
BCOT Global Holdings

**摘要** ..... **2**
**执行概要** ..... **3**

# 摘要

物联网(IoT)并不安全，我们打算解决其面临的安全问题。

Blockchain of Things, Inc.旨在通过正式推出 Catenis Enterprise（一个编入比特币区块链的易用网络服务层）来解决物联网的安全问题。通过网络服务层，Catenis 可为 Ethereum、Hyperledger 以及其他区块链等提供支持。Catenis 是一个拥有几个活跃企业客户的在线网络企业平台（beta 版）。

在本文中，我们首先描述了物联网安全威胁的性质以及其引起的有关企业物联网应用的关键障碍。然后，与传统的物联网基础设施相比，强调比特币区块链的安全优势。接下来，我们描述了组织机构将比特币网络应用于安全的物联网设备通信所面临的阻碍。我们描述了在利用比特币区块链的安全性和信任的同时，Catenis Enterprise 如何消除这些阻碍。最后，本文介绍了真实性认证和智能资产的概念，能够扩展 Catenis 功能的关键属性，以便使其包括超出物联网传统范围的应用程序。

# 执行概要

物联网(IoT)并不安全，我们打算解决其面临的安全问题。

**物联网并不安全：**一项针对 500 多家企业物联网买家的调查结果显示，阻碍行业物联网应用的第一大障碍是安全性不足[1]。由于目前物联网设备通信依赖于集中式服务器，所以安全问题在很大程度上困扰着传统的物联网市场。具体地说，物联网漏洞可以分为三类：

- **拒绝服务(DoS)攻击：**DoS 攻击可以无限期地破坏物联网服务的关键任务。
- **黑客攻击：** 各种各样的黑客攻击方式，如设备欺骗、中间人攻击和重播攻击，都可能导致数据盗窃或设备劫持。
- **缺乏可审核性：**缺乏审核跟踪意味着设备管理员可能在长达数月甚至数年的时间内对入侵毫无察觉。

**比特币是安全的：**比特币区块链是最古老、最历经考验的分布式分类账，它在本质上解决了这些安全问题，因为它没有中心故障点。比特币网络已经证明了它对各种黑客攻击和 DoS 攻击的抵抗能力。同时，鉴于分类帐条目的不可逆性，比特币网络也证明了它的审核能力。因此，管理员可以通过将设备连接到比特币地址，并使用比特币区块链将消息（例如命令和控制信号）发送到该地址，从而安全地激活并与物联网设备进行通信。

**Catenis 克服了比特币的物联网局限性：**尽管具备这些安全优势，但是，将比特币区块链应用于物联网仍受到许多限制。Catenis Enterprise 以一种保留比特币安全优势的方式克服了这些限制。由于 Catenis 是一个被编入比特币区块链的网络服务层，因此可以达成上述目标。对于行业物联网应用而言，比特币区块链的局限性以及 Catenis 相应的关键特性可以分为六类：

- **80 字节大小限制：**比特币消息字段仅为 80 个字节且不提供在物联网设备之间发送大量有意义的数据载荷的能力。Catenis 通过消除大小限制来解决这个问题，以便消息可以包含任何类型或大小的编程代码或数据文件。
- **缺乏授权许可：**如果物联网设备连接到一个公共比特币地址，由于该地址可接受来自任何人的消息，所以，未经授权的参与者可以激活该设备。Catenis 通过创建一个授权许可网络并编码到开放的比特币区块链来解决这个问题。
- **缺乏加密：**由于未经过加密，所以，通过比特币区块链发送的消息在全世界范围内均处于可见状态。Catenis 通过提供端对端加密解决了这个问题。安全特性并非局限于此，因为每次系统向该设备发送消息时，Catenis 都会自动给物联网设备分配一个全新的比特币地址。因此，发送到之前使用的比特币地址的任何消息都不会对该设备产生任何影响。这确保了完全正向保密[2]，信息通过临时通道，仅在极短的

时间内存在。端对端加密同时能够阻止未经授权的参与者对信息进行分析，以发现相关消息。

- **速度和规模方面的挑战：**比特币的确认时间较慢，并且，区块链在规模方面面临的挑战广为人知。Catenis 解决了这个问题，它运行的第二层结构类似于闪电网络[3]，允许我们提供即时的、可扩展的交易。然而，与闪电网络不同的是，我们可以在没有对手风险的情况下运行，因为 Catenis 是一个已经授权的网络。
- **对于 CTO 而言使用难度大：**比特币区块链使用难度大，因为大多数 IT 人员都不熟悉区块链协议。Catenis 通过创建一个网络服务层和一个易于使用的 API 来解决这个问题。
- **对于 CFO 而言难以管理：**比特币区块链难以管理，因为很多 CFO 都没有管理加密货币的经验。Catenis 通过在幕后进行必要的加密货币业务并从企业客户的角度抽象化加密货币来解决这个问题。

**Catenis 有助于进行真实性证明：**Catenis 的增强特性组合使应用程序能够超越物联网的传统范围，以便纳入一个真实性认证系统（又称为真实性证明）。通过 Catenis，人们可以追踪现实世界产品的真实性，减少零售和供应链产品欺诈 - 每年大约会发生价值 1.9 万亿美元的产品欺诈。[4] 在认证过程中有两个关键步骤：

- **确认产品制造商拥有真实性证书：**制造商可以将一份真实性证书的加密指纹记录到区块链，并为分销商/客户提供一个允许独立加密确认的参考 ID。产品制造商拥有记录真实性证书的端点。
- **确认真实性证书的真伪：**Catenis 可以显示独立加密身份验证。一个给定 Catenis 设备端点的所有者可以通过对适当的网站域名、政府注册或第三方认证的访问权限或所有权来证明他们的身份。当这两个步骤结合在一起时，允许出现不可信的真实性证书，这有助于减少供应链或零售环境中的欺诈行为。

**Catenis 确保智能资产可定制：**Catenis 通过授权客户将更多的东西数字化进一步扩展了自身的功能，超越了传统的物联网范围。这一目标是通过授权客户创建智能资产并将其从一位用户转移到另一位用户来实现的。Catenis 智能资产具有彩色币协议[5]的所有鲁棒性能和智能合同功能[0]，但在四个关键方面更加强大：

- **传输实际数字有效载荷的选项：** Catenis 智能资产及其消息传递功能可以被配置为传输实际数字有效载荷，这与许多其他加密项目形成了鲜明的对比。在这些项目中，数字资产仅仅是由第三方的承诺支持的有效载荷的代表，因此它必须通过一个不相关的外部系统进行请求。Catenis 智能资产可以被配置为传输实际的股票证书、房屋契约或 MP3 文件，这样，实际有效载荷可以从一位用户转移到另一位用户。
- **加密数字有效载荷的选项：** 使用 Catenis 智能资产传输的数字有效载荷可以使用目的地端点的公共密钥加密，这样，只有目的地端点才能访问有效载荷。这与加密项

目形成了鲜明的对比，在这些项目中，有效载荷是未加密的，而且对全世界来说均可见。

- **对信息作出反应的选项：** Catenis 智能资产可以配置为对来自其他端点的消息做出反应，这与对数字资产没有反应的加密项目形成了鲜明的对比。例如，Catenis 客户可以在收到消息的条件下，对智能资产的自动创建和分发程序进行编程。因此，Catenis 可以成为对任何数字资产进行高效、透明分配的平台，包括但不限于令牌销售。
- **授权网络：** 由于 Catenis 是一个授权网络，所以智能资产不会对未授权端点的消息做出反应。这与缺乏授权功能的加密项目形成了鲜明的对比。

**Catenis 是一个为第三方应用提供的平台：**Catenis 从根本上来说是一个平台，第三方开发者可以将 Catenis 核心功能（如安全消息、智能资产等）作为一个构建块来构建应用程序。本文强调了第三方程序员可以在未来努力集中开发的四个方面：

- **确保物联网安全的行业特色应用程序：**不同的行业和一项操作的不同环节更倾向于利用 Catenis 的安全物联网功能来处理不同的使用案例。因此，第三方开发人员可以构建具有行业针对性的应用程序，利用 Catenis 的安全性，为物联网市场的不同部分带来量身定制的解决方案。
- **硬件服务：**由于智能资产的数字键可以在连接到 Catenis 端点的远程硬件中解锁功能，所以 Catenis 可以提供安全的、以区块链为基础的硬件服务。第三方开发人员可以构建具有行业针对性的应用程序，在不同的行业以不同的方式利用这个功能。
- **门票市场：**Catenis 将允许智能资产的原始发行方赚取该资产的再销售佣金（即基于收费的智能资产）。例如，如果音乐会门票在二级市场上被转售，音乐会门票发行方就可以赚取佣金。第三方开发人员可以通过构建一个拥有智能资产意识的票务市场来实现这种功能的商业化，这种智能资产意识利用了 Catenis 的服务层。
- **股票市场：**特拉华州法律允许美国公司在区块链上交易股份，精简股份结算流程。Catenis 已经具备了编码智能资产的功能，可以传输实际的股票证书。Catenis 还拥有抽象加密货币的功能，这样传统的股票投资者就可以从他们的常规经纪公司购买股票，而不必直接与加密货币打交道。第三方开发商可以建立一个股票市场，简化股票结算流程。

1 http://www.bain.com/Images/BAIN_BRIEF_How_Providers_Can_Succeed_In_the_IoT.pdf

2 Scott Helme May 2014: “Perfect Forward Secrecy - An Introduction” https://scotthelme.co.uk/perfect-forward-secrecy/

3 Joseph Poon, Thaddeus Dryja: “The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments” https://lightning.network/lightning-network-paper.pdf

4 https://www.strategyand.pwc.com/reports/counterfeit-pharmaceuticals

5 Colored Coin Protocol: https://github.com/Colored-Coins/Colored-Coins-Protocol-Specification/wiki