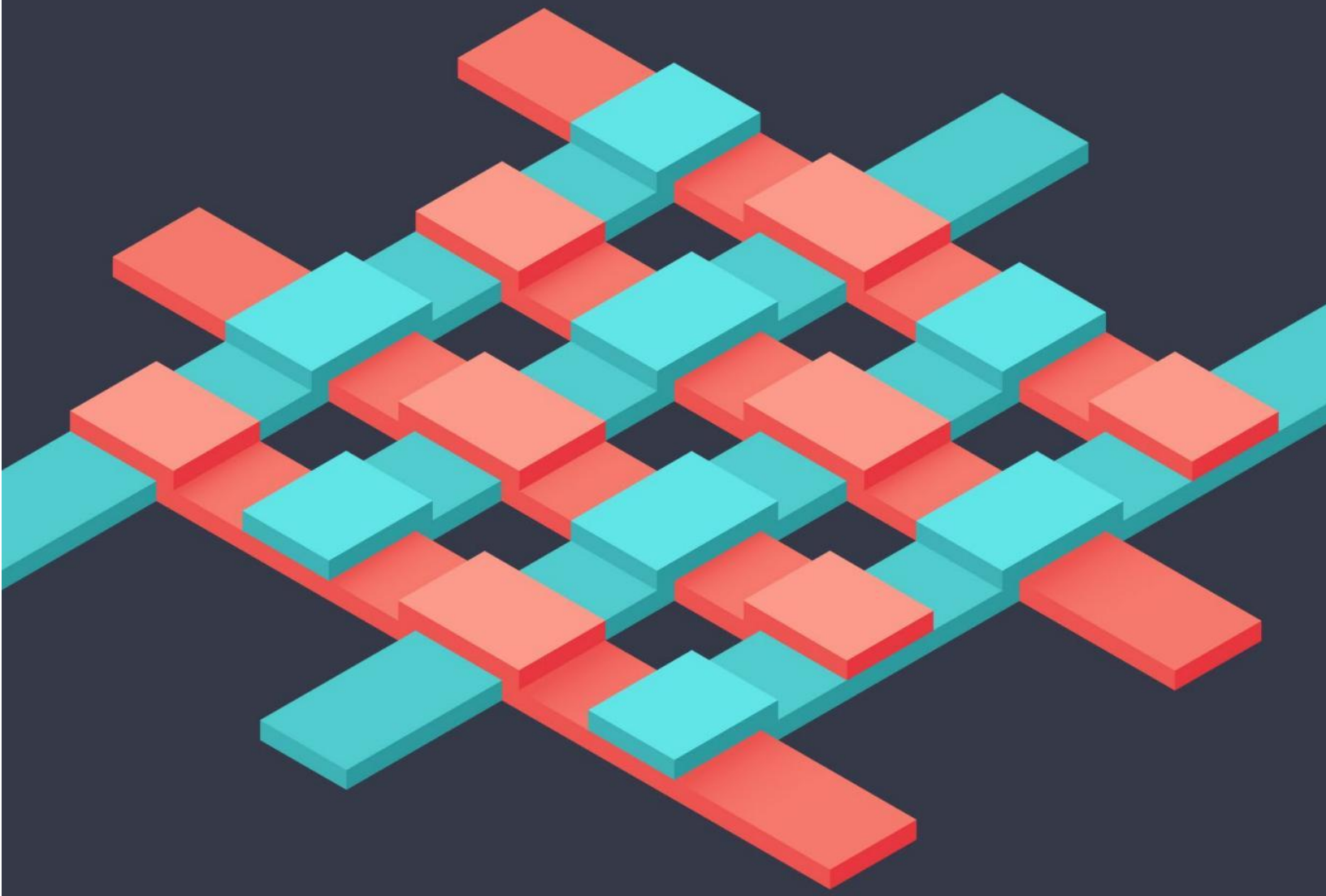
Hyperledger Fabric 2.0 架构安全报告



CSA GCR cloud security alliance® GREATER CHINA REGION

CSA cloud security alliance®

序言

区块链技术作为一种可以改变互联网底层基础设施的分布式账本技术，已经作为我国重点发展的战略性技术，逐渐在我国各行各业落地应用。

本报告聚焦贸易金融工作流程在 Fabric 中的落地实现，分析了 Fabric 体系架构在贸易金融工作流程运行时所面临的安全威胁，阐述了在云计算环境下，针对运行 Hyperledger Fabric 2.0 的许可链网络，如何通过“六步走”的策略，精准、有效地开展安全风险评估，最后从实战经验出发，提出了威胁缓解、安全事件响应准备的相关对策建议。值得金融行业安全从业者、风险控制管理者和金融行业监管机构参考。

李雨航 Yale Li

CSA 大中华区主席兼研究院院长

致谢

《Hyperledger Fabric 2.0 架构安全报告》(Hyperledger Fabric 2.0 Architecture Security Report)一文由 CSA 专家编写，CSA 大中华区秘书处组织翻译并审校。

中文版翻译专家组（排名不分先后）：

组　长：陈　钟

翻译组：卞乐彬　蒋蓉生　李安伦　刘广坤　茆正华　汤　霖

　　王　彪　姚　凯　于继万　余晓光　周利斌

审校组：卞乐彬　蒋蓉生　李安伦　刘广坤　茆正华　汤　霖

　　王　彪　姚　凯　于继万　余晓光　周利斌

感谢以下单位对本文档的支持与贡献：

北京启明星辰信息安全技术有限公司　　北京天融信网络安全技术有限公司

华为技术有限公司　　上海派拉软件股份有限公司

英文版本编写专家

项目负责人: Urmila Nagvekar

作　　者: Carlos Dominguez　Urmila Nagvekar

关键贡献者: John Carpenter　Frederic de Vaulx　Alex Ferraro　Ashish Mehta

　　Natividad Munoz　Teju Oyewole　Jyoti Ponnapalli　Ramesh Reddi

　　Michael Theriault　Huili Wang

CSA员工: Hillary Baron　Stephen Lumpe (Cover)　AnnMarie Ulskey (Layout)

审稿人: Goni Sarakinov　Kurt Seifried

在此感谢以上专家。如译文有不妥当之处，敬请读者联系 CSA GCR 秘书处给与雅正!

联系邮箱：research@c-csa.cn；云安全联盟 CSA 公众号。

目录

执行摘要

作为用价值互联网取代信息互联网的基础平台（Carter，2019），区块链技术正获得迅速应用（Global Blockchain Business Council，2020）（Global Blockchain Business Council，2020；霍夫曼等人，2020；Gartner，2020。由企业带来对外部业务工作流程的可追溯性和透明性，以及在不受信任和竞争激烈的业务环境中灌输信任和效率（IBM，2020）。考虑到许多外部业务工作流程涉及数字资产（欧盟委员会，2020）或其他高价值数据形式的交易和价值保管，隐私、保密性、完整性和可用性等网络安全属性无疑占据了区块链领域的中心舞台（Birge 等，2018）。[1]任何这些属性的妥协都可能导致严重的商业影响，即贸易损失、所有权损失和/或利益相关者之间的信任损失（Chia 等，2019）。

在这份面向金融行业安全和风险管理领导者和监管机构的 Hyperledger Fabric 2.0（Fabric 2.0）[1]架构安全报告中，我们旨在通过两种方式减轻上述业务影响：

1. 我们首先确定 Fabric2.0 的架构对网络安全属性（隐私、机密性、完整性、可用性）的风险（Angelis 等，2019），同时在基于云的环境中作为贸易金融业务的许可区块链企业网络实施。
2. 我们提供与 NIST 一致的完全可实施的“安全控制检查表”
   网络安全框架的控制措施[2]可主动预防、检测和应对上述风险，从而减轻因交易损失、信任损失和所有权损失而对贸易融资业务流程造成的下游业务影响。

由于本报告是云安全联盟（CSA）[3]的一部分，因此特意选择了一个云环境容纳 Fabric 网络，以利用 CSA 的专业知识安全地管理 Fabric 2.0 许可区块链网络的物理基础设施。

确定的风险范围和建议的相应安全对策已限制在 Hyperledger Fabric 2.0 网络环境的设计和开发阶段，以便使新加入 Hyperledger Fabric 的安全和风险管理领导者能够快速了解评估运营成本所需的相关组织风险，同时平衡安全需求与业务优先级。

---

1 Hyperledger Fabric 2.0 https://www.hyperledger.org/blog/2020/01/30/welcome-hyperledger fabric-2-0-enterprise-dlt-for-production

2 NIST CSF Framework https://www.nist.gov/cyberframework

3 Cloud Security Alliance https://cloudsecurityalliance.org/about/

主要调查结果

风险识别流程包括在云环境中的 Hyperledger Fabric 2.0 许可区块链网络上运行的典型进口商和出口商之间的贸易融资工作流程（Copigneaux&European Parliament，2020）。它贯穿于 Gartner 的区块链安全模型（Gartner，2018）的所有三个层面，即业务、风险和 IAM 流程以及技术/IT 层，并包括以下内容：

1.对贸易融资业务逻辑机密性和隐私的威胁评估以及执行和弹性
2. 区块链网络和 IAM 流程与贸易金融工作流运行时的威胁建模

当涉及到贸易金融业务逻辑和有效载荷保密性和隐私时，Fabric 2.0 许可的区块链网络发现在设计和默认方面是天然安全的。

它还可以防止对手在执行流程中操纵贸易融资的业务逻辑。

Fabric 2.0 架构威胁分析确定了 14 种[4]高影响和高可能性威胁，其中 50%源自具有“提升权限”的受损管理凭据。

上述发现表明，结构系统和证书颁发机构的分散管理，再加上缺乏可靠的治理策略保护管理通道和凭据不受危害，可能会大大扩大攻击面，从而有助于从在贸易融资网络中“建立立足点”，可能会危及整个 Fabric 网络，并导致贸易损失、所有权损失以及贸易融资工作流程中进口商和出口商之间的信任损失，从而造成严重的业务影响。

[4] “High” is as risk methodology definition described in Section “Risk Identification Process”

1 简介

1.1 概述 - Fabric 实现贸易金融的工作流

Hyperledger Fabric 2.0 许可区块链网络用于描述贸易融资工作流中的简单交易[5]:从一方到另一方的货物销售——来自不同国家的买方和卖方之间的传统复杂交易，没有共同的可信中介方确保出口商得到承诺的钱，进口商得到承诺的货物。

Fabric 具有不变［记录交易的永久性］和分布［跨多参与者网络的交易定义和验证］（IBM，2020 年）的固有属性。通过连接所有授权交易，金融参与者［进口商和进口商银行、出口商和出口商银行、承运人和监管机构］使用 Fabric 区块链分别在所有参与者之间同步分布式账本的交易状态，实现了这种传统工作流程的透明度和可追溯性。

为 Fabric 网络开发的基于软件的智能合约嵌入了贸易金融的业务逻辑：即进口商银行向出口商银行作出付款承诺，但分两期付款。 出口商从监管部门取得清关证明，将货物交给承运人，并取得收据。 收据的产生会触发从进口商银行到出口商银行的第一笔付款分期付款。 当货物到达目的港时，进行第二次也是最后一次付款，流程结束。 下面列出了此工作流程的详细信息。

1. 进口商以货币作为交换向出口商索要货品
2. 出口商接受贸易协议
3. 进口商向银行申请以出口商为受益人的信用证 (LC)
4. 进口商银行开具以出口商为受益人的信用证，并支付给出口商银行
5. 出口商银行代表出口商接受信用证
6. 出口商向监管部门申请 E/L
7. 监管部门向出口商提供 E/L
8. 出口商准备装运并交给承运人
9. (a)承运人在验证 E/L 后接受货物，并且(b)向出口商提供 B/L
10. 出口商银行向进口商银行索要一半货款
11. 进口商银行将一半金额转给出口商银行
12. 承运人将货物运送到目的地
13. 进口商银行将余款支付给出口商银行

[5] Trade finance scenario description and workflow diagram from Hyperledger Fabric GitHub Repository. See https://github.com/HyperledgerHandsOn/trade-finance-logistics.

以银行为中介的传统贸易金融工作流程及其相应的 Fabric 实现分别如图 1 和图 2 所示。

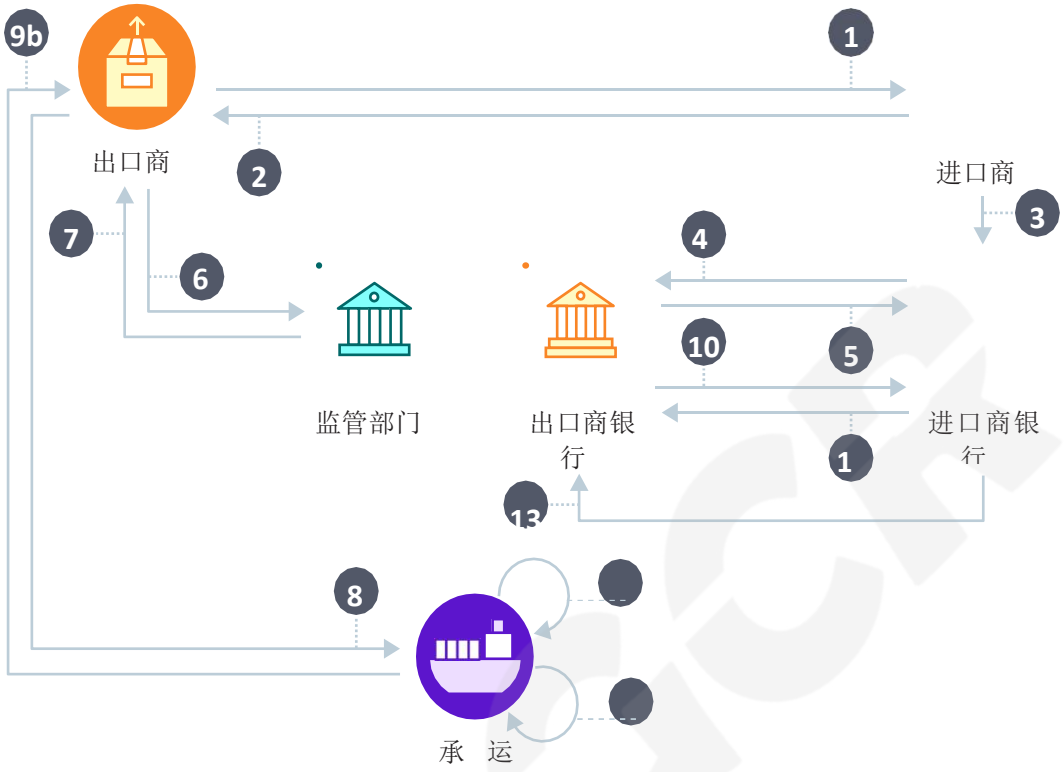


图 1：贸易金融用例的业务工作流图

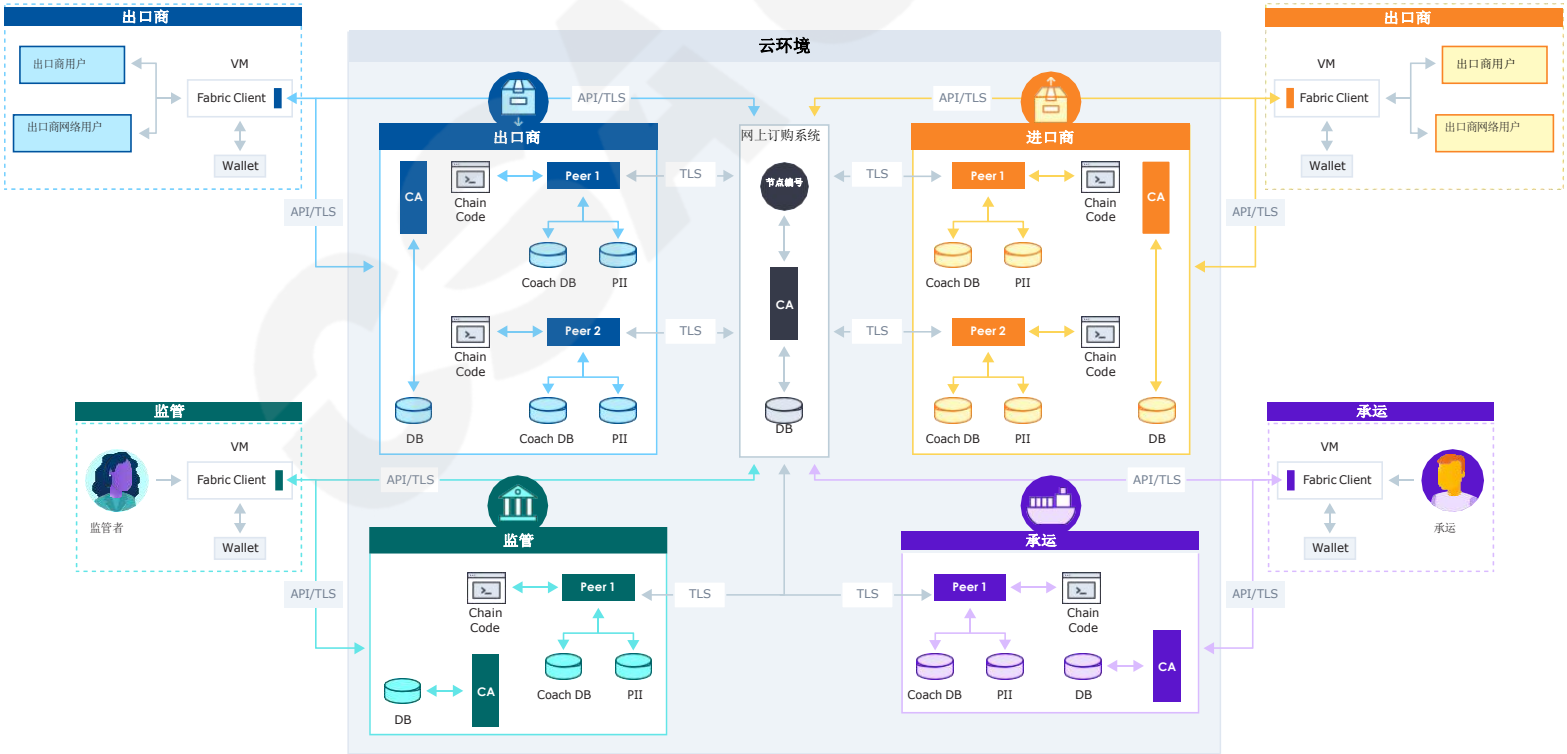


图 2:云环境下的贸易金融 Fabric 实现

区块链网络通常具有相当大的实施成本。 一个组织可以将其区块链实施与另一个合并以降低这些成本。 在图 2 中，进口商组织和进口商银行共同代表云端指定为“进口商”的 Fabric 节点，而出口商组织和出口商银行共同代表云端指定为“出口商”的 Fabric 节点。 通过在 Fabric 网络中称为“身份”的有效证书和密钥，允许访问 Fabric 节点。 每个 Fabric 利益相关者组织都拥有自己的证书颁发机构 (CA)，用于向其用户颁发“身份”。 为了使这些“身份”在登录期间可用，它们通常存储在称为“钱包”的存储库中，并且可以通过“Fabric 客户端”轻松访问，如图 2 所示。

贸易金融业务工作流包含在位于对等节点上的链码（即智能合约）中。 进口商组织的用户通过向出口商提交“货物”交易请求激活此工作流程。 Linux 基金会的 Accord Project[6]用于使这种基于软件的贸易金融工作流程与典型商业协议中的实际法律条款和义务绑定，以具有法律约束力。 Accord 项目是一项非营利性协作计划，旨在为称为智能法律合同的具有法律效力的机器可读协议开发生态系统和开源工具（欧盟委员会，2019 年）； 目标是帮助减少创建和管理商业关系时的摩擦和交易成本（Linux 基金会项目，2017）。

下面的图 3 和图 4 描绘了使用 Accord 项目的 Cicero 和 Ergo 工具为贸易金融工作流程开发的可执行智能合法供应协议的各个部分。

Smart Legal Supply Agreement for Trade Finance

This SUPPLY AGREEMENT (together with all schedules attached hereto, the "Agreement") is entered into as of {{ExecutionDate}} (the "Execution Date") between {{Exporter}}, a Delaware corporation ("Exporter"), having a principal place of business at 12345 Main Street, California 92705, and {{Importer}}, a company organized and existing under the laws of Sweden ("Importer"), with a place of business at 39E, TunaVagen Stockholm - SE114 55.

1.
Supply and Purchase of Products. {{Exporter}} shall supply and {{Importer}} shall purchase {{Product}} (the "Products", {{Shipment}}) in accordance with the terms of this agreement.

2.Creditworthiness Qualification for {{Importer}}. The {{Importer}} shall only be able to import {{Product}} based on their creditworthiness as determined in the sole and exclusive discretion of the {{ImporterLOCBank}}.

Letter Of Issue Date: {{IssueDate}}
{{ImporterCreditworthiness}}
L/C Number: {ImporterLOCNumber}}
{{ImporterLOCBank}} hereby issues this irrevocable documentary Letter of Credit, {{ImporterLOCNumber}} to {{Importer}} for {{ImporterLOCAmount}}.
An initial payment of {{% {{ImporterLOCAmount}}/2 %}} will be made immediately upon sight by a draft drawn against {{ImporterLOCBank}} in accordance with {{ImporterLOCNumber}}.
The draft is to be accompanied by the following documents:
1.{{OrderBillOfLading}}
2.{{PackingList}}
3.{{Invoice}}
The remaining {{% {{ImporterLOCAmount}}/2 %}} will be made upon acceptance of the {{Product}} by the {{Importer}} defined in section 6. below.

1.Orders.

1. Purchase Orders. The {{Importer}} shall submit all orders for {{Product}} to the {{Exporter}} in writing to the {{ExporterAddress}} and include in each {{PurchaseOrder}}
   2.each {{Product}} it is ordering, identified by model or part number,
   3.the {{AmountOfEachProduct}} it is ordering,
   4.the {{UnitPriceOfEachProduct}} it is ordering,
   5.the {{LocationForDelivery}}, and
   6.the {{DeliveryDate}}, allowing reasonable time for {{Exporter}} to receive, review, process the {{PurchaseOrder}}, and ship the {{Product}} by the {{DeliveryDate}}.
   7.the {{Importer}} {{ImporterLOCAmount}}

2.Accepting, Modifying, and Rejecting Purchase Orders

1. By Notice. Within {{TurnaroundTime}} Business Days' of receiving a {{PurchaseOrder}} from {{Importer}}, {{Exporter}} shall accept, reject, or propose a modification to the {{PurchaseOrder}} by sending the {{Importer}} written notice of its acceptance, rejection, or proposed modification.
2. Acceptance. {{Importer}} shall notify {{Exporter}} of its acceptance, rejection, or proposed modification of the {{PurchaseOrder}}.
3. An acceptance notice will include {{ExporterBankAccount}} information.
4. Modification of Purchase Order. {{Exporter}} may propose a modification to a {{PurchaseOrder}} by including in its notice to {{Importer}} a {{ModifiedPurchaseOrder}} for the {{Importer}} to accept or reject according to the acceptance and rejection procedures under paragraphs 3.b.i and 3.b.ii.
5. Canceling Purchase Orders. The {{Importer}} or {{Exporter}} may, at no expense to itself, cancel part or all of a {{PurchaseOrder}} up to {{CancellationDeadline}} Business Days before the {{DeliveryDate}}

图 3：贸易融资业务工作流的实际智能法律供应协议

[6] Accord Project https://accordproject.org/about

Smart Legal Supply Agreement for Trade Finance

2. **Bill of Lading**. This document will be issued by the {{Shipper}} to the {{Exporter}} once it takes possession of the {{Product}}. The Bill of Lading format will use following template:

{{Shipper}}
BILL OF LADING FOR OCEAN TRANSPORT
Shipper {{Exporter}}
BOOKING ID {{BookingId}}
Consignee {{Importer}}
Notify Party {{ImporterLOCBank}}
Place of Receipt {{ExportPort}}
Place of Delivery {{ImportPort}}
PARTICULARS FURNISHED BY {{Shipper}}
Description of Goods {{ProductDescription}}
Weight {{ProductWeight}}
Measurement {{ProductMeasurement}}
Freight Charges {{FreightCharges}}

Submission of the Bill of Lading to the {{ImporterLOCBank}} will trigger the first payment installation as documented in section 2 above.

3. Acceptance
   1. Acceptance of Delivery. The {{Exporter}} will be deemed to have completed its delivery obligations if
      1. the {{Importer}} notifies the {{Exporter}} in writing that it is accepting the {{Product}}. This will trigger the second and final payment installation as documented in section 2 above.
      2. Inspection and Notice. The {{Importer}} will have {{EvaluationTime}} Business Days to inspect and evaluate the {{Product}} on the {{DeliveryDate}} before notifying the {{Exporter}} that it is either accepting or rejecting the {{Product}}.
      3. Acceptance Criteria. If {{AcceptanceCriteria}} is true based on Annex B, attached to this agreement, then {{Importer}} shall pay {{Exporter}} {{% {{ImporterLOCAmount}}/2 %}}
4. Limited Warranty
   1. Warranty. The {{Exporter}} warrants that the Products
      1. will be free from material defects,
      2. are made with workmanlike quality, and
      3. will conform, within normal commercial tolerances, to the applicable specifications.
   2. Replacement Products. Subject to paragraphs 8.c and 8.d directly below, the {{Importer}} sole remedy for breach of this limited warranty will be the {{Exporter}} providing the {{Importer}} with a replacement {{Product}}, at the {{Exporter}} sole expense.
   3. Notice Requirement. The {{Exporter}} will only be required to replace {{Product}} under paragraph 10.2 if it receives written notice from the {{Importer}} of such defect or nonconformity within 90 days after delivery of the {{Product}}.
   4. Exclusions. This warranty does not extend to any {{Product}} the {{Importer}} abuses, neglects, or misuses according to the applicable documentation or specifications, or to any {{Product}} the {{Importer}} has had repaired or altered by a Person other than the {{Exporter}}.

图 4：提单（B/L），贸易金融业务工作流的智能法律供应协议的承诺和有限保证章节

1.2 Fabric 架构威胁模型的范围

由于风险识别主要侧重于在许可区块链网络的设计和开发阶段提供对 Fabric 2.0 架构风险的洞察。因此 Fabric 和 IT 运营环境以及智能合约软件和治理主题都超出了范围。

以下范围根据所选用例，由其架构和基础架构选择（云托管服务提供商）确定。 该范围缩小了已报告的 Hyperledger Fabric 威胁池中正在考虑的潜在威胁的数量，这些威胁的其中一些已被 Fabric 2.0 解决。(Baset 等,2018) (Dabholkar & Saraswat,2019)

1.2.1 适用范围

Fabric 规范:

> •Fabric 2.0 的身份和访问管理 (IAM) 和技术架构的详细威胁模型
> •Fabric 2.0 对业务逻辑隐私、机密性、执行和弹性的详细威胁评估
> •Fabric 信任边界
> •Fabric 子系统组件
> •Fabric 系统数据

•可插拔共识机制变体 (RAFT)[7]

•可插拔加密算法

•位于单个云服务提供商内的跨区域 Fabric 节点

通用:

•隐私监管要求-设计和默认安全

•使用现实生活中的金融用例进行威胁模型评估

1.2.2 超出范围

Fabric 规范:

•链码软件威胁模型

•跨多个云服务提供商的 Fabric 节点

•Fabric/IT 操作环境

•Fabric 网络治理

•去中心化的智能合约治理

•Fabric 网络与下游企业财务系统的集成注意事项

•深入分析加密算法以达成共识

•Fabric 证书颁发机构的 IT 组件（PKI、钱包或其他密钥存储选项）

通用:

•数据管理注意事项

•IT 流程/组件并非结构功能所独有

•（节点或客户端平台的变更和漏洞管理；Web 服务器；IT 通信网络等）

•用于 IaaS 实施的云服务提供商配置模块

[7] RAFT is the consensus mechanism in use by Hyperledger Fabric 2.0. See https://hyperledger-fabric.readthedocs.io/en/release-2.2/glossary.html?highlight=RAFT#raft.

2 风险识别流程

2.1 风险识别方法

风险识别流程是识别在云计算环境下，运行 Hyperledger Fabric 2.0 架构的许可链网络，买卖双方资金交易流程中的风险。风险识别流程贯穿了 2018 年 Gartner 提出的区块链安全模型的三个层级，即业务层、风险和身份识别与访问管理层、技术/IT 层，包括但不限于：

- 威胁评估不仅包括执行和恢复能力，还有资金交易业务逻辑的保密能力和隐私能力。
- 威胁模型分析运行 Fabric 2.0 架构的许可链网络，在身份识别与访问管理流程中，资金交易流程中的风险。

威胁模型分析采用 Shostack 在 2014 年提出的 STRIDE 方法，该方法包括确认架构信任边界、以及核查信息流、相关联数据、参与者、潜在威胁及其它活动。

2.2 商业交易业务逻辑的威胁评估

对 Fabric2.0 架构进行威胁评估的主要目的是为了确保资金交易业务逻辑、交易行为及交易内容的机密性和隐私性。

同时还评估了 Fabric2.0 架构在操作语义方面的脆弱性8，以确保智能合约中资金交易业务逻辑在执行流程中不会被非法者操作和控制，避免财物损失。

对 Fabric 2.0 架构专门进行了漏洞评估，这些漏洞是在以前非 Fabric 架构区块链中影响业务运行的罪魁祸首；(Dika & Nowostawski, 2018; Dingman 等, 2019; Perez & Livshits, 2020; Albreiki 等, 2020; Praitheeshan 等, 2020)。

这些脆弱性包括:

1、智能合约中的不确定性事务：执行非确定性事务可能会导致节点状态的不一致，从而导致产生分歧。由于区块链必须在执行交易后所有节点状态一致这一主要前提下运行，因此非确定性交易可能导致账本发生分叉。

2、交易重复：也称为“双花”，其中同一个数字资产状态包含在多个非法交易中，从而创

[8] The term “Operational Semantics” is used to indicate how the operational logic of the architecture was evaluated

建资产的新副本。

3、时间戳依赖性：引入依赖于块时间戳的逻辑触发的条件，然而该块时间戳不是智能合约逻辑的有效计时源。例如，使用块时间戳作为随机数生成器。

- 在超级账本结构中，交易延迟可以被计算为交易时间戳和交易块的块时间戳之间的延迟。在生成区块时，将为每个事务计算此指标。通过订阅超级账本的通道事件，可以为排序服务中被签名的每个块中的每个事务计算此指标。
- 由超级账本 SDK 签名的传出交易包含交易哈希和时间戳。这些信息可以发送到监控服（push）并由其跟踪。

4、事务排序依赖性：两个依赖事务调用同一个协定，并且这两笔交易归属于是同一块。在这种情况下，调用方希望调用的合同状态与执行时的实际状态之间存在差异。

5、第三方可信服务（Oracle）：第三方可信服务，通常称为 Oracle，是通过实施链外逻辑来扩展智能合约的机制之一，该逻辑将信任、可见性和透明度作为区块链网络的 QoS 维护（IBM，2019）。

评估结果详见“评估发现”章节

2.3 基于 STRIDE 模型的威胁分析

威胁模型详细评估了在 IAAS 云环境部署下，Hyperledger Fabric 2.0 许可链网络和 IAM（身份认证和识别管理）流程的风险。威胁分析步骤如下：

1. 识别 Fabric2.0 许可链网络的子系统
2. 标识和分解 Fabric 2.0 许可的网络信任边界（物理的、逻辑的）
3. 详细说明运行时 Fabric 2.0 许可网络上的商业交易工作流程
4. 基于 STRIDE 威胁模型在运行时识别商业交易工作流程中的漏洞。
5. 通过评估漏洞的可能性和影响确定风险
6. 根据网络安全功能域对漏洞分组、分类。

2.4 第 1 步-识别 Fabric 2.0 许可链网络的子系统

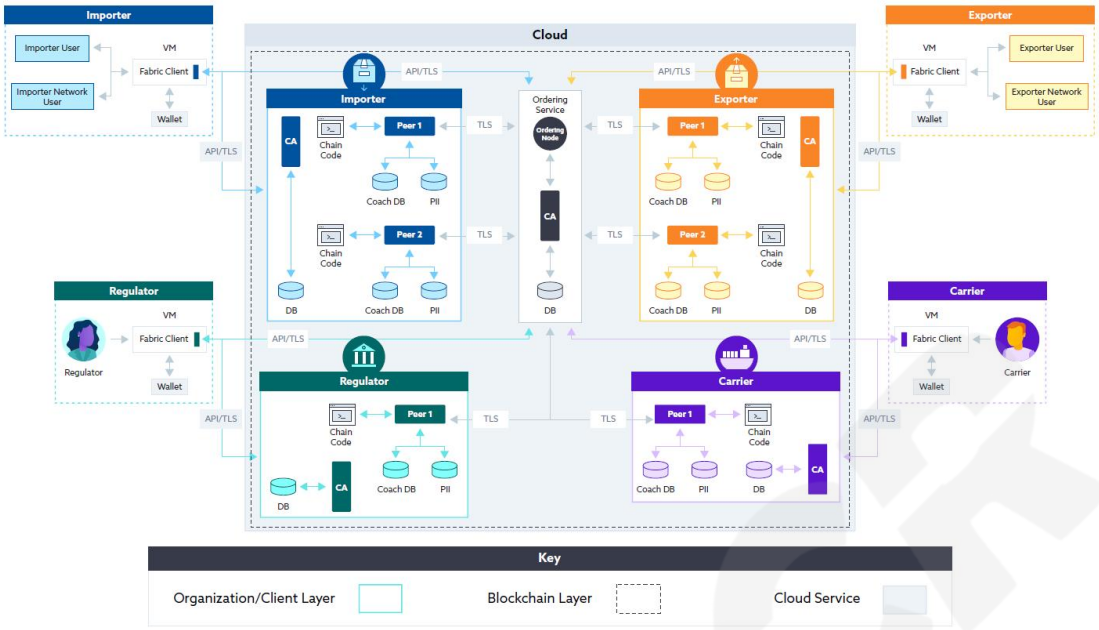


图 5：三层架构图

云环境中 IAAS 配置中的典型 Hyperledger Fabric2.0 实现将有三个不同层面，如上面的图 5 所示，它们共同组成了系统：

层级	描述
分布式网络，云服务服务商提供的数据中心（*在图5中，用“云”表示*）	这层是主要结构，它是位于云环境中的IAAS层上虚拟主机的网络节点上。 主要的组成部分是： • Fabr-CA（认证中心），含认证和认证服务提供给分布式客户端，点对点认证成员、申请认证等节点。 • 点对点、订单节点，交易流程中心 • 在对等节点上的链编码，交易流程触发 在点对点与订购之间、点对点与Fabric认证中心之间的通信协议是通过TLS实现。 两端点之间的通信是通过IP实现。 Fabric网络和客户端之间的通讯协议是TLS。 在点对点的链编码是在云docker容器内。
客户端网络，基于客户端（*在上面的图5中，由“进口商”、“出口商”、“承运人”和“监管机构”表示*）	在商业交易客户端这层中，构成者为进入、退出、载体、监管者。 他们的主机通过Fabric客户端的开发包提供的Fabric API登录。Fabric客户端开发包控制着客户通过使用一体化角色和基本访问控制属性。用户认证是是采用fabric网络认证用户和fabric的认证中心之间友好和信任关系，从而实现客户端和服务器之间的认证。 客户端网络上的导入程序调用链编码（智能合同）作为对进入者的交易加你请求的一部分。 此处启动了链编码在认可对等载体上执行，进而触发了业务交易的处理。 链编码驻留在Docker容器中。
组织节点网络，基于云服务数据服务中心（*“导入方”，由 蓝色阴影的*	如果共识策略是分散的，每一个组织都有自己的一组对等节点和可选的订购者节点. 每一个组织至少有一个认可对等节点和一个锚定对等节点。 事务的世界状态驻留在每一个对等节点的数据库中。

对等体和Fabric-CA; "出口商"用绿色阴影部分表示; 在上面的图5中，橙色阴影的对等点表示"承运人"，紫色阴影的对等点表示"监管者"，棕色阴影的对等点表示"订购服务"）	有选择的，为了遵循GDPR设计安全原则[9]，交易中任何私人或机密数据必须被存储.

2.5 第 2 步-解构/描绘 Fabric2.0 授权的网络可信边界（物理和逻辑）

2.5.1 物理信任边界

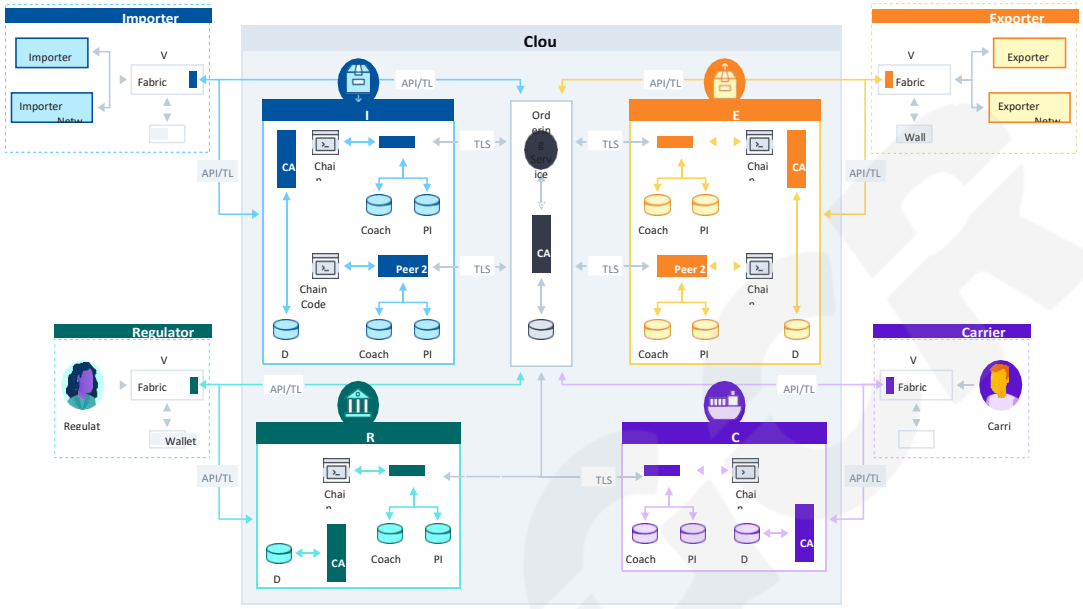
Hyperledger Fabric 网络作为 IaaS 配置组成部分应用在云环境，表 1.0 和图 6 将相应的显示下列物理信任边界。

范围	描述
Fabric 客户端 信任边界	该信任边界将搭载在云上的 fabric 环境和其他各类客户端环境隔离 进口商组织业务用户，出口商组织业务用户，组织用户的监管者和承运组织用户都可以通过 Fabric 客户端 API 接入 fabric 网络
云服务提供商 信任边界	该信任边界包含受攻击的 fabric 网络中的身份识别服务，订购服务和节点及其操作数据存储
订购服务 信任边界	该边界将对于 fabric 网络完整性来说很重要的主要信任模块与潜在的拜占庭对等系统和客户端隔离
成员服务提供商 信任边界	该信任边界在云内部向访问 fabric 对等节点和订购节点的已认证 fabric 客户端授权

[9] Local government regulations and laws supersede all recommendations made in this document.

对等信任边界	该信任边界包含单个组织的节点。组织内的节点彼此信任，但是不信任其他组织的节点

表1.0：Fabric 2.0信任边界



关键点：信任边界				
Fabric 客户端				**订购服务**
进口商	出口商	监督者	载体	
节点				
进口商	出口商	监督者	载体	

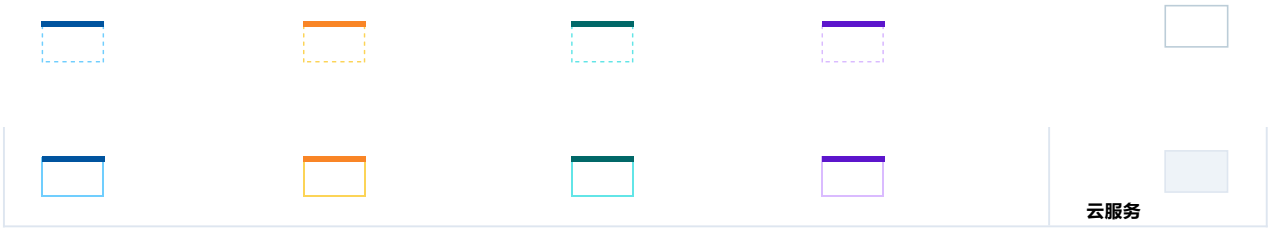


图 6：Fabric2.0 物理信任边界

2.5.2 逻辑信任边界

图 7 中的通道组成了逻辑边界，描述了在两个 实体之间如何隐秘的进行交易。Fabric 的链码实例化“应用程序通道”，仅允许组织中“需要知道”或者“需要交易”的节点之间彼此实施。“系统通道”就像 名称所表达的那用，用于对等节点之间和对等节点和订购节点之间的通信。成员服务提供方逻辑代表了由 Fabric 提供的服务，该服务授权“客户端”接入对等和订单节点。

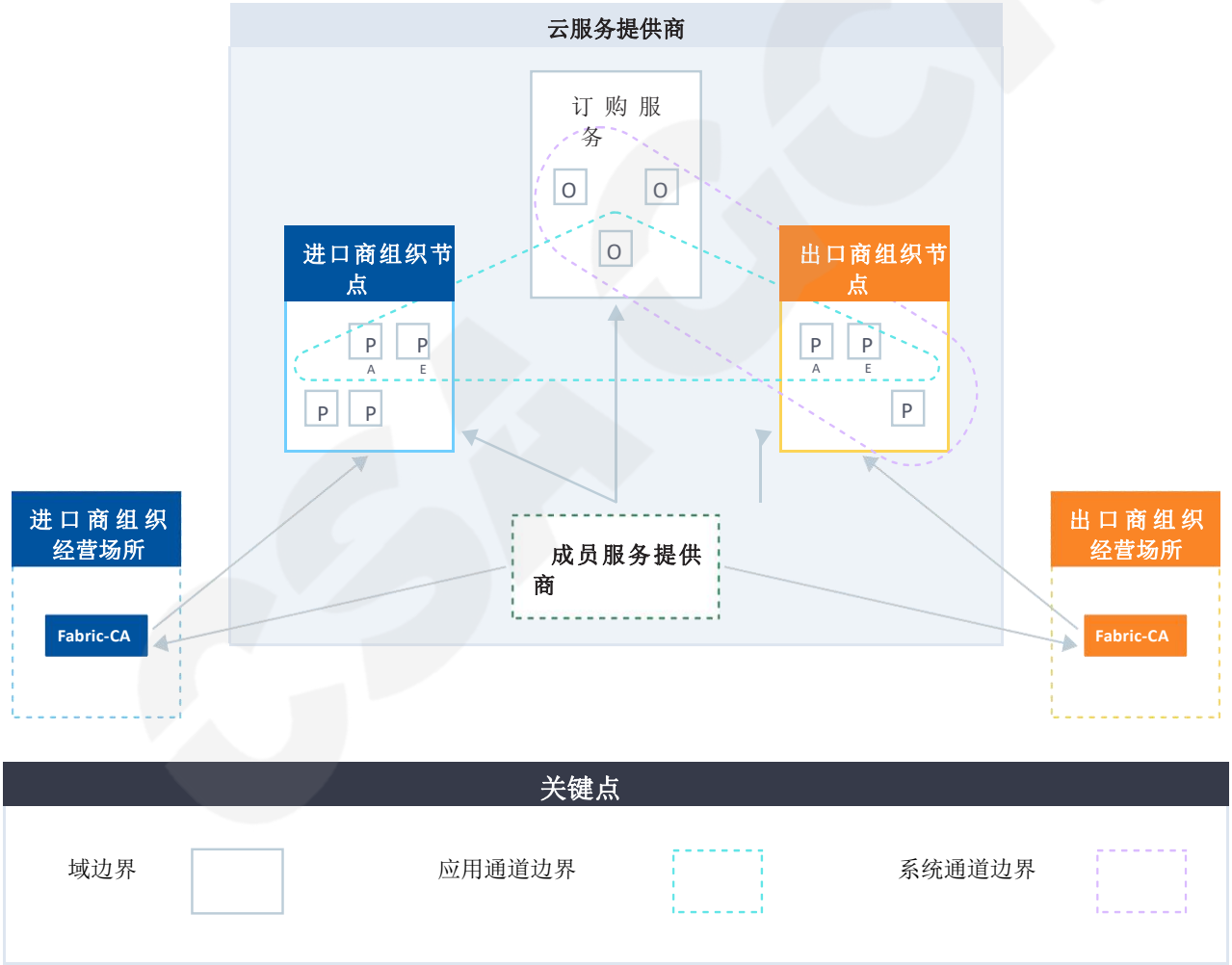


图 7：Fabric 2.0 逻辑信任边界

2.6 第 3 步-在 Fabric 2.0 授权网络运行时，交易金融工作流程的详细说明

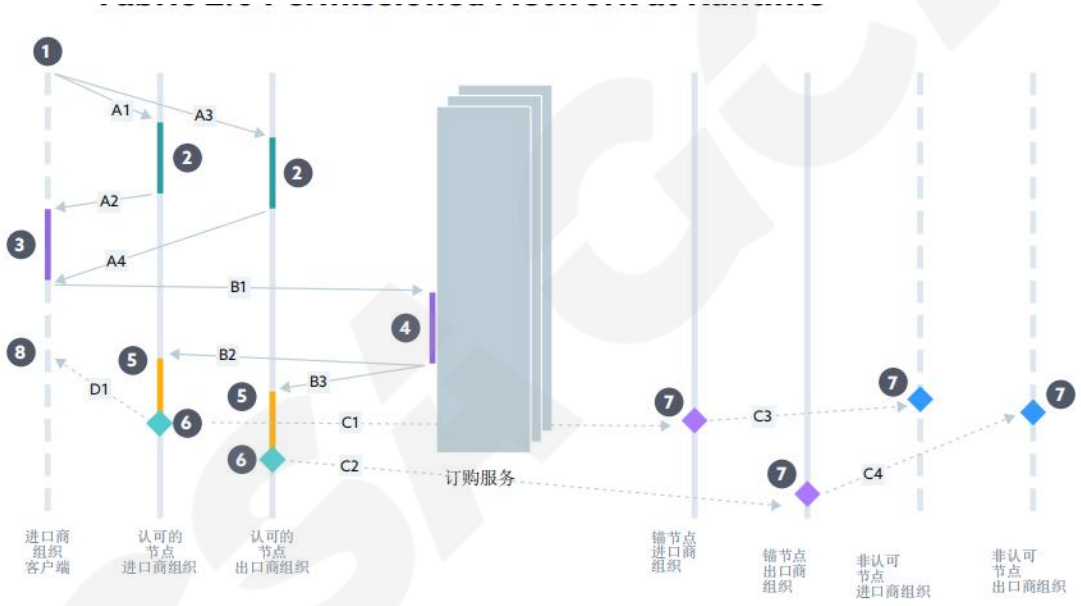


图 8:Fabric 2.0 中的私人贸易融资交易流程解构

图 8 以上详细说明了在 Fabic2.0 网络中，含有个人身份信息（PII）的交易从开始到结束的流程。

- 步骤 1（A1,A3）-进口商组织客户调用智能合约，该合约包含由通道中认可的节点签署的私有交易提案，其中认可的节点是被通道成员根据认可策略事先指定的。
- 步骤 2（A2,A4）-认可的节点根据本地分类账本执行本地安装的智能合同，从而向进口商组织客户发送提案响应。私有交易中的实际 PII 被隔离存储在认可的进口和出口组织节点的数据库中，在提案相应中由监督者和载体组织以哈希值的形式发送，以防止对于 PII 的未授权访问。

- 步骤 3：（B1）-进口商组织客户收集提案响应，当达到满足背书政策的规定数量时，将其发送给订购服务。
- 步骤 4：（B2,B3）(B4,B5)-运行 RAFT 的订购服务订购交易，该交易来自于同一通道中的其他客户端，将这些客户端分组为的哈希链序列区块，并将这些区块分发给认可的节点。
- 步骤 5：在通道中的认可节点验证交易区块
- 步骤 6：认可的节点根据分类账本确认交易，区块链世界状态被新的交易区块更新
- 步骤 7：（C1,C2）(C3,C4)-确认后的交易发送给锚节点，并进一步发送给非认可节点
- 步骤 8：（D1）-被确认的结果通过智能合约提示给进口商组织客户

2.7 第 4 步 使用 STRIDE 识别金融交易流程中的漏洞

“STRIDE”是微软的威胁建模方法，该方法可以对在 Fabric 2.0 许可网络上执行的贸易结算工作流进行详细的威胁分析(Shostack, 2014)。 图 9 列举了“STRIDE”所代表的几种威胁。

图 9 拓展 STRIDE

“STRIDE”威胁分析包括识别 Fabric 系统中的漏洞，这些漏洞可能被跨各种 Fabric 信任边界的工作流的枚举威胁所利用，即 Fabric 客户端、订购服务、成员服务提供者和对等信任边界。这些威胁已经在步骤 2 中的表 1.0 列出。对已识别漏洞进行的风险综合评级见步骤 5 中的图 13。

这些工作是云服务联盟(CSA)的一部分，CSA 的云控制矩阵(CCM)已被用于保护云服务提供的商用信任边界(见表 1.0)以及 Fabric 网络实现的物理基础设施层。

图 10 显示了一个示例应用程序，该应用程序用于传输事务协议，该程序的跨客户信任边界从入口的组织节点流向对等点。

注意:此工作的目标是深入了解业务工作流如何受到 Fabric 架构设计漏洞的影响。因此，常见的 IT 威胁(如“提升权限”的 Fabric 管理帐户的破坏)的来源并没有被深入研究，而是关注于这种破坏对贸易结算业务工作流的后果。

金融交易客户端信任边界						
动作：调用链码	进口商客户端@进口商组织		数据流（>>>>、<<<<）		同行背书	
Stride 方法论	漏洞	缓解方法	漏洞	缓解方法	漏洞	缓解方法
电子欺骗	客户端主机被盗用；交易提案挟持	终端设备安保需要到位	-	-	-	-
	客户端未撤销的过期数字凭证被恶意参与者欺骗，以扩展授权发送事务协议	Fabric 具有生成证书吊销列表的能力	-	恶意节点冒充有效客户端	Fabric 本身允许在节点级别进行签名验证	-
数据篡改	链码访问控制策略被篡改，包括未注册用户	确保只有 Fabric 管理员才能访问链码访问控制策略	未加密的事务协议在互联网上从客户端流向背书对等体时被拦截	确保通过 TLS 进行数据传输	同行使用被盗用的本地账本进行破坏	-
身份否认	API 访问日志丢失，无法追踪管理员[在生产环境]和开发人员在开发环境中的系统操作	-	-	-	-	-
数据泄露	-	-	专有交易数据因交易提案被拦截而泄露	在需要保证机密性的场景下加密交易提案	自营交易的机密性向渠道中组织的所有认可同行披露;这些同行包括 MSP 管理员和 Orderer 管理员	在需要保证机密性的场景下加密事务协议

服务拒绝	-	-	-	-	不受信任的链码对背书同行发起 DoS 攻击	使用 Docker 容器运行不可信链码
权限升级	由于 Fabric 客户端直接调用区块链网络的 API，Web 或终端设备的漏洞很可能会危及 Fabric 管理员或 MW 管理员帐户	使用中间件层将客户端 API 与区块链网络 API 隔离	-	-	-	-

图 10 ：进口商交易提案传输期间的客户端信任边界中对 STRIDE 的应用

2.8 第 5 步 通过对漏洞的可能性和影响进行评级以定义风险

使用 STRIDE 确定的漏洞对可能性和影响进行评级，并定义对 Fabric 2.0 网络的危害风险。如下面的图 11 [10]所示，可能性包括对攻击强度、漏洞流行度[11]和漏洞可检测性[12]进行评级，而影响是通过对攻击强度所利用的漏洞的技术影响进行评级确定的。评级分数是根据主题专家对漏洞细节的判断分配的。

风险评估方法不是一个定量的风险计算，而是一个定性的计算。使用定性方法来支持定义威胁模型的结果，一个经典的例子就是 STRIDE 的模型，该模型是根据设计流程中存在的技术因素得出分析结果的行业实践(Jones, 2019)。根据行业报告(Allianz,2021 年,Crowdstrike, 2021 年,Verizon, 2020 年)，攻击载体背后的行动者被认为是高级持续性威胁(APT)[13]。APT 威胁具有相对较高的接触频率的操作简化风险计算。

评分	攻击强度	漏洞流行度	漏洞可检测度	漏洞影响
3	容易	普及	容易	强
2	中等	寻常	中等	中等
1	困难	不寻常	困难	弱

可能性=中等(攻击强度，漏洞流行度，漏洞可检测性)

风险等级=可能性/影响

图 11：通过可能性和影响来计算风险

10 Figure 11 is a simplified version of OWASP Risk Rating Methodology. See https://owasp.org/www community/OWASP_Risk_Rating_Methodology

11 As defined by MITRE “How frequently this type of weakness appears in software” See: https://cwe. mitre.org/cwss/cwss_v1.0.1.html

12 As per OWASP Risk Factors defined as “How easily is to be detected by an attacker”. See: https:// owasp.org/www-project-top-ten/2017/Details_About_Risk_Factors

13 Refer to APT definition: https://en.wikipedia.org/wiki/Advanced_persistent_threat

风险等级[14]的计算方法是将技术影响等级和漏洞等级(攻击强度、漏洞流行度、漏洞可检测性)的平均值相乘。 图 12 是一个例子，该漏洞的风险等级为 7，计算方法为中等(3,2,2)* 3。注:风险等级是四舍五入到最接近的整数。

攻击强度	漏洞流行度	漏洞可检测度	漏洞影响
3 - 容易	2 - 寻常	2 - 中等	2 - 强
可能性= 中等 (3, 2, 2) = 2.3			风险等级 = 7

图 12：简单风险等级计算

上述例子的风险值为：

- 攻击强度：3
- 漏洞流行度：2
- 漏洞可检测性：2
- 漏洞影响：3

风险等级结果可以分为高、中和低，如下图所示：

- 低风险因子小于等于 3
- 中风险因子在 4 和 6 之间
- 高风险因子在 7 和最大值 9 之间

图 13 展示了一个简单的风险列表以及其对应的风险等级

14 The Risk Rating calculation is also a simplified version of OWASP Risk Rating Methodology

漏洞	攻击者属性	攻击强度	漏洞流行度	漏洞可检测度	漏洞影响	风险 低: <=3; 中: 4<=6; 高:7<=9
恶意参与者危及客户端：通过链码在背书政策中注入未经授权的节点列表作为背书点	黑客/犯罪组织	1	1	1	1	1
恶意参与者危及Fabric 管理员 账户：从Orderer Org的Fabric 管理凭证获得访问权限，该Orderer Org拥有背书策略	黑客/犯罪组织	3	3	3	3	9
被攻击的Fabric 管理员账户，用于实例化不可信的链码	黑客/犯罪组织	3	3	3	3	9
被攻击的Fabric管理员删除所有详细记录恶意活动的日志	黑客/犯罪组织	3	3	3	3	9
组织Fabric管理员或Orderer Fabric管理员的数字凭据在传输到外部客户端组织Fabric管理员时被攻击	黑客/犯罪组织	3	3	3	3	9
Fabric共识机制的服务提供者可以通过修改随机间隔来影响共识(订购)服务的一致性和可用性，从而操纵RAFT的领导者选举流程	内部组织	1	3	1	3	4
Fabric共识机制的服务提供者可以通过修改随机间隔来影响共识(订购)服务的一致性和可用性，从而操纵RAFT的领导者选举流程	黑客/犯罪组织	2	3	1	3	6
Orderer Org Fabric 管理员帐户被攻破，以获得对运行RAFT共识机制的Orderer Leader节点的复制日志的未经授权访问，导致违反机密性原则	黑客/犯罪组织	2	3	2	3	9
托管运行RAFT共识机制的Orderer Leader节点的归档复制日志的离线数据存储被破坏，导致违反机密性原则	黑客/犯罪组织	2	3	2	3	7

图 13：风险及其对应的风险等级

2.9 第 6 步-按功能区域将漏洞分组

为了使“控制措施清单”可交付给企业以帮助企业准备就绪，Fabric 网络中已识别的漏洞按网络安全功能区域组织，这些功能区域可以与企业现有的网络安全技能集和能力无缝集成，从而明确角色、责任和问责制的界限，从而可以更轻松地跟踪、管理和报告关键漏洞。

这些网络安全功能区域很容易[15]映射到各种网络安全框架中的“域或系列”，如 ISO 27001/27002 Ver 2013[16] 或 NIST 800-53 Rev4[17]，从而允许与外部框架交叉，以符合金融行业法规要求。

15 The mapping this report Functional Areas to Cybersecurity frameworks is not included in this report

16 ISO 27001/27002 Ver 2013 https://www.iso.org/standard/54533.html

17 NIST 800-53 Rev4 https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final

图 14 确定了报告中包含的网络安全功能区域，而图 15 将识别出的漏洞及其风险评分按相应的网络安全功能区域分组。

网络安全功能区域		
应用程序安全	共识安全	数据保护和密码学
终端设备和服务器安全	身份和访问管理	事件响应
对等网络安全	系统管理	

图 14：网络安全功能区域

网络安全功能区域	漏洞	攻击者属性	攻击强度	漏洞流行度	漏洞可检测度	漏洞影响	风险 低: <=3; 中：4<=6; 高：7<=9
终端设备和服务器安全	恶意参与者危及客户端：通过链码在背书政策中注入未经授权的节点列表作为背书点	黑客/犯罪组织	1	1	1	1	1
身份和访问管理	恶意参与者危及Fabric 管理员 账户;从Orderer Org的Fabric 管理凭证获得访问权限，该Orderer Org拥有背书策略	黑客/犯罪组织	3	3	3	3	9
身份和访问管理	被攻击的Fabric 管理员账户，用于实例化不可信的链码	黑客/犯罪组织	3	3	3	3	9
身份和访问管理	被攻击的Fabric管理员删除所有详细记录恶意活动的日志	黑客/犯罪组织	3	3	3	3	9
身份和访问管理	组织Fabric管理员或Orderer Fabric管 理员的数字凭据在传输到外部客户端组织Fabric管理员时被攻击	黑客/犯罪组织	3	3	3	3	9
共识安全	Fabric共识机制的服务提供者可以通过修改随机间隔来影响共识(订购)服务的一致性和可用性，从而操纵RAFT的领导者选举流程	内部组织	1	3	1	3	4
共识安全	Fabric共识机制的服务提供者可以通过修改随机间隔来影响共识(订购)服务的一致性和可用性，从而操纵RAFT的领导者选举流程	黑客/犯罪组织	2	3	1	3	6
身份和访问管理	Orderer Org Fabric 管理员帐户被攻破，以获得对运行RAFT共识机制的Orderer Leader节点的复制日志的未经 授权访问，导致违反机密性原则	黑客/犯罪组织	2	3	2	3	9
数据保护和密码学	托管运行RAFT共识机制的Orderer Leader节点的归档复制日志的离线数据存储被破坏，导致违反机密性原则	黑客/犯罪组织	2	3	2	3	7

图 15：按网络安全功能区域对漏洞分组

3 发现

本节报告了在运行时对贸易融资工作流执行的威胁评估和威胁分析（如“风险识别流程”部分所述）的结果，涵盖了 Gartner 区块链安全模型的所有三层，即业务、风险和 IAM 流程和技术/IT 层（Gartner，2018 年）。

3.1 业务层（Gartner 区块链安全模型）

3.1.1 对贸易金融业务逻辑机密性和隐私的威胁评估

> •超级账本 Fabric 2.0 的架构评估了业务逻辑和交易/有效负载的机密性和隐私，发现其在设计和默认情况下是本机安全的。
> •业务逻辑机密性和隐私：Fabric 2.0 允许将智能合约安装在客户端选择的对等节点上，而不是像非 Fabric 区块链那样安装在所有对等节点上，从而确保业务逻辑的机密性和隐私性
> •交易/有效负载机密性：Fabric 2.0 通过其“渠道”功能最大限度地减少了高度机密交易的风险，该功能允许将具有“按需所知”的实体指定为渠道成员。
> •当交易方需要对交易和随附数据保密或只是希望将整个交互保密时，渠道还可以实现“分类账本分离”。Fabric 2.0 还为交易方提供了使用私有数据收集的选项，其中专有或个人身份信息(PII)与交易的其余部分分开，并且仅在使用点对点(P2P)八卦协议的授权对等方之间交换，同时存储分类账上的私人数据的哈希值，以消除对个人身份信息(PII)或任何其他机密或专有信息的任何潜在未经授权的泄露。
> •客户端和区块链节点之间以及节点之间的端到端 TLS 确保对“传输中的数据”加密。原生 Fabric 加密也可在主机级别使用以加密“静态数据”。

注意：未经授权泄露存储在对等节点数据库中的私有数据或未经授权访问存储在链外或链上的交易日志是与 IT 相关的漏洞，并非特定于 Fabric 网络设计的漏洞。

3.1.2 对贸易金融业务逻辑执行和韧性的威胁评估

Fabric 2.0 的影响专门针对以下已知漏洞进行了评估，这些漏洞是非 Fabric 区块链网络中业务逻辑执行和韧性受损的主要原因。事实证明，Fabric 2.0 架构防止在运行时损害贸易金融的业务逻辑方面非常强大。

1. 智能合约中的非确定性交易：在 Fabric 2.0 中，非确定性交易的影响仅对手头的交易产生影响，如果有足够数量的对等方无法根据背书策略背书，则该交易可能会被拒绝

2. 交易重复：此漏洞不适用于 Fabric 2.0，因为重复交易在验证阶段被背书节点过滤，因此永远不会更新到世界状态

3. 时间戳依赖：Fabric 故意不使用提交应用程序的时间戳做任何事情，因此时间戳对 Fabric 处理没有影响。时间戳不是“网络时间”的反映，只要提交的应用程序是可信的时间戳就是可信的。增加区块高度是区块链时间流逝的唯一可信指示。如果应用程序确实引用了时间戳以获得额外的信息上下文，则应该相对于块的高度考虑，如时间戳是否随着区块高度的增加而增加。

4. 交易排序依赖：这个漏洞适用于 Fabric 2.0，其中排序服务的领导者排序交易以支持特定组织。时间戳对于检测事务重新排序攻击至关重要。如果网络中的组织依赖于时间关键合同，则应该跟踪客户端应用程序的传出事务。当交易包含在一个区块中时，可以通过比较时间戳检测重新排序。

5. 第三方可信服务（Oracle，预言机）：Fabric 2.0 通过使用三种不同架构模式的预言机访问解决扩展智能合约所产生的漏洞。

a. 在第一种方法中，可信方服务在区块链网络中拥有成员资格，并利用一个渠道将数据提供给网络的所有成员（IBM，2019）。

b. 在第二种方法中，区块链网络的所有成员都同意通过从智能合约中调用第三方服务的方式信任和利用第三方服务。在这种情况下，第三方服务的数据输入用于关联同一事务中发生的调用，从而保证确定性（IBM，2019）。

c. 在第三种也是最后一种方法中，索赔发布者通过向实体发布可验证的凭证充当预言机，然后在执行智能合约期间得到证实。客户端应用程序提供必要的声明作为智能合约的输入，然后通过验证签名的方式验证此类声明的真实性 (IBM,2019)。

3.2 风险/IAM 流程和技术/IT 层(Gartner 的区块链安全模型)

3.2.1 贸易金融工作流运行时的威胁模型分析

威胁模型确定了 **14 个可能性**和**影响评级为高的潜在威胁**。这些威胁的攻击者特征是“黑客/犯罪集团”类别。由于贸易融资工作流程对这些攻击者具有高价值资产，因此可以得出结论，这些威胁是高级且持久的[APT]。这些 APT 在 Gartner 区块链安全模型(Gartner，2018)中的分布如下：

- 这些威胁中有 50%属于 Risk 和 IAM 流程层，这些威胁源于 Fabric 和证书颁发机构系统的管理凭据可能受到“权限提升”的危害。

•其余 50%属于技术/IT 层，与未经授权暴露个人身份信息(PII)或专有交易、不受信任的 Fabric 客户端 SDK 或智能合约和失陷对等节点。

属于技术/IT 层的 APT 也被发现起源于“客户端信任边界”，在此，贸易融资工作流程的各个客户参与者(即，进口商和进口商银行、出口商和出口商银行、承运人和监管机构)与 Fabric 网络对接。

图 16 显示了 14 个高风险 APT 的详细信息。如下所示：

网络安全功能区域	漏洞	数量	攻击者属性	可能性&影响
身份和访问管理	所有类型的Fabric系统和证书颁发机构管理账户的泄露	7	黑客/犯罪组织	高
应用安全	不受信任的Fabric客户端SDK、未经验证的智能合约	2	黑客/犯罪组织	高
对等节点安全	失陷的对等节点	1	黑客/犯罪组织	高
数据隐私与密码学	未经授权访问保密交易和/或PII	4	黑客/犯罪组织	高

图 16：14 个高风险 APT 的详细信息

3.3 调查结果对贸易金融 Fabric 网络的影响

威胁模型分析表明，Fabric 系统和证书颁发机构的分散管理，再加上缺乏强有力的治理政策来保护管理渠道和凭证免受入侵，可能会扩大攻击面，从而有助于在贸易金融 Fabric 网络中“建立立足点”，危及整个 Fabric 网络，**并在贸易金融工作流程中导致贸易损失、所有权丧失以及进口商和出口商之间的信任丧失，从而对业务产生重大影响。**

3.4 威胁缓解策略的建议

这两个主要脆弱性可以按如下方式减轻：

- 去中心化 Fabric 管理漏洞：在云环境中选择单个服务提供商(最好是中立方)与联合证书颁发机构一起管理 Fabric 网络，将有助于减少由于去中心化 Fabric 管理而造成的攻击面。
- 缺少保护管理通道和凭据的治理策略：Fabric 网络利益相关者需要强制执行治理策略，以：
  -始终(静止、传输中和使用中)保护管理员身份凭据的安全；

-强制执行“职责分离”或“管理员三权分立”，限制管理员对任务直接使用 CLI 访问；

-通过选定的一组标准化工具限制管理员登录。例如：堡垒机、带外/专用通道、网络隔离等。

对于高/中/低风险的 APT，建议采用基于风险的缓解策略，如下所示：

- **高风险威胁：**缓解控制需要遵循“纵深防御策略”，涵盖审计、司法鉴定、检测和预防控制类别。至少需要涵盖 3 个控制类别，其中包括审计和检测。这使防御者能够在高风险攻击进行时为有效的事件响应赢得时间。图 17 显示了针对高风险威胁的示例“纵深防御”策略。
- **中等风险威胁：**缓解控制建议遵循“纵深防御策略”，涵盖审计、司法鉴定、检测和预防控制类别。至少需要涵盖 2 个控制类别，检测就是其中之一。图 18 显示了针对中等风险威胁的“纵深防御”策略示例。
- **低风险威胁：**缓解控制需要有司法鉴定控制。

网络安全功能区域	漏洞	风险 低：<=3; 中：4<=6; 高：7<=9	审计	司法鉴定	检测	预防
身份和访问管理	失陷的组织Fabric管理员账户用于篡改背书策略	9	审计以下内容： 审计包含背书策略的文件是否符合“数字版权管理”的要求 审计策略背书文件“拆分访问”的合规性 审计上述违规告警的流程	建立自动审计告警流程：对包含背书政策的文件违反“数字权利管理”	当包含背书策略的文件违反“数字版权管理”时告警S向Fabric管理员和MSP管理员发送告警	使用数字版权管理配置包含背书策略的文件 配置对包含背书策略的文件的“拆分访问”(需要Fabric管理员和MSP管理员登录才能访问背书策略) 配置“拆分访问”违规的实时检测

图 17：针对高风险威胁的 “纵深防御”缓解策略示例

网络安全功能区域	漏洞	风险 低: <=3; 中: 4<=6; 高: 7<=9	审计	司法鉴定	检测	预防
应用安全	链码访问控制策略被篡改，以包含未注册用户	4	对包含链码访问策略的文件进行“拆分访问”的审核证据 关于链码访问控制策略的警报和日志检测审核流程的审核证据 区块链网络用户验证审核流程的审核证据	查看未授权更新链码访问控制策略的日志	配置日志检测到非白名单账户和主机更新链码访问控制策略时的告警 将事件处理（SOC/NOC运行手册更新）的所有权限制为业务所有者	可以创建和/或更新链码访问控制策略的白名单主机和/或管理员账户 配置对包含链码访问控制策略的文件的“拆分访问”（需要Fabric管理员和MSP管理员登录才能访问文件） 定期检查访问控制策略。定期检查用户及其访问权限

图 18：针对中等风险威胁的 “纵深防御”缓解策略示例

3.5 事件响应策略推荐

如下所述，基于风险的事件响应策略与前面的威胁缓解策略相互配合，有助于防御者在攻击进行时组织良好的防御响应。因此：

- 在事件响应策略中明确要求所有已识别的**高风险**漏洞均需做好事件响应准备；
- 所有已识别的**中风险**漏洞都需要有适当的事件跟踪流程；
- 所有已识别的**低风险**漏洞都需要制定适当的监控流程，以防演变成事件。

4 Fabric 2.0 许可制网络的加密组件建议

与任何区块链一样，Hyperledger Fabric 2.0 的运行以密码学原语为核心。这些加密功能用于签署交易，为区块头和默克尔树创建数据哈希。密码学领域正在持续演进，不断研究和开发新的哈希函数和数字签名算法，而曾经认为是安全的东西现在可能已过时（Vlad 等，2017 年）（Kelly 等，2018 年）。

组织可以约束算法类型、模式和参数，以便切实有效地限制漏洞。

例如，美国联邦政府[18]通过《FISMA 法案》，要求联邦信息系统在使用联邦数据之前必须经过评估和

18 Local Government cryptographic rules/conditions supersede all recommendations made in this document

授权。FIPS 标准已由 NIST 制定，规范哪些加密算法可以由联邦政府批准使用。NIST FIPS 140-2 要求，必须验证那些用于保护敏感政府信息的加密算法实现。

Fabric 2.0 支持多种数字签名和哈希算法，如 ECDSA P256 曲线和 SHA256 哈希函数（均通过 NIST FIPS 标准批准）。

这些经批准的加密算法需要在由 NIST 验证的加密组件中实现，以便联邦信息系统处理敏感的秘密信息。这类组件的例子是谷歌的 BoringCrypto，该组件符合 FIPS 140-2（认证编号#3318[19]）标准。安装时需要在 140-2 模式下配置此组件，并且只能使用经验证和允许的算法。该组件可以替换当前 Fabric 2.0 中的加密功能实现。

19 See https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3318

5 术语

锚定对等点	频道上所有其他对等点都能发现并与之通信的对等节点。频道上的每个成员都有一个锚定对等点（或多个锚定对等点，防止单点故障），允许属于不同成员的对等点在频道上发现所有对等点。
（风险）可能性	指的是发生威胁事件的可能性或频率。事件很少发生，表明公司风险较低。相反，在这种或类似环境中发生过重大威胁事件表明风险较高。
区块链网络	区块链网络是一种技术基础设施，为应用提供账本和智能合约（链码）服务。
链码	链码是一段程序，实现了一个预定义接口，可以处理网络上成员的业务逻辑一致性。链码通过交易初始化和管理账本状态。该程序可以用 GO、Node.JS 或 Java 编写，并在容器中运行。链码也可认为是智能合约。
频道	是一种机制，允许一组特定的对等点和应用在区块链网络内相互通信。只有那些允许加入频道的才能看到数据，因此保证了数据的隔离和机密性。在 Hyperledger Fabric 中，频道还指仅允许特定对等点与频道特定账本交互。
共识	指的是网络中的大多数参与者就交易的有效性达成一致。在 Hyperledger Fabric 中，共识是节点网络提供交易顺序保证并验证交易区块的流程。
共识安全	运用如加密和哈希之类的安全协议保护数据完整性，并保护共识算法免受工作量证明、股权证明等的侵害。
控制措施	为缓解风险或识别威胁而实现的流程、检查或障碍。控制措施是在安全事件中的具体行动。 **预防：**在安全事件发生之前采取行动，目的是防止安全事件出现； **检测：**用于发现和描述正在发生事件的措施； **纠正：**旨在限制损害程度并将应用恢复到基线性能和配置的措施； **取证：**为支持事后调查而采取的措施。包括为支持调查流程及底层数据（事件数据和系统配置）的完整性而设计的任何措施。
CVE	“通用漏洞披露”的缩写，是一个公开披露计算机安全漏洞的列表。
DLT	分布式账本技术（DLT）是一种技术基础设施和协议，运行在去中心化网络上，使用加密签名和非中央授权方式，同时执行安全访问、验证和更新记录。
背书策略	规定了频道上的对等点必须执行与特定 链码关联的应用的交易，以及所需的响应组合。例如，某个策略可能需要一个最少数量的对等点背书。
背书对等点	在特定链码上下文中具有特定角色的对等点（节点），以便为交易背书。

Fabric 管理	组织中拥有“提升权限”特性的用户，可管理 Fabric 网络。
Fabric 客户端	应用与区块链网络交互的途径，通常是一个对等节点。
追随者	该节点将复制领导者发送的记录。
HSM	硬件安全组件的简称。提供密钥管理服务的组件，通常是基础设施的一部分。
Hyperledger	是一个开源区块链和社区的大型项目，专注于开发稳定的框架、工具和库，以适应企业级区块链（DLT）部署。
Hyperledger Fabric	分布式账本软件，可作为开发基于区块链的解决方案或应用的基础。
事件响应	处理可能导致业务损失或服务中断事件的流程。
失陷指标（IoC）	是一种数据元素，通常在系统日志或文件中发现，用于识别系统或网络上潜在的恶意活动。
领导者	该节点负责接收新的日志，将日志传递给追随者节点，并管理提交给账本的记录。
MSP	是成员身份服务提供者的简称。MSP 一个网络组件，用于验证客户端和对等点的凭证（用于对交易进行身份验证），以便客户端和对等点能够进入 Hyperledger Fabric 网络。MSP 抽象了用于颁发和验证凭证以及用户认证的加密机制。一个 Fabric 网络可以有多个 MSP。
排序点	参与排序服务的对等点（节点）（参见排序服务）
排序服务	一组将交易排序后送到区块中，然后将区块分发给连接的对等点验签的节点。该服务独立于对等点的处理流程。交易以先到先服务的方式排序。
Org	组织的缩写。指在许可制区块链网络中拥有成员身份的企业。也称为成员的集合。
Org MSP 管理	组织中拥有“提升权限”特性的用户，管理 Fabric 网络的成员身份服务。
对等点	区块链网络中的节点。对等点与组织关联（作为组织的参与者）。在 Hyperledger Fabric 中，对等点运行链码容器并对账本进行读/写操作。对等点由成员所有和维护。
策略	用于限制对区块链网络上资源访问的表达式，例如，谁可以读或写频道，谁可以使用 链码 API。
RAFT	Hyperledger Fabric 使用的共识算法，使用“领导者和追随者”模型，当领导者节点选出后，领导者做出的决策将流向追随者。
风险	由外部或内部漏洞引发或可能引发的威胁损害、伤害、责任、损失或任何其他负面事件，可以通过先发制人的控制措施避免。威胁或漏洞的减少也会降低风

	险。
风险评级	开展风险评估活动并分级： 1. 低 2. 中 3. 高 结合事件发生的可能性与影响分级。
SIEM	安全信息和事件管理，通常是个平台或系统。
智能合约	由客户端应用调用的代码，在区块链网络外管理对智能合约的访问和修改。
状态	也称为账本状态。网络中频道所有已完成交易的资产的聚合状态。
StateDB	Fabric 组件，存储交易中包含的键值对，是存储全局状态数据的地方。
VSCC	Chaincode 验证系统。用于根据背书策略验证交易。如果交易不满足策略，则该交易标记为无效。
漏洞	程序、硬件、软件或内部控制中的缺陷或弱点，可能被意外触发或故意利用，对 DLT 造成损害。
Web API	web 服务器或 web 浏览器的应用编程接口。
全局状态	是 Fabric 组件，表示链上交易日志中所有键的最新值。每当键值变化，全局状态就会改变。

6 参考

Adhav, P. (2020, August 25). *System Chaincodes in Hyperledger Fabric — VSCC, ESCC, LSCC, ESCC, QSCC*. Medium. https://medium.com/coinmonks/system-chaincodes-in-hyperledger-fabric-vscc escc-lscc-cscc-a48db4d24dc3

ALBREIKI, H., HABIB UR REHMAN, M., SALAH, K., & SVETINOVIC, D. (2020). Trustworthy Blockchain Oracles: Review,Comparison, and Open ResearchChallenges. *IEEE Access*. 10.1109/ ACCESS.2020.2992698

Allianz. (2021). Allianz Risk Barometer. https://www.agcs.allianz.com/news-and-insights/reports/ allianz-risk-barometer.html

Androulaki, E., Barger, A., Bortnikov, V., Christian Cachin, Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., SIngh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., VukolićJuvoli, M., … Yellick, J. (2018). Hyperledger fabric: a distributed operating system for permissioned blockchains. *Proceedings of the Thirteenth EuroSys Conference*, 1-15. 10.1145/3190508.3190538

Angelis, S. D., Zanfino, G., Aniello, L., Lombardi, F., & Sassone, V. (2019). Blockchain and Cybersecurity: A Taxonomic Approach. *University of Southampton*. https://www.eublockchainforum. eu/sites/default/files/research-paper/wrks-main_1.pdf

Baset, S., Desrosiers, L., Gaur, N., Novotny, P., Ramakrishna, V., & O'Dowd, A. (2018). *Hands-On Blockchain with Hyperledger* (ISBN: 9781788994521 ed.). Packt Publishing. https://www.packtpub. com/product/hands-on-blockchain-with-hyperledger/9781788994521

Birge, C., Craig, A., Dadoun, D., Glaros, M., Cristin, C., & Chamber of Digital Commerce. (2018). Advancing Blockchain Cybersecurity: Technical and Policy Considerations for the Financial Services Industry. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE1TH5G

Carter, H. (2019). Journey to Blockchain: A Non-Technologist's Guide to the Internet of Value. *BRI*.
Chia, V., Hartel, P., Hum, Q., Ma, S., Piliouras, G., Reijsbergen, D., Staalduinen, M. v., & Szalachowski, P. (2019). Rethinking Blockchain Security: Position Paper. *ArXiv:1806.04358*. http://arxiv.org/ abs/1806.04358.

Copigneaux, B., & European Parliament. (2020). Blockchain for Supply Chains and International Trade: Report on Key Features, Impacts and Policy Options Study. *European Parliamentary Research Service, and Scientific Foresight Unit*. http://www.europarl.europa.eu/RegData/etudes/ STUD/2020/641544/EPRS_STU(2020)641544_EN.pdf.

Crowdstrike. (2021). 2021 Global Threat Report. https://www.crowdstrike.com/resources/reports/global-threat-report/

Dabholkar, A., & Saraswat, V. (2019). Ripping the Fabric: Attacks and Mitigations on Hyperledger Fabric. *Applications and Techniques in Information Security, 10th International Conference, ATIS 2019, Thanjavur, India, November 22–24, 2019, Proceedings*, (pp.300-311). 10.1007/978-981-15-0871-4_24

Dika, A., & Nowostawski, M. (2018). Security Vulnerabilities in Ethereum Smart Contracts. *Conference: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. 10.1109/Cybermatics_2018.2018.00182

Dingman, W., Cohen, A., Ferrara, N., Lynch, A., Jasinski, P., Black, P. E., & Deng, L. (2019). Defects and Vulnerabilities in Smart Contracts, a Classification using the NIST Bugs Framework. *Atlantis Press*. 10.2991/ijndc.k.190710.003

European Commission. (2019). Legal and Regulatory Framework of Blockchains and Smart Contracts. *The European Union Blockchain Observatory and Forum*. https://www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf

European Commission. (2020). 2018-2020 CONCLUSIONS AND REFLECTIONS. E*U BLOCKCHAIN OBSERVATORY AND FORUM*. https://www.eublockchainforum.eu/sites/default/files/reports/report_conclusion_book_v1.0.pdf

Gartner. (2017). Blockchain Technology: How Security Relates to Use Cases. (ID:G00317396).

Gartner. (2018). Evaluating the Security risks to Blockchain Ecosystems. (ID:G003247104).

Gartner. (2020). Blockchain Trials Show Business Executives Drive Focused Solutions to Production. (ID G00733890).

Global Blockchain Business Council,. (2020). Chain Reaction: Blockchain Enters the Mainstream. *Annual Report 2020*. https://www.lw.com/thoughtLeadership/gbbc-report-blockchain-enters mainstream

Hoffman, C., Ignatova, P., Fong, F., Bischof, D., & Defeo, J. (2020). Blockchain & DLT in Trade: A reality
check. *WTO*. https://www.wto.org/english/res_e/booksp_e/blockchainanddlt_e.pdf

Homoliak, I., Venugopalan, S., Hum, Q., & Szalachowski, P. (n.d.). A Security Reference Architecture for Blockchains. *ArXiv:1904.06898*. Retrieved 2019, from http://arxiv.org/abs/1904.06898

IBM. (2020). Advancing global trade with blockchain. *Institute for Business Value*. https://www.ibm.com/downloads/cas/WVDE0MXG

International Finance Corporation. (2019). Blockchain. Opportunities for Private Enterprises in Emerging Markets. *World Bank Group Report*. https://www.ifc.org/wps/wcm/connect/2106d1c6-5361-41cd-86c2-f7d16c510e9f/201901-IFC-EMCompass-Blockchain-Report.pdf

Jones, J. (2019). *Understanding Cyber Risk Quantification*. FAIR Institute. https://www.fairinstitute.org/blog/download-understanding-cyber-risk-quantification-the-buyers-guide-by-jack-jones

Kelly, J., Lauer, M., Prinster, R., & Zhang, S. (2018). Investigation of Blockchain Network Security Exploration of Consensus Mechanisms and Quantum Vulnerabilities. https://courses.csail.mit.edu/6.857/2018/project/Kelly-Laurer-Prinster-Zhang-BlockchainNetSec.pdf

Koens, T. (2019, October 29). *Atomic Swaps for Distributed Ledgers.* Medium. https://medium.com/ing-blog/atomic-swaps-for-distributed-ledgers-cacfb7e1d90

Perez, D., & Livshits, B. (2020). Smart Contract Vulnerabilities:Vulnerable Does Not Imply Exploited. https://arxiv.org/pdf/1902.06710.pdf

Praitheeshan, P., Pan, L., Yu, J., Liu, J., & Doss, R. (2020). Security Analysis Methods on Ethereum SmartContract Vulnerabilities — A Survey. https://arxiv.org/pdf/1908.08605.pdf

Putz, B., & Pernul, G. (2020). Detecting Blockchain Security Threats. *2020 IEEE International Conference on Blockchain (Blockchain)*, 313–320. https://doi.org/10.1109/Blockchain50366.2020.00046

Rilee, K. (2018, February 14). *Understanding Hyperledger Fabric — Endorsing Transactions*. Medium. https://medium.com/kokster/hyperledger-fabric-endorsing-transactions-3c1b7251a709

Shostack, A. (2014). *Threat Modeling: Designing for Security* (1st ed.). Wiley Publishing.

Verizon. (2020). 2020 Data Breach Investigations Report. https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

Vlad, G., Gorbunov, S., Mosca, M., & Munson, B. (2017). QUANTUM-PROOFING THE BLOCKCHAIN. *Blockchain Research Institute*. https://evolutionq.com/quantum-safe-publications/mosca_quantum proofing-the-blockchain_blockchain-research-institute.pdf