节点在 8545 端口提供了 JSON RPC API 接口，数据传输采用 JSON 格式，可以执行 Web3 库的各种命令，可以向前端如 Mist 等图形化客户端提供区块链的信

息。Fabric 提供了一套可灵活扩展的 API 接口，其每个模块都定义了相应的 API 接口，因此这些模块可以实现“即插即用”。例如共识算法的 API 支持用户无需修改算法代码就可以在各类用例中使用这一算法。Corda 在流式架构的设计中，给出了对流程的实时监控和展示相应的接口，同时预留了 SQL 接口。BCOS 支持通用 API 接口，满足跨技术与跨系统对接要求。BCOS 对业务层提供接口服务，并通过接口和区块链节点进行交互、发送交易、查询数据等。平台也提供 HTTPS 的服务端口，采用 JSON 编码格式定义功能接口，包括用户数据查询、区块数据查询、合约部署和管理、发送交易、交易数据查询、进行节点之间通信等。BCOS 接口 SDK 的设计分为两种，一种是面向区块链底层功能接口的调用，调用者需要知晓区块链节点的具体部署情况，进行异步通信和容错处理，在接口字段里填入经过特定编码的数据参数；另一种 SDK 直接面向业务，提供业务级别的接口，业务开发者只需要关注业务数据的字段以及调用返回结果，不需要了解区块链节点的具体部署情况，不需要处理异步通信的细节。

（四）智能合约的可编辑性。Ethereum 是首个以图灵完备智能合约为主要功能的区块链，用户可以在 Ethereum 的平台上创建自己的合约，而合约的内容可以包含货币转账在内的任意逻辑。Fabric 使用现有的容器技术来支持智能合约功能，Fabric 的智能合约理论上可以用任何语言来编写，开发者将无需学习新的语言，并且可以复用现有的业务代码和丰富的开发库，并使用自己熟悉的开发工具。相对地，采用 Docker 的智能合约架构也有大量的问题：首先，它很难对智能合约的执行流程进行控制，从而无法对其功能进行限制；其次，它无法对合约运行所消耗的计算资源进行精确的评估；此外，运行 Docker 相对而言是极其耗费资源的操作，这就使得难以在移动设备上运行合约；最后，不同节点的硬件配置、合约引用的开发库等，都有可能会使合约的行为具有很强的不确定性。Corda 的智能合约功能与其自身一样，都是基于 JVM(Java Virtual Machine)的，因此可以使用任何与 JVM 兼容的语言来进行开发，比如 Java、Kotlin 等。不过，它对 JVM 进行了一定的改造，使得在其上运行的合约脚本具备确定性。Corda 使用 JPA(Java Persistence Architecture)来提供持久化功能，支持 SQL 语句和常用的数据库，不过需要安装相应的插件，并且由于数据仅存放在合约执行者的节点，因此无法进行全局的持久

化存储。BCOS 合约开发支持 Solidity 语言，该语言作为 Ethereum 的主要合约开发语言，具有图灵完备的特性。BCOS 平台计划在下一版本支持 JVM 虚拟机和 Java 开发语言。

9 维护支持能力

区块链企业在选择区块链技术平台的过程中，平台背后运营主体的实力也是一个不可忽视的问题。一般来说，社区规模越大、开发者数量越多，则平台技术发展越快；运营主体自身技术研发实力越强，平台的安全保障体系相对越可靠，相应地平台维护能力也越强。在维护支持能力维度方面，本次研究主要从版本升级维护机制、开发者数量等方面进行分析。平台版本发布规则、平台应急制度、平台管理规范等方面也是考量平台维护支持能力的重要组成部分，但由于缺乏有效的公开资料及信息，本次研究仍以前两方面的分析为主。

（一）在版本升级维护机制和保障方面。目前 Ethereum 的维护及研究升级主要由 Ethereum 基金会来负责运行。Ethereum 在建立伊始便制定了明确的规划，其发布分成了四个阶段：Frontier（前沿）、Homestead（家园）、Metropolis（大都会）和 Serenity（宁静），在前三个阶段 Ethereum 共识算法采用工作量证明机制（POW），在第四阶段会切换到权益证明机制(POS）。据不完全统计，截至 2017 年 7 月，Ethereum 的 Go 语言核心代码库已发布 118 次。

HyperLedger Fabric 是由 Linux 基金会发起创建的开源区块链分布式账本，联盟主要成员来自大型金融机构、大型 IT 企业、大型咨询机构等不同的利益体，具备强大的资金和技术能力。Fabric 源于 IBM，初衷为了服务于工业生产，IBM 贡献了 44,000 行代码开源。Fabric 最新的 1.0 版本已于 2017 年 7 月正式发布，官网显示，27 个组织、159 位开发者参与并作出贡献。截至 2017 年 7 月，Fabric 在 Github 上源码发布 7 次。

Corda 由 R3 CEV 联盟组织开发，其成员主要来自于全球知名的金融机构。Corda 于 2016 年 11 月正式开源，2017 年 6 月开始第一个 Beta 公测阶段，提供新

的 API 文档和更大的数据库。在 2017 年共识大会(Consensus 2017)上，R3 宣布进行一亿美元以上的融资。截至 2017 年 7 月，Corda 在 Github 上源码发布 27 次。

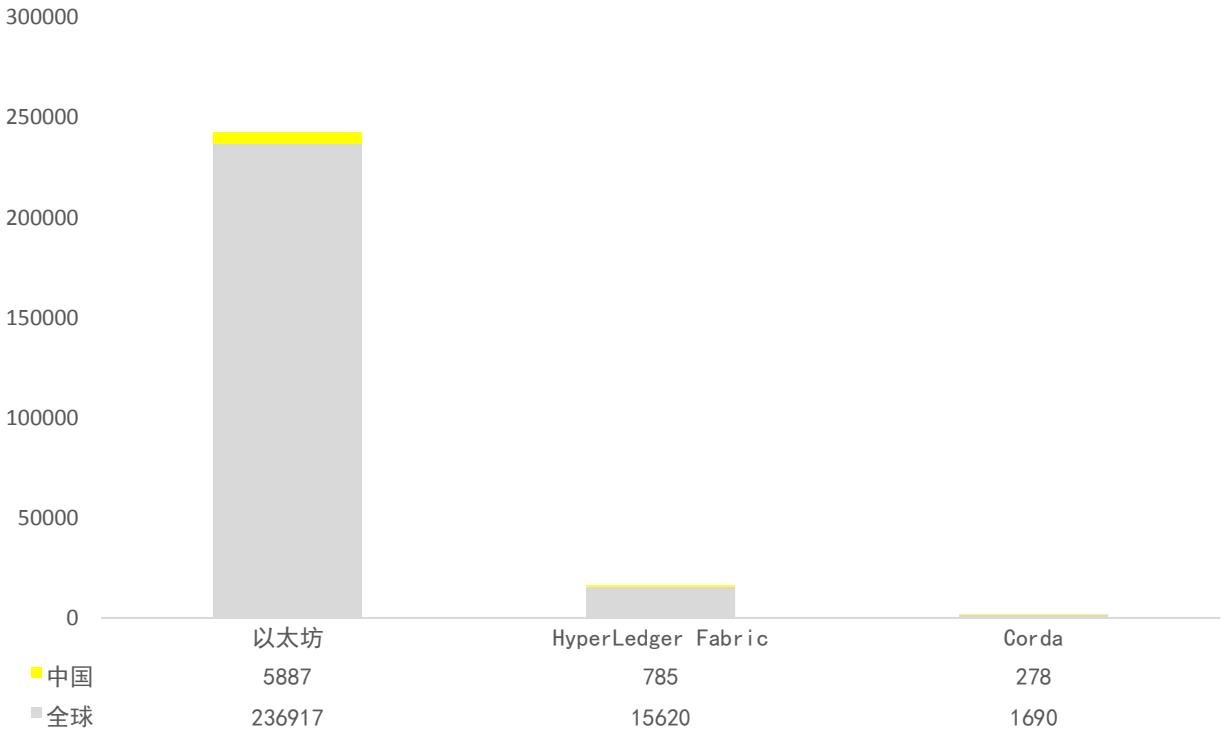
BCOS 由微众银行、万向区块链、矩阵元共同开发，有专业开发团队进行研发和维护，资金和技术实力在国内均处于领先地位。BCOS 升级原则上保证向下兼容，原链上的数据不会因升级而失效，且支持全网灰度升级，参与到联盟链的节点不要求同时升级或停机升级，可以按节点一一替换，运行新版本软件的节点和运行旧版本软件的节点可协同工作，直到旧版本被完全替换。值得注意的是，BCOS 平台借鉴 COBIT 模型，形成了一个三维治理体系结构，包括治理准则（Business Requirements）、治理对象（Resources）及治理过程（Processes）。其旨在有效利用资源，管理与区块链系统相关的风险，平衡商业风险、控制需求和技术问题之间的关系。治理模型从一定程度上降低了产品需求演变及版本升级给平台本身的技术路线、架构灵活性等方面造成的风险。

从总体上看，虽然各系统平台绝大多数升级比较平稳，但公有链的分叉也有导致社区决策艰难的场景，比如 TheDAO 被攻击后的善后处置和平台升级。

另外，值得注意的是，研究范围内的平台均支持智能合约，其不仅是契约更是程序，因此不可避免地遇到升级问题。平台处理智能合约的方式，升级前后智能合约的状态和逻辑能否有效衔接，以及智能合约升级和平台升级的相互促进，应是未来企业选择区块链平台的重要考量之一。

（二）开发者数量。目前暂时没有研究范围内的平台开发者数量的具体数据，但我们统计了各个平台官网上“Meetup Groups”在全球各地的分布人数，这在一定程度上与各平台开发者数量呈正相关。截至 2017 年 7 月 15 日，Ethereum 在全球拥有 1016 个“Meetup”，成员 236917 人，遍布全球 77 个国家和地区、405 个城市。中国 5887 人（大陆 1471 人，香港 2735 人，台北 1681 人）。Hyperledger 在全球拥有 62 个“Meetup”，成员数为 15620 人，中国 785 人（北京+上海+深圳+香港+台北）。Corda 在全球拥有 10 个“Meetup”，成员数为 1690 人，中国 278 人（北京+上海+深圳+香港+台北）。另外，由于 BCOS 平台于 2017 年 7 月 31 日刚刚开源，因此我们选择 Github 上该项目的“Star”(关注项目更新用户数)和“Fork”(拷贝项目到自己帐号用户数)数量做为替代。截至 2017 年 8 月 15 日，BCOS 平台

的“Star”数量为 245，“Fork”数量为 100。



资料来源：https://www.meetup.com/

图 4 各平台“Meetup Groups”成员

10 总结与展望

根据以上各维度分析，我们针对研究范围内的平台得到如下观点：

- 在区块链平台成熟度及设计思路表现方面。Ethereum 经过较长时间的公链运行，一定程度上经历了外部攻击和实战检验，代码和测试的成熟程度较高，其平台在软件质量和安全性方面有较好的保证；Fabric、Corda 和 BCOS 则在设计伊始便更加贴近商业需求，在满足合规和隐私方面，以及监管接入和架构设计方面有很多巧妙的设计之处，同时各平台也在不断更新换代以求更好地满足实际商业需求。
- 在区块链平台架构及应用设计方面。架构的发展还未进入成熟期，各个平台依然在实践过程中不断调整优化自身架构，以满足不同应用场景的需求。从应用场景来看，Ethereum 更适用于并发性不高、以公有链为主的应用场景。Fabric 和 BCOS 适合以联盟链形式开展的金融服务、供应链管理、文化娱乐等多行业应用场景。Corda 定位相对明确，更适合面向非公链、受监管的金融机构。
- 在信息共享和隐私保护方面，各平台在如何保证二者相互平衡的表现上，仍有待进一步完善。Ethereum 采用的状态旁路只从一定程度上保护了隐私性。以联盟链为设计初衷的 Fabric 和 Corda 将不同主体之间的交易进行隔离，形成多链的数据状态，然而，当数据需要在跨链共享时，需将冗余数据写入不同的链中或将系统设计成颗粒度很细，让冗余的节点加入到多个链中，无论使用何种方法都将使系统变得异常复杂。BCOS 则通过物理隔离、逻辑通道设计等方式防止隐私数据扩散。业内普遍认可的隐私解决方向，诸如零知识证明、同态加密等，大都基于较为复杂的密码学技术，目前还没有达到实际应用水平。因此各平台在隐私保护和信息共享方面仍有较大提升空间。

以下是研究范围内各平台各维度的对比分析结论：

分析维度	结论
架构能力	1、在架构灵活性方面，Fabric 采用松耦合设计，支持多通道结构；Corda 共识机制模块可插拔；BCOS 共识算法模块采用插件化设计实现。 2、在节点分类上， Fabric 节点分为验证节点和非验证节点，并通过授权和证书管理节点；Corda 节点分为普通节点、公证节点和管理节点，交易共识在公证节点达成；BCOS 节点分为共识节点和观察节点，共识节点参与共识算法，观察节点则只同步数据；Ethereum 正从 PoW 共识机制走向 PoS 共识机制，节点间将依据资产的多寡分配相应的记账权重，让处于核心地位的记账节点得到更好的资源倾斜，以更好地利用计算资源。
核心技术组件	1、在共识机制方面，Ethereum 目前采用 PoW 共识机制，算力成本高，正在向 PoS 过渡，可解决交易确定性问题、降低成本；Fabric 共识运用可插入式算法，用户可自行选择，一般用 PBFT；Corda 一般用 BFT 算法为公证服务；BCOS 采用 PBFT、Raft 作为联盟链的共识算法，系统的共识机制采用插件化实现。 2、在 P2P/通信技术方面，Ethereum 客户端 P2P 协议是一个标准的加密货币协议，能够容易地为其它加密货币使用；Fabric 运用 Google RPC 协议，能与现有的网络基础设施结合；Corda 的通讯协议基于 AMQP/1.0，采用 TLS 作为加密协议，并内嵌了一个支持 AMQP/1.0 的全功能的消息中间件，适合于嵌入式应用。 3、在存储方面，Ethereum 和 Fabric 采用状态快照节约硬盘空间；BCOS 支持分组多副本方式存储文件，还支持分布式数据存储的方案。

分析维度	结论
	4、在计算效率方面，Ethereum、Corda、BCOS 的交易可被并行验证以提高计算效率。 5、在数据结构方面，Ethereum、Corda、BCOS 均由区块头和区块体组成，Corda 中没有“区块”的概念。
应用功能	1、四个平台均支持智能合约。 2、在身份认证方面，Ethereum 采取匿名身份认证体系，对线上线下的身份匹配无强制要求；Fabric、Corda 和 BCOS 均支持数字证书的身份认证形式。 3、在账户设计方面，Ethereum 采用余额账户机制；Fabric 中没有代币概念，但可以通过 Chaincode 实现本币发行和账户功能；Corda 没有余额概念，所有余额均通过 UTXO 计算得出。 4、监管方面，四个平台均支持监管接入。但在 Ethereum 中，由于身份匿名性，监管接入的意义不大。 5、在特权机制的实现方面，Ethereum、Fabric 和 Corda 理论上可“隐性地”实现暂停、回滚或取消交易以及改正数据的特权；BCOS 可以针对特定的业务场景，制定特定的权限集合，其底层平台预置了控制交易和部署合约的权限和接口，通过监管工具、角色赋权等方案，让监管方可以直接实施联盟链的控制。
技术能力	1、在交易吞吐量方面， Ethereum 在真实应用程序负载下的交易可能会被限制到 10TPS 或者更低；Fabric 在 PBFT 共识机制下，吞吐量可达到 1000TPS 或更高；Corda 延迟程度跟交易复杂程度正相关；BCOS 利用 PBFT 共识机制，在 4 节点环境下，转账交易的合约调用，性能可达到数千 TPS。 2、在确认时间方面，Ethereum 每 12 秒左右才能够提交一个新

分析维度	结论
	的区块，确认时间也是在 12 秒左右；Fabric 默认一个交易出一个块，也支持多个交易一个块；Corda 可以对每一笔交易实时达成共识；BCOS 可支持 1 秒出块，出块即达成共识。 3、在可用性方面，Ethereum 采用的工作量证明机制(PoW)提供了较高的灵活性和可用性；Fabric 采用的拜占庭容错机制牺牲了一定的灵活性和可用性；Corda 由于没有统一总账，每个“节点”必须自行存储自己的交易数据，自行解决自身的网络级、系统级、应用级、数据级的容灾备份问题；BCOS 使用 PBFT 时系统可用性同 Fabric 一致，使用 Raft 算法时网络容错上限为 50%。
安全机制	1、四个平台均利用非对称加密算法生成公私钥。 2、在“防双花”方面，Ethereum 采用了余额机制；Fabric 运用了状态版本的概念；Corda 基于公证人进行交易确认；BCOS 基于账户模型和区块高度，对交易生命周期进行检验和控制。 3、在隐私保护方面，Ethereum 使用“状态旁路”方案，但只能达到部分保护效果；Fabric 利用多通道的机制保护隐私性；Corda 主要采用了 Tear-off 技术和复合签名技术两项隐私保护技术；BCOS 通过物理隔离、逻辑通道设计，交易明细仅发送给交易牵涉的节点以及可能存在的监管节点，从基础层面防止了隐私数据的扩散。还可使用数据脱敏、机构间点对点通信、数据明细链下保存、高强度加密数据信封方式等方式实现隐私控制，并且支持加法同态加密算法。

分析维度	结论
平台适用性	1、Ethereum 平台不仅适用于公链场景，也可以部署联盟链或私有链。Ethereum 可利用图灵完备的智能合约，适应金融应用、物联网、供应链管理、社交网络、去中心化自治组织（DAO）、预测市场等场景。 2、Fabric 可广泛应用于跨行业应用场景中，可满足金融服务、供应链管理、智能制造、文化娱乐、医疗健康、社会公益、教育就业等领域的应用。 3、Corda 聚焦于分布式账本技术在金融领域的应用，定位为面向非公有链的场景。 4、BCOS 定位为企业级应用服务的区块链技术平台，其在多链、跨链、分布式存储及隐私保护等方面上的设计，满足其在金融、健康医疗、供应链、工业、物联网、能源服务等多个领域上的适用性。另外 BCOS 可支持账号管理、资产管理、交易管理、安全控制等模块功能的配置，因此对于各多种场景下所需的功能其均能很好地实现。
开发及工具	1、在编程语言方面，Ethereum 的客户端主要通过 Go、C++和 Python 语言编写，再通过编译器转成 EVM 语言。合约编程支持四种语言，其中首选语言 Solidity 具有图灵完备的特性；Fabric 项目核心代码主要由 Go 编写，智能合约可以用 Go、Java 语言编写；Corda 主要由 Java 和 Kotlin 开发，合约以及分布式应用原则上可以基于 JVM 上的任何语言来开发；BCOS 业务层支持采用如 C++、Java、Python、Javascript、Go 等语言进行开发，可使用 Ethereum 的 Solidity 作为合约开发语言。 2、在配套开发工具方面，Ethereum 拥有仅次于比特币的社区，配套中英文技术文档及专门的技术问答网站，微软的

分析维度	结论
	Visual Studio 集成开发环境中也集成了编写 Ethereum 智能合约的 Solidity 语言；Fabric 在 Github 上公布了 Fabric 项目的源码，并提供了若干 SDK 工具包、技术文档和开发工具；Corda 在 Github 上开源，并为应用开发提供了开发模板；BCOS 在 Github 上公布了源码，并提供了安装说明、技术白皮书、License 以及服务邮箱等，同时提供了 SDK 工具包。 3、接口的完备程度方面，RPC 接口是 Ethereum 与其他 IT 系统交互的接口，JSON RPC API 接口可以执行 Web3 库的各种命令，向前端提供区块链信息；Fabric 提供了一套可灵活扩展的 API 接口，其每个模块都定义了相应的 API 接口，因此这些模块可以实现“即插即用”；Corda 在流式架构的设计中，给出了对流程的实时监控和展示相应的接口，同时预留了 SQL 接口；BCOS 对业务层提供接口服务，并通过接口和区块链节点进行交互、发送交易、查询数据等，BCOS 也提供 HTTPS 的服务端口。 4、智能合约的可编辑性方面，用户可以在 Ethereum 的平台上创建可以包含任意逻辑的合约；Fabric 的智能合约理论上可以用任何语言来编写，但采用 Docker 的智能合约架构也存在问题；Corda 的智能合约可以使用任何与 JVM 兼容的语言来进行开发；BCOS 合约开发支持图灵完备的 Solidity 语言，BCOS 平台计划在下一版本支持 JVM 虚拟机和 Java 开发语言。

分析维度	结论
维护支持能力	1、在版本升级维护机制和保障方面，各系统平台绝大多数升级比较平稳。Ethereum 的维护及研究升级主要由 Ethereum 基金会来负责运行，且有明确规划；Fabric 是由 Linux 基金会发起创建的开源区块链分布式账本，联盟主要成员来自大型金融机构、大型 IT 企业、大型咨询机构等不同的利益体，具备强大的资金和技术能力；Corda 由 R3 CEV 联盟组织开发，其成员主要来自于全球知名的金融机构，并于 2017 年 7 月宣布进行一亿美元以上的融资；BCOS 由微众银行、万向区块链、矩阵元共同开发，有专业开发团队进行研发和维护，资金和技术实力在国内均处于领先地位。 2、开发者数量方面，目前 Ethereum 拥有绝对领先地位，“Meetup”成员数为 236917 人；Hyperledger“Meetup”成员数为 15620 人；Corda 和 BCOS 由于开源时间较晚，开发者数量相对 Ethereum 和 Hyperledger 较少。

表5 各平台重点分析维度总结

随着企业对于区块链技术的认知不断深入，在应用场景落地的过程中，企业对于区块链平台的技术能力要求必然日益提高，因此专业的区块链服务平台显得尤其重要。但市场上区块链技术平台品类繁多，各有千秋，企业究竟该如何选择区块链技术平台？我们认为企业首先应在确定自身区块链战略发展规划路线的基础上，结合自身所处阶段制定不同的选型策略，比如在前期研究阶段不妨大胆尝试，在实践中检验区块链平台，在 PoC（Proof of Concept，概念验证）阶段，结合应用场景及未来发展规划谨慎选型，以检验平台的真实效果；其次，在应用阶段，企业应结合自身业务发展情况选择区块链平台，对于快速发展的高并发业务，尽量选择架构较灵活、可支持多种高性能共识算法的区块链平台，对于客户信息或交易数据较敏感的业务，应尽量选择在安全和隐私性等方面精心设计的区块链平台，如在多通

道、节点权限灵活可配等方面的设计；最后，企业还应将区块链平台的选择与企业自身情况进行统筹考量，如企业 IT 能力有限，应尽量选择平台较成熟、维护能力较强的区块链平台，以减少后期维护成本，如果企业自身已有较成熟的 IT 系统，则应在区块链平台的链上链下信息交互能力上着重考虑。

另一方面，在长期聚焦区块链应用和技术的研究过程中，我们始终认为，区块链技术平台的发展将很大程度上取决于区块链商业生态的构建和治理网络的形成，而技术平台也会反过来促进和引领区块链生态和治理的逐步完善。区块链商业生态和治理网络形成的过程，同样也是在回答以下问题的过程：我们希望利用区块链解决的问题是什么？是否需要我们改变原有的商业模式和参与者？新的商业生态由谁支配和管理？与现有政府管理体系的关系是怎样的？我们该如何设计新的商业生态和治理模式？也许，随着这些问题的解决，更加完善的区块链平台将会离我们越来越近。

11 参考信息

1. 《区块链将如何重新定义世界》，机械工业出版社，2016 年 6 月
2. 《中国区块链技术和应用发展白皮书》，2016 年 10 月
3. https://github.com/ethereum/wiki/wiki/Design-Rationale
4. 以太坊白皮书 https://github.com/ethereum/wiki/wiki/White-Paper
5. 以太坊黄皮书 https://ethereum.github.io/yellowpaper/paper.pdf
6. Corda 非技术白皮书 https://docs.corda.net/_static/corda-introductory-whitepaper.pdf
7. Corda 技术白皮书 https://docs.Corda.net/_static/Corda-technical-whitepaper.pdf
8. Hyperledger 白皮书 https://docs.google.com/document/d/1Z4M_qwILLRehPbVRUsJ3OF8Iir-gqS-ZYe7W-LE9gnE/pub
9. Welcome to Hyperledger Fabric：https://hyperledger-fabric.readthedocs.io/en/latest/
10. Welcome to Corda https://docs.Corda.net/
11. https://discourse.Corda.net/t/how-does-Corda-address-privacy-issues/1152
12. https://discourse.Corda.net/t/how-is-r3-engaging-regulators-on-the-legal-privacy-impact-of-data-processing-via-distributed-ledger-technology/1156
13. https://discourse.Corda.net/t/contract-state-plus-flows-smart-contract/498
14. https://discourse.Corda.net/t/Corda-network-deployment-pattern/965/2
15. https://github.com/ethereum/go-ethereum
16. https://github.com/ethereum/mist/releases
17. https://github.com/hyperledger/fabric
18. https://github.com/Corda/Corda
19. https://github.com/ethereum/wiki/wiki/Sharding-FAQ
20. https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ
21. https://github.com/ethereum/wiki/wiki/Patricia-Tree
22. http://ethfans.org/topics/800
23. https://www.altoros.com/blog/hyperledger-approaches-version-1-0-with-better-scalability-and-security/
24. https://www.leiphone.com/news/201705/yPLlmqU2btwE4L8r.html?uniqueCode=ZIk4e4ylUf2xCMWb
25. http://www.coindesk.com/inside-truebit-ethereum-scalability-effort/[DG1
26. https://www.ibm.com/developerworks/cn/cloud/library/cl-top-features-of-hsbn-blockchain/index.html
27. https://www.ibm.com/developerworks/cn/cloud/library/cl-top-technical-advantages-of-hyperledger-fabric-for-blockchain-networks/index.html
28. https://github.com/yeasy/hyperledger_code_fabric/blob/master/SUMMARY.md
29. http://mp.weixin.qq.com/s/_x6A0SEMVu6iBdvIPA6W1w
30. http://8btc.com/article-4514-1.html
31. https://steemit.com/eos/@trogdor/eos-vs-ethereum-for-dummies
32. http://ethfans.org/wikis/%E4%BB%A5%E5%A4%AA%E5%9D%8A%E5%8E%86%E5%8F%B2
33. http://ethfans.org/wikis/%E6%99%BA%E8%83%BD%E5%90%88%E7%BA%A6

34. http://ethfans.org/wikis/%E4%BB%A5%E5%A4%AA%E5%9D%8A%E5%BC%80%E5%8F%91%E8%AE%A1%E5%88%92
35. http://pool.ethfans.org/
36. http://ethfans.org/wikis/Serpent-%E6%8C%87%E5%8D%97
37. https://www.meetup.com/topics/ethereum/all/
38. https://www.meetup.com/pro/Corda/
39. https://www.meetup.com/pro/hyperledger/
40. https://www.ibm.com/blockchain/hyperledger.html
41. http://ethfans.org/posts/weekly-10
42. https://www.reddit.com/r/ethereum/comments/5y9bqb/video_excerpt_of_dev_discussion_on_metropolis/deo8p0f/
43. http://ethfans.org/topics/66
44. http://ethfans.org/topics/55
45. http://ethfans.org/topics/28
46. https://blog.p2pfoundation.net/ethereum-freenet-or-skynet/2014/11/19
47. https://blog.ethereum.org/2015/03/03/ethereum-launch-process/
48. http://ethfans.org/topics/74
49. http://ethfans.org/topics/697
50. http://ethfans.org/topics/331
51. http://www.8btc.com/r3-Corda-10-questions
52. http://lightning.network/
53. https://github.com/bcosorg/bcos
54. https://github.com/bcosorg/whitepaper/blob/master/BCOS_Whitepaper.md

EY 安永 | Assurance 审计 | Tax 税务 | Transactions 财务交易 | Advisory 咨询

关于安永

安永是全球领先的审计、税务、财务交易和咨询服务机构之一。我们的深刻洞察和优质服务有助全球各地资本市场和经济体建立信任和信心。我们致力培养杰出领导人才，通过团队协作落实我们对所有利益关联方的坚定承诺。因此，我们在为员工、客户及社会各界建设更美好的商业世界的过程中担当重要角色。

安永是指 Ernst & Young Global Limited 的全球组织，也可指其一家或以上的成员机构，各成员机构都是独立的法人实体。Ernst & Young Global Limited 是英国一家担保有限公司，并不向客户提供服务。如欲进一步了解安永，请浏览 www.ey.com。

关于金链盟

金融区块链合作联盟（深圳）（简称“金链盟”）是由深圳市金融科技协会、深圳前海微众银行、深证通等二十余家金融机构和科技企业于 2016 年 5 月 31 日共同发起成立的非营利性组织。金链盟作为一个开放式组织，自愿遵守章程的金融机构及向金融机构提供科技服务的企业等均可申请加入。至今，金链盟成员已涵括银行、基金、证券、保险、地方股权交易所、科技公司等六大类行业的七十余家机构。

金链盟旨在整合及协调金融区块链技术研究资源，形成金融区块链技术研究和应用研究的合力与协调机制，提高成员单位在区块链技术领域的研发能力，探索、研发、实现适用于金融机构的金融联盟区块链，以及在此基础之上的应用场景。

ey.com/china