

第25课：联盟链...

大家好，我是丹华。上节介绍了公有链的明星项目，本节我们介绍联盟链的明星项目。主要包括三个：

- 超级账本 Hyperledger
- R3
- Chinaledger 联盟

由于 Hyperledger 发展最成熟，阵营也最强大，目前看接受度最高，我们将重点介绍 Hyperledger。



超级账本 Hyperledger

<https://www.hyperledger.org/>

超级账本（Hyperledger）项目是 Linux 基金会于2015年发起的首个面向企业应用场景的开源分布式账本平台，旨在完善跨行业的区块链技术。超级账本致力于孵化和推广企业级开源的商业区块链技术，包括分布式账本，智能合约引擎，客户端库，图形界面，utility 库和示例应用。

在技术治理和开放合作的环境下，超级账本将努力吸引和邀请个人开发者，服务和解决方案提供者，政府部门，公司会员和终端用户等加入到这个技术社区中来。

超级账本的参与者包括200多家区块链、金融、银行、科技、互联网、物联网、供应链、制造和技术等领域的领导者。会员包括：瑞波、R3、埃森哲，普华永道，空中客车，美国运通、百度、思科、甲骨文、Vmware、德意志银行、荷兰银行（ABN AMRO）、DTCC、小米集团、招商银行、京东、联想、腾讯、中钞区块链等。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。

目前，超级账本已经或正在开发包括 Fabric、Burrow 等在内的数十个项目，旨在创建一个开放、标准化、企业级的分布式账本架构和代码库，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。

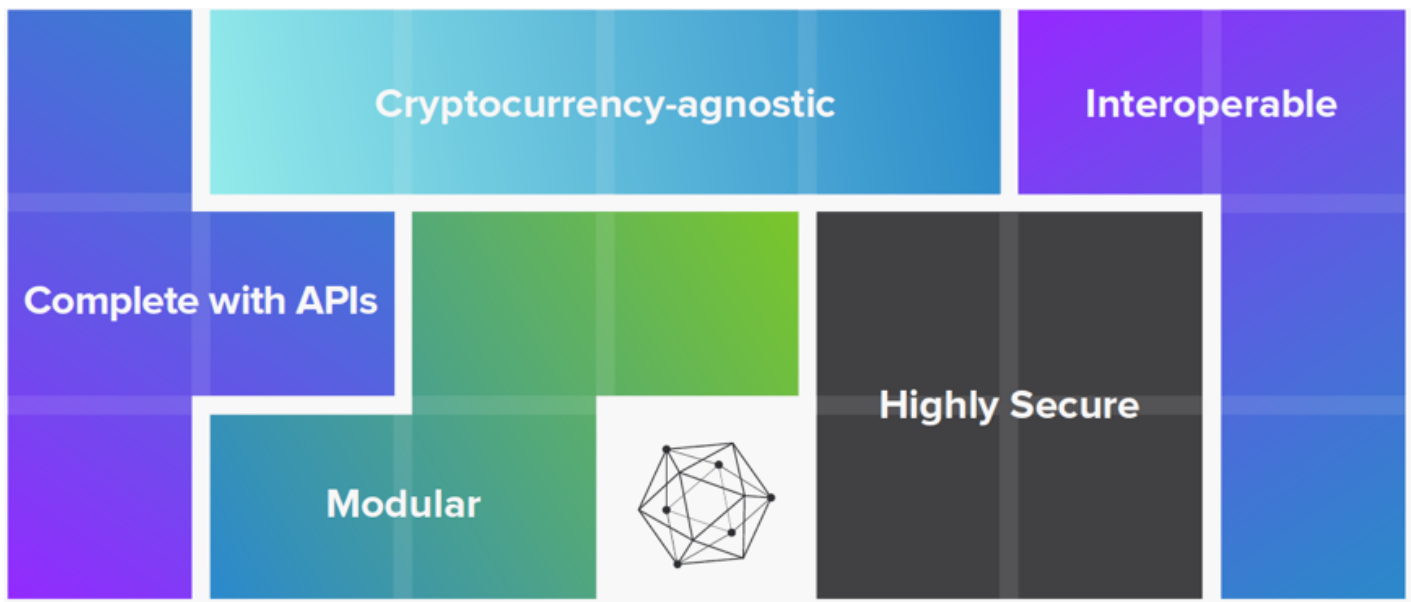
HyperLedger 使命

- 创建一个企业级、开源的分布式账本框架和代码库，用户可以在此基础上创建和运行强壮的、特定行业的应用、平台和硬件系统，以支持商业上的交易。
- 创建一个开源技术社区，来帮助由解决方案提供者和用户构成的生态系统，聚焦于区块链和共享账本的多行业用例。
- 鼓励生态系统中成员的参与，包括开发者、服务商和解决方案提供者、终端用户；
- 主导并维护超级账本的基础设施，建立一个中立的社区基础设施、会议、事件、合作讨论，并负责超级账本项目的商业和技术治理结构。

设计理念与哲学

Hyperledger 的所有项目都必须：

- 模块化
- 高度安全
- 互操作
- 无加密货币（但允许应用发行Token）
- 丰富易用的 APIs



Hyperledger 的技术架构










Hyperledger 作为一个通用的商业区块链，其技术架构包括以下几个部分：

共识层 Consensus Layer

共识层负责生成交易的序列并验证其正确性的机制，多个交易构成一个区块。

与公有链采用一个共识机制不同的是，Hyperledger 需要支持多个不同的共识机制。下图给出了可信区块链（联盟链）采用的两种共识机制与比特币 POW 共识机制之间的比较。

TABLE 1. COMPARISON OF PERMISSIONED CONSENSUS APPROACHES AND STANDARD PoW

	Permissioned Lottery-based	Permissioned Voting-based	Standard Proof of Work (Bitcoin)
Speed	 GOOD	 GOOD	 POOR
Scalability	 GOOD	 MODERATE	 GOOD
Finality	 MODERATE	 GOOD	 POOR

彩票机制的共识，包括 Proof of Elapsed Time (PoET) 以及 Proof of Work (PoW)，优点是支持大量的节点，但风险是可能会带来网络分叉。基于投票的共识机制，包括冗余拜占庭容错算法 (RBFT) 和 Paxos，优点是低延时，只要大多数节点认可交易或区块，则共识形成，单缺点是不支持大规模的节点部署，因为节点间的通信消耗太大。不同的算法对网络的要求也不同。

有鉴于此，Hyperledger 的开发者们假设，商业区块链的节点之间存在一定的信任度。这使得可信区块链可以采用更高性能的共识机制。具体地，超级账本各模块使用的共识机制有，Fabric 中使用的是 Apache Kafka，Indy 中的 RBFT，Iroha 中的 Sumeragi，这些是基于投票的共识机制，能够提供一定的容错空间。Sawtooth 中使用 PoET，是一种基于彩票的机制。

TABLE 2. COMPARISON OF CONSENSUS ALGORITHMS USED IN HYPERLEDGER FRAMEWORKS

Consensus Algorithm	Consensus Approach	Pros	Cons
Kafka in Hyperledger Fabric Ordering Service	Permissioned voting-based. Leader does ordering. Only in-sync replicas can be voted as leader. ("Kafka," 2017).	Provides crash fault tolerance. Finality happens in a matter of seconds.	While Kafka is crash fault tolerant, it is not Byzantine fault tolerant, which prevents the system from reaching agreement in the case of malicious or faulty nodes.
RBFT in Hyperledger Indy	Pluggable election strategy set to a permissioned, voting-based strategy by default ("Plenum," 2016). All instances do ordering, but only the requests ordered by the master instance are actually executed. (Aublin, Mokhtar & Quéma, 2013)	Provides Byzantine fault tolerance. Finality happens in a matter of seconds.	The more nodes that exist on the network, the more time it takes to reach consensus. The nodes in the network are known and must be totally connected.
Sumeragi in Hyperledger Iroha	Permissioned server reputation system.	Provides Byzantine fault tolerance. Finality happens in a matter of seconds. Scale to petabytes of data, distributed across many clusters (Struckhoff, 2016).	The more nodes that exist on the network, the more time it takes to reach consensus. The nodes in the network are known and must be totally connected.
PoET in Hyperledger Sawtooth	Pluggable election strategy set to a permissioned, lottery-based strategy by default.	Provides scalability and Byzantine fault tolerance.	Finality can be delayed due to forks that must be resolved.

智能合约层 Smart Contract Layer

智能合约负责处理交易请求，并通过执行商业逻辑来确定交易是否合法。

下图展示了超级账本中智能合约处理请求的逻辑。合约的输入包括合约标识符，交易请求，可选的交易参数和当前状态等。处于图中部的合约解释器，能够加载账本的当前状态和智能合约代码。当合约解释器收到一个请求时，会立即喝茶斌拒绝非法的请求。如果请求合法且被接受，就会执行，而产生一个输出，输出会包括新的状态等。当这些处理完成，解释器会将新的状态和正确性验证信息（attestation of correctness）及其他必要信息打包起来，发送给共识服务机制以登记在区块链上，最终完成合约交易。解释器对请求的验证包括两部分，语法验证和逻辑验证。

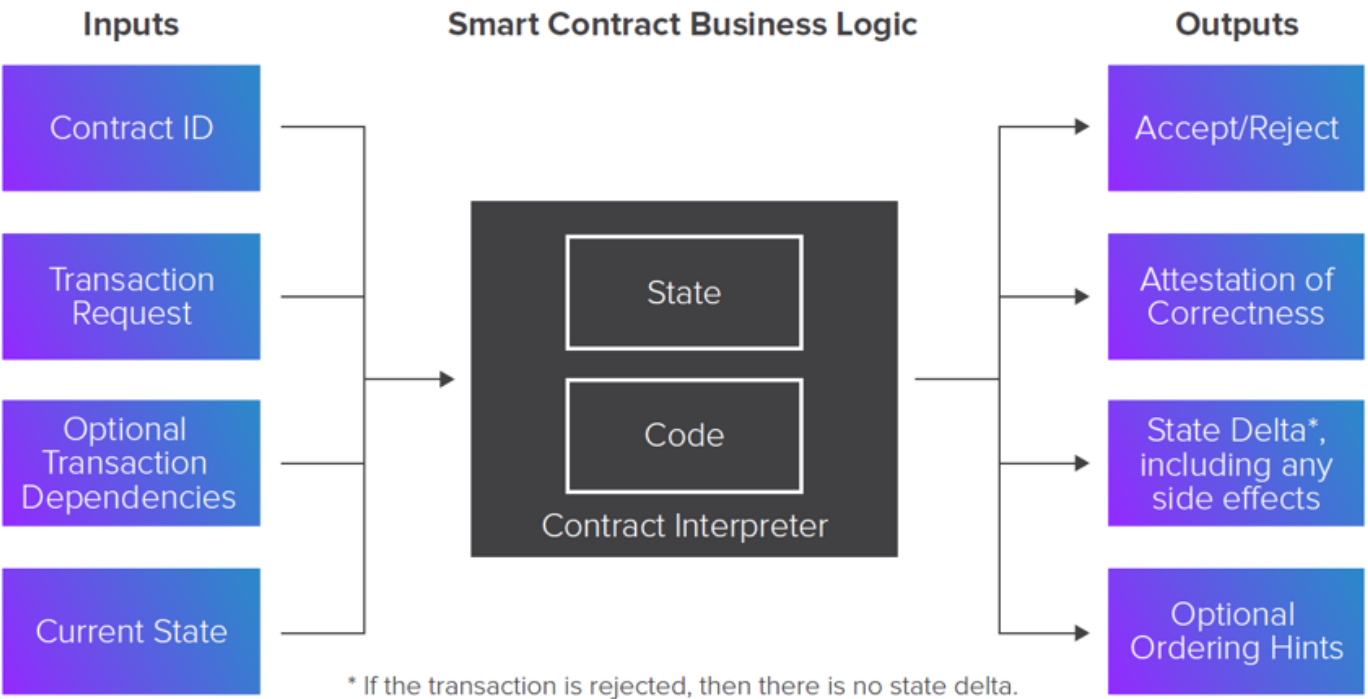


Figure 1: How Smart Contracts Process Requests

超级账本中的智能合约还支持依赖性，即多个智能合约间的多个交易。下图展示了智能合约层如何与其他层级适配的逻辑过程。基本上，你会发现，智能合约层将与共识层密切合作。

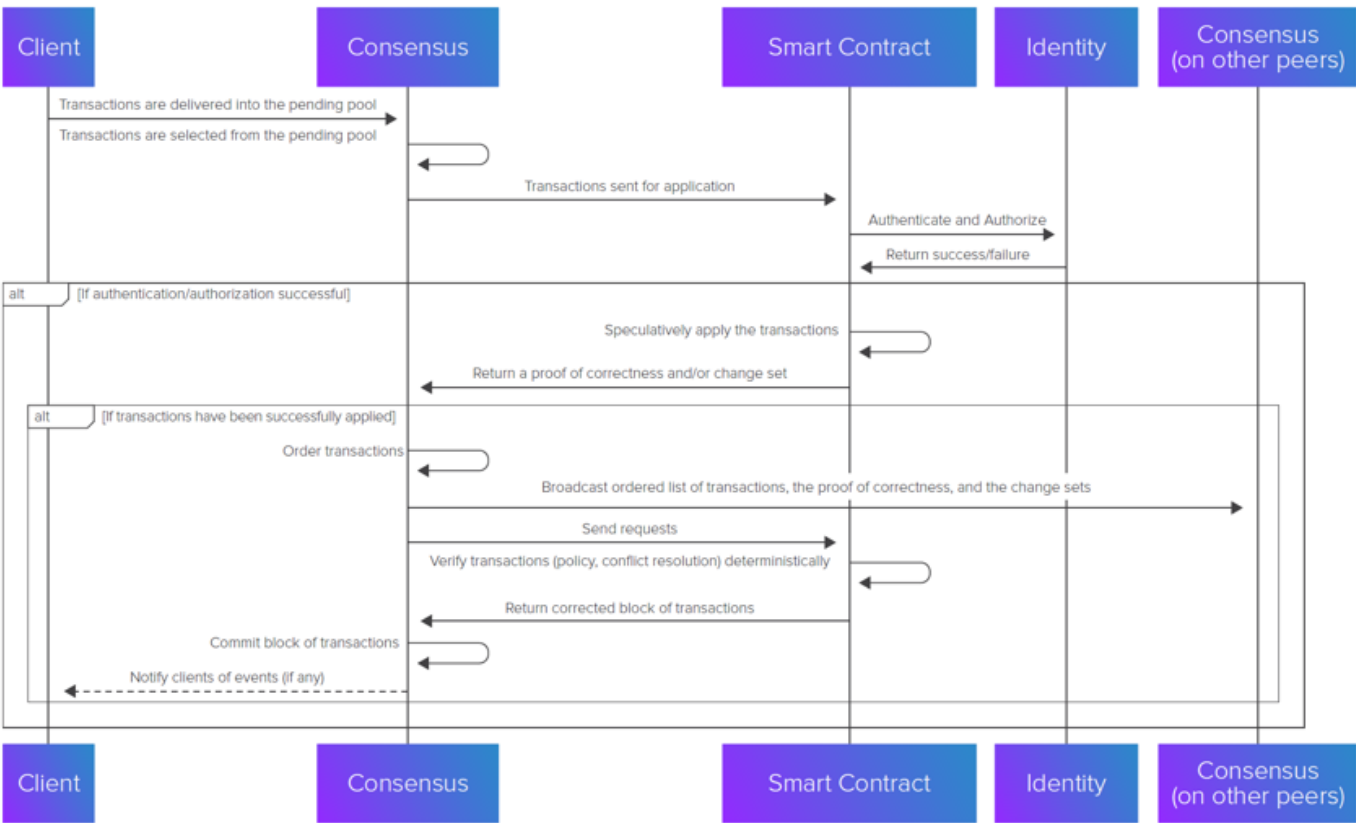


Figure 2: Hyperledger Smart Contracts and Other Layers

具体地，各个模块如何实施智能合约的参数可以参考下表：

Table 1. Smart Contract Implementations in Hyperledger Frameworks

Framework	Smart Contract Technology	Smart Contract Type	Language(s) for Writing Smart Contracts
Hyperledger Burrow	Smart contract application engine	On-Chain	Native language code
Hyperledger Fabric	Chaincode	Installed	Golang (> v1.0) or Javascript (> v1.1)
Hyperledger Indy	None	None	None
Hyperledger Iroha ²	Chaincode	On-chain	Native language code
Hyperledger Sawtooth	Transaction families	On-Chain and Installed	C++, Go, Java, JavaScript, Python, Rust, or Solidity (through Seth)

通信层 Communication Layer

负责在参与共享账本的节点之间实现一个点对点的消息传递；

数据存储抽象 Data Store Abstraction

允许各模块使用不同的数据存储

加密抽象层 Crypto Abstraction

允许自由替换多种密码学算法或模块，而不影响其他模块

身份服务 Identity Services

在建立区块链实例时，允许建立信任根 root of trust，网络操作中身份及系统实体的注册和登录，支持身份的授权、验证、添加、停止和撤销。

政策服务 Policy Services

负责管理系统中指定的各种政策，比如担保政策，共识政策，或组群管理政策。它通过互动并依赖其他模块来执行这些政策。

应用程序接口 APIs

允许客户端和应用能够与区块链互动。

互操作 Interoperation

支持不同区块链实例之间的互操作。

HyperLedger 的模块化分层架构

Hyperledger Modular Umbrella Approach

Infrastructure
Technical, Legal,
Marketing, Organizational

Ecosystems that accelerate
open development and
commercial adoption



Cloud Foundry

Node.js

Hyperledger

Open Container
Initiative

Frameworks

Meaningfully differentiated approaches
to business blockchain frameworks
developed by a growing community of
communities

Hyperledger
Indy

Hyperledger
Fabric

Hyperledger
Iroha

Hyperledger
Sawtooth

Hyperledger
Burrow

Tools

Typically built for one framework and
ported to other frameworks through
common license and community approach

Hyperledger
Quilt

Hyperledger
Composer

Hyperledger
Explorer

Hyperledger
Cello

Hyperledger
Caliper

Hyperledger 旗下的商业区块链框架包括：

Burrow

提供一个模块化的区块链客户端，具备可信的智能合约解释器和执行引擎，与以太坊的 EVM 相似。Burrow 是最早 Monax 开发的项目，后来进入 Hyperledger 孵化。

Fabric

区块链技术的一个实现，可作为开发区块链应用和解决方案的基础；允许诸如共识和会员服务等的组件实现即插即用，支持智能合约。

Iroha

一个可信的区块链平台，支持智能合约，旨在帮助商业和金融机构管理数字资产。

Sawtooth

一个模块化的平台，可以支持建立、部署和运行多样化的、可伸缩的分布式账本，支持智能合约。

Indy

一个支持独立的去中心化的数字身份分布式账本，提供工具、库、可复用组件。

Hyperledger 应用

根据网站信息来看，超级账本的落地应用案例包括跨境支付、健康记录、（州内）医疗资质许可证、海产品供应链追踪、钻石供应链、数字身份、面向难民的可验证身份、不动产交易、音乐和媒体的数字权利、信用证、碳资产交易等。

相关项目白皮书参见

<https://www.hyperledger.org/resources/publications#white-papers>

R3 区块链联盟（偏金融）



2015年9月，R3 区块链联盟由 R3CEV（R3 Crypto Exchange Venture）公司发起，吸引了众多金融机构的参与，包括富国银行、美国银行、德意志银行、汇丰银行、摩根史丹利、花旗银行等。目前 R3 联盟已经吸引了超过200家会员，技术专家180多人。R3 致力于为银行提供区块链技术以及建立区块链概念性产品。R3 使用以太坊和微软 Azure 技术。2016年，R3 宣布了其为金融机构量身定做的区块链技术平台项目 Corda，并于2017年将 Corda 项目代码开源。Corda 是一个开源的区块链平台，而 Corda Enterprise是一个针对企业用途的商业化版本。目前主要应用行业包括金融服务、船运、保险等。

主页 <https://www.r3.com/>

China Ledger 联盟

中国分布式总账基础协议联盟（China Ledger 联盟）是2016年4月19日由中证机构间报价系统股份有限公司等11家机构共同发起的区块链联盟上海证券交易所前工程师白硕出任了该联盟技术委员会主任，联盟秘书处则设在了万向集团旗下的万向区块链实验室。

<http://www.chinaledger.com/>

点评：2016年以来几乎停滞，网页都没有做好，除了首页外没有任何内容。