DOI: 10.16661/j.cnki.1672-3791.2019.12.006

浅析区块链技术在解决物联网安全问题上的应用

汪垚
(河南工业贸易职业学院 河南郑州 450012)

摘 要: 物联网技术,代表着今后互联网技术的前进方向,让我们逐步迈进万物互联的时代,并使人们的生活变得更加便捷。物联网技术的出现,将我们日常使用的各种器械、设备和工具与传感器连接起来,真正实现了实时监测和智能管理操作。伴随着物联网的蓬勃发展,其安全问题也逐渐凸显。因为物联网本身的结构原因,以往的安全处理技术并不能很好的适应物联网。区块链技术,具有与物联网类似的分布式以及去中心化等特征,通过数学计算方法,使产生的数据块带有时间标记,而且其信息的验证也是彼此关联的,从而使数据具有可追溯、不可篡改伪造等特点,能够从源头上确保信息的安全。区块链的这些特性,可以对物联网从设备接入、信息采集存储以及抵抗分布式拒绝服务等方面提供可靠地保护。

关键词: 区块链 物联网 信息安全 应用
中图分类号: TN929.5 **文献标识码:** A **文章编号:** 1672-3791(2019)04(c)-0006-02

1 物联网系统目前存在的主要安全问题

1.1 信息采集存在风险

物联网的原始数据来源于传感器等感知设备对各种终端设备信息的采集,由于整个物联网系统中感知设备数量庞大,而且不同的数据需要不一样的传感器进行采集,导致整个感知控制层面呈现出多源异构性,也正是这些特点,使得一般情况下传感器等设备功能比较简单,而且无法有效长期地对其进行监控,从而存在较大的安全隐患。另外,由于终端设备也很少采取保护措施,攻击者可以较为容易的获取关键节点的口令等身份信息,并利用这些信息进行错误信息的发布和交流、DoS攻击等操作,严重影响系统的正常运作。

1.2 信息传输过程存在风险

由传感器等感知设备采集的信息,因其数据总量不大,在传输的过程往往不会采取很复杂的保护措施,也就给了不法分子可乘之机,在数据传输时,易于遭受拦截、窃取和攻击破坏,一旦发生这种情况将使物联网系统受到很大的冲击,造成用户权益受损以及较多功能无法实现。

1.3 标签被嵌入风险

物联网数据采集后往往采用无线的形式直接传输给控制中枢,这种直接暴露的信号,并没有得到很好地保护,因此在感知控制层里,一些标签若被嵌入其他物质,就会使得终端设备时刻处在被监视的状态,这将使大量的基础信息被监视,也会导致用户的个人私密信息泄露,甚至引起社会公共安全问题。

1.4 数据存储存在安全风险

物联网系统会采集大量的终端设备设备,而且在其应用层中,还将保留用户的许多个人私密信息,例如密码设置、个人喜好等,针对存储的数据,怎样防止数据被盗用、破坏,以及在产生上述情况时,如何及时作出应对,都需要进行考虑。另外,当存储数据中,被恶意的混入“脏”数据后,将会使物联网系统做出错误的选择,因此还需要考虑如何应对数据污染等事件的发生。

1.5 认证与访问控制存在安全风险

传统网络的认证,一般分为身份认证以及消息认证。其中,身份认证需要用秘钥来确保可靠性,但是,在通信中,若其中一方的秘钥遭到窃取的话,整个通信过程的数据将被盗取,给通信双方都会造成一定的损失。消息认证,是通信双方在进行信息交互时,确保信息完整性和安全的保护方法,也是被物联网普遍采用的认证方式。但是在消息认证过程中,消息认证码往往是静态的,入侵者只需利用穷举或者监听等方式,就可以暴力获取正确的消息认证码,然后伪装成接收方进行信息的接收和交互,造成物联网系统中大量信息的外泄。

1.6 物联网架构存在安全风险

当前物联网的系统架构是中心化系统架构,在这种架构中,系统信任机制的建立非常简单,并且需要一个可靠的第三方对系统中所有的设备信息进行统一的管理。随着物联网技术的不断发展,物联网终端设备的数量将会达到百亿级别,如此庞大的数据来源,将会对第三方带来巨大的压力。因此,物联网需要一种新的架构来减少对第三方的依赖,并构建一种新的、降低对系统中心依赖的信任机制。

2 区块链技术特点

2.1 去中心化

区块链技术的一大特点就是去中心化。不同于传统的网络体系,在区块链的网络体系结构中,其数据信息的交互、下载以及信息核对等过程都是不存在中心节点,而是分布在多个节点构成的去中心化的结构网络中。并且,与传统的结构不同,网络中的各节点,不依靠统一的管理,彼此的功能和作用都是一样的。在不同节点间进行数据传输时,负责接收的节点会对发送节点进行一次身份验证,在验证成功后,会将其接收到的数据在全网进行广播。区块链技术,利用数学的算法实现信任机制,可以有效避免传统物联网体系的中心化结构,因中心节点遭受攻击而使整

个网络瘫痪的情况发生。

2.2 数据加密

在区块链技术中，信息传输时，采用了非对称加密算法来保证数据的安全。非对称加密算法的原理是，传输的两个节点都需要事先生成一对用来加密和解密的公钥和私钥，传输信息节点向接收信息节点传输消息之前，彼此会将公钥共享，然后传输端用接收端的公钥将信息加密，加密后的信息只有用接收端的私钥才可以解密，且私钥只有接收端才知道，因此就保证了传输信息的可靠性。另外由于不是利用对称加密算法，也就避免了密码在传输过程被破解的情况。非对称算法可以解决物联网系统中信息传输的安全问题，保障数据安全。

2.3 共识机制

在区块链技术体系中，使用非对称加密算法中与公钥相关联的地址来当作节点用户的标识，因此就不再需要传统的基于PKI的认证机构，避免了认证机构出现问题时导致的认证安全问题。区块链利用共识的算法，在全网节点构建一种信任机制，而且在这种机制中，各个节点没有必要将身份信息共享，只需要将地址进行交互即可，并且节点还可以变化自己的地址。因此，共识机制可以很好的解决物联网中信息传递时存在的安全隐患，保护具体设备或用户的隐私。

2.4 分布式数据库

在区块链存储技术中，其区块的作用就像一个记账簿，可以将整个区块链上所有的信息交换都进行记录，而且这些信息记录都是可以一直被其他节点进行查验的。与一般的记录方式不同，区块链的信息记录是分散在所有的节点上，没有中心，这就构成了一种典型的分布式数据库体系。当一些节点受到攻击或是数据遭受破坏时，由于其他的节点依然保存有完好无损的信息，因此并不会对系统产生影响，这一特点将显著提升物联网系统的数据信息存储安全性能。

2.5 时序数据不可更改

在区块链中，对系统中的每一笔信息交互都会用时间戳来确认，给交易添加一个时间维度，使得每一次的信息交互都可以追溯其时间先后，又因为每一个时间戳都会对前一个时间进行加强，因此大大加强了信息的不可篡改性。在物联网中，引入时间戳，可以对数据起到一种保护作用，也是一种重要的证据，可以证明物联网中一些数据是真实存在的，而且可以追溯其具体的时间，保证了信息的不可篡改。同时，引入时间戳，还可以防止物联网数据库被其他数据注入导致的数据污染，提升数据库的安全性。

3 区块链在物联网领域应用展望

3.1 区块链在车联网上的运用

随着物联网技术的普及，车联网也在逐步发展，越来越多的车主选择将车载系统联网，但是随之而来就是其安全问题，而且由于车联网目前的安全防护措施做的并不是特别成熟，所以较多的车载系统很容易遭受黑客的入侵，这将给广大车主带来很大的人身安全隐患。而区块链技术运用非对称加密算法，使得信息的传输不易被破解，而且时间戳的引入再一次保证数据不会被篡改和伪造，可以系统性的保证车联网的使用安全。

3.2 区块链在食品安全领域的运用

随着人们生活水平的提高，越来越多的人开始关注食品卫生安全问题，食品卫生安全与物联网技术结合也是一种技术趋势。利用传感器或RFID将食材的采摘、生产时间以及品质等所有信息上传至区块链，区块链系统可以确保这些基础数据安全和不可篡改，使所有上链的食材信息一目了然，不符合相关标准的食材，或是过期食品等，将无法更改自身信息而被监管部门或消费者快速辨认出，从而确保食品卫生的安全。

4 结语

伴随物联网技术在各行业的广泛利用，区块链技术也将得到越来越深入的应用。区块链去中心化的体系结构，能够为物联网系统营造一种安全的环境，时间戳和非对称加密技术、分布式数据库等技术的应用，使得物联网中信息的交互变得安全而又不可篡改，极大提升了物联网的数据信息安全。在今后的探究和应用中，可以继续研究区块链技术在物联网深层次的应用，将区块链技术于物联网技术进行更加深度的融合利用。

参考文献

[1] 邵奇峰,金澈清,张召,等.区块链技术:架构及进展[J].计算机学报,2018(5):1-20.
[2] 袁勇,王飞跃.区块链技术发展现状与展望[J].自动化学报,2016(4):481-494.
[3] 川朱岩,甘国华,邓迪,等.区块链关键技术中的安全性研究[J].信息安全研究,2016(12):1090-1097.
[4] 谢辉.王健区块链技术及其应用研究[J].信息网络安全,2016(9):192-195.
[5] 林小驰,胡叶倩雯.关于区块链技术的研究综述[J].金融市场研究,2016(2):97-109.
[6] 姚忠将,葛敬国.关于区块链原理及应用的综述[J].科研信息化技术与应用,2017(2):3-17.
[7] 庄需,赵成国.区块链技术创新下数字货币的演化研究理沦与框架[J].经济学家,2017(5):76-83.
[8] 袁勇,周涛,周傲英,等.区块链技术:从数据智能到知识自动化[J].自动化学报,2017,43(9):1485-1490.
[9] 李怡德,杨震,龚洁中,等.物联网安全参考架构研究[J].信息安全研究,201,2(5):417-423.
[10]张宁,王毅,康重庆,等.能源互联网中的区块链技术:研究框架与典型应用初探[J].中国电机工程学报,2016,36(15):4011-4023.