PUND-IT™
INVESTIGATE - INTERPRET - INFORM

市场更新

2017 年 4 月

- 确保企业区块链网络的安全：IBM 区块链与 LinuxONE 漫谈

作者：Charles King，Pund-IT, Inc.

Pund-IT, Inc.
Hayward, CA
U.S.A.94541

联系人：
charles@pund-it.com
电话：510-909-0750
www.pund-it.com

确保企业区块链网络的安全

IBM 区块链与 LinuxONE 漫谈

作者：Charles King，Pund-IT, Inc.

引言：安全格局与网络威胁

面对当今的数字化威胁格局，许多企业和商务人士感觉不知所措。有些问题由来已久，比如喜欢捣乱的黑客总是企图侵入企业的防火墙内。但是，除此之外，他们还面临有组织、有资助的网络犯罪。很多网络犯罪背后甚至有敌对国家和政府机构的支持。

这些网络犯罪团伙有时独立作案，有时又相互勾结。总而言之，他们瞄准的都是能立即获得经济利益的有形资产。但是，他们也会盯上相对无形的商业机密、知识产权以及任何能创造战略优势或竞争优势的资产。

这些都是潜伏在企业外部的问题。而在企业内部，企业不仅需要管理无法妥善保管网络证书或控制自己好奇心的员工，还需要解决商业间谍行为、信息资产意外损坏或毁坏，以及合作伙伴偷偷窥探宝贵数据等问题。

确保区块链解决方案安全无虞

企业如何才能最好地保护自己？一种新的技术 - 也就是我们常说的区块链 - 似乎在一夜之间突然出现。这种解决方案能帮助各个参与方建立和管理数字化信任，而在过去企业必须依靠信赖的第三方才能安全开展业务交易。

凭借其核心的高级加密和哈希算法，区块链不仅能大幅改进许多常见的互动，如交易结算，还能完善新的业务机会，比如钻石的可靠来源。事实上，有人认为得益于区块链原型应用比特币的固有分散架构，区块链可能已经解决了核心、关键的安全问题，因为比特币的核心网络从未被攻破。

尽管我们可以为区块链迄今为止成功抵御攻击的表现喝彩，但是，我们必须承认，没有产品或服务能保证绝对安全。这是因为，就其本质而言，支持个人互动和团队互动的联网解决方案包含的功能都是常见的攻击媒介。

其中包括一些热门的新兴技术，如区块链网络。但是与此同时，通过评估这些风险以及供应商采取的风险缓解措施，我们发现对于关心安全的企业来说，有些 IT 产品要明显优于其他产品。

私有区块链产品就是其中的典型，如基于 IBM LinuxONE 平台的 IBM Blockchain on Bluemix 服务和 Linux 基金会的 Hyperledger 项目。本报告探讨了企业当前面临的网络攻击模式和网络攻击背后最常见的原因，以及由 IBM LinuxONE 支持且构建于 IBM Blockchain 之上的网络如何阻碍、甚至挫败这些网络攻击。

网络攻击模式和动机

首先，我们来探讨一下攻击发生的方式和原因。一般而言，网络攻击有两种常见的模式或媒介；*网络攻击和一对一攻击*。

*网络攻击*可能来自任意地点，一般涉及享有权限的内部人员或企业外部的个人/团队滥用窃取的网络证书。*一对一攻击*往往发生在企业内部，由拥有合法证书的个人或团体发起。

在调查网络攻击的动机时，我们发现在有形资产类动机列表中，获取金钱利益高居榜首，比如银行和信用卡账户是网络攻击的最大目标之一，因为攻击者可以通过操纵银行和信用卡账户获取现金或购物。实际上，IBM X-Force Threat Intelligence Index 2017 报告显示，2016 年，网络黑客最常攻击的目标是金融服务行业，全球共有超过 40 亿条记录被泄露。

这比过去两年泄露的记录还要多。这种情况下，该行业的区块链采用率可能会迎来爆炸式增长。但是，网络犯罪也会瞄准无形资产，包括合同、法律协议和知识产权，因为这些资产的价值能带来战略优势或竞争优势。这些利益还会刺激一些国家发起攻击，他们会窃取与国防、贸易或政治有关的数据，从中获取长期利益。

但是，谋取金钱利益或实现竞争收益也是内部攻击的常见动机，因为部分虚伪、贪婪的员工可能会想方设法窃取企业的宝贵机密。不幸的是，有些看似"值得信赖的合作伙伴"也抱有同样的动机；事实上，这可能会导致那些想窥探其他参与者的区块链网络参与者实施攻击。

安全漏洞：不只是获利

但是，"获利"（或者采用一种更普遍的说法，"一切向钱看"）并不能完全概括网络攻击的动机。比如，攻击者可能会出于抽象或主观目的发起攻击，如动物权利主义者可能会攻击他们反对的研究人员和机构。有些攻击背后可能还有政治目的，比如为了增加个人或政党的财富，抹黑竞争对手，或者为了破坏政府的系统或数据合法性。

商业攻击背后可能也有类似的动机。员工因心怀不满而关闭或破坏公司的 IT 基础架构。或者，有政治想法的内部人员，如有名的爱德华·斯诺登和切尔西·曼宁窃取并公开了信息，他们认为自己是出于良心采取这样的行动，但是要是认为他们是第一个或者最后一个这样做的人，那就大错特错了。

最后，意外/无意的安全漏洞与那些精心策划的安全漏洞一样严重。由于网络无法鉴别内部漏洞的出现是故意为之还是一场意外，由此而来的调查往往会耗费大量时间和人力，大大增加本就不堪重负的 IT 员工的工作量和压力。

此外，无意的漏洞的破坏性丝毫不亚于有计划的攻击。比如，想象一下，如果商业合同或员工记录处分记录被意外公布，会发生什么事情？因为疏忽而破坏或改变文档和文件则可能导致企业违反规定，面临处罚和法律制裁。

简而言之，面对种类和复杂性不断增长的网络威胁，企业有必要尽可能学习更多的东西，采取更多的措施来保护自己。

为什么选择区块链？

一开始区块链是一种安全支持公有比特币加密货币交易的方法，但是随后其核心分布式账本技术 (DLT) 快速成熟，成为了一个面向业务流程和应用的平台。它是怎样做到的呢？主要是通过 Linux 基金会的 Hyperledger 项目。这是一个快速发展的商业区块链开发资源，背后有 40 多家 IT 供应商的支持。

此外，市场上还出现了其他区块链平台，比如瑞士公司 Ethereum Switzerland GmbH 于 2014 年初开发的 Ethereum。2015 年公开发布后，Ethereum 在加密货币支持者中的关注度相当高，但是该平台经历了四次硬分叉，其中一次出现在 2016 年 6 月，当时攻击者成功对利用 Ethereum 处理投资资本治理的 THE DAO 发起了一次网络攻击。

此次事件证明了，采用了创新型区块链设计和技术就认为这些解决方案完全无敌是一种多么愚蠢的想法。任何产品和服务都无法保证安全防御绝对牢不可破。请记住，区块链网络依然能够支持管理复杂交易和事务所用的方法，而且这些交易和事务要优于大多数传统流程。

封闭式 DLT

在 Linux 基金会的 Hyperledger 项目中，区块链被用于实施共享式账本，已授权的参与者能利用这些账本，审核 DLT 并与 DLT 交互，将新区块链交易无缝集成至现有的"记录系统"中。因此，这些"封闭式"DLT 能支持高价值有形及无形资产的无摩擦交易。

封闭式 DLT 支持以下四大功能：

1. **协作** - 让相关方轻松组织记录系统
2. **约束** - 利用"封闭式"设计，只允许通过验证的参与方读取、写入或验证交易
3. **共识** - 利用协商协议，审查、接纳和移除网络成员，以及落实所有成员一致同意的政策
4. **一致性** - 利用协议，防止因区块链数据出现临时偏差或"分叉"，导致参与者访问错误或不正确的信息

所以，封闭式 DLT 能支持企业准确维护并高效管理交易和流程。但是，这并不意味着 DLT 就不会被滥用。实际上，与传统工作负载一样，它们也很容易被攻击媒介抓住漏洞。但是，通过利用基于平台的安全功能和解决方案，企业可以解决部分或所有此类问题。

一个得到有效保护的封闭式 DLT 能够充当"中央权威信息源"，因为参与者能以透明的方式访问和审核账本中的所有交易。反过来，这又能让区块链网络参与者验证交易和整个账本的完整性，并认可账本的可信度。除了确保业务交易安全外，它还能消除因聘请第三方中介角色（如作为信用管理人而介入的银行和法律顾问）所产生的成本和复杂性。

为什么选择 IBM Blockchain 和 LinuxONE？

我们来看一下 IBM 对区块链的关注和参与度，包括其相关的解决方案和服务。IBM 与其他 40 多家供应商一起支持 Linux 基金会的 Hyperledger 项目。其中 IBM 为该项目贡献了大量代码，也有代表入选该项目的技术指导委员会。

为什么 IBM 如此热衷于发展区块链？是出于战略和实践的考虑。简单地说，区块链 DLT 支持的业务和交易流程恰好是 IBM 企业业务交易的最佳切入点。换句话说，IBM 拥有成功实施区块链 DLT 所需的专业技能，能帮助大量客户做好采用这些解决方案的准备。在这方面，IBM 也有丰富的经验。

但是 IBM 还有其他供应商没有的独特优势：LinuxONE 主机。这个平台仿佛就是为实施区块链量身打造的。

是什么让基于 LinuxONE 运行的 IBM Blockchain 如此适合区块链 DLT？LinuxONE 于 2015 年问世，是首款自下而上专为 Linux 工作负载设计的 IBM 主机解决方案。尽管 IBM 早在 2000 年就已经支持基于主机系统的 Linux，但是这些工作负载一般运行于专门的 Integrated Facility for Linux (IFL) 协同处理器之上，这些协同处理器由 z/OS 操作系统和 z/VM 虚拟化技术提供支持。

相比之下，LinuxONE 系统能与 Red Hat、SuSE 或 Canonical Ubuntu 等操作环境一同订购，而且支持 z/VM 和 KVM 虚拟化技术。IBM 主机能够交付业务关键的可靠性、可用性和可扩展性 (RAS) 等功能，因此，已成为数千家企业的关键平台。

此外，区块链还是一个典型的云工作负载。尽管 Microsoft Azure 和 Amazon AWS 也提供区块链即服务，但是只有 IBM Cloud 提供的 IBM Blockchain High Security Business Network (HSBN) 融合了一些独特的技术，来专门关闭重大区块链漏洞。简而言之，IBM Blockchain on LinuxONE 提供主机级别的混合和私有区块链云工作负载。通过在 LinuxONE 服务器上构建 IBM Blockchain HSBN，IBM Cloud 为客户的区块链网络提供了最安全的平台。

LinuxONE 提供的一些功能能提升 IBM Blockchain 网络的性能和安全性，其中包括：

- **多租户分离/隔离**：鉴于系统能够托管多个区块链网络，参与实体的数据和活动必须分开安全保存，确保参与实体只能看到和参与已授权的活动。IBM 通过逻辑分区 (LPARs) 实现了这种隔离。逻辑分区满足最高商用安全标准 - EAL5+ 安全认证。该公司的 LinuxONE 平台是唯一一个支持 EAL5+ 的区块链平台。
- **抵御外部攻击的安全功能**：Secure Service Container 是一种特殊形式的 IBM LPAR。它将所有软件封装在一个安全、可信且已签字的容器中，该容器与设备类似，而且进行了密封和验证，以防篡改，最终保护区块链实施项目免受外部攻击。如此一来，便可保护区块链 DLT 免受恶意软件攻击、特权用户证书滥用以及故意或无意的信息泄露。因为 Secure Service Container 的支持能够深入到 LinuxONE 固件层面，所以它几乎无可匹敌。

- **密钥安全**：IBM 的 LinuxONE 通过对区块链容器中的所有数据进行加密，进一步增加了安全性。此外，密钥保存在专门的防篡改 Crypto Express5S 卡中，以防止特权用户截图获取区块链数据。结果就是，IBM LinuxONE 区块链解决方案能满足最高的硬件安全管理器 (HSM) 安全标准 – FIPS 140-2 4 级。
- **集成式保护**：有些供应商已开始考虑在其网络中加入 HSM，但是这种"零配件式"的安全方法并不能关闭风险敞口。比如，当管理员损坏了区块链代码时，他们依然能启用 HSM，解密敏感数据，而且他们不会看到密钥。与之形成鲜明对比的是，通过结合利用 Secure Service Container 和密钥保护技术，IBM Blockchain on LinuxONE 已经领先了其他产品一大截。

鉴于区块链网络的固有业务价值，我们很容易理解为什么 IBM 认为该技术对其自身和客户都是一项关键的战略要务。同时，考虑到 IBM Blockchain HSBN 解决方案的关键功能，我们很难理解为什么重视实施最安全的区块链 DLT 的企业要使用任何其他平台。

Everledger – 案例之 IBM Blockchain 和奢侈品

使用 IBM Blockchain HSBN 且由 LinuxONE 支持的区块链 DLT 在真实应用中是什么样子？位于英国的初创企业 Everledger 利用 HSBN 管理和跟踪钻石的来源，这就是一个有名的例子。凭借其解决方案的创新和业务价值，Everledger 屡获殊荣。其首席执行官 Leanne Kemp 也频频现身各大行业展会发表主题演讲，其中就包括 IBM Edge 2016 和 InterConnect 2017。

Kemp 和 Everledger 到底解决了什么问题？据报道，每年，不法行为给钻石行业造成的经济损失高达数十亿美元，包括，钻石赝品、过高的钻石估值和被篡改的财务报表。此外，尽管保险行业每年投入数亿美元来防范欺诈，但是依然有近三分之二的欺诈性钻石被盗索赔逃过了他们的监管视线。问题是传统的钻石鉴定证书和所有权流程都是以纸质文档为基础，缺乏透明度，因此导致企业几乎无法核实和跟踪大部分交易。

Everledger 如何解决这个问题？他们采取的办法是将钻石鉴定实验室收集的重要信息输入区块链中，这些信息就相当于钻石的指纹。这些数据包括序列号，以及所谓的 4C（克拉重量、净度、色泽、切工）和 40 多种元数据和高清照片，这些照片显示了钻石腰部的镭射信息。除了以独特方式鉴别钻石外，该公司还在其全球数字化账本中保存有关钻石身份、所有权和移动的数据。迄今为止，Everledger 已经完成了超过 100 万颗钻石的数字化鉴定。

Everledger 的解决方案还能解决一些更棘手的问题。钻石算是最珍贵、最便携的"冲突"或"血腥"矿产之一，在有些国家钻石开采和加工是主要行业，比如塞拉利昂、利比亚、安哥拉、刚果共和国、科特迪瓦、中非共和国和刚果民主共和国。在这些国家，贪腐和内战导致成千上万的成人和儿童被奴役，他们在苦不堪言的环境下被迫从事采矿工作。

金伯利进程是一个 2000 年成立的国家组织，负责监督钻石交易，为合法交易出具证明。但是伪造者利用伪造的金伯利进程证书销售血腥钻石和假钻石，导致金伯利进程饱受其害。在 IBM Edge 2016 大会上，该公司首席执行官 CEO Kemp 发布了一个基于 IBM Blockchain HSBN 的全新 Everledger 平台，旨在以数字化方式鉴定通过金伯利进程跟踪的钻石。

尽管钻石为 Everledger 的初步成功贡献良多，但是他们并不打算局限于昂贵钻石领域。事实上，他们的区块链 DLT 能为鉴定各类奢侈品提供一个理想的平台，包括艺术品、品牌服装、饰品和珠宝这类经常被伪造的昂贵物品。经过一段时间的发展，Everledger 的 IBM Blockchain HSBN DLT 环境还能被应用于药物、高端制造，以及真实性对于实现和交付预期结果至关重要的其他领域。

换言之，对于 Everledger 及其首席执行官 Leanne Kemp 来说，钻石不是终点，而是起点。

最终分析结论：安全区块链的力量

对于被定为攻击目标的个人和企业来说，网络威胁技术和威胁格局的不断演变不仅会耗费他们的大量费用，还可能带来灾难性后果。但是，Everledger 的案例却表明了威胁的另一面，传统的交易流程被不法分子扭曲和玩弄，他们为了谋取个人利益牺牲整个行业。还有成千上万被奴役的成人和儿童被迫开采血腥矿石。

区块链 DLT 能帮助我们解决这些问题，由此我们可以看出区块链 DLT 技术所蕴藏的强大力量和灵活性。但是，区块链网络的安全程度取决于其基础软硬件。尽管无数的供应商和云提供商都能够提供区块链解决方案，但是基于 IBM LinuxONE 平台且通过 IBM Cloud 交付的 IBM Blockchain High Security Business Network (HSBN) 凭借其独一无二的功能和技术，不论从哪个角度衡量，都可以说是市场上最安全的区块链产品。

如果企业有兴趣挖掘区块链技术的价值，担心如何应对关键流程所面临的网络威胁，或者决心最大限度地保护其最有价值的资产，那么，我们强力建议他们考虑基于 LinuxONE 系统的 IBM HSBN 服务。

关于 Pund-IT, Inc.

Pund-IT™ (www.pund-it.com) 强调了对于技术和产品演变的理解，并说明了这些变化对于企业客户和广泛的 IT 市场将产生的影响。