企业应用区/快链技术时如何考量？

产品名称	企业应用区/快链技术时如何考量？
公司名称	东莞楚恒辰诺网络科技有限公司
价格	.00/件
规格参数	
公司地址	广东省东莞市松山湖园区瑞和路1号2栋302室03
联系电话	14778333741 13268813057

产品详情

区/块链技术基本概念

区/块链技术，可以理解为分布式数据存储，或者交易／数字事件的公开账本。想要记录和存储在公开账本上的每笔交易都需要按照共识机制，被系统中大多数的参与者通过后，才能够得到确认。而在交易信息计入区/块链之后，任何人都无法删除这份信息。所以说，区/块链中包含的是所有确定的经过验证的交易记录。

经典的CIA 安全三原则模型中，我们知道机密性、完整性和可用性是信息安全的三个目标。

一、数据机密性

从信息安全机密性角度来看，区/块链能够提供强验证机制。应用区/块链技术开发应用时，考虑网络的访问权限依旧是建立数据安全保护中蕞基础的一道防线。如果攻击者可以获取进入区/块链节点的权限，验证和授权控制仍然可能受到影响，蕞终可能像其他技术一样被黑客突破，影响数据保护策略。

网络权限

如果是公有链应用，我们通常不需要对网络权限进行限制，因为公有链的协议已经让所有人／节点参与到区/块链网络中来。而私有链则恰恰相反，我们需要更合适的安全控制策略来保护网络的访问权限。为了保障私有链的私有属性，本地的网络和系统还需要应用多层的安全防护措施来进行防护（防火墙，VPN，VLAN，入侵检测和入侵保护系统等等）来执行所谓的纵深防御策略。但现实是，这些安全控制策略依然不能够保证安全，更好的建议是直接在区/块链应用中加入安全控制功能，成为私有链上的第一道也是蕞重要的防线。

数据权限与披露

如果企业的区/块链数据传输是通过完全加密来进行的话，一般就可以保证数据不会被三方窃取和阅读了。但如果应用继续结合PKI和加密密钥，则可以为企业提供更高及别的安全防护。如果企业增加了了安全通信协议，那么即使在攻击者试图实施中间人攻击的情况下，攻击者都会无法伪造对方的身份或在传输

过程中泄漏数据。

二、数据完整性

保护数据的完整性，在信息系统的整个生命周期中都是尤为重要的环节。区/块链的内置特性，即共识机制和公开账本带来的数据不可篡改／可追踪性，也是为企业确保数据完整性的另一种方法。

不可修改性

区/块链技术一定程度上可被认为是安全技术，因为它能让用技术用户相信——存储在防篡改的分布式账本上的交易内容是有效的。它所采用的分布式架构、顺序散列和密码学机制，能够抵御蠢蠢欲动的黑客——攻击区/块链还是与攻击普通数据库显然是截然不同的。企业应用区/块链搭建的应用，可以在数据的完整性和可信任的两个维度上得到一定的保障。

数据的遗忘权

企业在实现区/块链应用数据的遗忘功能时，其中之一的解决方案是企业可对用户的个人数据加密后存储在区块上，在需要实施遗忘时将密钥删除，以确保敏感数据詠久无法访问。

可以追踪

由于添加在公有链或私有链上的每一笔交易，都经过数字签名并盖过时间戳。所以，企业可以追溯每个交易的特定时间，并在区/块链上识别交易的双方（通过公共地址）。这个可追踪的特性意味着交易双方不可否认，这样可以保证黑客无法复制签名进行伪造，避免区/块链应用遭受篡改交易内容和欺诈性交易的出现。任何一个新交易都会被包含在全球账本之中。在每一次迭代过程中，前一个状态会存储下来，形成可追踪的日志。这种可审计的能力能够给企业提供额外的安全性能。

数据质量

由于私有链和公有链都只是为数据放入区块之后的准确性进行保障，区/块链技术无法保障数据的质量。

三、数据可用性

由于信息是动态的，时刻在发生变化，授予了访问权限的用户需要在变化中仍然保持对于数据的访问。

对抗DDoS

区/块链分布式的特性则表现在，它没有可供入侵的“ 入口 ”或单点错误，和现在广泛的数据库驱动的交易存储结构相比更安全。在分布式平台上，如果黑客想要实施DDoS攻击首先会花费更大的成本，运用大量的交易来冲破区/块链网络的承载上限。其中去中心化的架构和P2P机制会减小以往中心化 C/S 架构中服务器端的压力。