区块链是一种去中心化的分布式电子记账系统，它实现的基础是一种受信任且绝对安全的模型。在加密算法的配合下，交易信息会按照发生的时间顺序公开记录在区块链系统中，并且会附带相应的时间戳。关键之处在于，这些数字“区块”只能通过所有参与交易的人一致同意才可以更新，因此攻击者无法通过数据拦截、修改和删除来进行非法操作。

因此，区块链就有成为安全社区一个重要解决方案的潜力，对于金融、能源和制造业来说亦是如此。就目前来说，验证比特币交易是它的一个主要用途，但这种技术也可以扩展到智能电网系统以及内容交付网络等应用场景之中。

区块链技术可以帮助我们提升加密以及认证等保护机制的安全性，这对于物联网安全以及DDoS防御社区来说绝对是一条好消息！

某家区块链初创公司声称他们的去中心化“记账“系统可以帮助用户抵御流量超过100Gbps的DDoS攻击。有趣的是，这家公司表示这种去中心化的系统允许用户出租自己的额外带宽，并将带宽访问权限”提交“到区块链分布式节点，当网站遭受DDoS攻击时，网站可以利用这些出租带宽来缓解DDoS攻击。

根据卡巴斯基实验室反病毒专家Alexey Malanov的说法，区块链技术有助于追踪黑客攻击，他补充道：

“网络入侵者通常会清除权限日志，以隐藏未授权访问设备的痕迹。但如果日志分

布在多个设备中（例如通过区块链技术实现），则可以将风险尽可能降低。”

数字经济发展基金主席German Klimenko表示：

“目前，国防部正在大力推动IT发展和研究工作，这对行业来说是一件好事。”

北约和五角大楼也在研究区块链“防御性”应用。该技术被积极用于保护系统免受网络攻击。北约将使用区块链来保护金融信息、供应和物流链，而五角大楼正在开发一个防黑客攻击的数据传输系统。

总的来说，区块链技术并不是万能的，至少现在还不是。无论是从技术完整性出发，还是从系统实现方面考量，现在的区块链技术都无法100%确保设备的安全。但无论怎样，我们2018年绝对会成为区块链技术非常重要的一年，专注于传统的解决方案已经无法拯救我们了，也许区块链技术可以帮助我们脱离境。

（本文仅代表作者观点，不代表链得得官方立场）