加密资产交易所安全指南

CSA GCR cloud security alliance ®
GREATER CHINA REGION

区块链工作组的官网：
https://cloudsecirtiyalliance.org/research/working-groups/blockchain/

序 言

区块链做为一种颠覆性技术，能够帮助多个应用场景的业务创新并促进业务转型。区块链的去中心化和不可篡改的特性可以使交易双方安全可信地执行交易、验证交易和审计历史交易。在政务、金融、身份管理、医疗健康、智能家居和物联网、供应链和物流、汽车行业等多个细分领域中有很多新兴应用案例。

同时，区块链技术也面临着诸多的安全挑战，与传统信息系统的安全架构相比，与加密资产交易所相关的系统架构、运作的边界、参与者和组件已重新定义，给用户，区块链服务提供机构及监管机构带来了全新的安全及监管的挑战。

本指南对于加密资产交易相关的安全威胁、安全架构、最佳安全实践、应对相关威胁的控制措施提供了指导，可以很好的帮助加密资产交易用户、服务提供机构及监管机构提升安全意识，了解相关威胁及防护措施。文章结构清晰，内容简洁，值得参阅。

李雨航 Yale Li

CSA 大中华区主席兼研究院院长

致 谢

本文档《加密资产交易所安全指南》(Crypto-Asset-Exchange-Security-Guidelines)由 CSA 区块链工作组专家编写，CSA 大中华区秘书处组织翻译并审校。

中文版翻译专家（排名不分先后）：

组　长：高　卓

翻译组：李　国　马晓艳　张　钊

审校组：黄连金　郭鹏程　姚　凯　刘　洁

感谢以下单位对本文档的支持与贡献：

北京江南天安科技有限公司　北京北森云计算股份有限公司

英文版本编写专家

主要作者： Boulevard A. Aldetoyinbo, Esq.　Ken Huang　Dave Jevans　Abdulwahab AL-Zuaby

区块链/DLT 工作组领导成员： Bill Izzo　Ashish Mehta　Jyoti Ponnapalli

CSA 全球人员： Hillary Baron　Frank Guanco　Kurt Seifried　AnnMarie Ulskey

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

1. 加密资产交易所威胁建模

作者：Dave Jevans

针对重点攻击加密币资产的威胁的建模框架（ABC, Asset-Based Cryptocurrency-focused threat modeling framework）能够识别这类风险。ABC 的一大关键创新是使用了共谋矩阵（collusion matrices）。共谋矩阵用一个威胁模型覆盖大量威胁案例，同时对整个流程实施管理以防止它变得过于复杂。我们通过展示现实世界用例和开展用户研究证明 ABC 是行之有效的。用户研究表明，约有 71%使用 ABC 的人能够识别金融安全威胁，而在使用流行框架 STRIDE 的参与者中，只有 13%的人能够做到这一点。

本文的完整 PDF 全文可以从 http://arxiv.org/pdf/1903.03422.pdf 下载。

这个模型可用于分析针对加密币本身的攻击以及分析针对通过智能合约控制交易的去集中化（分散式）交易所（DEX）的攻击。不过，若要对针对托管钱包（如基于云的交换、场外交易平台、加密币交换服务等）的攻击建模，或许还需要用一种聚焦点更突出的方法。下面，我们将列出针对交易所的十大威胁。

1.1 交易所威胁模型

我们见过的针对交易所的攻击可分为以下几类：

1. 用户凭证钓鱼，旨在访问加密币账户并转移资金。这些攻击手段有时会与 SMS 劫持结合使用，以获取目标用户的基于 SMS 的身份验证码。
2. 针对交易所的技术攻击，旨在渗透内部系统。
   a.创建或访问账户后发起 SQL 注入攻击。
   b. 利用交易所运行的软件存在的漏洞。
   c.利用交易所未打补丁的软件。
3. 对交易所员工实施鱼叉式网络钓鱼攻击，旨在打破提款控制。
4. 对交易所员工实施鱼叉式网络钓鱼攻击，旨在植入恶意软件（特别是远程访问木马），使攻击者得以访问内部系统并在基础设施之间来回跳转。

5. 攻击者一旦进入内部系统，往往会利用内部 API 或内部访问控制不充分的系统，从而实现跨系统移动。攻击者经常利用保存在内部计算机上的凭证来访问其他系统。

6. 用于保存私钥的冷钱包（离线钱包）存储与用于日常操作的热钱包（在线钱包）密钥存储的不当或错误使用。交易所应该把 90%的加密币保存在不与互联网连接的冷钱包里。需要有一个协议完全离线初始化冷钱包，从而在热钱包与冷钱包之间传递传输请求（通常要求有一个带签名指令的 USB 驱动器）。交易所应该考虑为访问冷钱包设置多重签名，必须有两名员工为交易签字，资金才能从冷钱包转移到热钱包。

7. 在交易所，员工可以访问热钱包密钥并可复制密钥、拥有冷钱包密钥访问权并可复制密钥，或者可以在内部系统中植入恶意软件或远程访问木马以便将来访问这些密钥进而偷窃加密资产，因此内部人员威胁普遍存在。

8. 反编译交易所 app（iOS 或 Android）并找出嵌在 app 里的秘密云 API 密钥，然后用这些密钥访问内部 API，进而通过这些 API 访问热钱包或用户凭证。

9. 复制钱包恢复密钥。交易所需要用比保护热钱包或冷钱包更大的力度保护钱包恢复密钥。攻击者如果拿到恢复密钥的拷贝，将能清空交易所的全部资产，冷数字钱包也不例外。因此切记千万不要把恢复密钥保存在电子介质上。而是应该把它们写在纸上保存到物理保险柜里。此外比纸张防火性更好的金属物理装置也可使用。

10. 利用交易所执行方案存在的漏洞对特定加密币实施攻击。例如，许多 XRP（瑞波币）的执行方案存在着一个会被人恶意利用的分批支付漏洞。交易所与 XRP Ledger 系统集成时，会假设付款金额字段始终是全额交付。在这种情况下，恶意行为者会利用这一假设从机构窃取资金。只要这些机构的软件没有正确处理分批支付，这个漏洞就可以被人用来攻击网关、交易所或商家（详情请见：https://xrpl.org/partial-payments.html#partial-payments-exploit）。2020 年 9 月的头 9 天，有 3 家交易所的 XRP 持有量被完全抹去。

2. 加密资产交易所安全参考架构

作者：**Abdulwahab Z**

随着加密资产行业不断发展，加密资产交易所（CaE）以越来越大的力度覆盖这个

几十年来一直被金融服务机构视为私人游乐场的领域——这在分布式账本技术（DLT）（如果采用得当）可以通过提供大量服务引领企业走向未来的企业环境/商业生态系统中，表现得尤为突出。

加密资产交易所有若干种存在形式；由于实体身份的缘故，这些形式之间呈两极分化的态势。中心化（集中式）交易所（Centralized Exchange, CEX）由已知且可识别身份的实体拥有和经营，依照一个司法管辖区或横跨多个司法管辖区的法规运行。而分散式（去中心化）交易所（Decentralized Exchange, DEX）顾名思义，几乎不受具体实体（组织、司法管辖区）制约——除非自愿选择接受制约——不过，一些在 DEX 和跨 DEX 进行交易的实体为了增强合法可信度，并不规避锁定司法辖区。

由于参考架构是一种预定义的模式架构集，这些模式被实例化、经过精心设计并被事实证明可以在应用环境下发挥既定功效，因此，把 CEX 拿去与“传统”（实在找不出更好的形容词）金融服务/系统的“安全”架构比较，在超出信息通信技术（ICT）和云安全基本要素的许多层面上既不全面也不现实——原因在于，与加密资产交易所及其超出词语（例如订单簿、买卖、交换、提款、交易、密钥等）语义范畴的功能相关的内部运作的边界、参与者和成分已全部重新定义。

加密资产交易所其实就是寻求交易的实体之间的中介；中介复杂介入的深度由 CEX 的企业架构、业务区间和服务范围决定；所有这些因素再加上适用法规，结合到一起形成了对集成/连接加密资产网络、对等服务供应商以及业务支持服务供应商的需求度，如 KYC/AML（“了解客户”/“反洗钱”）要求、金融机构、支付服务处理器等。加密资产交易所致力于在使用混合资产（政府发行的法定货币、公共区块链资产、封装/令牌化工具或它们的组合）的实体之间撮合交易。

本文将阐明适用于加密资产交易所广泛类型/格式的 CEX 参考架构，以此作为框架在未来形成 CEX 类型特有迭代的普遍适用起点。

中心化交易所（CEX）的运行/业务模式围绕着提供服务展开，而这些服务可以为感兴趣方（个人或企业）以手动或自动方式使用交易工具带来方便。服务在构成交易及其条款的参数方面各有不同功能；因此，每个配置都与一个产品名称关联（即储蓄、衍生

品、现货、抵押、托管、交换、期货等）。

提供给实体的抽象服务要以会员资格为前提，而会员资格需通过复杂程度各异的注册或密码密钥等方法（如往返交换、“匿名”交换、web3.0 等）获得。会员资格被抽象成交易实体带编号的标识符，供在中心交易所申请工具、规定权利、义务、实施拨款保护等时使用。

此外，CEX 服务通过借助 API 和软件客户端连接核心系统的 app 提供给会员——只要会员的 GUI/CLI 通过公开/回环 API 端点服务器或单独的本地化 API 守护进程与加密网络交互时使用的是 Web/移动应用或加密钱包/DEX 客户端即可。

因此可以说，CEX 环境是一个实体可以通过 app 借助各种现有服务“交易”的环境：根据交易方接受的既定条款实施/执行操作和功能。

我们之所以选择这个抽象级别，是为了引导读者面对安全和风险状况时放宽眼界，从大局着眼。而这反过来会形成对风险和抑制手段的全面探讨，从中确定 CEX 在安全计划、风险管理和运行策略方面的要求；这一点至为关键，特别是在一个不存在“低威胁”区域（即便在 CEX 内部）的环境里。

图 1 提供既定服务的 CEX 具有 3 个主要抽象块：A）逻辑 B）工具 C）集成

每个块的范围涵盖它的流程成分（代码、基础设施、人员）、逻辑和执行参数，同时控制着跨块交互、依赖和继承关系在本地通过内部 API 中间件流动的方式。

值得一提的还有另外一点，集成块会扩大范围，把补充 CEX 功能或帮助 CEX 以及来自对等实体、票务系统和社交媒体集成的产品的第三方系统和服务供应商也涵盖在内。

下图直观展示了上述抽象 CEX，可用作参考架构指南。

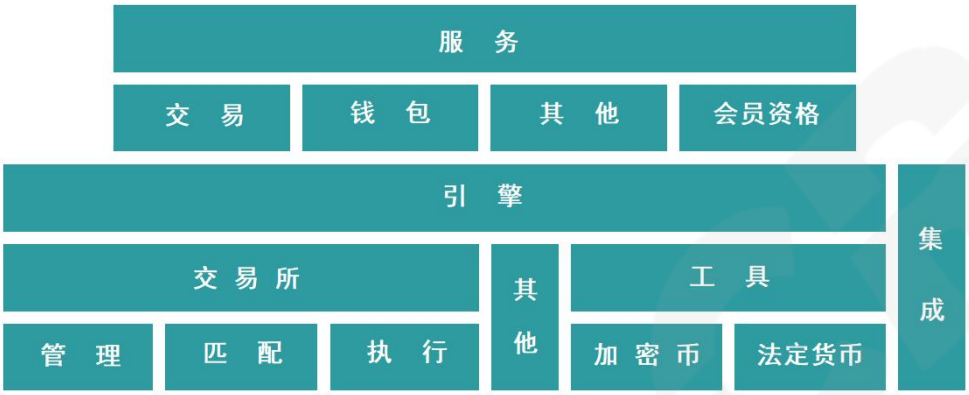


图 2 加密资产交易所抽象图

需要注意的是，图 2 中的“其他”是指并非 CEX 核心的服务（由 CEX、集成的第三方或 DLT 网络提供），因为它们是非交易性的，如投票、加密/解密消息、外部余额跟踪、dApp 查询等，抑或是因为它们是由会员/DLT 在外部执行的，但可能会对会员/CE 的地位产生影响（P2P 交换、采掘/铸造、令牌创建/交换、主站/服务/中继加密节点管理、电汇等）。

CEX 的目标是在一个构建在安全和隐私标准以及最佳实践（包括可追溯、可追踪、可问责和合规）基础上的环境中促成交易。为了适用于所有交易周期及其各阶段事项（即请求、开始、取消、兑回等），我们考虑把“交易”视为由两个各不相同、相互排斥，同时又相互依赖的范围组成：

> A:价值绑定的：促成价值转移（如存入、提取、收费、汇款、买卖、交换、dApp 交互等）的交易。
>
> B：价值未绑定的：不直接转移价值的交易或操作——但是它们对相关流程（如管理流程、角色和权限的分配、API 路由、通知、日志记录、dApp 查询等）具有辅助意义。

目前已有多种安全和隐私框架（NIST、Jericho、OSA、SAMM、SDLC、PMRM……）和架构（SABSA、O-ESA……）可供使用。就中心化交易所（CEX）而言，它们的主要构建块的边界尽管依然会保持它们的长处，但是如果不重新定义，势必会遇到挑战。

在分布式账本技术（DLT）领域开发有效的安全/隐私架构，这种挑战放大了现有框架/模型无论如何都无法完全适应个人具体情况和需要的缺陷。安全/隐私架构的概念涵盖了许多方面。每个框架都有各自的重点和优势，加密资产交易所可以在需要扩展的领域把这些重点和优势充分利用起来。

图 3 和图 4 用实例展示了 CEX 处于怎样一种态势，以及它们面临的对比鲜明的安全挑战。要想战胜这些挑战，只能把 CEX 及其所有组成部分都视作关键资产的容器，同时把“数据”视作每个容器核心中最重要的资产，以这样的方法分层保护和逐级防御。

CEX 架构要求确保在所有层级上落实安全信息交换指南和最佳实践，在启动下一个步骤之前对双向信息流动采用有效的方法。

图 3 加密资产交易所：集中式、或者去中心化的客户端和公共区块链

集中式和混合式交易所应该采用分层实施安全保护的方法，确保每个单独的防御组件都有备份，从而弥补其他安全防御手段存在的任何缺陷或漏洞。多层级安全保护法的每个层级都分别注重某一特定区域。这些层级协同一致形成的合力可以提高安全性和增加击败渗透破坏的机会。

回到集中式和混合式交易所的抽象体系中来，所有交易都将通过对警报阈值极为敏

感的价值绑定交易来提供监控和响应操作以及策略管理反馈流；价值未绑定交易将用于凸显/警告，表明/暗示可能发生了恶意价值绑定交易的异常情况。

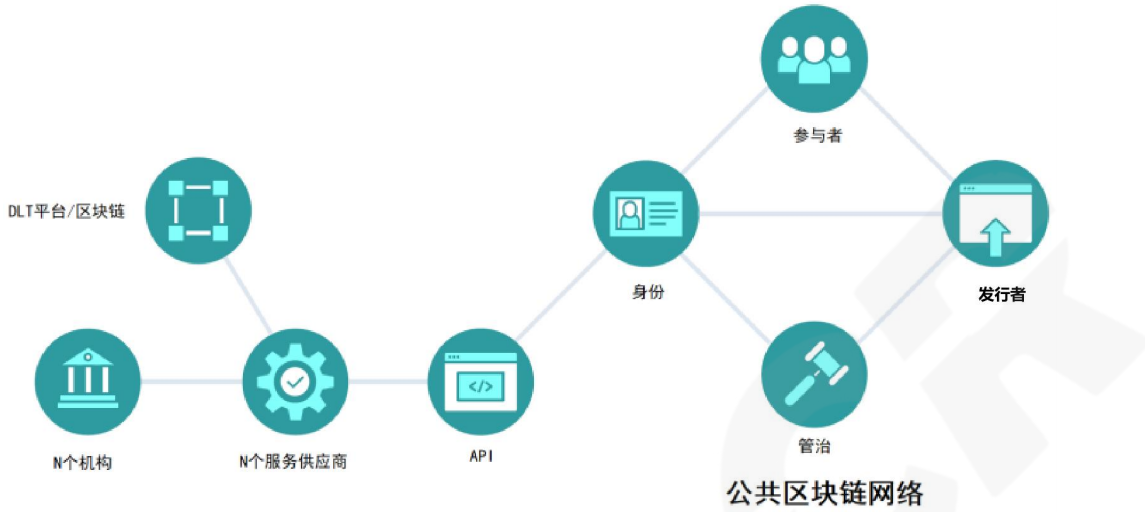


图 4 分散式加密资产交易所（dApp）

3. 加密资产交易所最佳安全实践

作者：Ken Huang

本章将从 3 个不同的角度（交易所用户、交易所运营商和审计者）推荐最佳安全实践。

3.1 交易所用户视角的最佳安全实践

3.1.1 信誉良好和安全的交易所

用户应该避开不道德的加密资产交易所，因为它们可能缺乏安全措施，具有不诚实和欺诈性商业行为。欺诈性行为的例子包括内幕交易、抽水和倾销计划，以从流动性低的价格变化中获利，无正当理由禁用提款或存款功能，以及因缺乏内部安全流程从而导致内部人员攻击频发。

3.1.2 口令管理和双因子或多因子认证

使用强口令，最少由 10 个字符组成，其中混合使用大小写字母、数字和特殊符号。启用双因子或多因子身份验证（用户不要使用任何不支持至少双因子身份验证的交易所）。由于存在发生 SIM 卡交换劫持的可能性，交易所应该用 Google Authenticator 取代 SMS 充当第二因子。

3.1.3 使用单独设备

如果可能，用户应该用单独的设备与加密资产交易所连接并只授予最小权限。KYC（“了解客户”）要求流程完成后，用户可以禁用对相册的访问。用户还可以禁用交易所对联系人列表的访问，并禁用对音频的访问。用户可能依然需要允许交易所 app 访问自己的存储空间，以便定期更新数据。

3.1.4 了解与钱包应用相关的密钥概念

去中心化交易所（DEX），私钥通常由客户端 app 持有。私钥用于给可以从钱包提取资金的交易签名。用户必须全面了解与私钥相关的密钥概念以及丢失私钥会造成什么后果，这一点至关重要。

1）公钥和地址

在公钥密码中，用户会拥有一个密钥对：公钥和私钥。用户可以从私钥派生公钥，但不能从公钥派生私钥。在以太坊中，地址发挥着类似公钥的作用，尽管它并不是公钥。公钥由私钥派生而来，是由 128 个十六进制字符组成的字符串。用户可以从中提取（64 个字符的）“SHA3”（Keccak-256）散列值；然后再提取最后 40 个字符，加上“0x”为前缀，形成自己的 42 字符地址。

2）私钥

私钥是用户的地址/公钥对或者由 64 个十六进制字符组成的字符串中保密的那一半。

（几乎）每个由 64 个十六进制字符组成的字符串都是一个私钥。这就是用户需要用来

确保安全的密钥。没有它，用户将无法动用自己的资金。

3）密钥库文件

密钥库文件是 JSON 格式私钥的加密版（尽管它没有 JSON 扩展名），或者是被用户选择用口令保护的私钥的精美版。

4）提示性短语（恢复短语）

提示性短语是可用来派生多个私钥的私钥的另外一个精美版。由 12 或 24 个单词组成的短语通常可以让用户访问不定数量的账户。为了保险起见，用户有时会给短语增加第 13 个或第 25 个单词。提示性短语起源于“第 39 号比特币改进规范提案（BIP）”。“派生路径决定了用户可以用此短语访问的账户。”

3.1.5 慎重安装或点击

用户应该避免访问未知网站或从不可信来源下载 app。这些网站和 app 往往运行着恶意软件，会把它们（偷偷）自动安装到设备上并对设备造成破坏。如果电子邮件出现非预期或可疑附件或链接，千万不要点击。

3.1.6 保护敏感数据

> 用户应该把敏感数据（如社会保障号、信用卡信息、学生记录、健康信息等）从安装了交易所 app 的设备上撤下来保存到别处。
> 当敏感数据文件不再被需要时，应该将它们从系统中安全移除。
> 存储或传输敏感数据时永远都要加密。

3.1.7 确保设备安全

> 用户应该用 PIN 或口令锁闭自己的设备，切勿将设备留放在没有保护措施的公共场所。
> 用户应该只从自可信来源（如 Apple App Store、Google Play）下载安装交易所 app。
> 用户应该即时更新设备的操作系统。

> 大多数手持设备都能使用数据加密——用户可到设备说明书中查阅可用选项。用户应该借助苹果的“查找我的 iPhone”或 Android 的设备管理器工具来帮助防止设备丢失或失窃。

3.1.8 永远只用安全的网络连接

用户应该避免通过公共网络与交易所交易（买/卖/存入/提取/抵押）。家庭或单位网络之外的任何网络都是不安全的。即便用户给设备里的数据都加了密，但是数据在连网传输时并不一定会采取加密格式。此外，用户连接的公共网络始终存在着被人搭线窃听的风险，这表明通过网络交换的数据始终处于风险之下。在使用可信网络以外的任何连接之前，始终要确保自己通过适当的 VPN 设置对连接实施了保护。

3.1.9 了解各种钱包类型和钱包的使用方式

加密资产钱包分纸质、硬件、云和在线四类。

1）纸钱包

纸钱包通常被归类为冷存储。“纸钱包”一词一般是指公钥和私钥的物理拷贝或纸质打印件。它有时又指用于生成会被送去打印的密钥对和数字文件的软件。无论属于哪种情况，纸钱包都可以为用户提供级别相对较高的安全性。用户可以把自己的纸钱包导入软件客户端，或者只需扫描它的二维码便可转移资金。尽管纸钱包很冷，但它们也是与风险共存的。例如，纸钱包很容易损坏、烧毁，容易被人复制、拍照，如果你不自己制作，那就需要选择相互信任。人们为了使纸钱包不那么脆弱，有时会把它们压薄，制作多个副本，把它们分别存放在多个不同位置，或者将它们刻在金属片或其他坚固材料上，等等。

需要注意的是，把纸质钱包的电子拷贝保存在 PC 机上绝对不是好主意。纸钱包的私钥永远都要离线保存。把自己的纸钱包文件保留在线上，会使它变得像热钱包一样不安全。

2）云钱包

用户的钱包若是拿到中心化交易所（CEX）使用，它便是一种云钱包。用户的资金可以被人用云钱包从任何计算机、设备或位置访问。它们确实很方便，但它们也将用户的私钥保存到了网上，可供交易所操控。因此，云钱包的设计在面对攻击和盗窃时，会显得比较脆弱。

3）软件钱包

软件钱包是指被下载并安装到个人电脑或智能手机上的热钱包。桌面和移动钱包都具有极高的安全性；但是它们无法保护用户免受黑客攻击和病毒侵害，因此用户应该尽力防范恶意软件。移动钱包通常比桌面钱包更小、更安全，使用起来也更方便。

4）硬件钱包

与软件钱包不同，硬件钱包把用户的私钥存储在 USB 等外部设备上。它们是完全冷的和安全的。此外，它们也能进行在线支付。一些硬件钱包与 Web 接口兼容并支持多种加密资产。它们的设计是为了让交易变得简单方便，因此，用户只需把钱包插入任何在线设备，将其解锁，发送加密资产并确认交易就可以了。硬件钱包被认为是存储加密资产的最安全方式。最妥当的做法是直接从制造商那里获取硬件钱包。从其他人手里购买是不安全的，尤其是那些不认识的人。另外，用户还需切记，即便你是从制造商那里获得硬件钱包的，你也应该亲手将其初始化和重置后再使用。

如果需要对这几种钱包做一次安全性排名，我们可以这样排列：硬件钱包 > 纸钱包 >软件钱包 > 云钱包。通常情况下，最好的做法是把数量多的加密资产存储在硬件钱包里，只把需要定期与交易所交易的资金保存在交易所的云钱包里。

3.1.10 大笔资金使用 Multisig

Multisig 代表多重签名，这是一种特定类型的数字签名，可使两个或多个用户作为一个组对文档签名。因此，多重签名是多个唯一签名组合在一起产生的。Multisig 技术一直在加密资产领域使用，但是这一原理早在比特币问世之前就已经存在了。

在加密资产的背景下，multisig 技术于 2012 年首次应用于比特币地址，最终导致

multisig 钱包诞生。用户使用了 multisig 钱包，可以避免出现私钥丢失或被盗带来的问题。因此，即便多个密钥中的一个失信，资金依然是安全的。

我们不妨假设这样一个例子：Alice 创建了一个三之取二 multisig 地址，然后把每个私钥分别存放到不同的地方或设备（例如，手机、笔记本电脑和平板电脑）中。即便 Alice 的移动设备失窃，小偷也无法只用 3 个密钥中的一个来访问她的资金。同样，钓鱼攻击和恶意软件感染也会被大大降低成功率，因为黑客极可能只掌握一台设备和一个密钥。撇开恶意攻击不谈，如果 Alice 丢失了其中一个私钥，她依然可以用另外两个密钥调用她的资金。

Multisig 技术常被加密资产企业用来管理公司资金；我们建议用户在家人或朋友中用这一技术当作一种防备万一的手段，以避免因一个密钥失窃或丢失而造成经济损失。

3.2 交易所运营商视角的最佳安全实践

本节列出了从加密资产交易所运营商视角看的最佳安全实践和相关技术安全控制。

3.2.1 分布式拒绝服务攻击（DDoS）保护

DDoS 攻击通过用请求访问的恶意数据包淹没服务器来利用网络漏洞。大量通信流的涌入最终会导致加密资产交易所服务器崩溃并中断服务。加密资产交易所与大多数高知名度企业一样，也已成为 DDoS 攻击的目标。随着人们对加密资产的兴趣激增以及随之而来的流量增加，门户已经为那些试图破坏加密资产资源，进而拒绝合法用户访问的那些恶意行为者打开。针对 DDoS 的防御措施包括：

1）增加网络带宽

由于 DDoS 攻击的基本原理是用巨量通信流压垮系统，因此，只要有额外的带宽（例如应对突发事件的带宽计划）处理超出预期的流量高峰，便可以提供一定程度的保护。但是，这种解决方案可能费用昂贵，因为会有许多带宽在大部分时间里是闲置的。更重要的是，额外的带宽目前在防止 DDoS 攻击方面已经不如以往奏效。这些攻击正变得规模越来越大、技术越来越先进，如果不辅以其他 DDoS 抑制措施，任何带宽都无法承受

超过 1T 的攻击。但是尽管如此，应对突发事件的带宽还是可以帮助缓解攻击的影响，为采取行动击退攻击赢得所需要的额外时间。

2）以早期检测和数据包监测手段抑制 DDoS 攻击

IT 安全团队可以采用多种手段监控入站通信流并识别对于阻止 DDoS 攻击至关重要的早期预警信号。大多数路由器支持流采样，这一性能可以检查入站数据包的样本从而创建一张显示网络流量趋势的大型图片。但是，由于流量采样一次只查看一小部分通信流，因此可能会错过潜在的破坏性趋势或出现“误报”。我们可以通过部署各种入侵预防系统/入侵检测系统（IPS/IDS）抑制 DDoS 风险。

3）管理和拦截恶意通信流

加密资产交易所发现有人正在实施 DDoS 攻击之后，可以采取各种措施保护自己的基础设施。预防 DDoS 攻击的第一策略通常是用“空路由”流量阻止恶意数据包到达服务器，空路由流量可以拦截和重新定向受僵尸网指挥的请求洪流。DDoS 优化防火墙也可以识别不完整的连接，并在它们达到特定阈值时将其从系统中清除。我们还可以评估路由器的工作状况，从而帮助防止服务器陷入不堪重负。在某些情况下，所有通信流都转移到一个“洗涤器”，由它把合法请求与恶意请求更彻底分离开来。然而，这些网络安全措施中有许多都依赖带宽，而且一遇大规模攻击，就有可能被击溃。

4）建设备份基础设施

随着 DDoS 攻击变得规模越来越大、技术越来越先进，IT 安全工作对冗余备份的投入已经到了与预防相提并论的地步。DDoS 攻击的终极目标毕竟是让服务瘫痪，那么，只要能够保持服务器在线正常运行，至于供应商采取什么手段，全都无关紧要。冗余备份并不是正面迎击攻击，而是允许机构扩展自己的基础设施，使其更具弹性。冗余备份还可以使机构腾出手来更轻松地主动对抗攻击，因为通信流可以被更有效地切断和重新路由。

5）引入备用互联网服务供应商

只依靠一家互联网服务供应商（ISP）会使公司面对 DDoS 攻击时脆弱不堪，因为旨在破坏供应商系统的任何攻击都有可能导致与之连接的所有系统宕机。此外，当 DDoS 攻击是通过一家 ISP 的连接发起时，几乎所有解决方案都是切断连接等待攻击结束。如果有提供 ISP 冗余的混合互联网服务方案，则公司可以设计备用网络，使自己在遇到 DDoS 攻击时得以根据需要在不同供应商之间切换。

6）用云解决方案阻断 DDoS 攻击

云 DDoS 解决方案供应商可以为机构提供一系列广泛的工具对抗 DDoS 攻击。由于它们具有更大带宽容量和更安全的路由器来管理入站通信流，因此数据中心安全保护方式具有比典型本地 IT 解决方案更强的能力挫败致瘫基础设施的企图。云供应商拥有通过混合 ISP 连接对抗最新 DDoS 攻击战略所需要的资源，这些连接可以提供得到预测分析和远程服务支持的多层次冗余和实时监控。

3.2.2 跨站点脚本（XSS 保护）

跨站点脚本（XSS）是一种安全漏洞，允许用户更改应用提供给用户，在用户的 Web 浏览器中执行的代码。它最常见于影响用户浏览器的 Web 应用，也会出现在具有嵌入式 Web 内容的其他应用中，例如交互式“帮助”内容查看器。当 XSS 漏洞被人用作攻击向量时，攻击者发送的输入会在应用内被以一种不安全的方式处理，允许 Web 浏览器执行经攻击者篡改后发送给受害者的代码。

要想修复这一漏洞，开发人员必须验证传输给应用的所有输入并对输出包含的所有信息进行编码。这是应用开发过程的一个重要组成部分，有助于防止多种不同的漏洞，而不是只对 XSS 有效。

有关 XSS 及其保护措施的更多信息，请访问：

https://owasp.org/www-project-top_ten/OWASP_Top_Ten_2017/Top_10-2017_A7-Cross-Site_Scripting_(XSS)。

3.2.3 不暴露服务器信息

把有关服务器、软件和操作系统的后台信息显示在外会带来安全隐患——这是在为黑客攫取秘密信息开绿灯；用户或许不清楚为什么会有一个快速链接指向 Apache 漏洞列表，但 Apache 至今也依然是最常用的 Web 服务器。在每个新版本中，开发人员都会修复错误并关闭漏洞。

详情请见：https://www.cvedetails.com/vulnerability-list/vendor_id-45/Apache.html。

3.2.4 Web 应用防火墙

Web 应用防火墙（WAF）可以保护 Web 应用免受各种应用层面攻击侵扰，如跨站点脚本（XSS）、SQL 注入和 cookie 中毒等。对应用实施攻击会直接造成数据泄露——应用程序是通向加密资产交易所珍贵数据的门户。

3.2.5 数据库防火墙

集中式加密资产交易所通常用数据库（SQL 的和非 SQL 的）存储用户数据、订单簿、交易历史、管理配置、设置等。

数据库防火墙是 Web 应用防火墙（WAF）的一种，可对数据库实施监视，识别并阻止专门针对数据库的，主要寻求访问存储在数据库中敏感信息的攻击。数据库防火墙还可以通过自身维护的日志监控和审计对数据库的所有访问。数据库防火墙通常是强化了安全的设备/软件，部署在数据库服务器内（挡在数据库服务器的前面）或靠近网关的地方（保护多个服务器中的多个数据库）。一些数据库服务器支持用安装在数据库服务器里的基于主机的代理来监控本地数据库事件。但是基于硬件的防火墙支持主机/网络监控，从而不会给数据库服务器带来任何额外负载。交易所还可以既部署硬件设备也部署软件代理，二者同时工作。

由于加密资产交易所用数据库存储关键财务信息，而数据的泄露对于交易所来说将是灾难性的，我们强烈建议部署数据库防火墙为关键数据库提供额外的安全保护。

3.2.6 第三方组件和补丁

使用第三方组件（TPC）已成为软件开发的事实标准，而且加密资产交易所一直都是这么做的。这些第三方组件包括开源软件（OSS）和商业现货（COTS）组件。被用作预制构建块的第三方组件可提供开箱即用的标准功能，使开发人员得以专注于开发产品特有的定制性能，从而缩短产品投放市场的时间并降低开发成本。尽管这些第三方组件往往被视为黑匣子，而且受审查的严格程度也低于内部开发的类似组件，但是这并不意味着它们没有风险。用户在采用第三方组件的同时也继承了它们的安全漏洞。从历史的经验看，第三方组件的挑选和使用是一项纯基于功能的工程决策。随着使用第三方组件逐渐成为一种趋势，挑选和使用第三方组件时也必须考虑它们的安全性。针对第三方组件（包括开源软件和专有商业现货软件在内）报告的漏洞数量强有力地证明，管理由第三方组件带来的安全风险是用户的一项基本职责。2014 年披露的 Heartbleed（CVE-2014-01603），以及研究人员 2015 年在 GNU C 库中发现的安全漏洞（CVE-2015-75474）就是很好的例子。这些漏洞触发业界以前所未有的规模开展分析和补救行动，在软件行业掀起一股“补丁狂潮”。第三方组件在软件开发中被广泛使用，成为攻击者进入未开发领地的引导者和邀请者。对于第三方组件不受控制随意使用的现状，必须以严格分析和充分考虑安全风险的方式来改变。

更多信息请见 NIST 出版物：

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf。

3.2.7 点击劫持攻击和 X-Frame 选项

加密资产交易所应该用“SAMEORIGIN”选项防御点击劫持。“X-Frame”选项可以让内容发布人预防攻击者把他们的内容用在不可见帧中。“DENY”选项最安全，可防止当前页面在帧中的任何使用。

有关这一安全问题的更多信息，请见：https://owasp.org/www-community/attacks/Clickjacking。

3.2.8 HSTS（HTTP 严格传输安全）和安全套接字层（SSL）

HTTP 严格传输安全（HSTS）是一个 Web 服务器指令，告知用户代理和 Web 浏览器应该怎样通过最初发送并返回浏览器的响应标头来处理连接。这将给 Strict-Transport-Security 策略字段设置参数并强制给连接实施 HTTPS 加密，从而忽略旨在通过 HTTP 给该域加载任何资源的任何脚本调用。HSTS 只是网络服务器或网络托管服务的一堆安全设置中的一个箭头而已。

究竟应该怎样为自己的网站执行 HSTS？如果你在内容结构中使用了子域，你将需要用一份通配符证书来涵盖“HTTPS ONLY”。否则的话，你需要用一份经过域验证、机构验证或扩展验证的 SSL 证书来确保安全。请务必保证这些安装正确并工作正常。有关为网站启用 HSTS 的详细信息，需向托管服务供应商咨询。

3.2.9 使用机器学习达到最佳保护效果

机器学习技术在各大交易所的安全和诈骗检测领域获得了发展动力。以下是机器学习在加密资产交易所的主要用途。

1）流分析

流分析检查资金正怎样被已知实体转移，同时把资金转移情况与先前已知的数据集进行比较。机器学习这样的技术可以用来检测潜在黑客活动。

2）地址分类

许多交易所采用了通过机器学习给钱包地址分类的方法。通过识别哪些钱包地址属于交易所钱包以及识别不同类型的个人钱包，交易所可以阻止黑客提取资金并保护用户免受诈骗。例如，面对各种 YouTube“赠品”骗局，如最近来自 Twitter 黑客的骗局，Coinbase 都能拦截资金提取。

详细信息请见：

https://www.theverge.com/2020/7/20/21331499/coinbase-twitter-hack-elon-musk-bill-gates-joe-biden-bitcoin-scam。

3）交易行为分析

循环神经网络是可以展示资产在加密资产市场上表现的一种创新方法，正被交易所用来深入了解和预测特定投资者的交易模式。这种类型机器学习可以在一组特定投资者中发现他们进行资本投资时所遵循的模式，从而把具体投资者识别出来，然后根据得出的数据准确预测他们的未来投资方式。这样的分析也可用于检测交易行为的异常和潜在的黑客活动。

4）诈骗检测

机器学习使用了由在反馈循环中相互支持的机器和人类分析师组成的一个预防系统。机器首先接受各种条件下的知名诈骗模式训练，从而掌握概括知识并在遇到类似模式时把它们识别出来的能力。人类分析师则在这一过程中逐步提高机器正确识别模式的能力，确保一切准确无误。

3.2.10 HTTP 公钥固定（HPKP）

HTTP 公钥固定（HPKP）是一种安全性能，可用来告知 Web 客户端把某一特定密码公钥与某一特定 Web 服务器关联，从而降低伪造证书的中间人（MITM）攻击风险。这一性能已被从现代浏览器中移除，不再受支持。

为确保传输层安全（TLS）会话所用服务器公钥的真实性，公钥被封装在通常由发证机构（CA）签名的 X.509 证书中。许多为任意域名创建证书的 CA 得到 Web 客户端（例如浏览器）的信任。攻击者若攻陷一个 CA，他们将能对各种 TLS 连接发起中间人攻击。HTTP 公钥固定（HPKP）则可以告知客户端哪个公钥是属于特定 Web 服务器的，以此来帮助 HTTPS 协议躲过这种威胁。

HPKP 是一种“首次使用选择信任”（TOFU）技术。Web 服务器第一次通过特殊 HTTP 标头告知客户端哪些公钥属于它时，客户端把这一信息保留一定时间。客户端再次访问服务器时，它期望证书链中至少有一个证书包含自己已通过 HPKP 知晓其指纹的公钥。如果服务器给出的是一个未知公钥，则客户端应该向用户发出警告。

有关如何启用 HPKP 的信息，请见以下链接：

https://owasp.org/wwwcommunity/controls/Certificate_and_Public_Key_Pinning。

3.2.11 使用启用了硬件安全模块（HSM）的钱包

黑客曾成功攻破加密资产交易所的在线热钱包，从中偷走数百万美元（参见 CSA GCR 发表的“加密资产交易所十大安全风险”：https://www.c-csa.cn/mobile/news-detail/i-289.html）。借助硬件安全模块（HSM）和相关安全操作把大笔资金存进冷钱包，已成为任何规模交易所工作的重中之重。

HSM 是保护和管理密码密钥并安全执行关键代码的一种物理计算设备。这些模块以“外围组件互连”（PCI）卡或可直接连接网络的外部机架式设备的形式出现。HSM 内置防篡改性能，可在发生物理破坏时擦除秘密内容。它们围绕安全密码处理器芯片以及网格等主动物理安全措施展开设计，旨在抑制旁路攻击或总线探测。这些设备在银行业和所有必须保护关键秘密的纵向行业中被大量使用。

以下是研发硬件数字钱包解决方案的公司 Ledger 推荐的一种 HSM 架构：

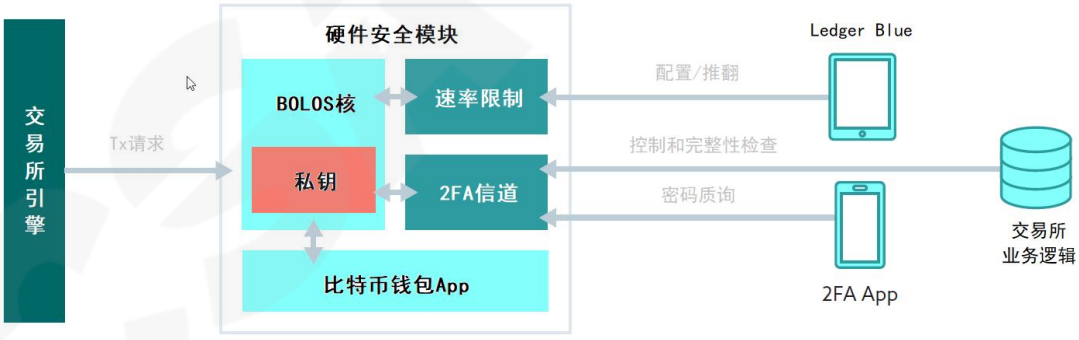


图 5 分散式加密资产交易所（dApp）

这里存在着不同的模块/服务：

1）交易所引擎：请求支付命令（客户要求提取）。

2）交易所业务逻辑：可查看所有客户余额、软/硬提取限制和支付历史的应用程序界面（API）。

3） 硬件安全模块：连接交易所数据中心服务器的 PCI 卡（如 Safenet ProtectServer HSM）。

4）Ledger Blue：由个人身份证号（PIN）代码保护并始终保持安全状态的安全设备。只有企业最高层（CEP/CTO）有权访问。

5）2-FA app：用户手机（内含非对称密钥）上的外部第二因子信道。

HSM 本身围绕以下单元形成架构：

1）区块链开放 Ledger 操作系统（BOLOS）核：Ledger OS 保护着所有密钥对的派生来源——暴露给 API 是为了让内部业务 app（如比特币钱包或撮合引擎一致性检查）都可以运行。这些 app 都经过线下测试和签名，并且在系统实时运行时无法更改。

2）速率限制器：为 HSM 得到授权可以签名的速度设置硬限制（如 1000 比特币/小时、15000 比特币/天）。这是一个巨大的数字，最终将决定整个系统遭受破坏时的最大损失量。只有得到由 Ledger Blue 签名的授权，才可以修改限制器的规则。

3）2-FA 信道：每个签名请求都必须经过它验证的内部插件。它要求得到两个质询批准：一个来自交易所业务逻辑（“请把你的新业务数据发送给我，以便我来检查它是否与之前的系统状态一致”），另一个来自用户本身（“你确认你真的要这么做吗？”）。

4）比特币钱包 app：包含为“未花费交易输出”（UTXO）池（也可以换做以太坊钱包或任何其他加密资产）构建和签名交易的所有逻辑。

详细信息请见以下链接：

https://www.ledger.com/how-to-properly-secure-cryptocurrencies-exchanges/。

3.2.12 部署零信任架构

零信任架构把所有用户视为潜在威胁，在用户能够通过适当身份验证并获得访问授权之前，阻止用户对数据和资源的访问。从本质上说，零信任架构允许完全用户访问，

但是只允许用户具有执行工作所需要的最低限度访问权。设备遭到破坏时，零信任可以保证把损害控制在一定范围之内。

零信任的概念尽管已经存在了十多年，但是支持它的技术刚刚开始进入主流。零信任架构高度依赖身份管理、资产管理、应用身份验证、网络分段和威胁情报组件和功能。零信任架构应该以不牺牲用户体验为前提增强网络安全。

如需进一步阅读，请参见以下链接：

https://threatpost.com/practical-guide-zero-trustsecurity/151912/。

3.2.13 错误处理

错误信息和堆栈跟踪不应显示在客户端的用户界面（UI）。否则黑客可以从错误信息中挖掘有关应用、数据库和服务器的信息。用户可以把未被代码捕捉到的未经处理错误记录到日志中，因为大多数语言都提供这样操作的方法（例如，.Net’s Application_Error 和 JavaScript global on_error handler）。任何未经处理的异常都代表了错误。用户的代码预料不到这一点，因此无法完美恢复或处理这种情况。把这些信息写进日志是不错的做法，可以为用户查找错误根源带来方便。于是，错误不会作为异常被连续抛出，那才属于异常情况。如果错误真的出现了，用户对它们进行分析，从而把它们捕捉出来加以处理。

3.2.14 2FA（双因子认证）

2FA 是一个额外的安全层，用于确保尝试访问在线账户者确实是他们自称的人。用户首先要输入自己的用户名和口令。接下来，他们不是被立即授予访问权限，而是被要求出示另外一条信息。

交易所的开发人员应该借助 Google Authenticator 等应用启用双因子认证（2FA）。用户应该避免用 SMS 充当第二因子，因为它的安全性比不上其他基于软件或硬件的第二因子。

3.2.15 51%攻击

51%攻击是指一群矿工控制了网络 50%以上挖掘散列率或算力后对区块链（如 ETC 区块链）发起的攻击。攻击者会阻拦对新交易的确认，从而终止部分或全部用户之间的支付。攻击者若是完全控制了网络，还可以兑回以前完成的交易，这意味着他们可以两次使用同一加密币（双花）。但几乎可以肯定的是，他们无法创造新加密币或改变旧区块。

如果黑客把加密资产 A 存入交易所并用它交易另一资产 B，然后提取资产 B，接下来对资产 A 发起 51%攻击，则加密资产交易所就要赔钱。

针对 51%攻击至少有四道防线，增加确认要求次数是其中之一。可以抵制发起攻击的实体，或者用更彻底的办法，通过分布式拒绝服务（DDoS）攻击攻击实体，也可以在协议层面更改编码。

由于攻击者在执行双花攻击之前必须等待交易确认，因此解决双花问题的简单办法是在交易完全完成之前增加确认次数。

这种做法之所以是第一道防线，是因为虽然 51%双花攻击会在 100%时间内成功，但是成功双花所需要的等待时间和金钱开支会随着每笔得交易需经确认的次数的增加而增加。确认次数越多，攻击者需要“兑回”的区块就越多。因此，“赶上”和“超越”公共分类账所需要的时间越长，成本就越高。

这条第一道防线的有效性取决于对攻击者做出更全面响应的时间期限。从理论上说，如果攻击者始终保持 51%控制权，他甚至可以兑回最久远的交易。然而，随着第一道防线以及其他防线部署完成，任何此类控制力很可能只会短暂存在。因此，增加确认次数将是对 51%双花攻击的最迅速和最简单回击。

接下来的是完全抵制攻击实体，这可能足以把散列率降到 51%以下。无论攻击的理由或原因是什么，任何此类抵制都可能是永久性的。因此，这条防线明确存在，会在攻击发生期间发挥作用，对任何追求利润的实体构成隐性威胁。

这两条防线有可能都不成功，这由攻击的时间期限和协议层面的反应有效性决定。对于这种情况，已经有人提出 DDoS 在理论上行得通，可以降低攻击者的散列率或至少

延缓他们的速度，取得立竿见影的效果；但我们只能把它当作一种临时防御手段。

对任何此类攻击的更全面响应包括，通过调整代码增加抵抗 51%攻击的能力乃至彻底消除发生 51%攻击的可能性，从而以加强针对这种企图的协议的方式获得额外的长期利益。这个层面的应对措施仍在研究之中，具体结果取决于区块链的实际执行方案。对于 ETC、比特币黄金（BTG）等比其他区块链更容易遭到 51%攻击的区块链，交易所如今可以做的只能是增加区块链的确认次数。

3.2.16 云服务安全保护

大多数加密资产交易所都通过云服务（如 AWS 和 Google Cloud）获取服务器资源。利用云安全保护云中资源至关重要。云安全包括协调一致形成保护基于云系统、数据和基础设施之合力的策略、控制、规程和技术。这些安全措施旨在保护云数据、支持法规遵从、保护客户隐私以及为个人用户和设备设置身份验证规则……。从验证访问者身份到过滤通信流，云安全可以根据企业的特定需要配置。由于这些规则可以在一个地方集中配置和管理，减少了行政管理开销，从而得以让 IT 团队把精力集中投放到企业的其他专业领域。

提供云安全的方式由特定云供应商或云安全解决方案决定。但是，云安全流程的具体执行应该是企业拥有者和解决方案供应商之间的共同责任。

有关云安全及其关键重点的详细信息，请参阅：https://downloads.cloudsecurityalliance.org/assets/research/securitguidance/security-guidance-v4-FINAL.pdf。

3.3 审计者视角的最佳安全实践

下表是区块链安全公司 SlowMist.com 为审计交易所安全状况推荐的最佳实践清单或检查列表。

该表的最新更新请见：https://www.slowmist.com/en/service-exchange-security-audit.html。

审计类别	审计子类
开源情报收集	Whois 信息收集
	真实 IP 发现
	子域名检测
	邮件服务检测
	证书信息收集
	Web 服务组件指纹收集
	端口服务组件指纹收集
	C 段服务获取
	人员结构收集
	GitHub 源代码泄漏定位
	Google Hack 检测
	隐私泄露发现
App 安全审计	App 环境测试审计
	代码反编译检测
	文件存储安全检测
	通信加密检测
	权限检测
	接口安全测试
	业务安全测试
	WebKit 安全测试
	App 缓存安全监测
	App Webview DOM 安全测试
	SQLite 存储安全审计
服务器安全配置审计	CDN 服务检测
	网络基础设施配置测试
	应用平台配置管理测试
	文件扩展名解析测试

	备份、无链接文件测试
	枚举管理接口测试
	HTTP 方法测试
	HTTP 严格传输测试
	Web 前端跨域策略测试
	Web 安全响应标头测试
	弱口令和默认口令测试
	管理后台发现
节点安全审计	节点配置安全检测
	节点数据同步安全检测
	节点交易安全审计
	节点通信安全检测
	节点开源代码安全审计
身份管理审计	角色定义测试
	用户注册流程测试
	账户权限变更测试
	账户枚举测试
	弱用户名策略测试
认证和授权审计	口令信息加密传输测试
	默认口令测试
	账户锁闭机制测试
	认证绕过测试
	口令记忆功能测试
	浏览器缓存测试
	口令策略测试
	安全测验测试
	口令重置测试
	OAuth 身份验证模型测试
	权限提升测试

	授权绕过测试
	双因子身份验证绕过测试
	散列强度测试
会话管理审计	会话管理绕过测试
	Cookie 属性测试
	会话固定测试
	会话令牌泄露测试
	跨站点请求伪造（CSRF）测试
	注销功能测试
	会话超时测试
	会话令牌过载测试
输入安全审计	跨站点脚本（XSS）测试
	模板注入测试
	第三方组件漏洞测试
	HTTP 参数污染测试
	SQL 注入测试
	XXE 实体注入测试
	反序列化漏洞测试
	服务端请求伪造（SSRF）漏洞测试
	代码注入测试
	本地文件包含测试
	远程文件包含测试
	命令执行注入测试
	缓冲区溢出测试
	格式化串测试
业务逻辑审计	接口安全测试
	请求伪造测试
	完整性测试
	超时检测

	接口频率限制测试
	工作流绕过测试
	应用误用保护测试
	非预期文件类型上传测试
	恶意文件上传测试
密码安全审计	弱 SSL/TLS 加密、不安全传输层保护测试
	SSL 固定安全部署测试
	未加密信道传输敏感数据测试
热钱包架构安全审计	谁有权访问热钱包？什么是存入和提取确认逻辑？
私钥管理系统安全审计	是否使用了硬件安全模块（HSM）？HSM 安装在什么位置？谁有权访问 HSM？

4. 加密资产交易所行政管理和物理安全

作者：**Boulevard A. Aladetoyinbo**

本章涵盖了涉及范围很广的加密资产交易所行政管理和物理安全控制措施。其中涉及的领域包括：

- 行政管理控制；
- 加密资产交易所运行的法律方面；
- 投保（对内和对外）；
- 交易所安全事件联盟；
- 风险管理流程；
- 被指定的安全责任；
- 策略和规程；
- 信息访问管理；
- 安全意识和培训；
- 安全事件处理规程；

- 应急预案；
- 评估；
- 商业合同；
- 物理控制；
- 设施访问；
- 工作站使用；
- 工作站安全；
- 设备和介质控制。

为了起到强调的作用，尽管存在着管理安全、操作安全和物理安全控制等三个基本安全控制域或分类单元，本章还是把加密资产交易所的基本行政管理和物理安全控制域以及相关加密资产交换聚合平台也包括了进来。

资料来源请见：https://www.lbmc.com/blog/three-categories-of-security-controls/。

4.1 行政管理控制

在加密资产交易所环境中，行政管理控制是操作和管理交换活动不可或缺的控制，即加密资产交易所基础设施的后端操作和功能。但是一般来说，行政管理控制定义了安全系统的人类因素。机构内各级人员都通过以下方式介入了用户访问权限确定，即用户可以访问哪些资源和信息：

- 人员登记和审核；
- 人员招聘和职责分离策略；
- 灾害防范和恢复计划；
- 培训和意识。

资料来源请见：

https://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-en-4/s1-sgs-ov-controls.html#:~:text=1.2.,-1.&text=Physical%20control%20is%20the%20implementation,Motion%20or%20thermal%20alarm%20systems。

ISO/IEC27002:2013 包含的安全目标和控制检查列表（具体请见 ISO/NP TR 23576“区

块链和分布式账本技术——数字资产托管人的安全管理”——该标准正在制定之中）与加密资产交易所行政管理控制密切相关且具有指导意义。ISO/IEC 27002:2013 引用的检查列表包括以下内容：

1. 信息安全策略；
2. 信息安全组织体系；
3. 人力资源安全；
4. 资产管理；
5. 访问控制；
6. 密码；
7. 物理和环境安全；
8. 操作安全；
9. 通信安全；
10. 系统采购、开发和维护；
11. 供应商关系；
12. 信息安全事件管理；
13. 业务连续性管理的信息安全方面；
14. 订单合规。

作者建议加密资产交易所平台出于行政管理和物理安全目的考虑执行 ISO/IEC 27002:2013 检查列表项目，如信息安全策略、信息安全组织体系、通信安全、人力资源安全、操作安全、信息安全事件管理、资产管理、访问控制、加密资产交易所持续管理的安全方面、合规、系统采购、开发和维护等。

上文所列各项对于加密资产交易所平台采用和落实信息安全实践规范具有很强的指导意义，可以作为交易所信息安全控制目标的部分基石。

4.1.1 基础设施配置不同并分属不同分类单元的集中式、分散式和混合式加密资产交易所

加密资产交易所的基础设施可以按集中、分散和混合三种模式配置。与分散式和混

合式交易所这两个分类单元相比，集中式加密资产交易所是更受欢迎和被更广泛采用的一种配置模式。加密资产交易所的特殊配置会影响交易所基础设施的行政管理和物理安全考虑，也就是说，中心化交易所（CEX）具有与去中心化交易所（DEX）或混合式交易所（HEX）不同的行政管理和物理安全考虑，反之亦然。

作者进一步建议，对于加密资产交易所，应该根据其交易的可能会产生经济、金融、法律、监管等影响的加密资产的技术架构、性质、功能、特征和现实状况进行大致分类。

1） 中心化交易所（CEX）

与去中心化交易所不同，这是一个托管的中心化交换平台，它借助数据库（SQL 的或非 SQL 的）进行用户数据存储、管理、维护、发行、交易，以及清算、结算、托管等活动。CEX 的订单簿、出价、加密资产交易所交易数据历史、市场数据、AML/KYC 数据，以及客户交易私钥、事件、设置、配置等，都由一个中央数据库服务器系统集中控制和管理。市场上目前总共有 600 多家集中式加密资产交易所。

资料来源请见：https://www.cryptowisser.com/exchanges/。

2） 去中心化交易所（DEX）

点对点（P2P）分散式加密资产交易所的市场基础设施直接构建在去中心化分布式加密分账共识算法上，如工作量证明（PoW）、股权证明（PoS）、分布式股权证明（DPoS）、异步拜占庭容错（aBFT）等。DEX 与构建在集中式交换撮合引擎上的 CEX 不同，后者没有加密共识算法，也没有分布式分账技术（DLT）后端平台。

去中心化交易所有别于其他加密资产交易所分类单元，几乎不可能被黑客入侵，原因在于它往往散布在全球各地。此外还因为它没有中央服务器数据库系统。广布于全球无数节点上的服务器通过转化降低了风险，绝对不会出现服务器宕机情况，对网络攻击具有天然的虚拟免疫力。虽然媒体时不时爆出中心化交易所遭遇黑客攻击的消息，但是迄今还没有人报道去中心化交易所的黑客事件。

资料来源请见：

https://www.cryptowisser.com/centralized-exchanges-vs-decentralizedexchanges/。

3） 混合式交易所（HEX）

HEX 结合了集中式和去中心化交易所的价值定位和特征，例如 DEX 的安全性和保密性以及 CEX 的流动性和功能性。尽管与 CEX 乃至 DEX 相比，HEX 的采用率要低很多，但正在逐渐兴起。

有关混合式加密资产交易所运行和概念的直观详细信息，请参见：https://www.espay.exchange/hybrid-crypto-exchange-software 以及下文所示另一网址展示的 Legolas 混合式交易所结构图解：https://decenter.org/en/hybrid-crypto-exchanges：

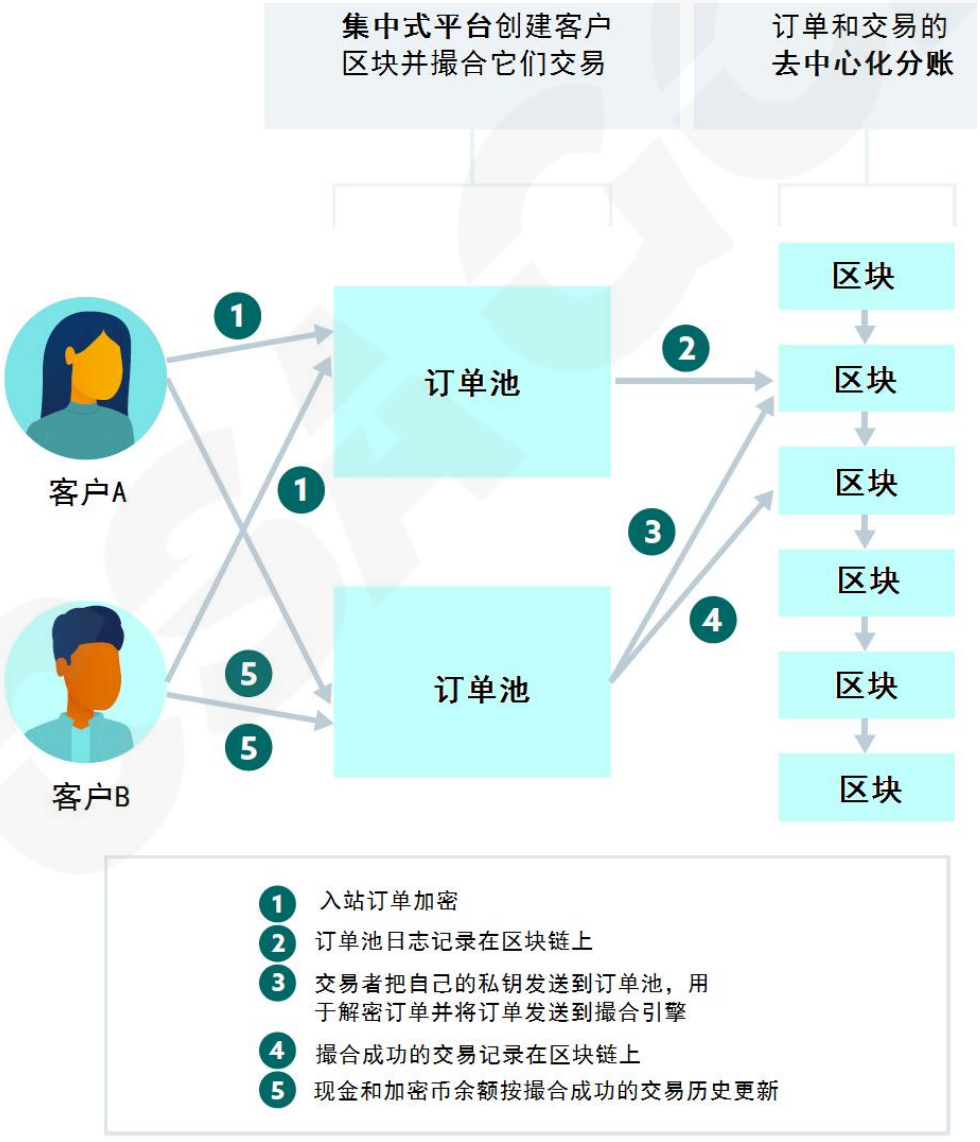


图 6

4.1.2 三种加密资产交易所基础设施配置的差异和特点

中心化交易所（CEX）	去中心化交易所（DEX）	混合式交易所（HEX）
托管（加密资产交易所交易私钥始终托管）	非托管（不托管加密资产交易所交易私钥）	同时托管和非托管（两者特性的结合）
构建在 Internet Web 2.0 上	构建在 Internet Web 3.0 去中心化计算网站应用接口上	同时构建在 Internet Webs 2.0 和 3.0 去中心化计算系统上
保留订单簿	不保留订单簿	灵活处理
不安全，保密性不强	安全和保密	”
被采用得更普遍	被采用得不太普遍	与 CEX 和 DEX 相比，被采用得远要更不普遍
高流动性	低流动性	”
非去中介化；非点对点；具有中央权限或可信第三方（TTP）	去中介化；点对点；无中央权限；无可信第三方（TTP）	”
要求在“了解客户”（KYC）/“反洗钱”（AML）方面遵守当地法律法规	不要求在 KYC/AML 方面遵守当地法律法规（但是 KYC/AML 法规和程序可以通过算法自动化将法规逻辑写进分布式分账智能合约，从而融入底层协议）	”

1）加密资产交易所聚合平台

除了在基础设施配置和分类单元方面各具特色的集中式、分散式和混合式加密资产交易所之外，还存在着许多聚合平台，这些平台基本上是加密资产交易所集成平台，通过一个统一的通用接口简化用户体验，从而消除了跨多个加密资产交易所多次登录的规程困难。

这些平台还得到最佳安全实践指南关注进而被写进相关内容，因为它们属于加密资产交换信息系统值得赞赏的部分，尽管它们处在常规配置和分类单元之外。

资料来源请见：

- https://hedgetrade.com/what-are-dex-aggregators/
- https://coinmarketcap.com/alexandria/article/what-are-dex-aaggregators-a-deep-dive-by-1inch
- http://blog.ionixxtech.com/5_benefits_of_building_a_cryptocurrency_aggregator_platform/

4.1.3 以安全的十个方面为依据确定加密资产交易所信息资产的安全级别

加密资产交易所必须符合并遵守某些行业行政管理最佳安全实践标准，如 RedTeam Security 的 “加密货币安全标准（CCSS）”开放标准，这是旨在管制存储、接受或交易有效比特币、以太坊等加密资产的所有信息系统的一套要求。CCSS 强化了标准信息安全实践，同时还补充了现行信息系统安全标准，如 ISO/IEC 27002:2013、PCI DSS 等。虽然 CCSS 是加密资产交易所理所应当落实的，因为交易所本身就是一种存储、接受和交易加密资产的信息系统，但是，加密资产交易所还应该补充其他安全控制防护措施，用以保护安全管理组件运行的环境。

1) 安全级别确定

同时也用于系统安全意识评分的 CCSS 是确定加密资产交易所整体安全合规级别的一个评定体系。安全级别共分三级，CCSS 指导委员会对它们分别进行了描述。

a. 安全一级——最低加密资产安全评级，但还是为经过审计证明的信息资产提供了强有力的安全措施。一级安全措施涉及在信息资产风险已得到抑制的情况下使用行业标准控制。

b. 安全二级——二级采用经过强化的控制，安全措施的强度超过一级。机构使用实现了多重签名的去中心化安全技术，基本上可以为关键系统遭破坏或关键人员出事的情况提供冗余备份便是安全级别二级的例子。

c. 安全三级——最高级别，提供了最全面的安全措施。加密资产交易所的信息系

统应该证明自己达到了这个安全级别，而这意味着加密资产交易所不仅正式制定了策略和规程，而且还把它们落实到业务流程范围内的每项干预措施之中，从而超越了经过强化的安全级别。这个级别的突出特点是关键操作必须有多个行动者参与，通过高级身份验证机制保护数据的真实性，以及把资产分散保存在多个地理区域和机构，最大限度减少乃至彻底消除资产遭破坏的任何机会。

2) 安全的十个关键方面

“加密货币安全标准”（CCSS）强调的十个关键方面涉及硬件和软件组件、人员、策略、规程等。它们分别是：

- 密钥/种子生成；
- 钱包创建；
- 密钥存储；
- 密钥使用；
- 防密钥泄露策略；
- 密钥持有人资格授予/撤销策略和规程；
- 第三方安全审计/评估；
- 数据清理策略；
- 储备证明；
- 审计日志。

资料来源请见：https://cryptoconsortium.github.io/CCSS/。

加密币安全标准	一级	二级	三级
密钥/种子生成			
钱包创建			
密钥存储			
密钥使用			
防密钥泄露策略			
密钥持有人资格授予/撤销策略和规程			
第三方安全审计/评估			
数据清理策略			
储备证明			
审计日志			

4.2 加密资产交易所运行的法律方面

加密资产交易所的运行在法律方面主要涉及在一个司法管辖区内建立法人资格并达到该司法管辖区的合规标准。目前，分散式加密信息系统兴起、监管不力、缺少立法等情况，再加上某些跨司法管辖区的其他因素，使实际上并未注册的虚拟组织形式的加密资产交换平台不断涌现。不仅如此，需要与上述因素更广泛结合考虑的还有这样一个事实：基于互联网的加密资产交易所基础设施解决方案具有跨国性质，不仅需要有国家层面的立法和监管行动，法律合规框架、指南、政策和标准，而且还需要有国际标准制定机构的监督和各国的跨国合作。把加密资产交易所基础设施与已知特定国家的司法管辖区（而非“数字司法管辖区”）“挂钩”就是在形成一个门槛，而这恰恰是加密资产交易所必须重视并加以解决的。尽管有法人资格的加密资产交易所实现正规化是所有加密资产交易所都必须做到，但是还有许多涉及持续和积极遵守纳税、“反洗钱”（AML）/“了解客户”（KYC）和“反资助恐怖主义”（CFT）等法规的多层面问题有待交易所给出答案。加密资产交易所基础设施在法律方面也是跨加密资产交易所配置和分类单元的。

加密资产交易平台的所有特征和表现形式都必须在其所涉及的法律方面符合所有规定。加密资产交易所基础设施要围绕以下几个领域解决基本、法律和运行方面的问题。

1） 法人实体的设立问题

法人实体问题涉及加密资产交易所的基础设施是否属于实际上没有注册的虚拟组织（即所谓“不受监管的交易所”）。如果是，则说明它设立不当，必须在称职法律顾问的帮助下纠正过来，确保在所涉公认司法辖区内合法合规。国家层面和国际上的法律、法规和政策都会对法人实体问题产生影响。

资料来源请见：

https://www.nortonrosefulbright.com/en/knowledge/publications/e383ade6/cryptocurrency-exchanges-and-custody-providers-international-regulatory-developments。

由于分布式分账基础设施具有跨国境性质，而加密资产交易所的信息系统又是在这个基础设施上构建而成的，因此有着密切的国际关系。值得注意的是，即便是集中式和混合式加密资产交易所，由于基于互联网，也是跨多个司法管辖区存在的，因为用户可以在系统上从不同司法管辖区注册。

2) 反洗钱（AML）和反资助恐怖主义（CFT）合规

落实尽职调查要求是加密资产交易所接纳新用户的先决条件。而通过“反洗钱”（AML）/“了解客户”（KYC）审查则是加密资产交易所获得行业准入资格的必要条件——无论交易所设立在在哪个司法管辖区都是如此。CipherTrace 的“2020 年春季加密货币犯罪和反洗钱报告”指出，主要发展趋势突出显示，加密资产交易所收到的直接非法资金在比例上已经减半，像 LocalBitcoins 这样的集中式加密资产交易所连续第三年成为直接犯罪资金的首选。在交易所之间的转账总量中，跨国境加密资产交易所占据了四分之三，因为美国的比特币用户越来越偏好通过高风险交易所开展加密资产交易活动。

金融行动特别工作组（FATF）成员国的加密资产交易所必须遵守“旅行规则”（Travel Rule）；这个规则要求虚拟资产服务供应商（VASP）在进行虚拟资产转移操作的过程中，立即安全地获取、持有和传输交易发起人和接收人信息，以应对洗钱和资助恐怖主义威

胁。这些要求尽管不是强制性的，但是既有说服力也切实可行，乃至非 FATF 成员国也纷纷效仿。加密资产交易所应该认真研究 FATF 的虚拟货币 AML/CFT/KYC 建议和标准，以及有关全球打击洗钱和资助恐怖主义行动的报告。FATF 发布了多项建议，寻求在“旅行规则”的范畴内简化传统上适用于现有金融服务行业参与者的加密资产交易所操作。FATF 的第 16 条建议主要要求加密资产交易所在发起人和接收人之间共享客户交易数据。

资料来源请见：

- https://fas.org/sgp/crs/misc/R43339.pdf；
- https://getid.ee/aml-kyc-crypto-exchanges-wallets/；
- https://ciphertrace.com/spring-2020-cryptocurrency-anti-money-laundering-report/；
- https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rbavirtual-assets.html；

3) 纳税合规考虑

尽管许多司法管辖区还没有颁布全面的加密资产纳税监管制度，但是大多数司法管辖区依然为加密资产交易所依照现行法律规定了虽然可以享受必要豁免但也必须在一定程度上履行的义务。这方面的典型案例是美国国税局诉 Coinbase Inc.等公司案（Case No.17-cv-01431-JSC-2017）。加密资产交易所应该全力遵守即将出台的税法——这些法律将为经营相关信息资产的加密资产交易所充分履行其具有纳税含义的义务指明合规路径，将体现这一领域的内在特性。

资料来源请见：https://casetext.com/case/united-states-v-coinbase-inc。

4) 可疑交易举报（STR）/可疑活动举报（SAR）义务

在金融监管词汇中，“可疑交易举报”（STR）/“可疑活动举报”（SAR）背后的理念是，为金融机构规定举报潜在、可疑违法行为之义务具有迫切必要性。尽管各国对于在什么情况下必须举报可疑金融交易没有统一标准，但有一点是一致的：在金融机构看来没有意义的交易属于应该举报的情况。此外，对于特定客户介入异常交易或有意把两笔单独的交易混为一谈的情况，金融机构也有举报义务。

加密资产交易所有义务根据其建立或常驻地所属司法辖区的法律以及相关和适用国际、双边和/或互惠条约向有关当局举报交易所发生的可疑交易。

资料来源请见：https://en.m.wikipedia.org/wiki/Suspicious_activity_report。

5) 隐私保护合规义务

加密资产交易所的运营商有义务保护其平台上的用户私人数据。因此，他们有义务遵守自己所在国和地区或国际数据保护法律中适用于相关事实和情况的现行和新颁布的法规。《欧盟通用数据保护条例（EU GDPR）》、《欧盟第 5 号反洗钱指示令（5th EU AMLD》和《欧盟第 6 号反洗钱指示令（6th EU AMLD）》等是这方面法规的几个例子。

6) 制裁筛查控制

制裁筛查原本是传统金融机构内部用于检测和预防制裁风险的一项管理措施，如今范围已经扩大到视为金融市场基础设施不可分割组成部分的加密资产交易所基础设施。因此，加密资产交易所的信息系统也必须做到制裁筛查合规。

加密资产交易所的用户、客户和姓名筛查应该针对加密资产交易所金融市场基础设施上个人和企业实体的目标身份识别和客户关系生命周期进行设计和准备。

资料来源请见：

https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/Wolfsberg%20Guidance%20on%20Sanctions%20Screening.pdf。

4.3 交易所投保：对内和对外

4.3.1 加密资产交易所的对内和对外投保义务

集中式加密资产交易平台一直很脆弱，过去和现在都饱受遭遇黑客攻击。没有哪种解决方案或手段可以保证完全挡住可能的未来黑客攻击。因此，向保险公司投保的策略具有减轻黑客攻击所可能给交易所带来的任何财务负担或难题的必要潜力。加密资产交

易所和托管存储平台必须为抵御盗窃、第三方黑客攻击、诈骗、欺瞒、破坏 API 凭证、网络钓鱼软件、暴力破解攻击、恶意软件攻击、侵吞、人为错误、钱包密钥丢失、以刑事犯罪手段敲诈勒索、数据无意泄露等风险同时对内和对外投保。

就交易所基础设施加密资产责任险保护、客户资金保险实践等而言，由于加密资产交易服务供应商目前尚处于起步阶段，几乎没有历史经验可供借鉴，好在现在有许多行业标准零星开发或发布出来并被公共和私营部门参与者采用，旨在建立相关原则和指南，用以保护客户资金，并在加密资产交易服务供应商、用户、公共和私营机构之间培育出一种加密资产交易所资产保险实践文化。

作为一项最低安全标准保护措施，加密资产交易平台应该预留一部分交易保证金给自己投保，用以在发生任何黑客攻后补偿客户。Binance 加密资产衍生品交易所的自筹资金投保计划“确保用户资产安全基金（SAFU）”具有典范意义，作为一种可实现客户资金保护战略目标的标准加密资产行业实践规范，值得大力推广。加密资产交易所必须像传统非加密资产交易基础设施模式的实践和标准那样，吸收、整合和推行内部和外部客户资金保险最佳实践文化。交易所可以在自保之外与保险公司等机构等订立保费保单合同。

资料来源请见：

- https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.forbes.com/sites/jeffkauflin/2019/09/05/lloyds-of-london-aon-and-others-poised-to-profit-fromcryptocurrency-hacker-insurance/amp/&ved=2ahUKEwikhI-7-OfrAhVzqHEKHX3wBNsQFjALegQIARAB&usg=AOvVaw1hD4nkg9JNgJuCSenbhvPM&ampcf=1
- https://www.binance.com/en/blog/421499824684900373/Liquidation--Insurance-Funds-How-They-Work-and-Why-They-Are-Important-to-CryptoDerivatives-Part-2。

保险机构系统以及加密资产交易基础设施内部和外部信息系统中可投保的关键部分包括以下系统：加密资产持有人系统（H）、保险公司系统（I）、区块链网络（B）和加密资产交易所系统（E），下图将用浮雕图形粗体字的形式把它们分别标识出来：

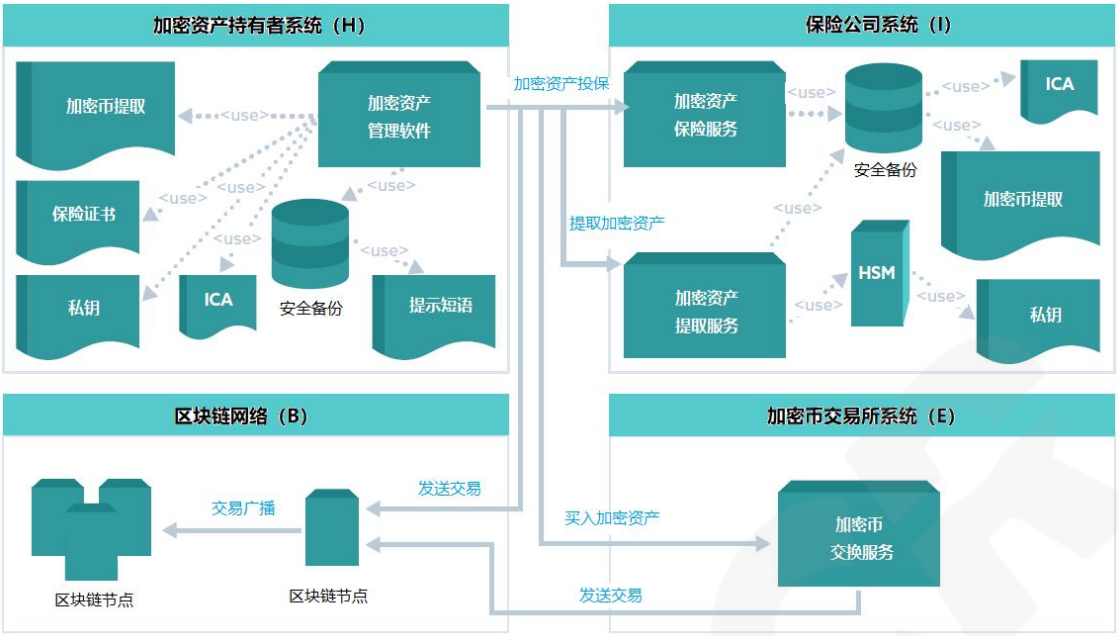


图 7 加密资产交易所系统和保险公司系统交互图

资料来源请见：https://link.springer.com/chapter/10.1007/978-3-030-57805-3_4。

1) 区块链网络（B）

这是一个分布式分账节点聚合系统，由网络节点总体、交易广播和交易发送组成。

2) 加密资产交易所系统（E）

加密资产交易所系统主要由加密资产买入、发送交易等加密资产交易服务组成。

3) 加密资产持有者系统（H）

由加密资产提取、加密资产管理软件、保险证书、安全备份、私钥、独立计算架构（ICA）、助记短语等成分和活动组成。

4) 保险公司系统（I）

保险公司系统由加密资产保险服务、数据库、ICA、加密资产提取服务、加密资产提取、硬件安全模块（HSM）和私钥组成。

4.3.2 加密资产、热钱包、冷钱包和多重签名钱包投保

现有和新兴的保险公司和机构都可提供加密资产保险服务，覆盖加密资产、热（在线）钱包和冷（离线）钱包。伦敦劳合社便是这样一家保险公司。除了前文用粗体文字和图形显示的可投保加密资产交易所资产外，加密资产交易所的其他可投保基本资产包括：

1) 加密资产

加密资产是可投保的基于密码资产，给它们投保，是为了抵御经营和操作风险。但是事实证明，在这一过程中，履行监管机构规定的加密资产交易所资产投保要求义务却是一项艰巨任务。加密资产交易所方面之所以会遇到这种困难，是因为保险公司对加密资产固有和关联的风险缺乏深入了解，没有能力为加密资产提供合格的保险覆盖。为身处传统金融服务业的加密资产交易所和加密资产贸易公司提供适当的保险，要求保险公司及其承销商花大力气研究加密资产数字投资方面的知识。

一些司法管辖区针对加密资产交易所颁布政策和监管许可证计划的公告称，保险公司和加密资产交易所经纪人可能不具备尽职合规所需要的知识资源、经验和适当的加密资产信息系统。香港证券及期货事务监察委员会（SFC）的加密资产交易所和加密资产投资公司许可证计划要求考虑了以下内容：

客户加密资产托管。加密资产交易所运营商必须确保对冷存储中保存的加密资产实施高达 95%的实质性和主动保单风险覆盖，而对热存储中保存的加密资产则须实施百分之百覆盖。

挑选保险公司的数据驱动决策标准。加密资产交易所运营商必须把数据驱动的研究、可验证性和可量化性用作为加密资产交易所挑选投保保险公司的基本依据。由此可以得出参保加密资产估值方案、每次事件的最大覆盖范围、总体最大覆盖面以及每次事件的任何其他独有因素。

黑客攻击事件的理赔处理。索赔要求应该由加密资产交易所运营商、关联实体或保险公司全面解决。客户的索赔诉求产生于因加密资产交易所关联实体违约而发生的黑客

攻击事件。

资料来源请见：

- https://www.hedgeweek.com/2020/06/04/286220/crypto-exchanges-and-investmentsfirms-g-insurance-challenges-says-evertas。
- https://news.bitcoin.com/the-difference-between-custodial-and-noncustodialcryptocurrency-services/#:~:text=Custodial%20cryptocurrency%20services%20include%20most,your%20assets%20within%20their%20system。
- https://www.internationalinvestment.net/news/4011749/lloyd-launch-crypto-insuranceservices#:~:text=Insurance%20giant%20Lloyd%27s%20of%20London,price%20changes%20of%20crypto%20assets。

2) 在线钱包（“热钱包”）

在线存储钱包与互联网连接，因此完全在线。加密资产交易所应该制定加密资产在线钱包投保计划，用以保护客户保存在交易所保险库和在线存储中的加密资产，并在发生黑客攻击和相关事件时给予充分赔偿，以防客户加密资产蒙受损失。

由于加密资产交易所的在线存储系统存在已知和未知漏洞，面临各种风险、威胁和攻击，加密资产交易所进行在线钱包存储设施维护时，应该恪尽职守，格外小心。大多数“热钱包”都没有被制定保险政策；因此，加密资产交易所必须为其在线钱包基础设施投保，这更是因为与离线钱包相比，在线钱包安全性较低，更容易受黑客和技术漏洞的影响。

作为在线钱包投保策略的一部分，加密资产交易所应该建立一个与在线钱包所持金额相等的保险基金，以防客户加密资产资金未来发生损失，进而影响交易所的经营和声誉。

资料来源请见：https://www.techriskreport.com/2020/04/cryptocurrency-insurance-for-hot-wallets/。

3) 离线钱包（“冷钱包”）

冷钱包是与热钱包相对而言的。加密资产在冷存储时完全保持离线状态，因此不会以任何方式连接互联网。纸钱包应该用来创建离线存储钱包系统，使私钥公钥对与令牌关联，除非出于特殊目的需要通过 USB 设备或任何其他便捷方式连网交易，否则绝不与互联网连接。

资料来源请见：

- https://www.bitcoin.com/get-started/setting-up-your-own-cold-storage-bitcoin-wallet。
- https://www.coindesk.com/crypto-com-lands-record-360m-insurance-cover-for-offlinebitcoin-vaults。
- https://www.google.com/url?a=t&source=web&rct=j&url=https://www.forbes.com/sites/jeffkauflin/2019/09/05/lloyds-of-london-aon-and-others-poised-to-profit-fromcryptocurrency-hacker-insurance/amp/&ved=2ahUKEwikhI-7-OfrAhVzqHEKHX3wBNsQFjALegQIARAB&usg=AOvVaw1hD4nkg9JNgJuCSenbhvPM&ampcf=1。
- https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.financemagnates.com/cryptocurrency/exchange/bittrex-scores-300-million-in-crypto-insurance-from-lloydsof-london/amp/&ved=2ahUKEwikhI-7-OfrAhVzqHEKHX3wBNsQFjAOegQIBBAB&usg=AOvVaw2re_y6NQv5rL6nO_gFP6RV&ampcf=1。

4) 多重签名钱包（Multisig）

多重签名钱包是指需要用多个实体的私钥授权才能交易的钱包配置。这种钱包的主要使用者是加密资产交易所，目的是确保交易所加密资产客户的资金在保护下不受心生歹意的内部员工侵害。由于多重签名钱包存储介质保存了加密资产，因此它是可投保的，理应被针对第三方黑客攻击、私钥盗窃或其他相关潜在事件而设的险种覆盖。相对于非托管加密资产钱包，加密资产交易所更应该采用多重签名钱包来提升安全能力。

多重签名钱包账户应全部投保或一定金额投保。在多重签名钱包投保环境下，会有多个不同实体持有密钥并控制钱包内的交易执行。加密资产交易所、交易所用户和保险公司服务供应商都是密钥持有者。这营造了一种充分分散风险、适当调整和转移风险的状态，确保加密资产多重签名钱包得到安全保障，因为它们会使技术和非技术用户对自己持有加密资产产生一种安全感，把他们从对恶意加密资产黑客攻击或加密资产资金失

窃的担心中解脱出来——他们只需保持警惕，谨慎从事，便可挡住任何社会工程黑客。

资料来源请见：

- https://www.coindesk.com/lloyds-backs-new-crypto-hot-wallet-insurance-scheme-fromcoincover。
- https://link.springer.com/chapter/10.1007/978-3-030-57805-3_4。
- https://coincentral.com/bitcoin-insurance-policies/。
- https://news.bitcoin.com/how-to-use-multisig-to-keep-your-coins-ultrasafe/#:~:text=Multi%2Dsignature%2C%20or%20multisig%2C,has%20applications%20for%20end%2Dusers.(v)https://www.google.com/amp/s/cointelegraph.com/news/civicwallet-now-offers-1m-fdic-like-insurance-for-crypto/amp。

4.4 交易所安全事件联盟

协同合作是密码系统必须具备的有力工具，可用来防止、抑制或完全阻止针对加密资产交易所的各种可能攻击。业内的加密资产交易所应该建立预防或管理安全事件的行业联盟。加密资产交易所应该本着确保加密资产客户资金和交易所基础设施安全的目的携手组成行业联盟。这种联盟和合作应该促进加密资产交易运营商、网络安全主题专家、分布式账本区块链协议（制定者）、专门从事加密资产交易合规工作的公司等之间的团结。这种加密资产交易所联盟在安全事件管理方面的进一步目标，应该是抵御不良行为者和行骗者的外部第三方攻击、加密资产交易所（尤其是集中式加密资产交易所）常年面临的潜在风险、威胁和漏洞。尽管分散式和混合式加密资产交易所在风险、威胁和漏洞方面的情况有所不同，但是总的来说，任何信息系统都不可能对安全事件免疫。

使业界为对抗潜在加密资产交易所攻击和提高安全保护水平而协同合作的努力真正发挥作用的行动措施包括，建立一个去分散式事件报告响应系统，在加密资产交换行业组织成员之间收集和共享情报，形成打击和抵御诈骗、洗钱以及困扰加密资产交换基础设施服务市场的其他异常现象的强大力量。通过聚合算法跟踪分账交易数据历史、可疑交易监控以及将恶意加密资产交易钱包地址列入黑名单等，都是行之有效的策略。

协同合作可以在加密资产交换行业参与者之间达成共识，形成得到共同承认的安全

保护标准，同时还有助于保持系统完整性。由于加密资产交换行业是一个充满竞争的新兴增长领域，参与者应该齐心协力，把韧性、信誉、正直、诚信等优良品质注入行业体系。业界应该有一个渠道，用来在不损害每个系统运行的独特性，保持行业竞争态势的前提下共享和学习有用的知识和信息。这种协同合作的深入展开应能形成一种深度防御，实现实时监控、数据共享、诈骗检测，使交易所区块链/分账数据的隐私和保密性得到保护。

资料来源请见：

- https://www.binance.com/en/blog/421499824684900916/Cryptosafe-Alliance-Bringing-Better-Security-for-the-Crypto-Industry。
- www.cryptosafe.org。

4.5 风险管理流程

加密资产交易所的金融交易往往必须满足一定的先决条件，唯有如此，才能保持交易所运行的完整性、保险性、安全性并最大限度规避风险。金融运行的风险涉及波动性以及不可能合理预期加密资产交易所可为交易所用户承担的某些其他市场风险。下文将列举加密资产交易所所面临的风险以及相应的风险应对措施。

1) 交易所服务器故障风险

为加密资产交易所的运行服务的服务器存在着容易发生故障，从而导致信息系统数据丢失、无法恢复的风险。数据中心云存储系统的数据泄漏到外部服务器上也是一种潜在数据丢失风险。

交易所服务器故障风险的应对措施

加密资产交易所必须通过一项数据备份应急预案协议来应对加密资产交易所服务器故障风险。数据存储设备应该单独安放在远离加密资产交易所服务器的地方，并且对交易所服务器的运行和活动没有任何依赖。作者建议交易所通过一切可能的手段分散和平摊交易所服务器故障风险，以此作为一项应对措施。

交易所在开始运行之前，就应该制定一项备份计划，然后定期更新和调整实际做法和需要考虑的因素。此外，还建议和推荐交易所定期进行备份协议检查，确保发生事故时能快速恢复数据。

2) 交易所监管合规风险

加密资产交易所必须满足法规遵从要求，但有时也有可能出现无法满足一些法规要求的情况，因此极易受法规遵从风险的影响。加密资产交易所的常规合规具有跨国境的性质，因为可能会有来自交易所所在主权国所在地以外不同司法辖区的公民和居民登录和使用交易所系统，从而带来交易所用户所在司法辖区的“了解客户”（KYC）/“反洗钱”（AML）法规合规风险问题。因此，地方监管机构、国际标准制定组织以及监管官员都有介入调查交易所经营情况的潜在可能性。不合规可能会导致交易所网站屏蔽，银行可能关闭集中式加密资产交易所的法定货币银行操作账户。

交易所监管合规风险的应对措施

对于这个基本门槛问题，作者建议，加密资产交易所首先必须遵守其主要开展经营活动的主权国所在地的当地法律，以此作为先决条件性最低标准。合规要求包括获得经营许可证、履行纳税义务等。随着业务往前推进，遵守投资者保护、安全控制、可疑交易人工验证、用户身份识别、KYC/AML 计划要求等国际最佳实践标准也会成为这个过程的关键。

3) 交易所用户资金损失风险

集中式加密资产交易所存在客户资金损失风险，这种风险通常以黑客攻击、未经授权访问基础设施、盗窃、数据泄漏、内部人员作业/破坏、第三方黑客攻击、人为错误等形式出现。

交易所用户资金损失风险的应对措施

交易所必须确保客户资金在严密保护下可以抵御每种固有的信息系统风险。因此，交易所必须针对软件和基础设施的脆弱性、错误和漏洞利用点集中执行保护措施，从而

强化系统，使其具有应对攻击、人为错误等的良好韧性。

其他相关应对措施还有，建立事件快速响应安全管理团队，培训开发人员尽快识别系统漏洞，推动内部和外部安全审计团队协同合作，配备系统管理员监测和调查可疑活动，启用双因子认证（2FA）功能作为额外的客户资金保护措施，把交易所客户资金合理分布在离线和在线钱包中等。

4) 加密资产交易所基础设施故障风险

交易所在进行提取和交易操作时，会遇到伴随需求和相关增长不断提升而来的问题。因此，现场基础设施故障风险表现为黑客攻击风险、声誉损失风险、与第三方服务集成风险、客户资金余额管理风险、担责风险等。

加密资产交易所基础设施故障风险的应对措施

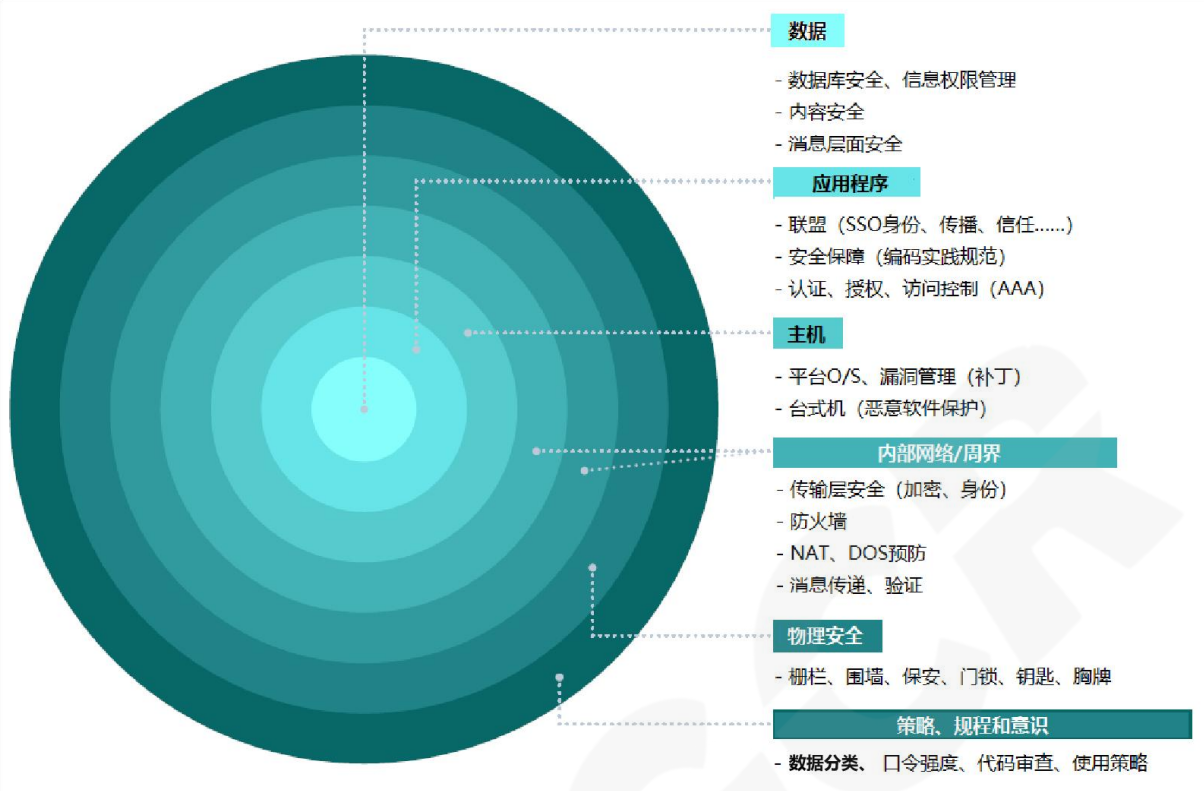
加密资产交易所基础设施可以把扩展策略和模拟测试用作应对故障风险的措施。交易所应该用微服务架构解决方案预防基础设施发生故障。所采用的软件算法必须允许在不影响整个基础设施性能的情况下更改任何服务，从而提升安全水平并保证基础设施的不间断运行。

资料来源请见：

https://www.0hub.com/blog/crypto-exchange-risk-management#:~:text=Any%20exchange%20deals%20with%20financial,market%20risks%20for%20their%20owners。

4.6 指定的安全责任

尽管机构担任着重要角色，但是在机构供职的人员也都有遭遇技术和非技术攻击的危险，因此他们全都要对交易所的安全问题或被指定的安全责任负责。加密资产交易所对实施安全保护责无旁贷，因为整个信息系统架构的安全取决于交易所落实的最佳安全实践。交易所必须把整个信息技术系统分成多个层级部署安全控制措施，以此营造一种“深度防御”文化，让最大限度提高安全水平的思维方式态渗透到业务流程的每个方面。交易所必须对涵盖了骚乱和攻击预防、业务连续性规划、用传输层安全（TLS）协议给



通信流自动加密、网络、应用防火墙功能以及其他相关信息系统基本资产的交易所各个关键基础设施安全保护领域做通盘考虑。

图 8

关于加密资产交易所的网络安全责任，交易所的每名工作人员都必须参与其中。事实上，一种涵盖人、流程和技术等所有方面的方法可以确保网络安全风险管理和抑制最佳实践规范得到全方位落实。

4.6.1 交易所人员的安全责任角色分配

1) 高管团队

首席执行官（CEO）。由董事会和股东选出，是公司里级别最高的高管成员。CEO 的基本职责涉及公司的重大决策、整体运行和资源管理，同时充当董事会与公司运营之间的主要信息沟通渠道，并在公司发生重大改变时与公众交流。

CEO 在公司组织体系内具有巨大影响力，他们有权力也有责任为交易所设定基调和愿景，从而在机构组织体系内营造出一种最佳网络安全实践文化。

首席技术官（CTO）/首席信息官（CIO）。CTO 公司内级别最高的技术官员，通常向 CEO 报告并担任为加密资产交易所安全负责的角色，其中包括主管研发工作。CTO 的角色深入介入对机构技术需求和资本投资利用战略的短期和长期分析，以实现加密资产交易所的既定目标。

首席信息安全官（CISO）。由于信息安全问题已成为包括加密资产交易所在内的商业机构的头等大事，首席信息安全官的角色和责任对于机构抵御信息系统安全风险具有战略性的重要意义。

建议 CISO 应该在充满挑战的加密资产交易所业务环境中积极开展建立正确安全制度、良好治理实践规范、无风险支持框架和可扩展业务运行体系的工作。

首席运营官（COO）。COO 作为高管团队的关键成员直接向 CEO 报告。建议首席运营官承担设计和落实交易所业务发展战略、计划和规程的责任，同时负责制定促进形成企业文化、实现远期愿景的政策，并且还负责监督加密资产交易所公司的运行，其中包括公司其他高管的工作，通过对相关数据和指标的分析和说明充分发挥绩效评估的作用。

首席财务官（CFO）。作为公司高管团队的成员之一，首席财务官应该监督加密资产交易所公司的财务安全问题，分析交易所的财务实力并提出必要的改进和提高建议，以克服被识别出来的交易所财务弱点和缺陷。首席财务官的工作角色应该是跟踪现金流，监督资本投资，把控公司的资本结构，做出预算，预测未来的业务发展，参与相关谈判并处理上报来的财务事项。

风险与合规管理官。建议风险与合规管理官负责执行合规策略和规程，其中包括定期内部审查合规表现，以确保加密资产交易所完全符合所有法律和监管条件。

风险与合规管理官的角色和责任涉及用第三方分析工具筛查存取操作，确保 KYC/AML 合规并监控经由加密资产交易所系统的所有交易，其中包括进一步执行提取控制，要求对提取请求进行可疑交易和可疑速度筛查，以预防可能的诈骗，同时还严格控制资金访问权限。

风险与合规管理官应该担任的其他角色还包括，为加密资产交易所提供认证和评估

机会。

2) 开发团队

交易所技术基础设施开发团队负责开发和监督源代码的部署和运行，以保持源代码的逻辑和质量，同时还参与安全编码，把编好的代码交给同行审议，严格按交易所安全软件开发生命周期（SSDL）的规律行事，结合使用各种静态源代码分析工具，由此最大限度确保交易所安全。

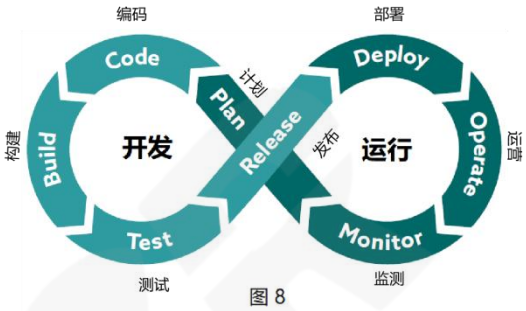


图 8

加密资产交易所部署的智能合约必须接受外部审计认证。对于交易，必须通过双因子认证（2FA）加以保护，而口令加生物特征识别、电子邮件验证、电话验证和认证凭证验证等手段也必须采用。作为交易所交易保护策略的一部分，还应通过电子邮件验证来监测强制性外部地址白名单，将此列为交易所最佳安全实践措施之一。

开发团队应负责威胁建模、通过多种攻击向量对加密资产交易所信息系统基础设施进行渗透测试，以及外包第三方渗透测试进行独立外部审计。这种内外结合的网络安全专业研究的介入极为重要，有潜力确保交易所信息系统基础设施的安全和稳定。开发团队还应负责引入和监督详细的安全评价和评估措施，以找出并披露有可能对加密资产交易所系统造成破坏的脆弱性、错误和漏洞利用点。

安全评价和评估措施应该包含以下详细内容：

- 威胁建模，确保安全控制完备无缺；
- 风险控制检查，确保隐私风险管理最佳实践标准真正落到实处；
- 认证并遵守 PCI:DSS3.2.1（支付卡行业合规要求标准）、ISO/IEC 27002:2013（信息安全管理）、ISO/IEC 22701:2019（隐私风险管理）和“加密币安全标准”（CCSS）等标准，以及专门针对包括去中心化 Web 应用、加密资产交易所和加密资产存储解决方案在内的加密资产信息系统的各项合规要求标准。

3) 计算机安全事件应急响应小组（CSIRT）

这是一个常备不懈的信息技术专业人员团队，其任务和职责是围绕着预防、管理和协调潜在网络安全紧急情况向加密资产交易所提供服务和支持。

在任何情况下，只要加密资产交易所系统发生数据泄露或其他安全事件，CSIRT 都有责任通过有效的事件响应和恢复援助及时做出响应，以重获控制权并最大限度减少损失，进而确保防止安全事件在未来再次发生。

资料来源请见：

- https://news.bitcoin.com/drawbacks-of-cryptocurrency-exchanges-how-non-custodialservices-are-the-solution/。
- https://crypto.com/en/security.html。
- https://www.sciencedirect.com/science/article/pii/B9780124199675000053。
- https://aws.amazon.com/security/。
- https://www.investopedia.com/terms/c/chief-technology-officer.asp。
- https://www.roberthalf.co.nz/our-services/finance-accounting/cfo-jobs。
- https://resources.workable.com/coo-job-description。
- https://resources.workable.com/coo-job-description。
- https://whatis.techtarget.com/definition/Computer-Security-Incident-Response-Team-CSIRT。
- https://www.bmc.com/blogs/ciso-chief-information-security-officer/。
- https://www.synopsys.com/blogs/software-security/secure-sdlc/。

4.7 策略和规程

目前新兴加密资产交换行业已经一次性或持续将一些标准式实践规范措施用在交易所新客户注册上。这些措施将构成交易所策略和规程的基石。这便是加密资产交易所平台落实“了解客户”（KYC）/“反洗钱”（AML）要求并设置客户注册条件或制定相关规程的标准。建议加密资产交易所应该建立新用户注册规程，新的预期用户必须经过多个阶段并接受过尽职调查后才可注册成为合法用户。

若要签发、交易、清算、结算、发送、接收、存入或提取个人托管在加密资产交易所的加密资产等，首先必须满足客户身份验证和验证流程要求。为此，加密资产交易所必须制定一个全面的 KYC/AML 方案并建立注册规程。加密资产交易所在必须满足许多必要条件的同时（其中包括使用条款、客户保护、法律和合规以及隐私策略），还必须提交一份完整的披露安全陈述，说明加密资产交易所会怎样或计划怎样保护属于托管性交易所基础设施保护义务范围内的用户加密资产。为了防止金融诈骗和犯罪风险，加密资产交易所必须安排客户接受严格的尽职调查。客户注册的身份验证参数应能确保，试图把交易所用作犯罪和洗钱活动渠道的不良行为者得不到任何便利。

4.7.1 加密资产交易所“了解客户（KYC）”的组成模块

1) 策略

交易所的隐私策略/可接受政策/注册策略。业界必须有一套通行的交易所隐私策略指南，用以指导客户数据收集、存储、保管、使用、控制、处置等操作，供交易所据此管理客户的个人可识别消息。加密资产交易所应该根据自身经营的变化、新的发展趋势以及法律法规的演变不断修改自己的隐私策略。交易所必须在这些修改或修订正式生效前通知交易所用户。

隐私政策应明确阐明在访问和注册交易平台上提供服务的信息处理做法。用户在访问和使用交易所之前，首先要表明自己接受使用条款。交易所对信息的收集和处理必须符合适用数据隐私保护法律法规包含的制约规定、相关限制和保护要求。每当个人可识别信息必须得到用户同意才可处理时，应事先征求用户意见并获得用户同意。

交易所应该依照适用法律时常通过第三方渠道获取用户信息，其中包括来自公共数据库、征信机构和身份验证合作伙伴的信息。由于这些信息非常重要和十分敏感，加密资产交易所应该在第三方合同条款中规定，第三方必须采取适当的物理、技术和行政管理保障措施来保护被委托给交易所或由第三方拥有并支配的个人隐私信息的安全性和保密性。

2) 规程

识别规程。加密资产交易所的“了解客户”（KYC）验证产生于洗钱和资助恐怖主义漏洞方面的考虑。因此，需要有一套规程在加密资产交易所平台的入口点乃至客户在平台上的整个生命周期中定期和持续识别潜在客户。其中包括通过以下方式识别和验证个人用户：

A. 个人可识别信息；

a. 全名；

b. 出生日期；

c. 国籍；

d. 签名；

e. 性别；

f. 费用单；

g. 电话号码；

h. 电子邮箱地址；

i. 家庭住址，等等。

B. 正式身份信息：

a. 居民身份证；

b. 纳税身份号；

c. 签证信息；

d. 护照号和所有相关信息都应收集，确保最大限度达到和遵守“反洗钱”（AML）和“了解客户”（KYC）尽职调查要求。

C. 供职单位信息：

a. 工作证（或政府签发的等同证件）的号码；

b. 法律信息形成的证明（由公司文件，即公司章程、组织大纲等，提供的证明）；

c. 所有有用的材料、雇主的个人身份信息。

D. 财务信息：

a. 银行账户详细信息；

b. 支付卡主账号（PAN）；

c. 交易历史；

d. 交易数据；

e. 纳税识别方式。

E. 交易信息：

a. 交易发起者信息（即姓名等）；

b. 交易接受者信息（即姓名等）；

c. 金额；

d. 公共区块链交易数据散列分析；

e. 时间戳；

f. 其他交易信息相关数据。

F. 受雇信息：

a. 工作单位地点；

b. 职务；

c. 角色描述。

G. 通信往来：

a. 调查响应；

b. 提供给加密资产交易所（交易所支持团队或用户研究团队）的信息；

c. 潜在加密资产交易所用户注册成功之前，需经历多个级别和阶段的身份识别；潜在用户需要在每个阶段接受一系列行动或指令，然后再进入下一个阶段，直到身份验证和检验过程全部完成。个人可识别信息（PII）保护应该是加密资产交易所最需要重视的问题，因为它们是客户敏感财务数据的保管人，有义务也有责任把这些信息照管好。

3) 风险管理

处理、管治、控制、引导和维护加密资产交易所托管风险是加密资产交易所运营商的固有角色和责任，特别是当有实体代表用户用托管在交易所的私钥签署加密资产交易的时候。这种情况在分布式分账智能合约去中心化金融（DeFi）应用中可能会有所不同，例如在去中心化交易所（DEX），用户在本地托管自己的私钥并用来签署交易，因此无需像在中心化交易所（CEX）那样，每次签署数字交易都要求助去中心化交易所调用托管给它的私钥。

4) 交易所加密资产交易监控

作为“了解客户”（KYC）尽职调查义务的组成部分，加密资产交易所应该定期和持续监控所内进行的交易。对交易的监控包括对交易所分账/区块链上交易数据活动的监视，对操作和状况的检测，以及对入站和出站交易数据流（从加密资产到加密资产，从法定货币到加密资产以及从加密资产到法定货币）的跟踪和持续检查。

5) 投诉管理框架/客户支持服务

加密资产交易所必须设置一个有力的框架来管理客户投诉，或者建立一种客户投诉支持机制来处理会对客户活动和数据保护产生影响并且可能会在某个重要时刻登上交易所公告的问题。交易所必须安排一名数据保护官（DPO）全天候值班，随时处理客户投诉的数据保护问题。客户合理地认为自己的数据权利受到侵犯并向交易所内部客户服务支持机制提出投诉后，交易所即便自身缺乏能力解决问题，也必须被允许向外部相关数据保护权威机构求助。

资料来源请见：

- https://www.google.com/amp/s/cointelegraph.com/news/memo-to-crypto-exchanges-kyc-compliance-can-be-a-competitive-advantage/amp。
- https://www.google.com/url?sa=t&source=web&rct=j&url=https://readwrite.com/2020/04/20/know-your-customerregulations-in-crypto-exchanges/amp/&ved=2ahUKEwjn_fikmKXtAhVOD2MBHZ38CCoQFjAQegQIBhAB&usg=AOvVaw0GjcemPka9lEPD2Y_V1C6_&ampcf=。
- https://www.google.com/amp/s/readwrite.com/2020/04/20/know-your-customerregulations-in-crypto-exchanges/amp/。
- https://cointelegraph.com/news/more-than-half-of-all-crypto-exchanges-have-weak-or-noid-verification。
- https://ciphertrace.com/2020-geo-risk-report-on-vasp-kyc/。
- https://www.coinbase.com/legal/privacy#:~:text=We%20will%20not%20use%20your,personal%20information%20with%20third%20partie。

4.8 信息访问管理

身份与信息访问是相互交织、相互关联的。加密资产交易所的身份和信息访问管理制度或战略必须确保，只有正确、适当和被指定的人员可以在得到授权的情况下按被指定的时间访问加密资产交易所信息基础设施。加密资产交易所应该建立一个策略和技术框架，用以保证只有适当职位的适当人员拥有并保持对交易所企业资产和技术资源的适当访问权。加密资产交易所的系统管理需要借助相关工具和技术来实施机构内关键信息的用户访问控制。严格管理哪些人有权在什么时候、以什么方式访问加密资产交易所的信息系统，对于交易所的安全运转来说至关重要。这其中必须考虑和挑选交易所机构需要的最有效和最安全的访问认证形式、物理防范措施、对各种系统信息的访问限制，以及监控谁正在访问、谁有权访问或他们在访问什么类型信息的能力。无论使用的是哪种数据存储设施，也无论把数据存储或复制在本地、远程服务器还是到云端，都要把这些因素考虑周全。

1) 需要强调的风险

拥有信息访问权的员工可能会擅自更改、与人共享或删除敏感文件，如工资单、人事档案、公司保密数据等。其他伴随而来的风险还包括员工可能会未经授权访问特定应用程序，以及身份盗用、勒索、破坏、诈骗、间谍活动等。

2) 权限访问控制（管理权）

交易所应该控制哪些人可以通过 Windows 服务器或其他操作系统等类似渠道以个人或群组身份访问哪些文件、文件夹和应用程序。这里的典型情况是，财务部门的所有人员都可以访问交易所的采购分类账。但是尽管如此，只有具有额外访问权限的财务人员可以查看交易所的工资明细。

加密资产交易所的信息访问管理实践规范必须确保以下几点：

- 系统性审查人员信息。在权限到期和必要时访问和更改人员权限。
- 限制人事“管理员”权限的数量和范围。

- 周密考虑访问权的分配，即在规模较大的机构环境中，权限的分配要以个人担任的角色而非人与人交互的情况为依据。
- 考虑只授予用户账户与用户工作相关的权限。例如，备份用户不需要安装软件，而只需运行备份和与备份相关的应用程序；应该避免授予备份用户任何其他权限，例如允许安装新软件的权限（这就是所谓“最小权限原则”）。
- 考虑采用额外的控制措施，例如严密监控拥有特殊访问权限的用户。
- 每名员工都应拥有一个唯一的用户 ID，通过用户名和口令认证后登录。对待用户 ID 应该像对待办公室钥匙或个人报警码一样，不得以任何方式与人共享或泄露给他人。
- 在类似于建立新员工记录的问题上，必须安排不同的人员参与这个过程，其中包括由不同的人员分别负责工资和信息技术访问权部分（这就是所谓“职责分离”）。
- 在向新入职、调动职位或升职的交易所员工授予访问权时，必须仔细考虑应该授予哪些访问权限。
- 所有计算机都必须设置成要求安全登录访问，若几分钟无人看管，可自动注销。
- 用户离开交易所业务信息系统体系后，必须立即取消他们的访问权限。

3) 认证访问控制

当行使访问权的用户通过用户名和口令登录凭证识别识自己，从而暗示他们有权访问特定文件、文件夹或应用程序时，系统应该提示他们，他们必须证明他们确实是自己声称的那个人。现有三种识别身份的基本证明方法可供使用：

- 用户拥有的某物，可以是密钥、电子令牌、唯一的随机加密密钥或智能卡。
- 用户知道和记住的某物，比如助记短语、口令、个人身份识别号码（PIN），甚至可以是父亲的名字。
- 可供生物特征扫描的某物，即指纹等。

上述因子的部署和使用相互补充，尤其再配以更常用的口令（但建议口令采用字母数字的复杂组合，以形成更强的安全保障），可以从控制系统访问的角度更让人放心地识别用户自称的身份。通过双因子、三因子或多因子认证实施保护，可以提供更强的安

全信心，因为它们会使出于获得访问权目的冒充用户的行为变得更难得逞。

有关使用得更普遍的口令，建议加密资产交易所注意以下几点：

- 加密资产交易所信息系统必须设置得只接受强口令访问，同时锁闭用错误口令进行访问的尝试。
- 系统默认口令必须更改，以加强和强化访问条件。
- 预定的定期更改口令的要求必须强制执行。
- 处置弃用设备时，必须确保设备上安全清除了口令和用户名登录凭证以及所有相关保密信息。
- 对用户开展有关口令重要性和社会工程风险教育。

4) 单点登录（SSO）策略

强烈建议加密资产交易所考虑采用单点登录策略，作为信息访问管理最佳实践文化的一部分。这是一种集中式会话认证和用户服务，其中用户名和口令登录凭证可用于访问多个应用程序。此项策略的精髓是，用户一旦登录，便可访问无数服务，无需每项服务都重新登录。

资料来源请见：

- https://www.csoonline.com/article/2115776/what-is-sso-how-single-sign-on-improvessecurity-and-the-user-experience.html。
- https://www.google.com/amp/s/www.csoonline.com/article/2120384/what-i-iam-identityand-access-management-explained.amp.html。
- https://www.getsafeonline.org/information-security/information-access-management/。

4.9 安全意识和培训

加密资产交易所应该调动必要力量就安全保护的各个环节开展培训，以抵御可能会对交易所信息系统安全产生负面影响的内部和外部攻击向量。有关基础和基本知识的安全意识培训计划和教材应该具有针对性，面向具体交易所人员制定，而不能仅限于泛泛

之谈，即便它们匹配并反映了加密资产交易所的商业价值、目标、使命和愿景。

从交易所网络安全本身，到隐私问题、社会工程攻击、其他风险、潜在威胁、漏洞及相关问题，全都应该被培训的基本主题和典型领域涵盖。

交易所的安全意识教育和培训计划涉及两个方面。首先是针对交易所人员的专门培训，其中着重强调涉及持有密钥的员工的安全意识、角色和规程，因为他们拥有并体现了加密资产交易所信息的访问权限，因此他们是培训的重中之重。

第二个方面是组织主要客户就如何使用加密资产交易所并与之交互接受培训和教育——这方面的培训是形成新兴行业统一最佳实践规范的必要条件。

资料来源请见：

- https://www.sciencedirect.com/book/9780124199675/building-an-information-securityawareness-program#book-description。
- https://www.sciencedirect.com/topics/computer-cience/workstation-security。
- https://www.sciencedirect.com/book/9780128047545/cyber-security-awareness-for-ceosand-management。
- https://www.sciencedirect.com/topics/computer-science/security-awareness-program。

4.10 安全事件管理规程

加密资产交易所必须采用结构化安全事件管理规程和方法，以此响应和处理交易所信息系统生命周期中可能发生的网络威胁、入侵和其他安全事件。条理清晰的事件响应计划（IRP）必须针对已经识别出来的威胁或漏洞，把损害的影响降至最低限度，加大网络攻击成本并预防未来可能发生的系统攻击。交易所必须建立适当的事件响应规程来限制网络安全事件的影响，必须明确规定，安全团队在发生事件期间面对忙碌的 IT 环境活动时必须严格依照哪些规程要求行事。建议加密资产交易所除了制定全面的事件响应计划外，还应编制完整的事件响应计划检查列表。制定一项事件响应策略，是在开始落实事件响应计划之前补充计划欠缺内容一种有效手段。标准做法是，安全分析人员发现网络安全事件后立即报告，同时马上通知相关数据主体方和有关部门。

《加州消费者保护法（CCPA）》等隐私法规提出了许多隐私方面的规定，就企业收集的消费者的个人可识别信息（PII）授予消费者以额外的数据隐私拥有控制权。CCPA要求，发生任何网络安全事件后须公开通知数据主体，在有些情况下还必须就个人信息的状况向数据主体做出陈述。《欧盟通用数据保护条例（EUGDPR）》也就个人可识别信息数据泄露通知的问题授予了数据主体类似的权利。世界上其他国家的隐私立法也有相似的规定。与此相关的还有《支付卡行业数据安全标准（PCI DSS）》，该标准为支付卡行业规定了一系列要求，旨在确保负责处理、存储或传输信用卡数据的机构营造出高度安全的 IT 环境，用以维护最佳实践文化，从而保持最高数据安全和隐私水准。

4.10.1 事件响应计划检查列表规程

加密资产交易所响应事件的各个阶段应该有序涵盖针对网络安全事件检测、反应、范围和固有风险等预先确定的所有步骤。此外，还应该有复合式的全面快速响应步骤可供使用。按步骤做出周密计划的事件管理响应可以避免意外情况频发以及机构对品牌和客户造成损害。事件响应计划应该考虑如何就意外风险以及事件响应安全结果跨业务单位和地域在利益相关者之间沟通。

1) ISO/IEC 27035-1:2016 标准“五步骤规程概述”

- ISO/IEC 标准 27035 提出了一个涉及安全事件管理的五步骤流程。这五个步骤分别是：
- 为处理事件做好充分准备；
- 通过监测和报告识别潜在安全事件；
- 对识别出来的事件进行评价，确定抑制风险的适当后续措施；
- 根据得到认可的事件评价通过控制、调查和解决等步骤做出事件响应；
- 总结和归纳安全事件的关键要点，为应对将来可能发生的任何事件做好准备。

2) NIST 计算机安全事件处理指南（SP 800-61）

NIST 的这个标准与 ISO/IEC 27035 略有差异，但有异曲同工之妙。SP 800-61 建议的事件响应管理标准和阶段如下：

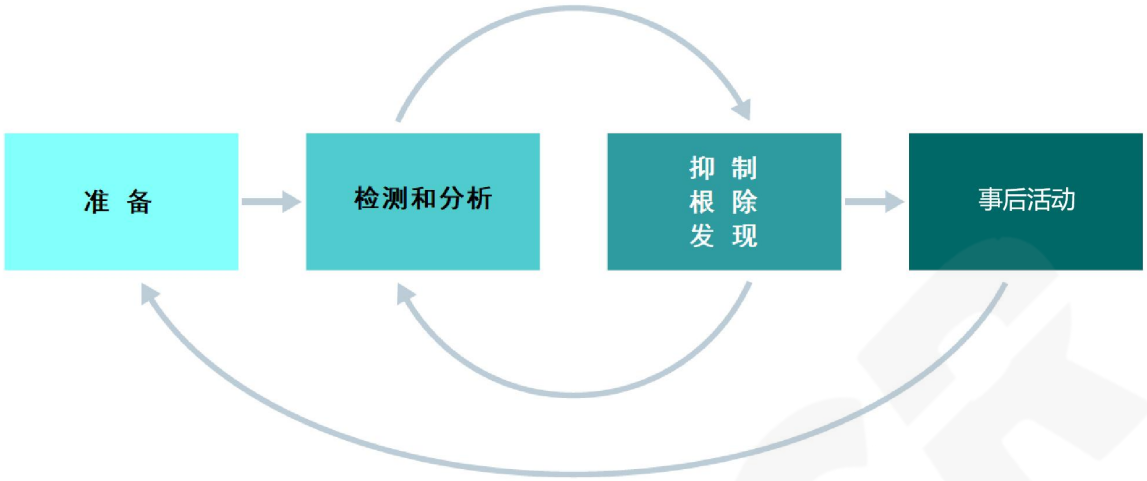


图 9 NIST 建议的网络安全事件响应阶段

- 准备；
- 检测和分析；
- 遏制、根除和发现；
- 事件后的行动。

资料来源请见：

- https://www.exabeam.com/incident-response/steps/。
- https://digitalguardian.com/blog/five-steps-incident-response。
- https://www.exabeam.com/incident-response/the-three-elements-of-incident-responseplan-team-and-tools/。
- https://wou.edu/ucs/files/2015/11/WOU_Incident_Resp_Plan.pdf。
- https://www.bitlyft.com/what-is-security-incident-response-plan-2/。
- https://oag.ca.gov/privacy/ccpa。
- https://digitalguardian.com/blog/what-security-incident-management-cybersecurityincident-management-proces。

4.11 应急预案

加密资产交易所（集中式、分散式和混合式）常年处于网络攻击和黑客攻击之下，因此必须建立全面的网络安全应急预案；应急预案是内含针对加密资产交易信息系统基础设施提出安全实践指示说明、注意事项和行动建议的风险管理书面文件，用于应对紧急情况、灾害、发生事件安全破坏事件或系统运行中断时的数据恢复。作者建议加密资产交易所制定一项基本危机管理计划，定期举行危机演习或模拟，以此作为交易所应急预案安排的组成部分。

NIST 的《联邦信息系统应急预案规划指南（NIST SP 800-34）》具有很好的指导意义和针对性，可帮助公司和机构制定布局合理、实际操作性强的信息系统应急预案。网络安全应急预案由多个成分组成，分别针对加密资产交易所信息系统中必须得到重视的不同方面。这些成分包括：

1) 灾害恢复计划

灾害恢复计划是正式成文的书面规程和策略，用于指导发生网络攻击事件、自然灾害或任何重大系统运行中断事故后如何恢复和保护信息系统。在信息技术环境中，灾害恢复计划是通过从备用信息存储系统（即为应对紧急情况而设置的站点）恢复加密资产交易所信息系统和应用来落实的。

2) 紧急模式运行计划

业务连续性计划提出了相关指南和规程，主要针对发生安全破坏事件（即紧急情况、灾难或加密资产交易所信息系统运行中断）期间和之后怎样保持日常业务的正常运行。而紧急模式运行计划（EMOP）则包含需要得到支持的系统和操作。EMOP 的缺点体现在它只涉及短期保持业务的连续运行，而对业务的长期连续运转和恢复缺乏规划。EMOP 在系统遇到勒索软件入侵等网络攻击时可以发挥抑制风险和减少系统关键资产损失的作用。

3) 数据备份计划

有关加密资产交易所运营商在关键信息资产遭遇网络攻击时应该如何运作的应急预案，目前已经有了全面的定义。不过还要建议交易所应该制定一项行之有效的数据备份计划，以便发生网络攻击后快速恢复服务。

4) 灾害恢复计划(DRP)

该计划把数据和信息快速重导入存储系统，以此作为一项灾后恢复措施。灾害恢复计划是涉及面更广的整体业务恢复计划（BRP）的组成部分，发挥着关键性的作用。加密资产交易所运营商需要通过灾害恢复计划来实现并保持加密资产交易所信息服务基础设施的持续平稳运行。

灾害事件的分类尽管不能穷尽所有类别，但是根据信息系统类型的独特性，还是能够广泛涵盖各种损害的自然后果的。

资料来源请见：

- https://study.com/academy/lesson/cybersecurity-contingency-plans-purposedevelopment-implementation.html。
- https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7149346/。
- https://www.financemagnates.com/cryptocurrency/news/nydfs-wants-crypto-exchangescorona-contingency-plans/。
- https://www.cisecurity.org/spotlight/cybersecurity-spotlight-disaster-recovery-plan-drp。

4.12 评估

建议从传统信息技术环境普遍存在的威胁、漏洞和网络安全风险的角度评价和评估加密资产交易所。其他评估内容还包括加密资产交易所信息平台独有的新威胁、漏洞和网络安全风险——加密资产交易所网络安全最佳实践评估也应基于这一准则。

加密资产交易所在开始运行之前，必须了解和掌握处理交易和加密资产时必须掌握的网络安全基础知识。此外，交易所还应出于多种目的实践这些网络安全基础知识，保护加密资产信息系统架构免受恶意网络攻击侵扰。通常情况下，集中式加密资产交易所

被黑客入侵，客户资金被盗，即便没有产生其他附带后果，也意味着交易所败给了恶意黑客。提供托管服务的集中式加密资产交易所，只要接受了资产托管，就必须在加密资产的整个金融数据生命周期内对客户加密资产金融数据的安全和保障负责。

以上述准则所列必须考虑和确定的内在因素为基点对可持续发展的加密资产交易所进行的评估可使客户得到足够的安全感。“CER and Hacken”的专家在一份题为“网络安全评分（CSS）百强加密交易所”的报告中证明了这一点，其中的标准是对加密资产交易所系统基本成分进行安全审计的全面评价模型，其中包括：

- 服务器安全；
- 用户安全；
- 持续众包安全评价（OCSA）。

加密资产交易所应该出于强化网络安全并对其进行评估的目的发起发现漏洞有奖众包活动，邀请网络安全研究人员和黑客帮助查找交易所系统软件代码中存在的可能躲过了交易所开发人员和整个安全架构团队眼睛的漏洞和配置错误。

资料来源请见：

- https://www.secureworldexpo.com/industry-news/cryptocurrency-exchange-cybersecurity。
- https://www.securitymagazine.com/articles/87925-how-to-evaluate-your-securitysystems-cyber-ris。
- https://www.securitymagazine.com/articles/87925-how-to-evaluate-your-securitysystems-cyber-risk。
- https://hacken.io/research/researches-and-investigations/top-100-crypto-exchangesaccording-to-the-cer-cyber-security-score-css/。
- https://hacken.io/wp-content/uploads/2019/07/100-Exchanges-CSS-Report.pdf。

4.13 物理控制措施

物理控制是指按结构化定义执行的安全措施，用于威慑或防止对敏感系统材料的未经授权访问。这些控制措施可以规定，只允许对关键系统数据库基础设施和日期记录进

行逻辑、合理、物理和受权访问。物理控制和逻辑控制是两种涉及面很广的访问控制类型。物理访问控制适用于物理信息技术资产、建筑物、房间和任何物理硬件财产并限制对它们的访问。而逻辑访问控制针对的则是计算机网络访问、连接和系统数据文件。

资料来源请见：https://searchsecurity.techtarget.com/definition/access-control?amp=1。

相关物理安全控制的例子有：

- 闭路监视录像；
- 运动或热警报系统；
- 安保人员；
- 带照片的身份证件；
- 上锁的和有固定门闩的房门；
- 生物特征识别（包括指纹、语音、人脸、虹膜、笔迹和用于识别人的其他自动化方法）。

资料来源请见：

- https://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-en-4/s1-sgs-ovcontrols.html#:~:text=1.2.,-1.&text=Physical%20control%20is%20the%20implementation,Motion%20or%20thermal%20alarm%20_system。
- https://www.f5.com/labs/articles/education/what-are-securitycontrols#:~:text=Physical%20controls%20describe%20anything%20tangible,areas%2C%20systems%2C%20or%20assets。

作者强烈建议加密资产交易所为加密资产风险评价定义明确的控制目标，同时挑选适当的安全控制。安全控制分类模型按类型把控制划分为物理控制措施、技术控制措施和管理控制措施三类，按功能把控制措施划分为检测、预防和纠正三类：

资料来源请见：

https://www.f5.com/labs/articles/education/what-are-securitycontrols#:~:text=Physical%20controls%20describe%20anything%20tangible,areas%2C%20systems%2C%20or%20assets。

物理控制措施还包括加密资产渗透测试，针对存储、接受或交易加密资产的更广义机构（加密资产交易所也在其中）的三层渗透测试：

1) A 级

第一层 A 级包括针对交易所加密资产的网络和应用程序渗透测试阶段。这一层主要由网络安全专家对应用软件以及网络、系统、设备、主机等进行测试。渗透测试旨在模拟实际网络物理攻击场景并模仿实际恶意方采用的方法。

加密币服务	网络和应用 渗透测试	社会工程	物理渗透 服务测试
A级	✓		
B级	✓	✓	
C级	✓	✓	✓

2) B 级

第二层 B 级包括网络和应用渗透测试以及社会工程测试阶段。在这个阶段，渗透测试人员主要测试电子邮件/电子邮件附件、电话和现场谋略，查验人力资产对恶意攻击的易感性。社会工程渗透测试的目标包括加密资产交易所利益相关人、员工和供应商，攻击向量可能包括鱼叉式钓鱼、网络钓鱼、电话诈骗、网页、冒充他人、病毒、即时消息、欺骗、恶意软件、弹窗等。

3) C 级

第三层 C 级包括网络和应用程序渗透测试、社会工程和物理渗透测试。物理渗透测试评价是为了了解加密资产设施、加密资产交易所、矿机、矿场、硬件存储设施、销售部门、计算机设备、比特币 ATM 机等受到物理攻击时会发生什么情况。除此之外，所设置的三个层级可以共同和分别探究各种因素在加密资产交易所遭遇恶意网络攻击的场景中的表现。

资料来源请见：

- https://www.redteamsecure.com/services/penetration-testing/cryptocurrencypenetration-testing/。
- https://www.redteamsecure.com/blog/4-key-cryptocurrency-security-measures-are-youfollowing-them。
- https://www.sciencedirect.com/science/article/pii/B9780124199675000089。
- https://www.sciencedirect.com/science/article/pii/B9780124160071000133。
- https://www.upguard.com/blog/attack-vector。

4.13.1 设施访问

设施访问是安全保护的关键成分之一，提到它时，人们往往会想起它的传统含义，例如安排安保人员全天守在办公楼设施的大门前。这就是企业保护设施和员工的方式。然而随着时间的推移，人们对这种设施安全保护措施的认识发生了变化。设施还会面临工业间谍、火灾和其他自然灾害的威胁；即便机构采用了防盗报警系统，心怀歹意的人

也能在没有授权的情况下混进设施大门。保护员工和资产免受伤害和损失是企业的责任，这种保护应该从设施大门开始。对设施和工作现场实施访问控制，是确保工作场所安全的关键环节。

1) 设施访问控制

加密资产交易所运营商应该对设施和工作场所的人员进出保持控制，只允许得到授权的访客、供应商和员工出入；并在可能的位置实施限制和约束。交易所应该建立一个便于查阅的记录，记下进出的访客、供应商和员工，他们去了哪里，在做什么以及是什么时候离开的。发生火灾或自然灾害事件时，可把员工、供应商和访客的下落告知现场急救人员。访客和供应商的出入管理功能也可以实现自动化。

Apposite 是一种基于技术的系统，可用来扫描政府签发的身份证件（如驾驶执照），查询访客的性侵犯者行为即时评估结果、犯罪历史记录等，还可以打印带照片的临时身份标牌；这种电子门禁系统可以通过查验用户、供应商、员工、访客的登录访问凭证、门禁读卡器、审计和报告来跟踪员工、供应商和访客。交易所还应该设置第二次扫描，用以记录员工、供应商和访客离开交易所的时间。发生紧急情况时，交易所可以当即查看滞留在设施内的员工、供应商和访客人员名单。

作者向加密资产交易所推荐三种访问控制功能：

- 身份验证，是指对员工、访客、供应商、用户进行的身份识别和认证，旨在确保他们不是会对设施构成潜在威胁的恶意行为者。
- 授权，是指验证用户、雇主、供应商、访客身份后准许他们进入设施。
- 控制，是指限制和约束个人在什么条件下才允许访问哪些区域的决定，如访客造访设施时必须有人员伴随。控制还包括通过记录系统跟踪离开设施的材料等其他方面。

资料来源请见：

- https://content.boonedam.us/pillar/making-physical-security-part-of-cybersecurity-bestpractices。
- https://www.securitymagazine.com/articles/92518-the-need-for-cybersecurity-andphysical-secu

rity-convergence。

- https://www.sans.org/reading-room/whitepapers/physical/physical-securityimportant-37120。
- https://www.energy.gov/sites/prod/files/2018/01/f46/cyber_securing_facilities.pdf。
- https://facilityexecutive.com/2020/08/cyberattacks-cybersecurity-and-facilities-systems/amp/。
- https://searchsecurity.techtarget.com/definition/access-control?amp=1。
- https://www.officespacesoftware.com/blog/5-ways-facilities-managers-can-helpstrengthen-cybersecurity。
- https://safetymanagementgroup.com/facility-access-is-a-critical-component-of-safety/。

4.13.2 工作站使用

一般来说，工作站是一种高性能、高可扩展专用计算机系统，秉承单用户基本设计理念，具有先进的图形能力、大存储容量和强大的微处理器 CPU。工作站这个词还指不具备处理能力但与大型计算机连接的终端。

工作站的能力是个人计算机（PC）不可比的。然而尽管如此，工作站在管理各种外围 PC 工作站网络并在这一过程中管理大数据处理和报告任务方面的进步，已经被中档计算机落下。大多数工作站的微处理器都执行了“精简指令集计算”（RISC）架构，这与执行“复杂指令集计算”（CISC）架构的大多数个人计算机形成对照。在 RISC 架构下，数据处理、加速和流线化三位一体，因此，工作站运行的应用软件必然比 CISC 架构下的应用程序包含更多的指令而且也更复杂。

与大多数个人计算机中速度呈指数级增长的 16 位系统相比，工作站的微处理器通常提供 32 位地址（表示数据处理速度）。但是，还有一些高级工作站实现了 64 位微处理器，其数据寻址能力是 32 位机的 40 亿倍。

工作站固有的高端原始处理能力可接纳高分辨率或 3D 图形界面、多软件复杂运行以及与其他计算机相互通信的高级能力。

1)工作站的用途

工作站的使用是为了执行分配给它的日常操作和活动。

密集计算。典型工作站的性能高于个人计算机。它具有更强的 CPU 处理能力、同时执行多项任务的能力等。工作站的主要用途是执行涉及科学工程任务的密集计算。

工作站还可用于比较密集的任务，如数据可视化和相关操控、3D 设计、模拟、制作动画、数学绘图、渲染图像或视频文件、搜索海量数据库、重新计算大型电子表格并对其进行操控、计算机辅助设计制图或同时运行多个大型应用程序。

金融和商务应用。工作站会用于复杂的金融和商业应用场景，因为个人计算机运行这些商务应用的速度太慢。个人计算机的低速特性是由于它们缺乏足够的处理能力和可用内存造成的。

高端工作站可用来通过本地工具和应用程序为连网的“客户端”个人计算机网络提供数据访问和操作服务。

资料来源请见：

- https://store.hp.com/us/en/tech-takes/top-5-uses-for-workstation-laptops。
- https://www.britannica.com/technology/workstation。
- https://smallbusiness.chron.com/desktop-pc-vs-workstation-47069.html。
- https://www.constructionbusinessowner.com/technology/how-select-right-workstationyour-company。

4.13.3 工作站安全

尽管与网络和服务器相比，工作站和家用 PC 机不太容易受到攻击，漏洞也较少，但是工作站会在用户不知情的情况下被人拿去充当从机，用于发起步调一致的分布式拒绝服务攻击。了解工作站系统存在的漏洞，有助于避免出现遭遇攻击后重装操作系统以及数据被盗后恢复数据的困难。

典型的加密资产交易所工作站应该采用传统工作站的安全评估标准。“Red Hat Enterprise Linux”工作站安全评估标准考虑了以下因素：

- **”BIOS 和启动加载器安全** 未经授权用户是否可以在无口令的情况下物理访问计算机并引导系统进入单用户或救援模式？
- **口令安全** 机器上的用户账号口令有多高安全强度？
- **管理控制** 谁在系统上有账号，他们具有多大管理控制权？
- **可用网络服务** 哪些服务正在听候来自网络的请求调用，它们是否应该运行？
- **个人防火墙** 需要配备什么类型的防火墙（如果有的话）？
- **强化了安全的通信工具** 工作站之间的通信应该使用哪些工具？哪些工具应该避免使用？”

以上是相关工作站安全评价标准提出的问题；未经授权用户是否可以在无口令的情况下物理访问机器并引导进入单用户或救援模式，主要由工作站信息系统所存信息的敏感性和机器所处位置决定。BIOS 和启动加载器的口令保护可防止已物理访问系统的未经授权用户通过可移动介质引导系统进入单用户模式访问根。

用于确定机器上用户账号口令安全强度的问题涉及了验证用户身份的一种方法，对于用户、工作站和网络保护至关重要。口令安全系统的内在重要价值体现在它是与机器上用户账号口令安全强度相关的重要决定因素。

在管理控制方面，对标准用户账号应该不按管理状态级别授予网络访问权。用户只有得到授权才能拥有适当的访问权限。此外，服务只有得到授权才能运行并听候来自网络的请求调用。

需要使用哪种个人防火墙的问题由系统安全策略的设计考虑因素决定。这与控制着防火墙连接的网络间通信的策略的传统防火墙恰成对照——个人防火墙通常只保护安装它的计算机。

“OpenSSH 协议”被《工作站安全指南：Red Hat Enterprise Linux 4》第 4 章第 4.7 节“强化了安全的通信工具”（前面的引文引自与此）推荐为最高效网络通信增强工具，可借助基于公钥密码的高级加密算法来保护通过互联网传输的信息。OpenSSH 作为一种用于网络通信系统加密的免费 SSH 协议取代了 telnet、rsh 等未经加密服务，可提供对远程机器的更安全访问。其他未被推荐的工具还包括“Gnu 隐私卫士”（GPG，又叫“良好隐私”(PGP)）等。

4.13.3.1 直接内存访问（DMA）攻击

加密资产交易所应该加强防范直接内存访问（DMA）攻击。DMA 攻击对加密资产交易所工作站的安全运行构成极大威胁，应该予以高度重视。对加密资产交易所工作站的 DMA 攻击一旦得逞，工作站会在物理上变得非常脆弱。DMA 攻击允许计算机系统攻击者把高速扩展端口用作旁道攻击渠道渗透系统。直接内存访问（DMA）附件和连接可使攻击者绕过操作系统的所有安全机制（其中包括锁屏）对计算机系统的部分或全部物理内存地址直接进行设施访问。此外，它们还允许攻击者读取所有计算机活动、窃取数据或密码密钥、安装或运行间谍软件并利用其他漏洞，甚至修改计算机系统以启用后门或其他恶意软件。

直接内存访问（DMA）尽管有许多明显好处和合法用途，但是攻击者同样可以利用 DMA 通过系统端口和安全系统直接访问来发动恶意攻击。作者建议加密资产交易所把防范针对工作站的直接内存访问控制当作一种基线安全措施。

工作站系统必须在严密保护下防范对其端口进行的已知攻击，以确保用户和公司不会暴露在针对工作站的漏洞利用、威胁和攻击之下。攻击者会利用特定计算机设备和服务器允许外围设备直接访问系统内存的 DMA 特性。以下是作者推荐的可部署来发现或抑制工作站安全入侵或 DMA 等攻击的方法。

1) 工作站的例行检查和维护

加密资产交易所应该对工作站进行维护和例行检查。现代计算机设备的工作站系统测试可以揭示潜在的、隐藏的工作站安全系统攻击风险。尽管固件制造商提供了 DMA 安全问题解决方案，但是这些攻击有可能通过 USB 端口的关键网络威胁入口点实现，或者干脆通过打开机箱实现。

有研究表明，在攻击者可以实际访问系统并植入恶意软件的假设研究攻击场景中，DMA 攻击可能会给公司带来供应链危险。此外，同一项研究还发现，带可编程开发平台的惠普笔记本电脑的无线网卡可以在启动时修改系统 RAM，从而获得设备控制权。计算机硬件制造商惠普公司后来更新 BIOS 版本，补救了这个问题。

从以往的经验看，由于硅材料、硬件和芯片组供应商给产品内置了许多现代安全特性、功能和保护措施，修复攻击后果一直都是一项艰巨任务。另一个困难是，各个供应商在向交易所用户交付产品之前，需要花费大量时间编写支持硬件保护和系统安全配置的代码。特定程序会通过端口入侵计算机系统，对系统内存进行直接高速访问。这些被渗透的端口原本是用来驱动外部显示器、内存扩展和图形升级的。

2) 强化工作站设备抵御攻击能力的硬件制造商工具部署

尽管硬件制造商可以部署工具来提升工作站设备抵御潜在攻击的能力，但是此类建设性措施的最终目的必须是向交易所用户交付安全性能良好的系统。根据一份“Eclypsium 报告”，尽管芯片供应商、设备供应商和操作系统供应商开发了抵御威胁和攻击的控制，但是研究表明，许多内置了硬件保护措施的设备依然有潜在脆弱性。

相关人士透露，要想让一个系统在插入或连接 USB 端口的设备上无法自动执行，恐怕还要等数年时间，其间还要有大量黑客破坏事件来刺激。

3) 限制系统自由访问

不加选择地授予对工作站的物理访问权会带来重大安全风险。交易所人员不应将计算机设备遗留在任何地方，因为可能会有人插入另一台恶意设备进行破坏，进而损坏和致瘫整个系统。

4) 严密关注设备系统固件

Eclypsium 引用了一份报告，就加密资产交易所工作站的安全环境提出一条建议。该建议强调了这样的事实：尽管需要把漏洞攻击一一识别出来，但是系统原本就有漏洞并不是新鲜事。它建议加密资产交易所把注意力和精力放到采购来的设备的固件上。现在市面上有不少公开发布的 DMA 弱点恶意利用工具，例如 Frisk 的 PCILeech，它使攻击者得以对 Windows、Linux 和 Mac 系统肆意妄为。

按照 Frisk 的说法，除了取消登录要求、加载无签名的驱动程序、执行代码和生成系统壳之外，PCILeech 还具有将各种植入物插入目标内核的能力，允许攻击者通过所谓

“挂载驱动器”轻松访问实时 RAM 和文件系统。

资料来源请见：

- https://www.darkreading.com/vulnerabilities---threats/enterprise-hardware-still-vulnerableto-memory-lane-attacks/d/d-id/1336921?_mc=rss_x_drr_edt_aud_dr_x_x-rss-simple。
- https://en.m.wikipedia.org/wiki/DMA_attack。
- https://zephyrnet.com/enterprise-hardware-still-vulnerable-to-memory-lane-attacks/。
- https://eclypsium.com/2020/01/30/direct-memory-access-attacks/。
- https://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-en-4/ch-wstation.html。
- https://en.m.wikipedia.org/wiki/Personal_firewall(vii)https://www.cmu.edu/iso/governance/guidelines/appropriate-use-admin-access.html。

4.13.4 设备和介质控制

作者建议加密资产交易所按安全控制计划执行设备控制风险遏制措施。

1) 设备控制

设备控制保护措施不允许用户访问设备，可以最大限度减少企业或机构基础设施数据资产所可能面临的风险。相关设备控制检查列表是一份综合清单，其中包含了可移动设备、打印机、调制解调器、外部网络适配器、USB 等连接总线、多功能外围设备等。

大多数设备控制措施通过系统访问控制规则限制用户的访问。这些基于访问控制规则的限制被设置成参数，用于识别设备控制组件功能。它们既是向特定类型用户或用户组授予在指定时间内访问特定类型设备权限的依据，也是限制读取、编辑数据存储数据库系统中文件等组件功能的规则集。

2) 设备控制的益处

设备控制无论是作为单独的解决方案独立使用，还是作为涉及面更广的数据保护解决方案的组成部分使用，都会带来许多益处，强烈建议加密资产交易所充分利用下文所列的这些益处：

- 数据预防；
- 盗窃预防；
- 介质加密；
- 监控；
- 恶意软件保护；
- 犯罪取证。

设备控制软件的益处

- 直观显示哪些人在哪些端点上使用哪些设备。
- 确保设备只用于合法业务用途。
- 数据经加密后才传输给移动设备，可防止数据被未经授权使用和传播。
- 监控文件在网络上的往来传输。
- 记录设备使用情况和网络上的数据传输活动。
- 保证元数据拷贝/文件内容在网络上的安全传输。

加密资产交易所应该通过执行以下设备控制基本安全最佳实践措施来保持对从 USB 端口引入的恶意软件的持续防范：

- 控制计算机端口和端点上的设备使用。
- 控制可下载和“可打开”文件类型。
- 显示哪些文件已被下载。
- 作为一项最佳实践，优先考虑只将可信移动介质或设备插入计算机。
- 在计算机上安装、运行和更新反恶意软件程序/杀毒软件。
- 禁用已安装在介质或设备上的任何程序的自动运行性能。
- 数据一旦过了使用期限，就将其从介质、设备和计算机上删除，因为数据冗余有可能导致潜在漏洞风险。
- 应该考虑使用数据拦截器和强口令，当有理由怀疑口令泄露时，还应立即实施口令轮换。

3) 介质控制

介质保护控制是指针对数字和非数字类型介质实施的信息安全防护。标准数字介质的例子包括计算机、存储卡、拇指驱动器、外部硬盘驱动器、光盘（CD）、数字视频光盘（DVD）等。非数字介质是指纸质形式的业务文件。介质保护控制可能是仅限于得到授权的人员可以访问，同时给敏感信息贴上保密标签，并且会在发生可疑情况时发出介质销毁或信息删除指令，使任何未经授权者都无从尝试重建或恢复信息。介质保护控制的例子包括：

- 介质访问；
- 介质存储；
- 介质传送；
- 介质标记；
- 介质清理，等等。

资料来源请见：

- https://digitalguardian.com/blog/what-device-control-device-control-definition。
- https://www.google.com/url?sa=t&source=web&rct=j&url=https://staysafeonline.org/blog/security-best-practices-for-removable-media-and-devices/&ved=2ahUKEwiEnbHVhdztAhWofMAKHUAxCGwQFjAVegQIFxAB&usg=AOvVaw2M9CMNNszDhpwX7mv_9BUs。
- https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security/the-10-steps/removablemedia-controls。