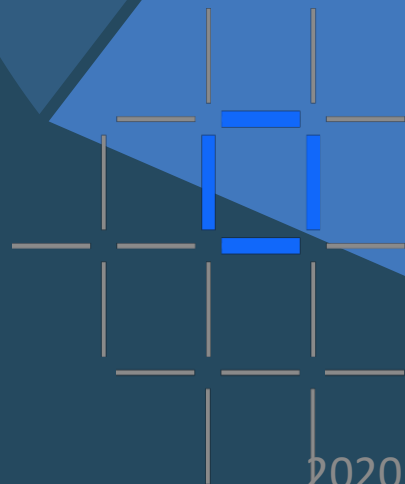




developerWorks
COURSES

IBM Blockchain Foundation



LING Zong, Ph. D.

Senior Software Engineer / Scientist
IBM Almaden Research Center
San Jose, California, U.S.A.

2020/10/7

What is a business blockchain network?

商业区块链网络是一种分散的网络，它使用分布式账本技术(DLT)在网络中的成员组织之间有效和安全地转移商业资产。资产可以是实体的，也可以是数字的，比如汽车、钻石、新鲜农产品或保险记录。一个共享的、分布式的账本记录了网络参与者之间所有资产交易的不可变的历史，并且编目了这些资产的当前状态(世界状态)。管理交易的业务规则由成员商定并封装在智能合约中

- A **business blockchain network** is a decentralized network that uses distributed ledger technology (DLT) for the efficient and secure transfer of business assets between member organizations in the network. Assets can be physical or digital, such as vehicles, diamonds, fresh produce, or insurance records. A shared, **distributed ledger** records an immutable history of all asset transactions between participants in the network, and catalogs the current state (world state) of those assets. The business rules that govern transactions are agreed upon by members and encapsulated in **smart contracts**.

区块链网络的成员没有依赖中央权威机构或可信的中介(如银行或经纪公司)来验证交易，而是使用共识机制来提高整个网络的交易处理速度、透明度和可靠性。为了增加机密性，成员加入一个或多个允许数据隔离的通道；特定于通道的分类账由该通道中经过身份验证的对等方共享

- Instead of relying on a central authority or trusted intermediary, such as a bank or brokerage firm, to validate transactions, members of a blockchain network use a **consensus** mechanism to improve transaction processing speed, transparency, and accountability across the network. For additional confidentiality, members join one or more **channels** that allow for data isolation; a channel-specific ledger is shared by the authenticated peers in that channel.

企业区块链网络由一组可识别和可验证的机构(如企业、大学或医院)共同拥有和操作。在这样一个许可的网络中，参与者彼此都是已知的，交易的处理速度比在没有许可的公共网络中(比如比特币网络)要快得多。在比特币网络中，成员是匿名的，这迫使人们依赖工作证明和其他类型的共识机制，这些机制需要耗时的计算来确认身份和验证交易

- A blockchain network for business is collectively owned and operated by a group of identifiable and verifiable institutions, such as businesses, universities, or hospitals. In such a **permissioned network**, the participants are known to each other, and transactions are processed much faster than in a non-permissioned, public network like the Bitcoin network. In the Bitcoin network, members are anonymous, forcing the reliance on “proof-of-work” and other types of consensus mechanisms that require time-consuming computations to confirm identities and validate transactions.

Topics

- **Blockchain Architecture**
- **Blockchain Fabric Development**
- **Blockchain Components**
- **Blockchain Operations**
- **Hyperledger Composer**



Blockchain Architecture

Blockchain provides a single version of truth

区块链是一种共享账本技术，商业网络的参与者可以使用它来记录不能更改的商业交易历史。

Blockchain is a **shared ledger technology** that participants in a business network can use to record the history of business transactions that cannot be altered.

区块链提供了一个唯一的事实：一个共享的，篡改明显的账本。

Blockchain provides a single point of truth: a **shared, tamper-evident ledger**.

这种方法将交易跟踪从竖井模型(其中多个分类账是单独维护的)更改为跨整个网络提供公共视图的模型。

This approach changes transaction tracking from a siloed model, where multiple ledgers are maintained separately, to one that provides a common view across the entire network.

新的用于傻瓜的区块链有描述真实区块链网络的用例、来自IBM区块链平台的最新用例等等。

The new [Blockchain for Dummies](#) has use cases that describe real blockchain networks, the latest from the IBM Blockchain Platform, and more.

因为区块链使用一致意见将交易提交到总账，所以结果是最终的。每个成员都有一份相同的账本，因此资产的来源和可追溯性是透明和可信的。区块链可应用于任何行业

Because blockchain uses consensus to commit transactions to the ledger, the results are final. Each member has a copy of the same ledger, so asset provenance and traceability are transparent and trusted. [Blockchain can be applied to any industry](#).

The power of blockchain

区块链在以下几个方面为企业提供支持：

- 利用生态系统的力量，以更大的信任更快地完成事务。
- 通过消除低效、浪费和重复，极大地降低了跨企业业务流程的成本和复杂性。
- 支持新的数字交互方式的发明。
- 减少市场摩擦和低效，释放资本。
- 创建成本效益高的商业网络，几乎任何有价值的东西都可以跟踪和交易，而不需要一个中心控制点。
- 通过处理风险和不确定性来减少交易周期时间。
- 减少来自电子犯罪和网络攻击的欺诈行为。

Blockchain empowers enterprises in several ways:

- Use the power of ecosystems to complete transactions **faster with greater trust**.
- Vastly reduce the cost and complexity of cross-enterprise business processes by **eliminating inefficiencies, waste, and duplication**.
- Support the invention of new styles of **digital interactions**.
- Reduce friction and inefficiencies in the market, freeing capital.
- Create **cost-efficient** business networks where virtually anything of value can be tracked and traded without requiring a central point of control.
- **Decrease transaction cycle times** by addressing risk and uncertainty.
- **Reduce fraud** from e-crime and cyber attacks.

Security: Public vs. Private Blockchains

Public blockchains



- For example, Bitcoin
- Transactions are viewable by anyone
- Participant identity is more difficult to control

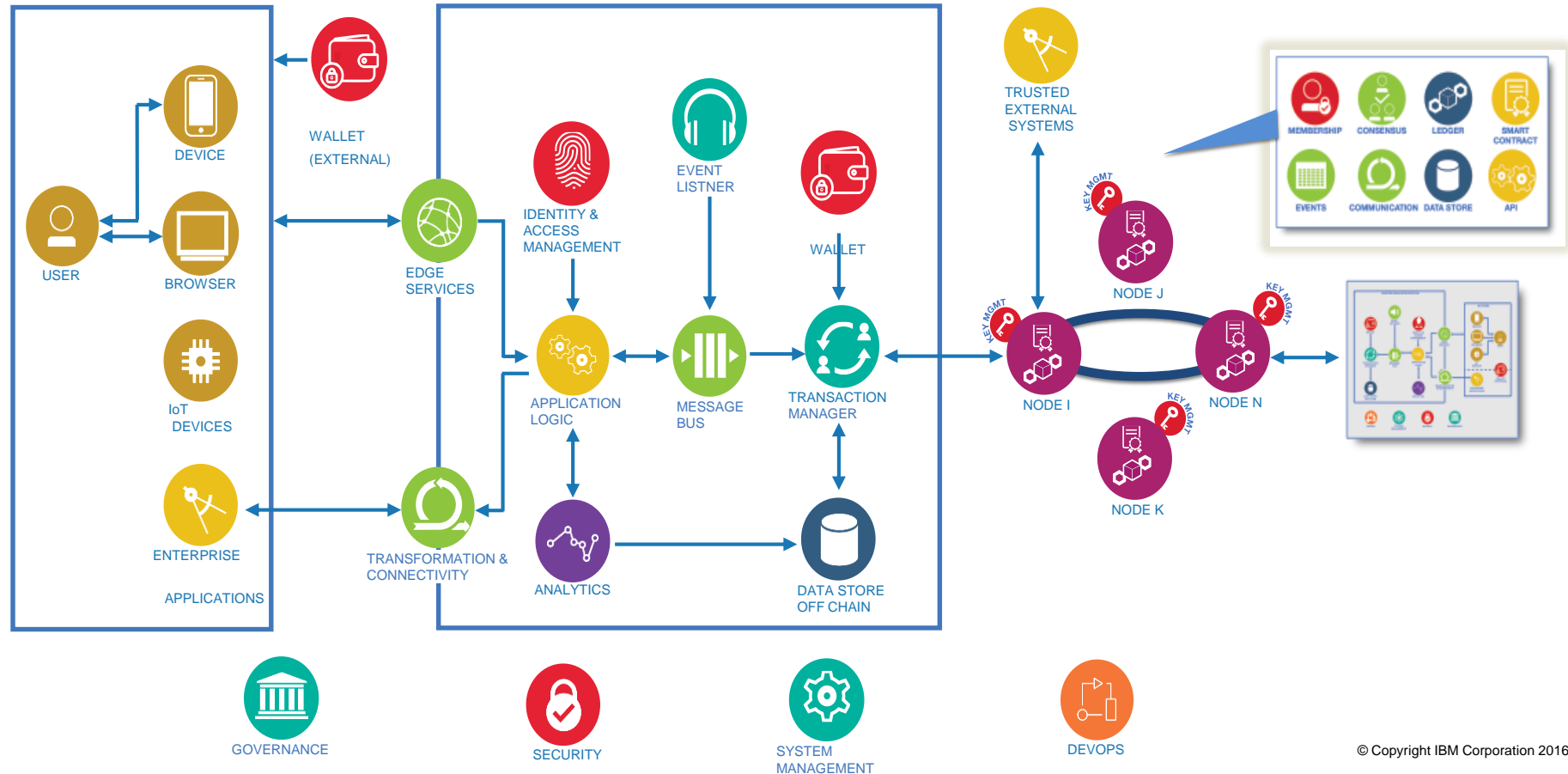
Private blockchains



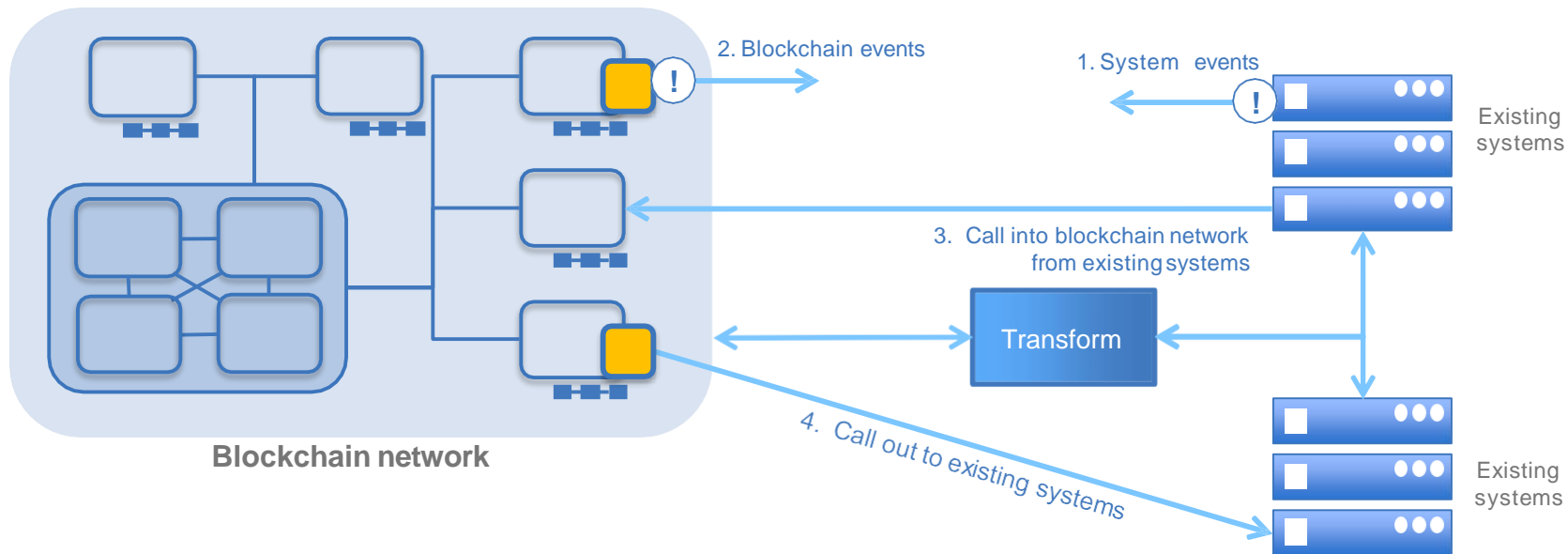
- For example, Hyperledger Fabric
- Network members are known but transactions are secret

- Some use cases require anonymity, others require privacy
 - Some may require a mixture of the two, depending on the characteristics of each participant
- Most **business** use cases require private, permissioned blockchains
 - Network members know who they're dealing with (required for KYC, AML, etc.)
 - 交易(通常)在相关参与者之间保密 Transactions are (usually) confidential between the participants concerned
 - Membership is controlled

Blockchain architecture



Integrating with Existing Systems



Blockchain makes it better.

- A** Single shared ledger that is tamper-evident. Once recorded, transactions cannot be altered
- B** All parties must give consensus before a new transaction is added to the network
- C** Eliminates or reduces paper processes, speeding up transaction times and increasing efficiencies



Blockchain in action: The diamond industry

· 为了理解区块链的价值, 考虑一个实际的示例。钻石行业面临着许多挑战, 包括走私、欺诈、伪造钻石和不道德开采的钻石。区块链可以用来缓解其中一些挑战。
· 从矿山到消费者的过程包含了一个复杂的过程, 包括法律、监管、金融、制造和商业实践。每一步都有挑战。消费者冒着购买不道德开采的钻石的风险。政府必须追踪钻石出口并支付出口税。顾客想要确定他们得到了付钱买的钻石。

- To understand the value of a blockchain, consider a practical example. The diamond industry faces many challenges, including smuggling, fraud, counterfeit diamonds, and unethically mined stones. A blockchain can be used to mitigate some of those challenges.
- The journey from mine to consumer covers a complex journey through legal, regulatory, financial, manufacturing, and commercial practices. Challenges exist every step of the way. Consumers run the risk of buying unethically mined diamonds. Governments must track diamond exports and pay export taxes. Customers want to be sure that they're getting the diamonds that they're paying for.

- ① The use of a blockchain can eliminate vulnerabilities through transparent transactions. All parties have access to a secure, synchronized record of transactions. The ledger records every sequence of transactions, from beginning to end.
- ② Blockchain can record the mining, refining, and distribution of diamonds. A diamond's path can be traced from the mine to the hands of the consumer with security and transparency.
- ③ The ledger keeps the diamond's records, including high-resolution photos at each block of the chain, from where it's excavated in the mine, to where it's cut and refined, to where it's sold.
- ④ The blockchain holds certificates of authenticity, payment transactions, and detailed characteristics of the diamond, including color, cut, clarity, carat, and the diamond serial number. At the end of a buying cycle, the diamond has a complete, auditable, undisputable record of information.

Tracking diamonds from mine to final customer is complex. Diamond smuggling, fraud, counterfeit diamonds and unethically mined stones pose real challenges. With blockchain, it's possible to:

Keep a record of high-resolution photos of each diamond at every touchpoint along its journey.



Track real-time records of every payment transaction.



Hold certificates of authenticity.



Maintain product details like cut, clarity, color, carat and diamond serial numbers.



1. 使用区块链可以通过透明的事务消除漏洞。所有各方都可以访问安全的、同步的事务记录。分类帐从头到尾记录了每笔交易的顺序。
2. 区块链可以记录钻石的开采、精炼和分布情况。钻石的路径可以从矿场追踪到消费者手中, 既安全又透明。
3. 账本上保存着钻石的记录, 包括钻石链上每个区块的高分辨率照片, 从钻石在矿井中被挖掘到的地方, 到钻石被切割和加工的地方, 再到钻石被出售的地方。
4. 区块链拥有真伪证书, 支付交易, 以及钻石的详细特征, 包括颜色, 切割, 净度, 克拉和钻石序列号。在购买周期结束时, 钻石拥有完整、可审核、无可争议的信息记录。



Blockchain Fabric Development

Requirements for Enterprise Blockchain

For enterprise use, we need to consider the following requirements:

- Participants must be identified/identifiable
- Networks need to be *permissioned*
- High transaction throughput performance
- Low latency of transaction confirmation
- Privacy and confidentiality of transactions and data pertaining to business transactions

对于企业使用，我们需要考虑以下需求：

- 参与者必须被识别
- 网络需要得到许可
- 高交易吞吐量性能
- 交易确认的低延迟
- 与商业交易有关的交易和数据的隐私和机密性

虽然许多早期的区块链平台目前正在适应企业使用，但Hyperledger Fabric从一开始就为企业使用而设计。

While many early blockchain platforms are currently being *adapted* for enterprise use, **Hyperledger Fabric** has been *designed* for enterprise use from the outset.

Hyperledger Fabric Concepts (1)

Hyperledger Fabric是一个开放源码的企业级许可分布式账本技术(DLT)平台，为在企业环境中使用而设计，它提供了一些与其他流行的分布式账本或区块链平台不同的关键功能。

Hyperledger Fabric is an **open source enterprise-grade permissioned distributed ledger technology (DLT) platform**, designed for use in enterprise contexts, that delivers some key differentiating capabilities over other popular distributed ledger or blockchain platforms.

一个关键的区别是Hyperledger是在Linux基金会的基础上建立的，而Linux基金会本身就有在开放管理下培育开源项目的长期和非常成功的历史，这些项目可以培育强大的持续的社区和繁荣的生态系统。
Hyperledger由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的维护人员管理。它拥有一个开发社区，从最早提交开始，已经发展到超过35个组织和近200名开发人员。

One key point of differentiation is that Hyperledger was established under the **Linux Foundation**, which itself has a long and very successful history of nurturing open source projects under **open governance** that grow strong sustaining communities and thriving ecosystems.

- Hyperledger is governed by a diverse technical steering committee, and the Hyperledger Fabric project by a diverse set of maintainers from multiple organizations. It has a **development community** that has grown to over 35 organizations and nearly 200 developers since its earliest commits.

Fabric具有高度模块化和可配置的体系结构，支持对广泛的工业用例(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交付)进行创新、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领域特定语言(DSL)编写智能合约的分布式账本平台。这意味着大多数企业已经具备了开发智能合约所需的技能，并且不需要额外的培训来学习一种新的语言或DSL。

Fabric has a highly **modular** and **configurable** architecture, enabling innovation, versatility and optimization for a broad range of industry use cases including banking, finance, insurance, healthcare, human resources, supply chain and even digital music delivery.

- Fabric is the first distributed ledger platform to support **smart contracts authored in general-purpose programming languages** such as Java, Go and Node.js, rather than constrained domain-specific languages (DSL). This means that most enterprises already have the skill set needed to develop smart contracts, and no additional training to learn a new language or DSL is needed.

Fabric平台也是许可的，这意味着，与公共的无许可网络不同，参与者彼此是已知的，而不是匿名的，因此完全不可信。

这意味着尽管参与者可能没有完全相互信任(例如，他们可能会在同一行业是竞争对手)，网络可以在一种治理模式下运行，这种治理模式建立在参与者之间确实存在的信任之上，例如处理争端的法律协议或框架。

The Fabric platform is also **permissioned**, meaning that, unlike with a public permissionless network, the participants are known to each other, rather than anonymous and therefore fully untrusted.

- This means that while the participants may not *fully* trust one another (they may, for example, be competitors in the same industry), a network can be operated under a **governance model** that is built off of what trust *does* exist between participants, such as a legal agreement or framework for handling disputes.

Hyperledger Fabric Concepts (2)

平台最重要的区别之一是它对可插入共识协议的支持，该协议使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，当部署在单个企业中或由可信的权威机构操作时，完全拜占庭式容错共识可能被认为是不必要的，并且会对性能和吞吐量造成过度的拖累。在这样的情况下，一个崩溃故障处理协议 (CFT) 可能就足够了，而在一个多方、分散的用例中，可能需要一个更传统的拜占庭容错 (BFT) 协议。

One of the most important of the platform's differentiators is its support for **pluggable consensus protocols** that enable the platform to be more effectively customized to fit particular use cases and trust models.

- For instance, when deployed within a single enterprise, or operated by a trusted authority, fully byzantine fault tolerant consensus might be considered unnecessary and an excessive drag on performance and throughput. In situations such as that, a [crash fault-tolerant](#) (CFT) consensus protocol might be more than adequate whereas, in a multi-party, decentralized use case, a more traditional [byzantine fault tolerant](#) (BFT) consensus protocol might be required.

Fabric可以利用不需要本地加密货币的一致协议来激励昂贵的挖掘或促进智能合约执行。

避免加密货币减少了一些重要的风险/攻击向量，而不需要加密挖掘操作意味着该平台可以以任何其他分布式系统大致相同的操作成本部署。

Fabric can leverage consensus protocols that **do not require a native cryptocurrency** to incent costly mining or to fuel smart contract execution.

- Avoidance of a cryptocurrency reduces some significant risk/attack vectors, and absence of cryptographic mining operations means that the platform can be deployed with roughly the same operational cost as any other distributed system.

这些差异化设计特性的结合使得Fabric成为当今在交易处理和确认延迟方面性能更好的平台之一，并且它使交易和实现它们的智能合约 (Fabric称为“链码”) 具有私密性和保密性。

The combination of these differentiating design features makes Fabric one of the **better performing platforms** available today both in terms of transaction processing and transaction confirmation latency, and it enables **privacy and confidentiality** of transactions and the smart contracts (what Fabric calls “chaincode”) that implement them.

让我们更详细地探讨这些不同的特性。

Let's explore these differentiating features in more detail.

Modularity

Hyperledger Fabric被专门设计为模块化架构。无论是可插拔的共识协议，还是可插拔的身份管理协议(如LDAP或OpenID连接)，密钥管理协议或密码库，该平台的核心设计都是配置以满足企业用例需求的多样性。在高水平上，Fabric由以下模块化组件组成：

- 可插拔排序服务建立对事务顺序的一致意见，然后向对等方广播块。
- 可插拔会员服务提供者负责将网络中的实体与加密身份关联起来。
- 一个可选的对等八卦服务通过排序服务向其他对等点来传播块输出。
- 智能合约(链码)在容器环境(例如Docker)中运行以进行隔离。它们可以用标准编程语言编写，但不能直接访问分类账状态。
- 可以将分类账配置为支持各种DBMSs。
- 可插入的支持和验证策略实施，可为每个应用程序独立配置。

Hyperledger Fabric has been specifically architected to have a **modular architecture**. Whether it is pluggable consensus, pluggable identity management protocols such as LDAP or OpenID Connect, key management protocols or cryptographic libraries, the platform has been designed at its core to be configured to meet the diversity of enterprise use case requirements. At a high level, Fabric is comprised of the following modular components:

- A pluggable **ordering service** establishes consensus on the order of transactions and then broadcasts blocks to peers.
- A pluggable **membership service provider** is responsible for associating entities in the network with cryptographic identities.
- An optional **peer-to-peer gossip service** disseminates the blocks output by ordering service to other peers.
- **Smart contracts** (“chaincode”) run within a container environment (e.g. Docker) for isolation. They can be written in standard programming languages but do not have direct access to the ledger state.
- The **ledger** can be configured to support a variety of **DBMSs**.
- A pluggable **endorsement and validation policy enforcement** that can be independently configured per application.

There is fair agreement in the industry that there is no “one blockchain to rule them all”. Hyperledger Fabric can be configured in multiple ways to satisfy the diverse solution requirements for **multiple industry use cases**.

Permissioned vs Permissionless Blockchains

在一个未许可的区块链中，几乎任何人都可以参与，而且每个参与者都是匿名的。在这样的上下文中，除了区块链在某个深度之前的状态是不可变的之外，不可能有其他信任。为了减轻这种信任缺失，无许可区块链通常采用挖掘的本地加密货币或交易费用来提供经济激励，以抵消参与基于工作证明(PoW)的拜占庭容错共识形式的额外成本。

In a permissionless blockchain, virtually anyone can participate, and every participant is anonymous. In such a context, there can be no trust other than that the state of the blockchain, prior to a certain depth, is immutable. In order to mitigate this absence of trust, permissionless blockchains typically employ a “mined” native cryptocurrency or transaction fees to provide economic incentive to offset the extraordinary costs of participating in a form of byzantine fault tolerant consensus based on “proof of work” (PoW).

另一方面，被许可的区块链在一组已知的、被识别的和经常被审查的参与者之间运行区块链，在一个产生一定程度信任的治理模式下运行。

· 经过许可的区块链提供了一种方法来保护具有共同目标但可能不完全信任彼此的一组实体之间的交互。

· 通过依赖参与者的身份，一个被许可的区块链可以使用更传统的崩溃容错(CFT)或拜占庭容错(BFT)一致协议，不需要昂贵的挖掘。

Permissioned blockchains, on the other hand, operate a blockchain amongst a set of known, identified and often vetted participants operating under a governance model that yields **a certain degree of trust**.

- A permissioned blockchain provides a way to secure the interactions among a group of entities that have a common goal but which may not fully trust each other.
- By relying on the identities of the participants, a permissioned blockchain can use more traditional crash fault tolerant (CFT) or byzantine fault tolerant (BFT) consensus protocols that do not require costly mining.

此外，在这种许可的环境中，参与者通过智能合约有意引入恶意代码的风险降低了。

· 首先，参与者彼此都是已知的，所有的动作，无论是提交应用程序事务、修改网络配置还是部署智能合约，都按照为网络和相关事务类型建立的支持策略记录在区块链上。

· 不是完全匿名的，可以很容易地识别出犯罪的一方，并且根据治理模型的条款处理事件。

Additionally, in such a permissioned context, the risk of a participant intentionally introducing malicious code through a smart contract is diminished.

- First, the participants are known to one another and all actions, whether submitting application transactions, modifying the configuration of the network or deploying a smart contract are recorded on the blockchain following an endorsement policy that was established for the network and relevant transaction type.
- Rather than being completely anonymous, the guilty party can be easily identified and the incident handled in accordance with the terms of the governance model.

Smart Contracts

A smart contract, or what Fabric calls “chaincode”, functions as a trusted distributed application that gains its security/trust from the blockchain and the underlying consensus among the peers. It is the business logic of a blockchain application.

There are three key points that apply to smart contracts, especially when applied to a platform:

- **many smart contracts run concurrently in the network,**
- **they may be deployed dynamically (in many cases by anyone), and**
- **application code should be treated as untrusted, potentially even malicious.**

智能合约 (Fabric称为链码) 作为受信任的分布式应用程序发挥作用, 它从区块链和对等方之间获得安全性/信任。它是区块链应用程序的业务逻辑。
有三个关键点适用于智能合约, 特别是应用于一个平台:
· 许多智能合约在网络中同时运行,
· 它们可以动态部署 (在许多情况下由任何人部署)
· 应用程序代码应该被视为不受信任的, 甚至可能是恶意的。

Most existing smart-contract capable blockchain platforms follow an **order-execute architecture** in which the consensus protocol:

- validates and orders transactions then
- propagates them to all peer nodes
- each peer then executes the transactions sequentially.

大多数现有的有智能合约能力的区块链平台遵循排序-执行架构, 其中共识协议:

- 验证和排序交易
- 将它们传播到所有对等节点
- 每个对等节点按顺序执行事务。

排序-执行架构几乎可以在所有现有的区块链系统中找到, 从Ethereum (基于PoW的共识) 等公共/无许可平台到Tendermint、Chain和Quorum等有许可平台。

The order-execute architecture can be found in virtually all existing blockchain systems, ranging from public/permissionless platforms such as [Ethereum](#) (with PoW-based consensus) to permissioned platforms such as [Tendermint](#), [Chain](#), and [Quorum](#).

在使用排序-执行架构的区块链中执行的智能合约必须是确定性的; 否则, 可能永远无法达成共识。为了解决非确定性问题, 许多平台要求智能合约使用非标准的或领域特定的语言 (如Solidity) 编写, 以便消除非确定性操作。这妨碍了广泛采用, 因为它要求开发人员编写智能合约来学习一种新语言, 并可能导致编程错误。

Smart contracts executing in a blockchain that operates with the order-execute architecture must be deterministic; otherwise, consensus might never be reached. To address the non-determinism issue, many platforms require that the smart contracts be written in a non-standard, or domain-specific language (such as [Solidity](#)) so that non-deterministic operations can be eliminated. This hinders wide-spread adoption because it requires developers writing smart contracts to learn a new language and may lead to programming errors.

此外, 由于所有事务都是由所有节点按顺序执行的, 因此性能和规模受到了限制。由于智能合约代码在系统中的每个节点上执行, 因此需要采取复杂的措施来保护整个系统免受潜在恶意合约的侵害, 以确保整个系统的弹性。

Further, since all transactions are executed sequentially by all nodes, performance and scale is limited. The fact that the smart contract code executes **on every node** in the system demands that complex measures be taken to protect the overall system from potentially malicious contracts in order to ensure resiliency of the overall system.

A New Approach in Fabric

Fabric introduces a new architecture for transactions that we call **execute-order-validate**. It addresses the resiliency, flexibility, scalability, performance and confidentiality challenges faced by the order-execute model by separating the transaction flow into three steps:

- **execute** a transaction and check its correctness, thereby endorsing it,
- **order** transactions via a (pluggable) consensus protocol, and
- **validate** transactions against an application-specific endorsement policy before committing them to the ledger

Fabric为交易引入了一个新的体系结构，我们称之为执行-排序-验证。它通过将交易流分成三个步骤来解决排序-执行模型所面临的弹性、灵活性、可伸缩性、性能和机密性挑战：

- 执行交易并检查其正确性，从而背书，
- 通过(可插拔的)一致协议排序交易
- 在将交易提交到分类账之前，根据特定于应用程序的背书策略验证交易

这种设计从根本上背离了Fabric中的“排序-执行”范式，即在对交易的顺序达成最终协议之前执行交易

This design departs radically from the order-execute paradigm in that Fabric executes transactions before reaching final agreement on their order.

在Fabric中，特定于应用程序的背书策略指定哪些对等节点(或它们中的多少节点)需要担保给定智能合约的正确执行。因此，每个交易只需要由满足交易的背书策略所需的对等节点子集执行(背书)。这允许并行执行，从而提高系统的总体性能和规模。这个第一阶段也消除了任何不确定性，因为不一致的结果可以在排序之前被过滤掉。

In Fabric, an application-specific endorsement policy specifies which peer nodes, or how many of them, need to vouch for the correct execution of a given smart contract. Thus, each transaction need only be executed (endorsed) by the subset of the peer nodes necessary to satisfy the transaction's endorsement policy. This allows for parallel execution increasing overall performance and scale of the system. This first phase also **eliminates any non-determinism**, as inconsistent results can be filtered out before ordering.

因为我们消除了非确定性，所以Fabric是第一种支持使用标准编程语言的区块链技术

Because we have eliminated non-determinism, Fabric is the first blockchain technology that **enables use of standard programming languages**.

Privacy and Confidentiality - Problems

在利用PoW作为其共识模型的公开的、无许可的区块链网络中，事务在每个节点上执行。这意味着合同本身和它们处理的事务数据都不具有机密性。每个事务以及实现它的代码对网络中的每个节点都是可见的。在这种情况下，我们已经交换了合同和数据的机密性，以获得由PoW交付的拜占庭容错共识

In a public, permissionless blockchain network that leverages PoW for its consensus model, transactions are executed on every node. This means that neither can there be confidentiality of the contracts themselves, nor of the transaction data that they process. Every transaction, and the code that implements it, is visible to every node in the network. In this case, we have traded confidentiality of contract and data for byzantine fault tolerant consensus delivered by PoW.

对于许多业务/企业用例来说，这种保密性的缺乏可能是一个问题。
· 例如，在供应链合作伙伴的网络中，一些消费者可能被给予优惠价格，作为巩固关系或促进额外销售的一种手段。如果每个参与者都能看到每一份合同和交易，就不可能在一个完全透明的网络中维持这样的商业关系。

· 再举第二个例子，以证券业为例，交易员在建立头寸(或出售头寸)时，不会希望其竞争对手知道这一点，否则他们就会试图加入这个游戏，从而削弱交易员的策略。

This lack of confidentiality can be problematic for many business/enterprise use cases.

- For example, in a network of supply-chain partners, some consumers might be given preferred rates as a means of either solidifying a relationship, or promoting additional sales. If every participant can see every contract and transaction, it becomes impossible to maintain such business relationships in a completely transparent network — everyone will want the preferred rates!
- As a second example, consider the securities industry, where a trader building a position (or disposing of one) would not want her competitors to know of this, or else they will seek to get in on the game, weakening the trader's gambit.

为了解决在交付企业用例需求时缺乏隐私和机密性的问题，区块链平台采用了多种方法。它们都有各自的优缺点

In order to address the lack of privacy and confidentiality for purposes of delivering on enterprise use case requirements, blockchain platforms have adopted a variety of approaches. All have their trade-offs.

Privacy and Confidentiality – Solutions (Channel)

加密数据是提供机密性的一种方法;然而,在利用PoW达成一致的无许可网络中,加密的数据位于每个节点上。只要有足够的时间和计算资源,加密就可以被破解。对于许多企业用例,它们的信息可能被破坏的风险是不可接受的。

Encrypting data is one approach to providing confidentiality; however, in a permissionless network leveraging PoW for its consensus, the encrypted data is sitting on every node. Given enough time and **computational resource**, the encryption could be broken. For many enterprise use cases, the risk that their information could become compromised is unacceptable.

零知识证明(ZKP)是解决这个问题的另一个研究领域,这里的权衡是,目前计算一个ZKP需要相当多的时间和计算资源。因此,在这种情况下,权衡的是性能和机密性

Zero knowledge proofs (ZKP) are another area of research being explored to address this problem, the trade-off here being that, presently, computing a ZKP requires considerable time and computational resources. Hence, the trade-off in this case is **performance for confidentiality**.

在可以利用其他形式的共识的许可环境中,人们可能会探索将机密信息只分发给授权节点的方法。

In a permissioned context that can leverage alternate forms of consensus, one might explore approaches that restrict the distribution of confidential information **exclusively to authorized nodes**.

Hyperledger Fabric是一个许可的平台,通过它的渠道架构和私有数据特性实现了保密性。

Hyperledger Fabric, being a permissioned platform, enables confidentiality through its **channel architecture** and private data feature.

- In channels, participants on a Fabric network establish a sub-network where every member has visibility to a particular set of transactions. 在通道中, Fabric网络上的参与者建立一个子网络,其中每个成员都对特定的事务集具有可见性
- Thus, only those nodes that participate in a channel have access to the smart contract (chaincode) and data transacted, preserving the privacy and confidentiality of both. 因此,只有那些参与信道的节点才能访问智能合约(链码)和进行数据处理,从而保护了两者的隐私和机密性
- Private data allows collections between members on a channel, allowing much of the same protection as channels without the maintenance overhead of creating and maintaining a separate channel. 私有数据允许在通道上的成员之间进行集合,允许与通道相同的保护,而无需创建和维护单独通道的维护开销。

Pluggable Consensus

事务的顺序被委托给一个模块组件以达成一致，这个组件从逻辑上与执行事务和维护分类账的对等组件解耦。

The ordering of transactions is delegated to a modular component for consensus that is logically decoupled from the peers that execute transactions and maintain the ledger.

具体来说，就是排序服务。因为共识是模块化的，所以它的实现可以根据特定部署或解决方案的信任假设进行定制。这种模块化架构允许平台依赖于已建立好的CFT(崩溃容错)或BFT(拜占庭容错)排序工具包。

Specifically, the ordering service. Since **consensus is modular**, its implementation can be tailored to the trust assumption of a particular deployment or solution. This modular architecture allows the platform to rely on well-established toolkits for CFT (crash fault-tolerant) or BFT (byzantine fault-tolerant) ordering.

Fabric目前提供了基于Raft协议的etcd库的CFT排序服务实现。

• etcd是一种强一致性的分布式键值存储，它提供了一种可靠的方式来存储需要被分布式系统或机器集群访问的数据——<https://etcd.io>

• Raft是一个被设计成易于理解的共识算法——<https://raft.github.io>

Fabric currently offers a CFT ordering service implementation based on the [etcd library](#) of the [Raft protocol](#).

- **etcd** is a strongly consistent, distributed key-value store that provides a reliable way to store data that needs to be accessed by a distributed system or cluster of machines - <https://etcd.io>
- **Raft** is a consensus algorithm that is designed to be easy to understand - <https://raft.github.io>

有关当前可用的排序服务的信息，请参阅有关订购的概念文档

For information about currently available ordering services, check out this [conceptual documentation about ordering](#).

还要注意的，它们并不是相互排斥的。一个Fabric网络可以有多个排序服务，以支持不同的应用程序或应用程序需求

Note also that these are not mutually exclusive. A Fabric network can have multiple ordering services supporting different applications or application requirements.

Performance and Scalability

区块链平台的性能会受到许多变量的影响，比如事务大小、块大小、网络大小以及硬件的限制等等。Hyperledger Fabric性能和规模工作组目前在一个名为Hyperledger Caliper的基准测试框架上工作

Performance of a blockchain platform can be affected by many variables such as transaction size, block size, network size, as well as limits of the hardware, etc. The Hyperledger Fabric [Performance and Scale working group](#) currently works on a benchmarking framework called [Hyperledger Caliper](#).

已经发表多篇研究和测试Hyperledger Fabric性能的论文。最新的伸缩Fabric达到每秒20,000个事务

Several research papers have been published studying and testing the performance capabilities of Hyperledger Fabric. The latest [scaled Fabric to 20,000 transactions per second](#).

任何对区块链平台的认真评估都应该将Hyperledger Fabric列入其候选名单。

Any serious evaluation of blockchain platforms should include Hyperledger Fabric in its short list.

结合起来，Fabric的差异化能力使其成为一个高度可伸缩的系统，用于支持灵活的信任假设，从而使平台能够支持广泛的行业用例，从政府，到金融、供应链物流、医疗保健等等

Combined, the differentiating capabilities of Fabric make it a highly scalable system for permissioned blockchains supporting flexible trust assumptions that enable the platform to support a wide range of industry use cases ranging from government, to finance, to supply-chain logistics, to healthcare and so much more.

Hyperledger Fabric是最活跃的Hyperledger项目。围绕该平台的社区建设正在稳步增长，每一个后续版本所带来的创新都远远超过了其他企业区块链平台

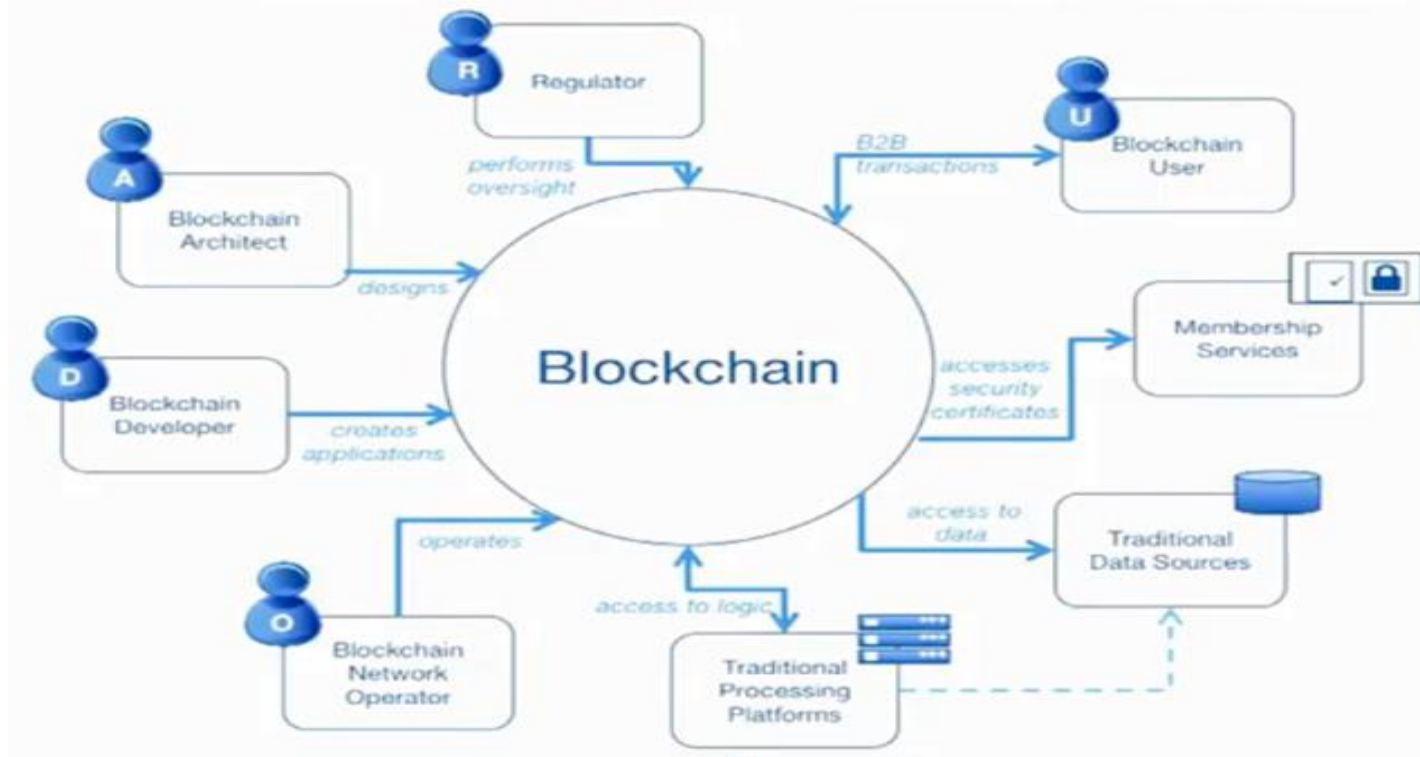
Hyperledger Fabric is the most active of the Hyperledger projects. The community building around the platform is growing steadily, and the innovation delivered with each successive release far out-paces any of the other enterprise blockchain platforms.



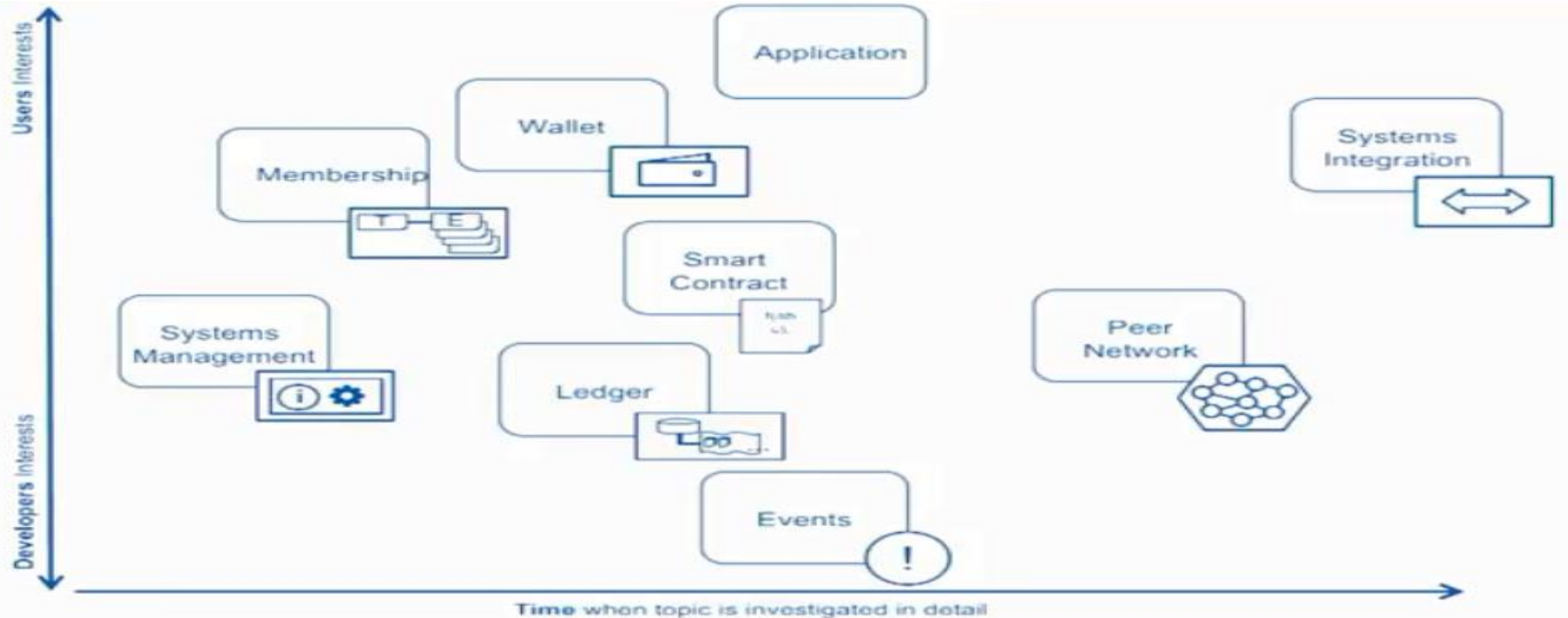
Blockchain Components

Participants & components overview

Who are the participants in a blockchain network



Components in a Blockchain



- Ecerts (enrollment certificates) identify individuals in a network. 注册证书用于识别网络中的个人
- Tcerts (transaction certificates) capture the events of a transaction. 事务证书捕获事务的事件
- Anyone in the network can look up an Ecert or Tcert. 网络上的任何人都可以查询Ecert或Tcert

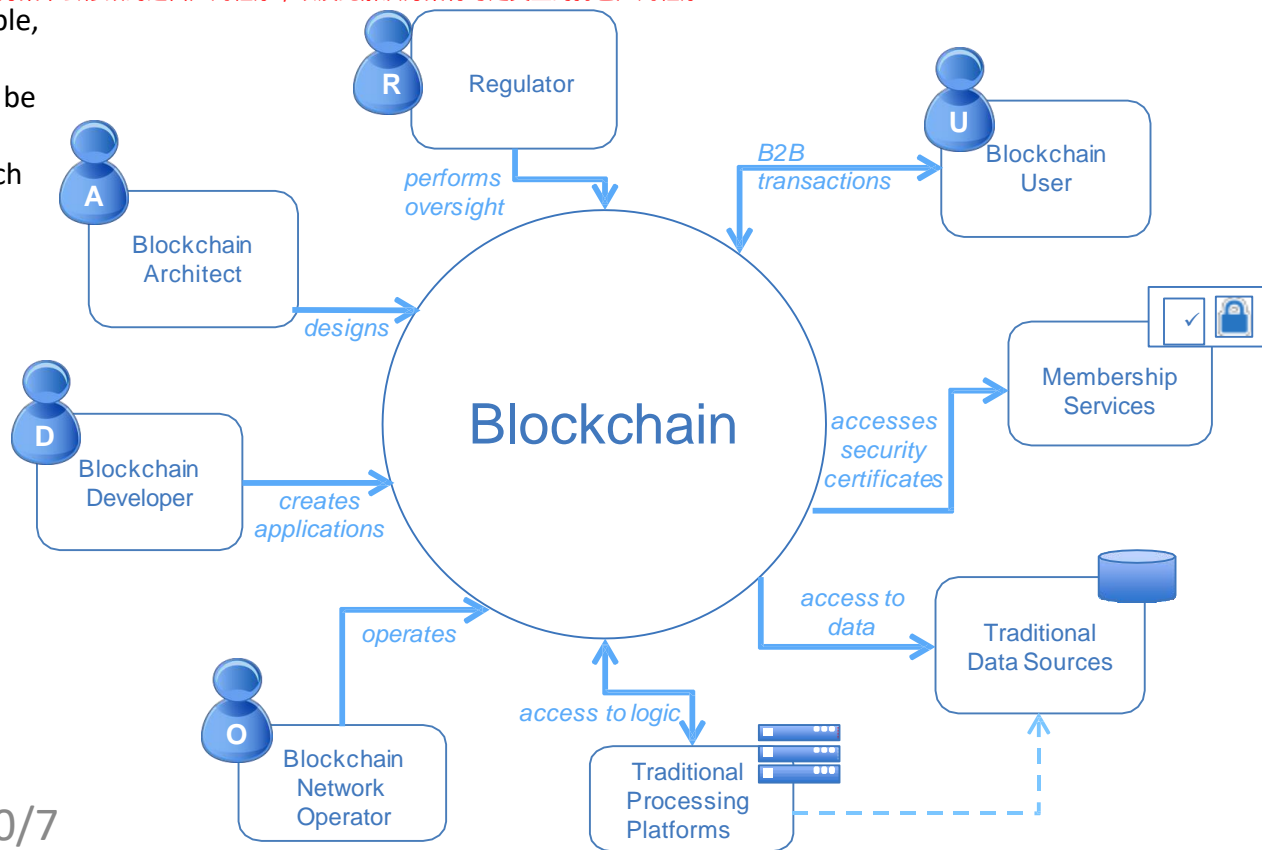
Actors in a Blockchain Solution (1)

参与者表示存在于解决方案范围之外的实体，但对其完整性至关重要

The actors represent entities that exist **outside** the scope of the solution, but are critical for its completeness.

例如，参与者可以是人、设备、外部机构、此解决方案不会修改的遗留应用程序，以及此解决方案将与之交互的打包应用程序

- For example, actors can be people, devices, external institutions, legacy applications that will not be modified by this solution, and packaged applications with which this solution will interact.



Actors in a Blockchain Solution (2)



Components in a Blockchain Solution

Ledger



一个分类账是一个信道链和当前状态数据，它由信道上的每个对等点维护
A ledger is a channel's chain and current state data which is maintained by each peer on the channel.

Smart Contract



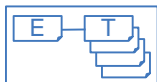
在分类帐上运行的软件，用于对资产和修改资产的交易指令(业务逻辑)进行编码
Software running on a ledger, to encode assets and transaction instructions (business logic) for modifying the assets.

Peer Network



覆盖整个事务流的更广泛的术语，用于生成订单协议并确认组成块的一组事务的正确性
A broader term overarching the entire transactional flow, which serves to generate an agreement on the order and to confirm the correctness of the set of transactions constituting a block.

Membership



会员服务对已授权的区块链网络上的身份进行验证、授权和管理。
Membership Services authenticates, authorizes, and manages identities on a permissioned blockchain network.

Events



创建区块链上重要操作的通知(例如一个新的区块)，以及与智能合同相关的通知。
Creates notifications of significant operations on the blockchain (e.g. a new block), as well as notifications related to smart contracts.

Systems Management



提供创建、更改和监视区块链组件的能力
Provides the ability to create, change and monitor blockchain components

Wallet



安全管理用户的安全凭据
Securely manages a user's security credentials

Systems Integration



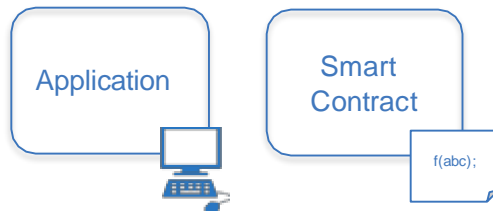
负责区块链与外部系统的双向集成。不是区块链的一部分，但与它一起使用。
Responsible for integrating Blockchain bi-directionally with external systems. Not part of blockchain, but used with it.

The Blockchain Developers



Blockchain
Developer

区块链开发者的主要兴趣是
Blockchain developers' primary interests are...



以及它们如何与分类账和其他记录系统相互作用
...and how they interact with the ledger and other systems of record:



他们不应该关心操作方面的问题，比如
They should NOT have to care about operational concerns, such as:

X

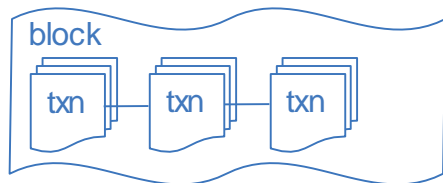
Peers

Consensus

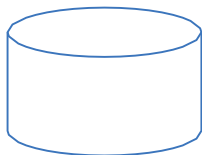
Security

How the Developer Interacts with the Ledger

A ledger often consists of two data structures



Blockchain



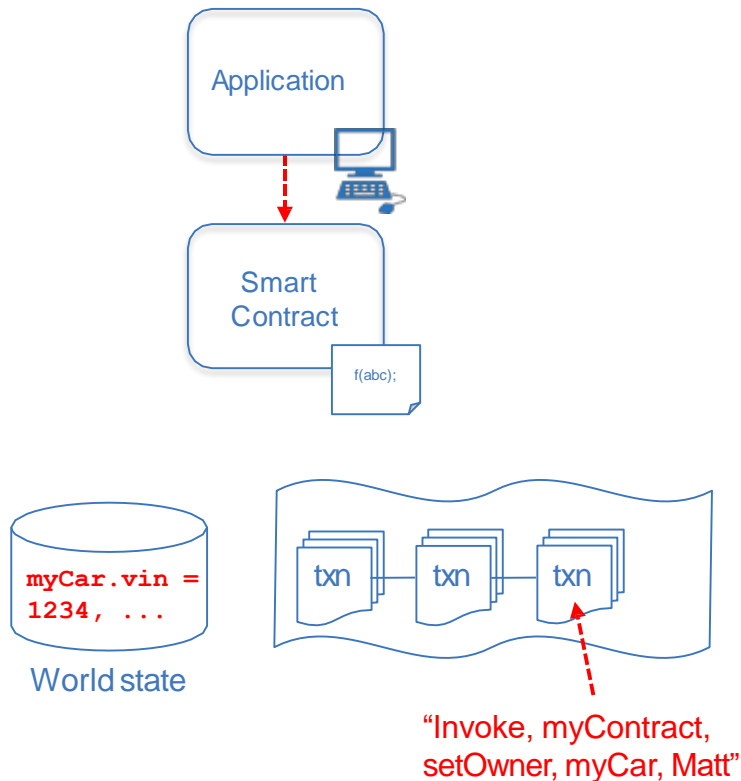
World state

- Blockchain
 - **A linked list of blocks**
 - 块的链表
 - 每个块描述一组事务(例如智能合约调用的输入)
 - 不可变--块不能被篡改
 - **Each block describes a set of transactions**
(e.g. the inputs to a smart contract invocation)
 - **Immutable – blocks cannot be tampered**
- World State
 - **An ordinary database (e.g. key/value store)**
 - **Stores the combined outputs of all transactions**
 - 存储所有事务的组合输出
 - 通常不是不变的
 - **Not usually immutable**

Working with the Ledger

所有权变更交易的例子

Example of a Change of Ownership Transaction (change car1 owner to Matt)



Transaction input - sent from application

```
invoke(myContract, setOwner, myCar, Matt)
```

Smart contract implementation

```
setOwner(Car, newOwner) {  
    set Car.owner = newOwner  
}
```

World state: new contents

```
myCar.vin = 1234  
myCar.owner = Matt  
myCar.make = Audi  
...
```

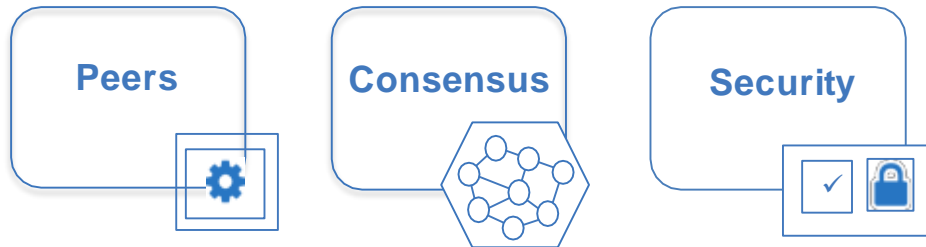

The Blockchain Administrators (Operators)



Blockchain
Administrator

区块链管理员的主要兴趣是部署和操作部分区块链

Blockchain administrators' primary interests are in the deployment and operation of part of the blockchain:



他们不应该关心开发问题，比如

They should NOT have to care about development concerns, such as:

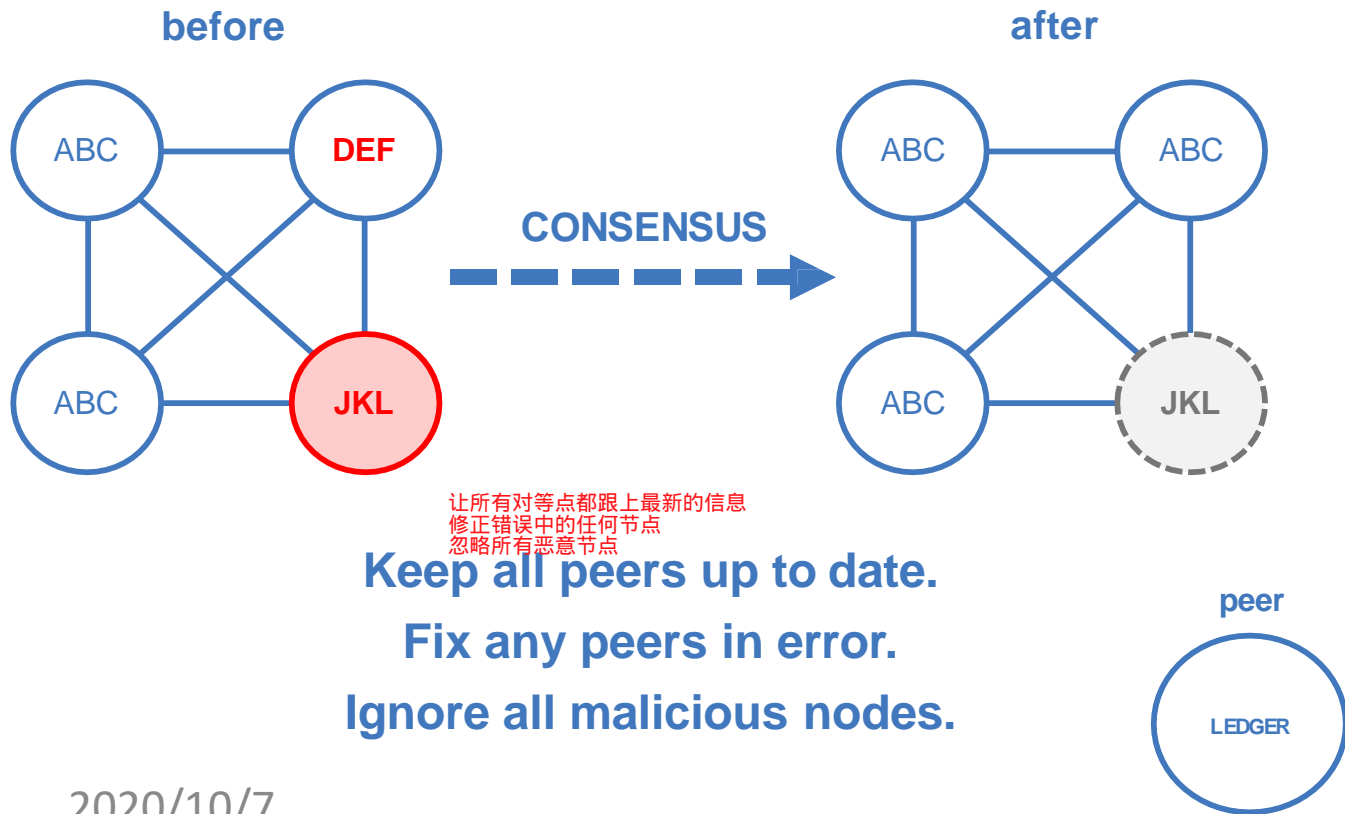
X

Application code

Smart contract code

Events and integration

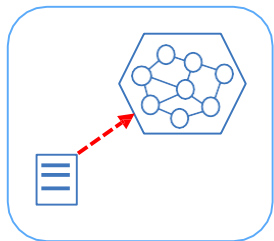
Consensus: The Process of Maintaining a Consistent Ledger



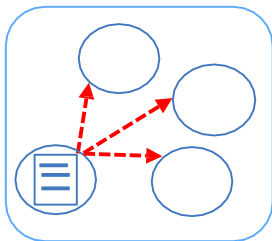
Consensus: Typical Flow of Execution

区块链实现之间的细节差别很大，但是一个典型的流程是：

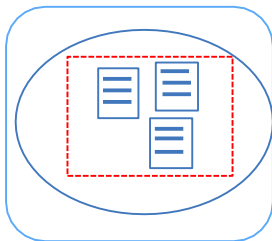
Details vary significantly between blockchain implementations, but a typical flow is:



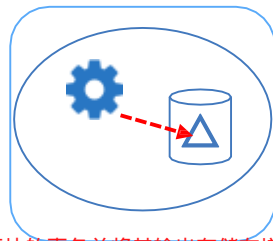
The application submits a request to invoke a transaction
应用程序提交请求来调用事务



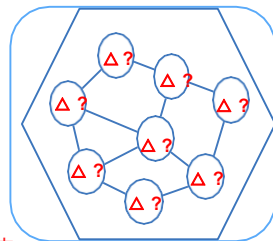
The transaction is shared around the network
事务在网络中共享



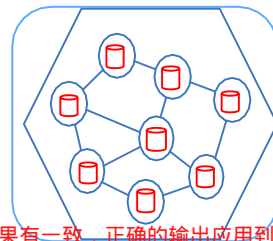
A designated peer creates a block containing the transaction
指定的对等点创建包含该事务的块



执行块的事务并将其输出存储在增量中
The block's transactions are executed and output stored in a delta



The network attempts to agree on the correct result
网络试图达成正确的结果

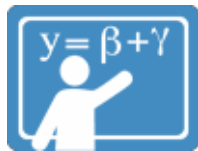


如果有一致，正确的输出应用到世界状态
If there is agreement, the correct output is applied to the world state

分类帐达成一致状态的过程称为共识

- The process to agree the consistent state of the ledger is known as **consensus**

Some Examples of Consensus Algorithms



Proof of work



Proof of stake



Solo



**Kafka/
Zookeeper**



**Proof of
Elapsed Time**



PBFT-based

Consensus Algorithms have Different Strengths and Weaknesses



Proof of work

需要验证器来解决困难的密码谜题

Require validators to solve difficult cryptographic puzzles

依赖能源的使用; 确认事务缓慢

PROs: Works in untrusted networks, CONS: Relies on energy use; slow to confirm transactions

在不可信的网络中工作

Example usage: Bitcoin, Ethereum



Proof of stake

要求验证器在托管中持有货币

Require validators to hold currency in escrow

需要内在(加密)货币, 没有利害关系的问题

PROs: Works in untrusted networks, CONS: Requires intrinsic (crypto)currency, "Nothing at stake" problem

在不可信的网络中工作

Example usage: Nxt, <https://nxtplatform.org>



Proof of Elapsed Time

可信执行环境中的等待时间使块生成随机化

Wait time in a trusted execution environment randomizes block generation

PROs: Efficient, CONS: Currently tailored towards one vendor 目前专为一厂商定制

Example usage: Sawtooth-Lake, <https://sawtooth.hyperledger.org>



Solo

验证器应用接收到的无共识的事务

Validators apply received transactions without consensus

没有共识; 会导致分裂链

PROs: Very quick; suited to development, CONS: No consensus; can lead to divergent chains

适合开发

Example usage: Hyperledger Fabric V1



PBFT-based

实用的拜占庭容错实现

Practical Byzantine Fault Tolerance implementations

验证器是已知的并且是完全连接的

PROs: Reasonably efficient and tolerant against malicious peers, CONS: Validators are known and totally connected

合理的效率和容忍恶意对等点

Example usage: Hyperledger Fabric V0.6



Kafka/
Zookeeper

排序服务将块分发给对等点

Ordering service distributes blocks to peers

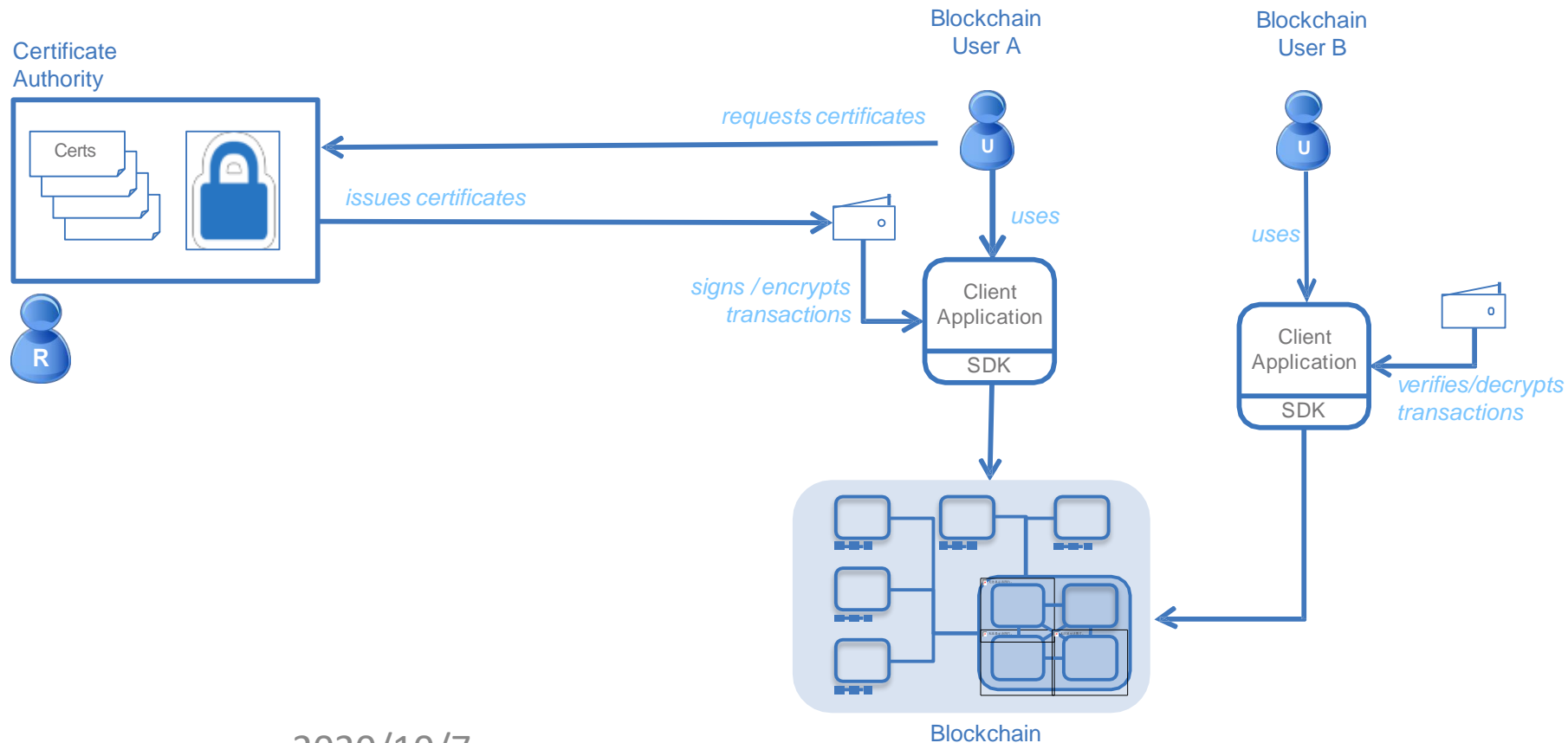
不防范恶意活动

PROs: Efficient and fault tolerant, CONS: Does not guard against malicious activity

高效和容错

Example usage: Hyperledger Fabric V1

Certificate Authorities and Blockchain



Other Nonfunctional Requirements

- **Performance**

- The amount of data being shared
- Number and location of peers
- Latency and throughput
- Batching characteristics

-共享的数据量
-对等点的数量和位置
-延迟和吞吐量
-批处理特性

考虑性能、安全性和弹性之间的权衡

**Consider the trade-offs
between performance,
security, and resiliency!**

- **Security**

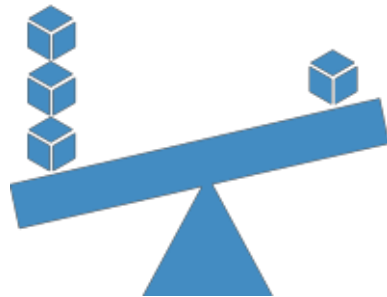
- Type of data being shared, and with whom
- How is identity achieved
- Confidentiality of transaction queries
- Who verifies (endorses) transactions

-要共享的数据类型，以及与谁共享
-身份认同是如何实现的
-交易查询的机密性
-谁验证(认可)事务

- **Resiliency**

- Resource failure
- Malicious activity
- Non-determinism




-资源失败
-恶意行为
-非确定性





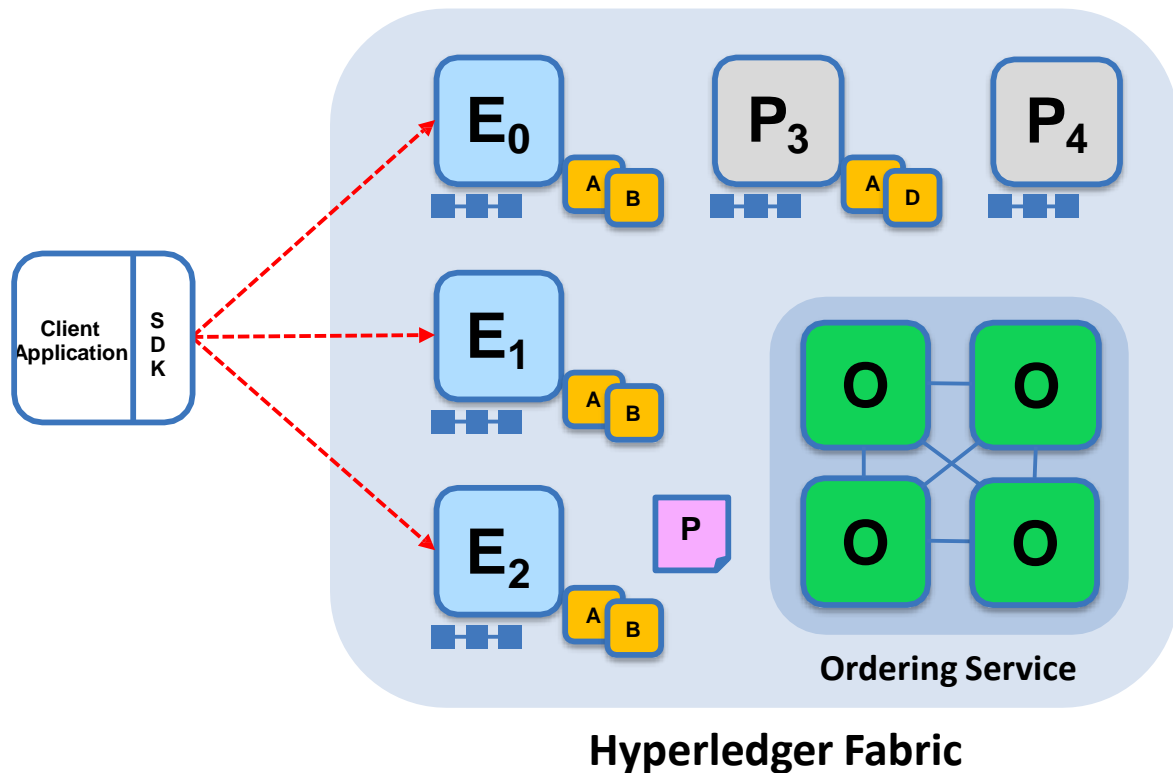
Blockchain Operations

Nodes and Roles in Hyperledger Fabric

	<p>提交Peer: 维护分类帐和状态。提交事务。可持有智能合约(链码)</p> <p>Committing Peer: Maintains ledger and state. Commits transactions. May hold smart contract(chaincode).</p>
	<p>Endorsing Peer: Specialized committing peer that receives a transaction proposal for endorsement, responds granting or denying endorsement. Must hold smart contract</p> <p>认可Peer: 接受认可交易建议, 回应批准或拒绝批准的专门提交peer。必须遵守智能合约</p>
	<p>Ordering Nodes (service): Approves the inclusion of transaction blocks into the ledger and communicates with committing and endorsing peer nodes. Does not hold smart contract. Does not hold ledger.</p> <p>排序节点(服务): 批准将交易块包含到总账中, 并与提交和认可的对等节点进行通信。不持有智能合同。不持有分类帐。</p>

Sample Transaction: Step 1/7 – Propose Transaction

提出交易



Application proposes transaction

Endorsement policy:

- “E₀, E₁ and E₂ must sign”
- (P₃, P₄ are not part of the policy)

Client application submits a transaction proposal for Smart Contract A. It must target the required peers {E₀, E₁, E₂}.

客户端应用程序为智能合约A提交一个交易建议，它必须以所需的对等点为目标

Key:

Endorser			Ledger
Committing Peer			Application
Ordering Node			
Smart Contract (Chaincode)			Endorsement Policy

Sample Transaction: Step 2/7 – Execute Proposal

背书人执行提案

Endorsers Execute Proposals

E₀, E₁ & E₂ will each execute the *proposed* transaction. None of these executions will update the ledger.

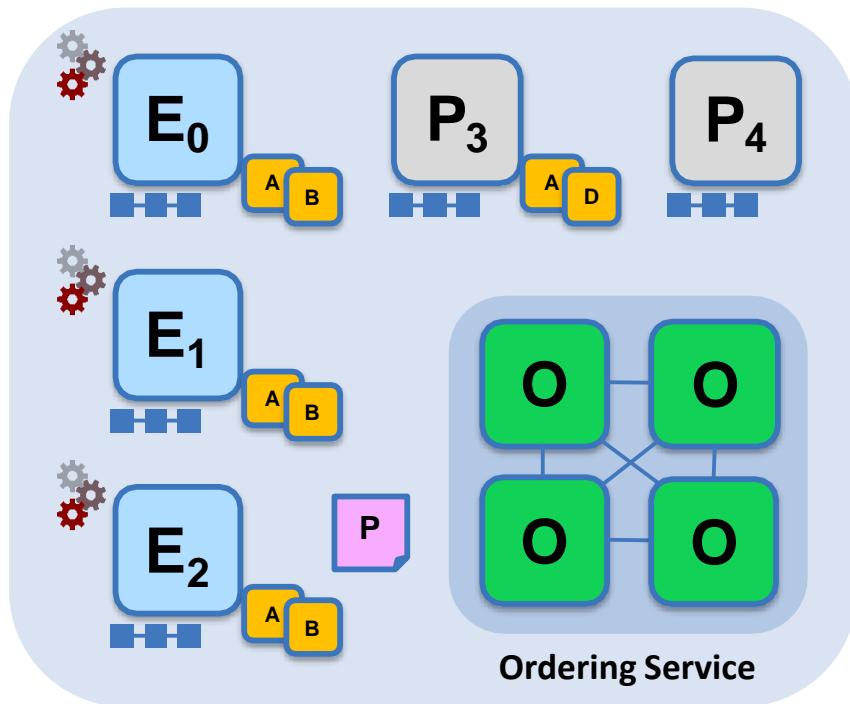
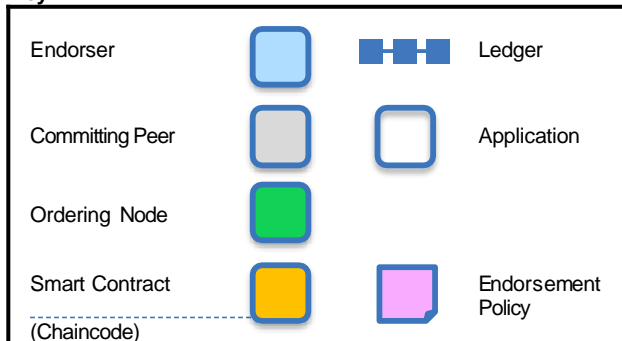
每次执行都会捕获被称为RW集的读和写数据集，这些数据现在将在 fabric 中流动

Each execution will capture the set of Read and Written data, called RW sets, which will now flow in the fabric.

可以对事务进行签名和加密

Transactions can be signed and encrypted.

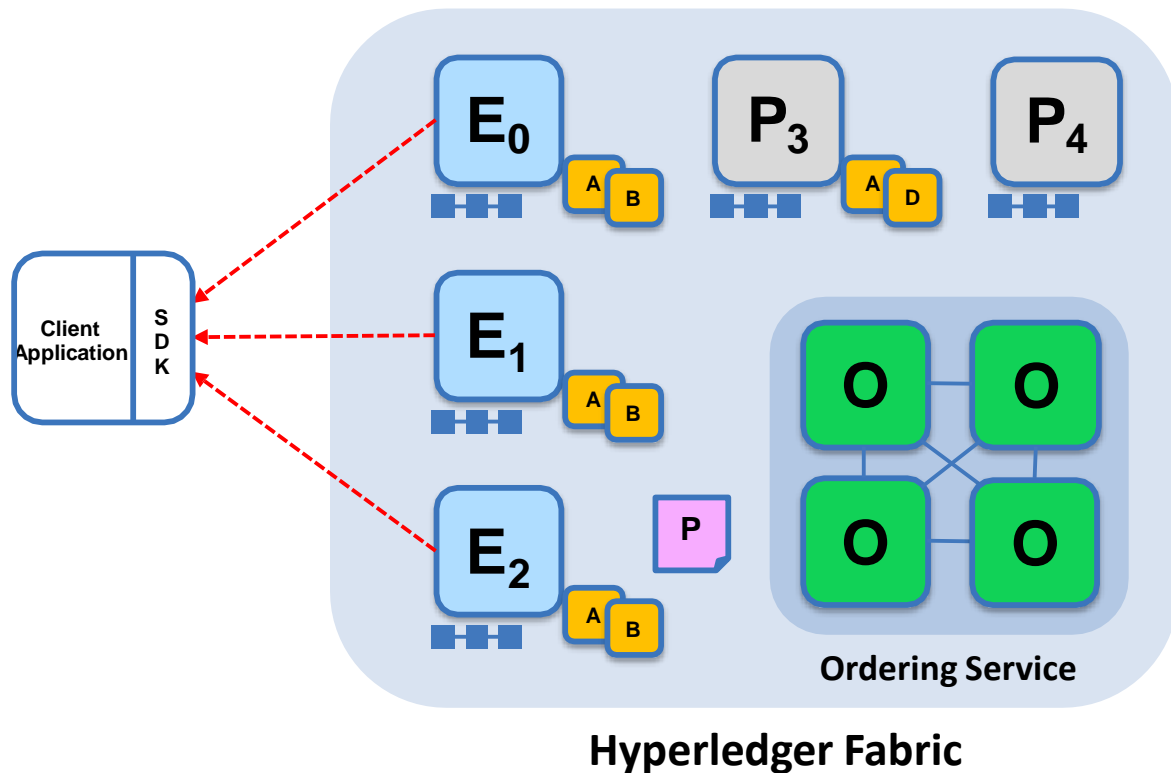
Key:



Hyperledger Fabric

2020/10/7

Sample Transaction: Step 3/7 – Proposal Response



Application receives responses

RW集被异步地返回到应用程序。

RW sets are asynchronously returned to application.

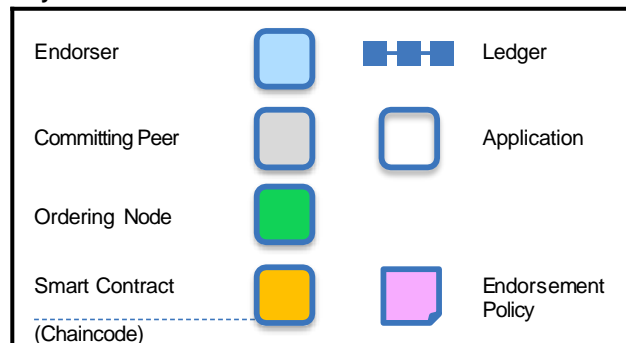
RW集由每个背书人签名，还包括每个记录版本号。

The RW sets are signed by each endorser, and also includes each record version number.

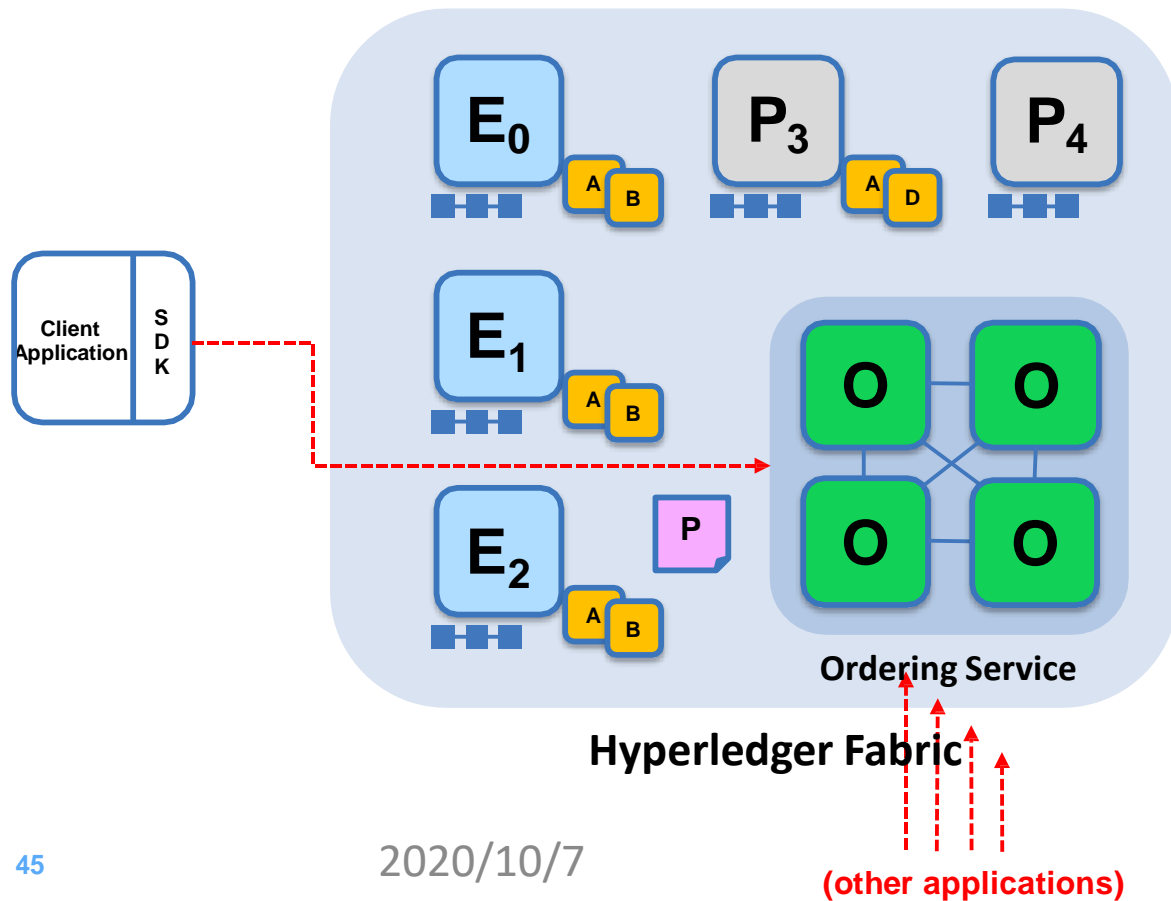
这一资料将在协商一致进程中稍后加以核查

This information will be checked much later in the consensus process.

Key:



Sample Transaction: Step 4/7 – Order Transaction



应用程序提交响应以排序
Application submits responses for ordering

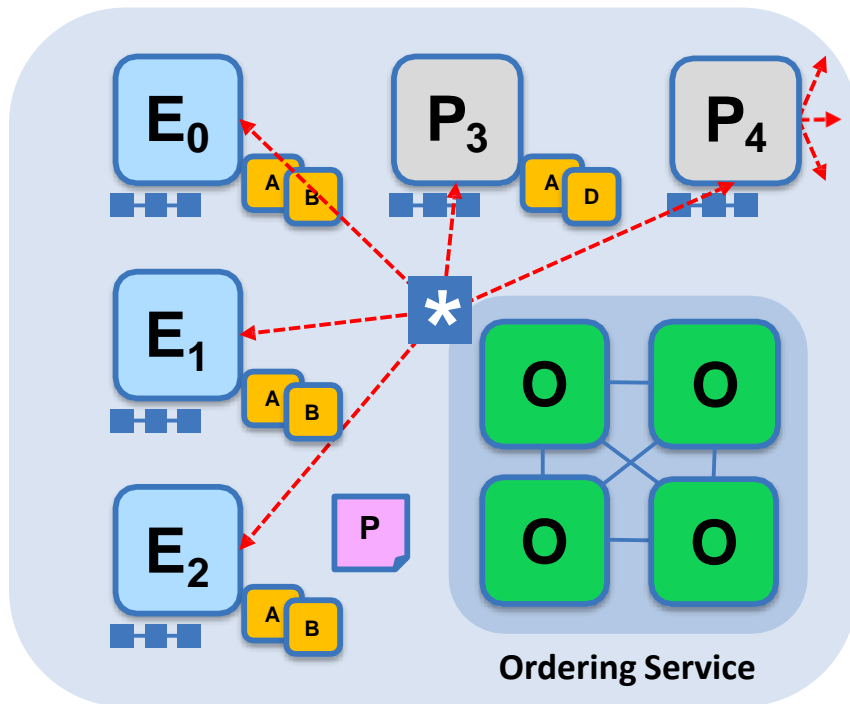
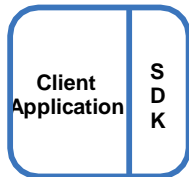
应用程序将响应作为一个待排序事务提交。
Application submits responses as a transaction to be ordered.

与其他应用程序提交的事务并行地跨Fabric进行排序
Ordering happens across the fabric in parallel with transactions submitted by other applications.

Key:

Endorser		Ledger
Committing Peer		Application
Ordering Node		
Smart Contract (Chaincode)		Endorsement Policy

Sample Transaction: Step 5/7 – Deliver Transaction



Hyperledger Fabric

排序点交付给所有提交方

Orderer delivers to all committing peers

排序服务将事务收集到建议的块中，以便分发给提交的对应点。对应点可以交付给层次结构中的其他对应点(未显示)

Ordering service collects transactions into proposed blocks for distribution to committing peers. Peers can deliver to other peers in a hierarchy (not shown).

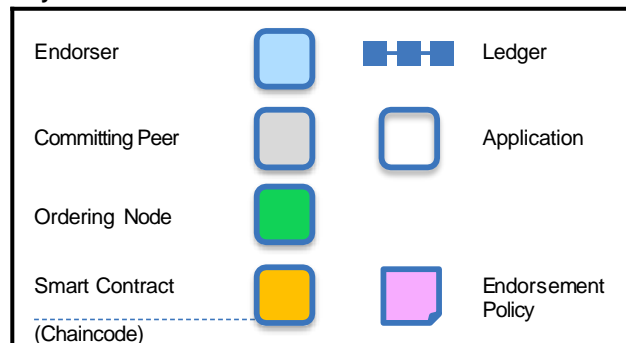
Different ordering algorithms available:

- SOLO (Single node, development)
- Kafka (Crash fault tolerance)

不同的排序算法:

- SOLO(单节点, 开发)
- Kafka(崩溃容错)

Key:



Sample Transaction: Step 6/7 – Validate Transaction

提交对等点验证事务

Committing peers validate transactions

每个提交对等方都根据背书策略进行验证。同时检查RW集对于当前世界状态仍然有效。

Every committing peer validates against the endorsement policy. Also check RW sets are still valid for current world state.

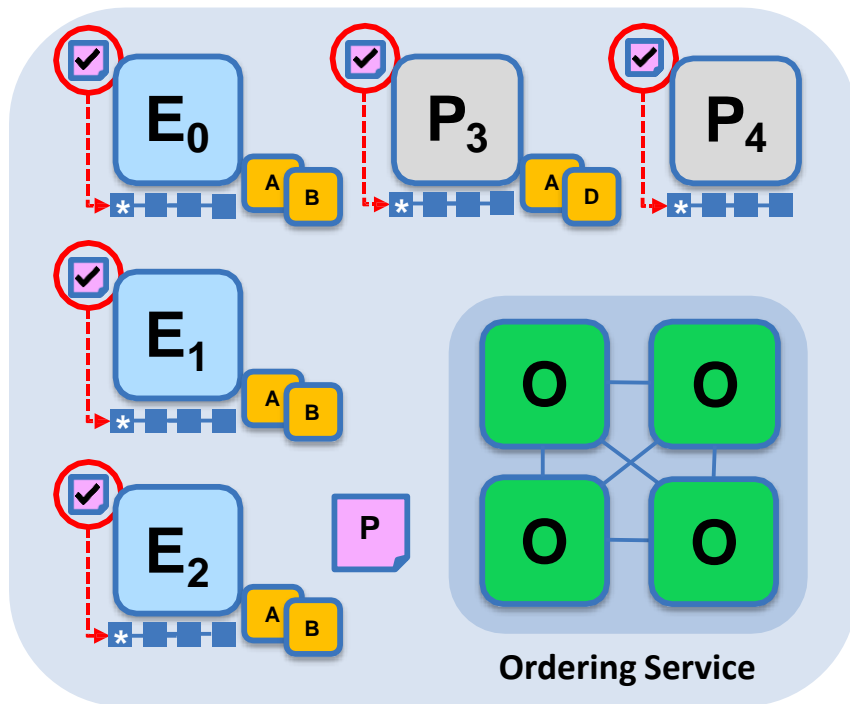
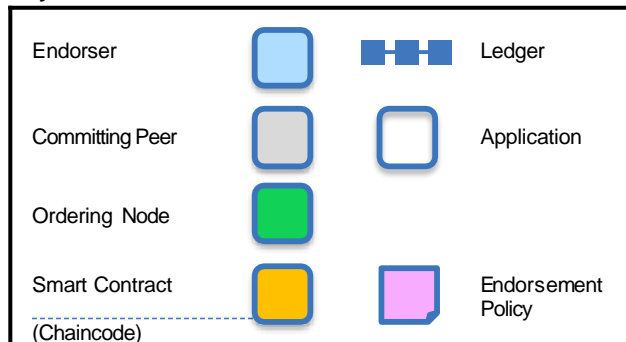
经过验证的交易应用于世界状态并保留在分类帐上。

Validated transactions are applied to the world state and retained on the ledger.

无效的交易也保留在分类帐上，但不更新世界状态。

Invalid transactions are also retained on the ledger but do not update world state.

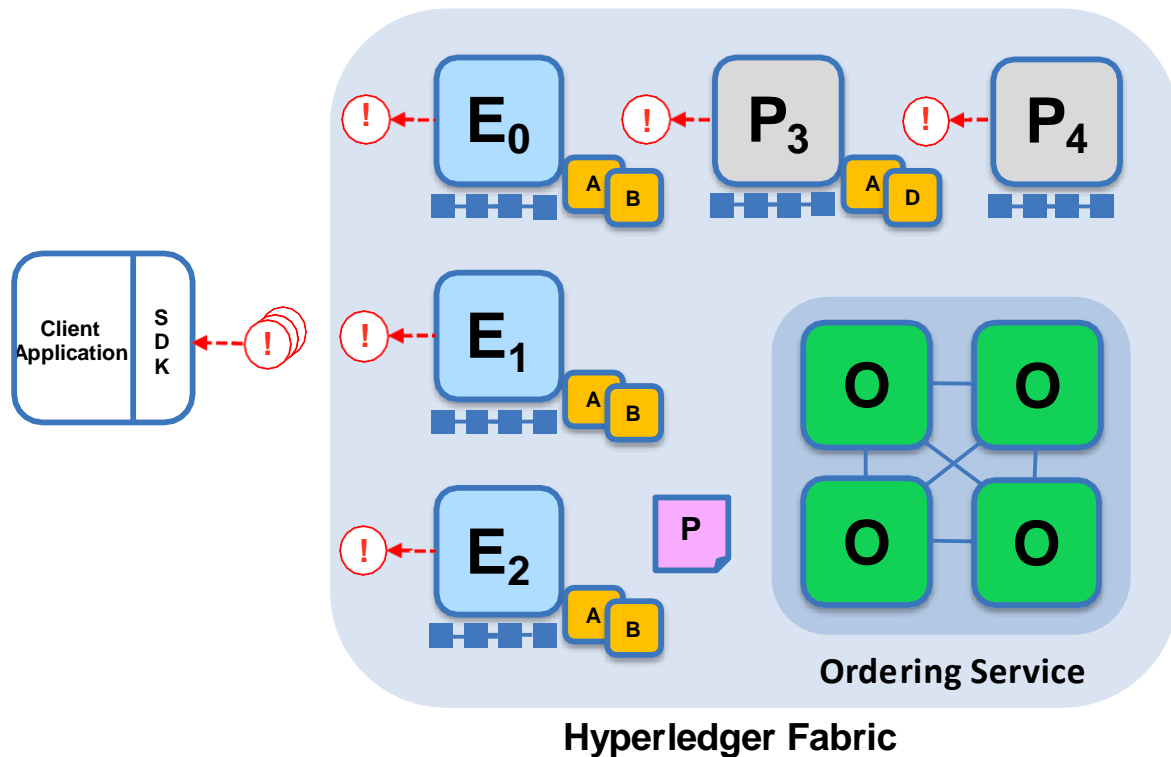
Key:



Hyperledger Fabric

2020/10/7

Sample Transaction: Step 7/7 – Notify Transaction



提交对等点通知应用程序 Committing peers notify applications

应用程序可以注册，以便在事务成功或失败以及块被添加到分类账时得到通知。

Applications can register to be notified when transactions succeed or fail and when blocks are added to the ledger.

应用程序将被连接的每个对等点通知。

Applications will be notified by each peer to which they are connected.

Key:

Blockchain Ecosystem	Hyperledger Fabric
Endorser	Ledger
Committing Peer	Application
Ordering Node	
Smart Contract (Chain code)	Endorsement Policy

Summary

We covered:

我们知道:

- Hyperledger Fabric的组成和结构, 以及你如何与之交互
- 区块链解决方案组件, 如钱包、账簿、参与者、共识、安全性和智能合约
- 帮助建立、建模、运行和维护区块链业务网络的主要考虑事项和职责:
 - 开发人员
 - 管理员
- 达成共识的方法
- 工具和应用程序, 您可以使用与网络交互

- The components and structure of Hyperledger Fabric and how you can interact with it
- Blockchain solution components, such as wallets, ledgers, participants, consensus, security, and smart contracts
- Key considerations and responsibilities of those who help to build, model, run, and maintain a blockchain business network:
 - Developers
 - Administrators
- Methods to arrive at consensus
- Tools and applications that you can use to interact with the network



Hyperledger Composer

截至2019年8月29日，Hyperledger Composer项目已处于废弃状态。没有一个维护人员在积极开发新特性。没有一个维护人员通过GitHub问题积极提供支持。但是，如果您希望通过pull请求提交代码更改，这些将被合并。

As of the 29th August 2019, the Hyperledger Composer project is in deprecated status. None of the maintainers are actively developing new features. None of the maintainers are actively providing support via GitHub issues. However, if you wish to submit code changes via pull requests, these will be merged.

强烈建议您使用Hyperledger Fabric v1.4+，它显著改善了开发人员的体验，包括一个新的编程模型。

It is highly recommended that you use Hyperledger Fabric v1.4+ instead, which features significant improvements to the developer experience, including a new programming model.

Hyperledger Composer是一个广泛的，开放的，开发工具集和框架，使开发区块链应用程序更容易。我们的主要目标是加速实现价值的时间，并使区块链应用程序与现有业务系统的集成更加容易。您可以使用Composer在几周而不是几个月内快速开发用例并部署区块链解决方案。Composer允许您为业务网络建模，并将现有系统和数据与区块链应用程序集成。

Hyperledger Composer支持现有的Hyperledger Fabric区块链基础设施和运行时，支持可插入的区块链共识协议，以确保事务根据指定的业务网络参与者的策略进行验证。日常应用程序可以使用来自业务网络的数据，为终端用户提供简单的、可控制的访问点。

What is Hyperledger Composer?

您可以使用Hyperledger Composer快速建模您当前的商业网络，包括您现有的资产和相关的交易；资产是有形或无形的商品、服务或财产。作为业务网络模型的一部分，可以定义与资产交互的事务。业务网络还包括与之交互的参与者，每个参与者可以跨多个业务网络与一个唯一的身份相关联。

- Hyperledger Composer is an extensive, open development **toolset and framework** to make developing blockchain applications easier. Our primary goal is to accelerate time to value, and make it easier to integrate your blockchain applications with the existing business systems. You can use Composer to rapidly develop use cases and deploy a blockchain solution in weeks rather than months. Composer allows you to model your business network and integrate existing systems and data with your blockchain applications.
- Hyperledger Composer supports the existing [Hyperledger Fabric blockchain](https://hyperledger.github.io/fabric) infrastructure and runtime, which supports pluggable blockchain consensus protocols to ensure that transactions are validated according to policy by the designated business network participants. Everyday applications can consume the data from business networks, providing end users with simple and controlled access points.
- You can use Hyperledger Composer to quickly model your current business network, containing your existing assets and the transactions related to them; assets are tangible or intangible goods, services, or property. As part of your business network model, you define the transactions which can interact with assets. Business networks also include the participants who interact with them, each of which can be associated with a unique identity, across multiple business networks.

Why use Hyperledger Composer?

- Blockchains provide a low-level interface for business applications
 - Smart contract code run on a distributed processing system
 - Inputs go into an immutable ledger; outputs to a data store
 - Applications are built on top of a low level of abstraction
- Hyperledger Composer
 - A suite of high level application abstractions for business networks
 - Emphasis on business-centric vocabulary for quick solution creation
- Features
 - Model your business network, test and deploy
 - Applications use APIs to interact with a business network
 - Integrate existing systems of record using loopback/REST
- Open Tools, APIs and libraries to support these activities
 - Exploits Hyperledger Fabric blockchain technology
 - Fully open and part of Linux Foundation Hyperledger

-区块链为商业应用程序提供了一个底层接口
· 智能合约代码运行在分布式处理系统上
· 输入进入一个不可变的分类账, 输出到数据存储
· 应用程序构建在较低的抽象级别之上

-Hyperledger设计者

- 一套用于业务网络的高级应用程序抽象
- 强调以业务为中心的词汇表, 以便快速创建解决方案

-特性

- 为您的商业网络建模, 测试和部署
- 应用程序使用api与业务网络交互
- 使用环回/REST集成现有的记录系统

-打开工具、api和库来支持这些活动

- 利用Hyperledger Fabric区块链技术
- 完全开放和部分Linux基金会Hyperledger

Business Application

Hyperledger Composer

Hyperledger Fabric

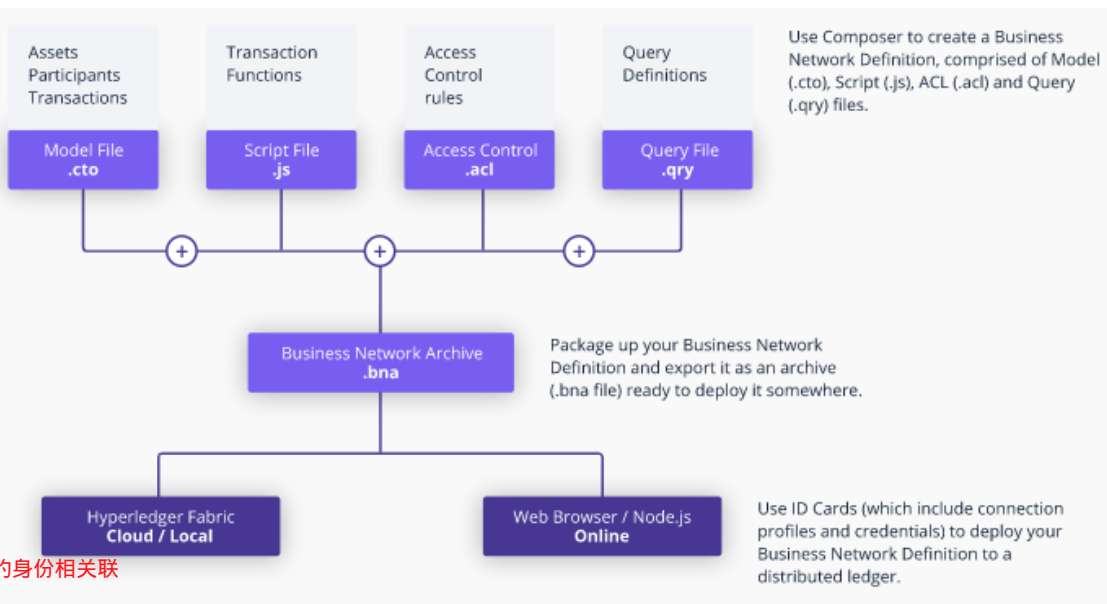
How to use Hyperledger Composer?

您可以使用Hyperledger Composer快速建模您当前的商业网络，包括您现有的资产和相关的交易；资产是有形或无形的商品、服务或财产。

- You can use Hyperledger Composer to quickly model your current business network, containing your existing assets and the transactions related to them; assets are tangible or intangible goods, services, or property.

作为业务网络模型的一部分，可以定义与资产交互的事务

- As part of your business network model, you define the transactions which can interact with assets.
- Business networks also include the participants who interact with them, each of which can be associated with a unique identity, across multiple business networks.



How does Hyperledger Composer work in practice?

For an example of a business network in action; a realtor can quickly model their business network as such:

举例说明运作中的商业网络; 一个房地产经纪人可以快速建立他们的商业网络模型如下:

- 资产: 房屋和房源
- 参与者: 购房者和房主
- 交易: 买卖房屋, 创建和关闭清单

- **Assets:** houses and listings
- **Participants:** buyers and homeowners
- **Transactions:** buying or selling houses, and creating and closing listings

- Participants can have their access to transactions restricted based on their role as either a **buyer, seller, or realtor**. The realtor can then create an application to present buyers and sellers with a simple user interface for viewing open listings and making offers.
- This business network could also be integrated with existing inventory system, adding new houses as assets and removing sold properties.
- Relevant other parties can be registered as participants, for example a land registry might interact with a buyer to transfer ownership of the land.

· 参与者可以根据他们作为买家、卖家或房地产经纪人的角色限制他们的交易权限。然后, 房地产经纪人可以创建一个应用程序, 为买家和卖家提供一个简单的用户界面, 以便查看公开的清单和报价。
· 这个商业网络也可以与现有的库存系统整合, 增加新的房屋作为资产, 并移除出售的房产。
· 相关的其他各方可以登记为参与者, 例如, 土地注册中心可能与买方交互以转让土地所有权。

Benefits of Hyperledger Composer



Increases understanding

Bridges simply from business concepts to blockchain

简单地从业务概念连接到区块链



Saves time

Develop blockchain applications more quickly and cheaply

更快、更便宜地开发区块链应用程序



Reduces risk

Well tested, efficient design conforms to best practice

经过良好的测试，有效的设计符合最佳实践

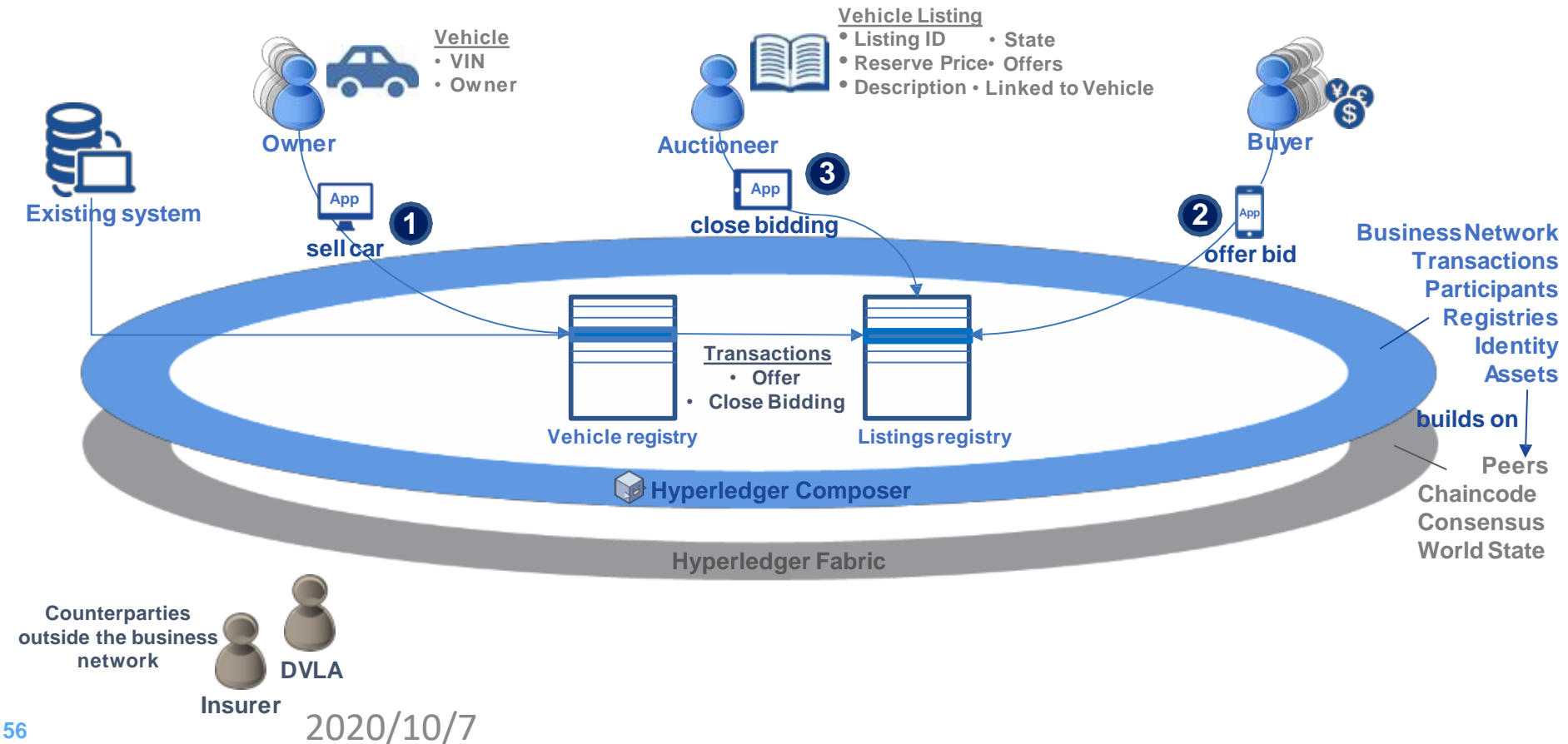


Increases flexibility

Higher level abstraction makes it easier to iterate

更高层次的抽象使迭代更容易

An Example Business Network – Car Auction Market



Conceptual Components and Structure of Composer

业务网络由模型、脚本文件、acl 和元数据定义，并打包在业务网络归档文件中

Business Network is defined by **Models, Script Files, ACLs and Metadata** and packaged in a **Business Network Archive**



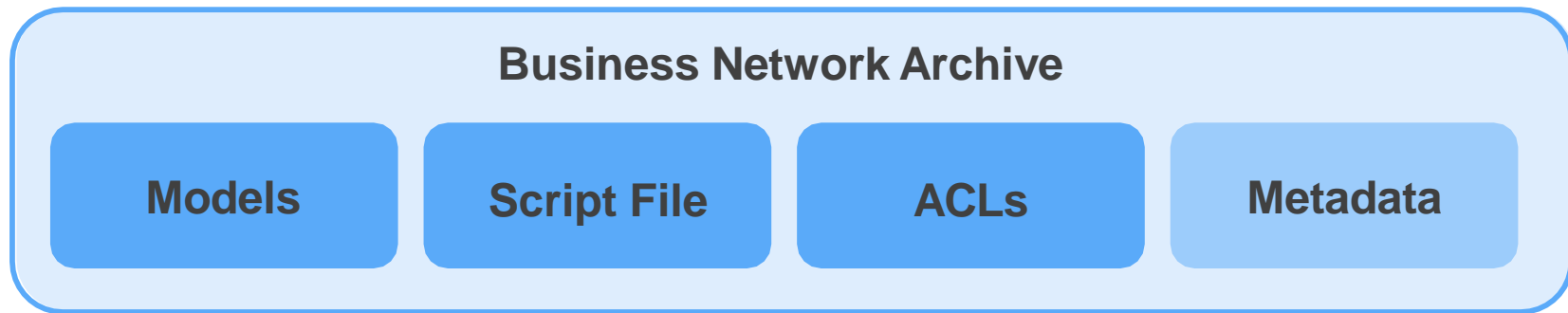
解决方案开发人员对业务网络建模，实现定义事务行为的脚本文件，并将其打包到业务网络归档文件中

Solution Developer models the business network, implements the script files that define transaction behaviour and packages into a business network archive



解决方案管理员提供目标环境并可以管理部署

Solution Administrator provision the target environment and may manage deploy



Extensive, Familiar, Open Development Toolset

```
asset Animal identi
  o String animal
  o AnimalType sp
  o MovementStatu
  o ProductionTyp
```

Data modelling



JavaScript
business logic



Web playground

```
composer-client
composer-admin
```



Client libraries



Editor support

\$ composer

CLI utilities



Code generation

Powered by



LoopBack
Node.js Framework



Swagger

Existing systems and
data

Topics

- ✓ **Blockchain Architecture**
- ✓ **Blockchain Fabric Development**
- ✓ **Blockchain Components**
- ✓ **Blockchain Operations**
- ✓ **Hyperledger Composer**

END !

धन्यवाद

Hindi

多謝

Traditional Chinese

ขอบคุณ

Thai

Спасибо

Russian

Gracias

Spanish

Thank You

English

شكراً

Arabic

Obrigado

Brazilian Portuguese

Grazie

Italian

多谢

Simplified Chinese

Danke

German

Merci

French

நன்றி

Tamil

ありがとうございました

Japanese

감사합니다

Korean