区块链技术在物联网安全相关领域的研究

何渝君，龚国成

（中移物联网有限公司，重庆 401336）

摘　要　区块链是数字货币——比特币的底层技术。区块链是由节点参与的分布式数据库系统，具有去中心化、不可伪造的特点，受到了金融世界的高度重视。本文从区块链技术的技术架构、关键技术等方面阐述了区块链技术在网络安全方面的优势，提出了区块链应用于物联网安全的思考，旨在对区块链技术在物联网安全相关领域的研究提供帮助。

关键词　区块链；分布式；去中心化；物联网安全

中图分类号　TP393　　**文献标识码**　A　　**文章编号**　1008-5599（2017）05-0012-05

DOI:10.13992/j.cnki.tetas.2017.05.004

1　引言

2008 年，中本聪发表《比特币：一种点对点的电子现金系统》，2009 年 1 月 3 日，比特币诞生。比特币是一种网络虚拟货币，不依靠特定的货币机构发行，不存在中央管理机制，而是通过特定算法的大量计算产生，区块链（Blockchain）的概念也随之浮出水面。区块链是一种分布式共享数据库，利用去中心化和去信任方式集体维护一本数据簿的可靠性技术方案，融合了分布式架构、P2P 网络协议、加密算法、数据验证、共识算法、身份认证、智能合约等技术，解决了中心化模式存在的安全性低、可靠性差、成本高等问题。

物联网是继计算机、互联网与移动通信网之后的第三次信息浪潮，被我国列为重点发展的战略性新兴产业之一，国家相继出台了多项政策，明确要切实推进物联网建设。物联网安全问题一直备受批评，区块链恰好能提供最佳的解决方案，融合匹配物联网。区块链技术可以为物联网提供信任、透明、安全的通信保障，通过去中心化的共识机制建立物联网身份验证机制，提高物联网的安全私密性。

本文对区块链技术原理进行了梳理，包括区块链基础架构、关键技术等，阐述了区块链技术的安全性优势，提出了区块链在物联网安全方面应用的思考，为物联网安全相关领域的研究提供思路。

2　区块链概述

区块链是比特币的底层核心技术，本质上是一个去中心化的分布式账本数据库，任何人都可以参与到区块链网络中，每一台设备都能作为一个节点，每个节点都允许获得一份完整的数据库拷贝，节点间基于一套共识机制，通过竞争计算共同维护整个区块链，任一节点失效，其余节点仍能正常工作，解决了传统中心化模式容易遭受到攻击、篡改的缺陷。

收稿日期：2017-04-10

区块链发展到今天，经历了区块链 1.0、2.0 和 3.0 三个阶段。区块链 1.0，即可编程货币的出现，让货币在网络中实现流通。区块链技术建立了去中心化的数字支付系统，降低了交易的运营成本。当智能合约加入到区块链系统中，形成了可编程金融—区块链 2.0。智能合约将区块链的应用范围从单一的货币领域扩展到了经济领域的更多方面。随着区块链技术的快速发展，去中心化、数据不可篡改等特性得到越来越多的重视，它的应用也不再局限于金融领域，而是逐步扩展到社会生活的各个领域，形成一个可编程的社会—区块链 3.0。

3 区块链架构

区块链的基础架构包括：数据层、网络层、共识层、激励层、合约层和应用层，其中合约层为区块链 2.0 的特点，具体架构如图 1 所示。

图1 区块链基础架构

数据层描述了区块链技术的物理结构，封装了底层交易数据。

网络层封装了区块链的组网方式、传播机制以及验证机制，维持着整个网络的正常运行。区块链网络采用广播机制作为整个网络的传播方式，并以 P2P 的组网方式实现了区块链网络中节点之间的信息交流。

共识层负责提供一种算法机制以证明区块的正确性，使各个节点达成共识。目前，区块链的共识机制包括：POW、POS、DPOS。

激励层使用通过设计合理的激励机制，使网络节点在参与数据安全验证的同时获取收益，保证区块链系统的共识稳定。

合约层包含了多种脚本代码、算法机制以及智能合约。其中智能合约成为区块链技术革命中最重要的部分。智能合约可视作由事件驱动、具有状态、获得多方承认、运行在一个可信、共享的区块链之上的自动运行的程序。

应用层为区块链技术的应用提供了接口，但目前应用层的实际应用还较少。

4 区块链关键技术

4.1 区块和链

区块链由区块和链式结构组成，能够有效防止更改已有某个区块的交易信息和控制新区块的生成。区块（Block）即区块链的网络节点，是一种记录交易的数据结构，每个区块由区块头（Header）和区块体（Body）两部分组成，结构如图 2 所示。

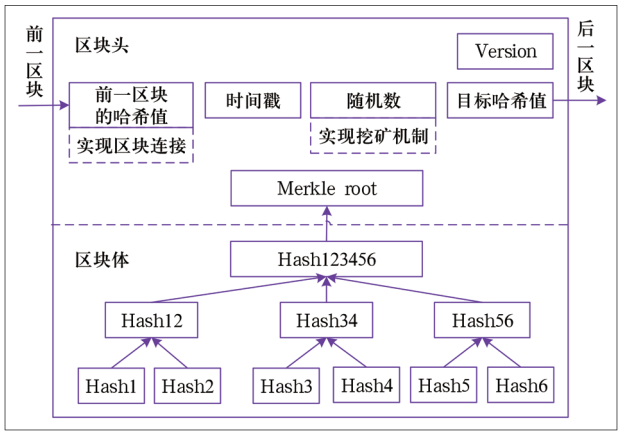

图2 区块结构示意图

区块头包含了除交易信息以外的所有信息，其中父哈希（Hash Used）用于该区块与前一区块的连接，形成链式结构；时间戳负责记录每一区块产生的时间；Merkle根归纳一个区块中所有交易信息，最终生成这个区块所有交易信息的统一的哈希值，该值随着交易的改变而产生变化，通过动态调整目标数的难度值；最先找到正确的随机数（the Nonce）解并经过验证的矿工将会获得当前区块的记账权。

区块体只负责记录前一段时间内的所有交易信息，交易信息是区块所承载的任务数据，具体包括交易双方的私钥、交易的数量、电子货币的数字签名等。

4.2 非对称加密算法

非对称加密算法是由一对唯一的公钥和私钥组成的加密方法。公钥与私钥是一对，如果用公钥对数据进行加密，只有对应的私钥才能解密；如果用私钥对数据进行加密，那么只有对应的公钥才能解密。

在比特币系统中，私钥是一个随机数，通过不可逆的加密函数生成一个公钥；再通过公钥，使用哈希函数生成一个比特币钱包地址，如图3所示。

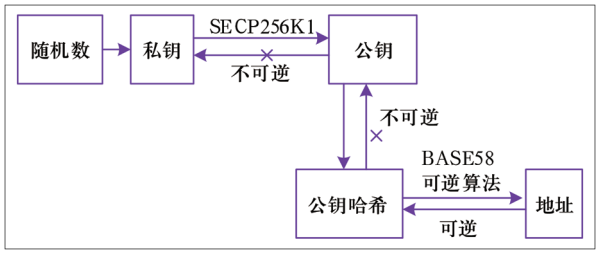

图3 比特币钱包地址生成过程

区块链技术运用非对称加密算法，满足了数据交易的安全性需求，确保了信息的来源，主要应用场景包括：数据加密和数字签名。

4.3 工作量证明机制

工作量证明机制（POW）是比特币的证明机制，核心思想是通过分散节点的算力竞争来确保数据一致性和共识的安全性。区块链网络中任何一个节点，想要生成一个新的区块并写入区块链，必须解出一个具有一定难度的SHA256的数学题。第一个正确求解的节点将信息广播给网络中其他节点，当大多数节点（51%）验证通过，新区块才能被连接到主链。通过POW机制，维护了区块链的整体运行及安全性。

4.4 分布式结构

区块链的分布式结构让数据的存储分布在网络各个节点上，而不是集中记录在中心化服务器主机上。全网每个节点在记录存储数据的同时，也对其他节点的数据进行了验证。只有超过半数的节点验证通过，数据才能被写入区块。分布式结构增加了整个区块链网络系统的健壮性，不会因为部分节点的失效而影响整个网络系统的运行。

4.5 智能合约

智能合约封装了若干预置响应条件、触发条件以及操作等内容，签署合约的各方就合约内容达成一致，以代码的形式部署在区块链上，当满足特定的触发条件时，自动激活智能合约并执行，其模型如图4所示。智能合约对区块链发展具有重要的作用，为其提供了更为广阔的前景。应用于物联网，在智能农业系统、智能家居、智能电力等多个领域可以实现智能自动化，如温湿度自动控制、远程电力抄表等。

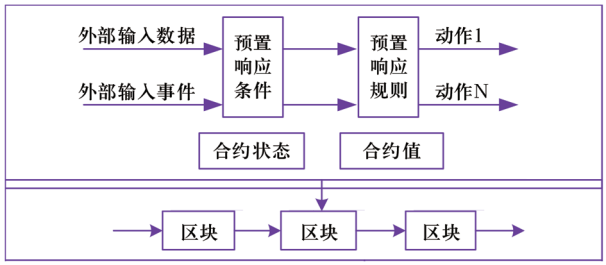

图4 智能合约模型

5 区块链技术与物联网安全

5.1 物联网安全问题

随着物联网应用规模不断扩大，物联网面临的安全问题愈发凸显。安全是制约物联网发展的关键，对物联网安全体系进行改进完善，是发展物联网需要解决的重点问题。

物联网通过传感器、摄像头、RFID、扫描仪等各种设备获取信息。由于设备之间的信息传递一般是通过无线网络进行，因此设备容易遭受攻击，设备的身份安全得不到保障，可能引起隐私及机密信息泄露。

物联网在信息传递过程中，由于无线网络本身具有开放性特点，缺少安全保障的节点十分脆弱，设备之间传输的无线信号很容易被非法窃听、干扰和屏蔽。恶意设备非常容易入侵，从而导致物联网遭受干扰、拒绝服务攻击（DoS）、分布式拒绝服务攻击（DDoS）等攻击。

物联网现有的中心化管理模式，在判断各类信息的真实性、安全性时，可能出现设备丢失故障，导致工作效率下降；信息量过大，无法准确对信息定位判断等问题。

5.2 区块链与物联网的相似点

区块链与物联网都具有去中心化、分布式的特点。区块链系统网络是典型的 P2P 网络，具有分布式异构特征，而物联网天然具备分布式特征，两者的网络特性决定了物联网可以利用区块链技术在网络安全的优势，为物联网安全问题提供解决途径。物联网是互联网的延伸和扩展，通过应用智能感知、识别技术等计算机技术，实现信息交换和通信，能满足区块链系统的部署和运营要求。

区块链与物联网都符合智能合约的发展。区块链系统能够通过智能合约来实现合同自动化、智能化执行；物联网的应用系统中，如智能家居、智慧能源等可以通过设置恰当的智能合约，实现系统智能化服务。

区块链与物联网都需要加密算法来保障系统的安全运行，是实现数据信息隐私保护的重要手段。区块链通过非对称加密算法实现了信息加密和数字签名，利用私钥加密信息，公钥解密验证信息来源的真实性。同样，物联网网络中也需要可靠的加密算法来保护网络中的信息交流安全。物联网可以运用区块链技术的加密思想，建立一套可信的加密系统，提高网络安全性能。

5.3 区块链在物联网安全的思考

据市场研究公司 Gartner 称，到 2020 年物联网设备数量将达到 204 亿。随着物联网设备数量的增长，以传统的中心化模式进行管理，花费巨大且存在安全隐患。区块链的去中心化特性为物联网的自治提供了途径，可以帮助物联网中的设备理解彼此，让物联网中的设备了解异构设备之间的关系，实现对分布式物联网的去中心化控制。下面从物联网设备鉴权、共识网络和设备追踪方面来阐述区块链解决物联网安全问题的方法与思路。

5.3.1 物联网设备鉴权

在物联网设备接入网络时，需要对设备进行鉴权，确认设备的身份。物联网可以运用区块链技术思想，采用非对称加密算法和智能合约，利用 P2P 网络中的网络设备节点对待接入设备进行鉴权，待接入物联网设备只需向物联网平台和网络设备节点发送接入和鉴权请求，即可实现物联网设备在物联网平台的鉴权和连接。将区块链技术运用于物联网设备鉴权，无需借助第三方设备，可以有效降低鉴权成本，提高物联网设备的安全性，防止非法设备伪装，同时还能保护设备遭受外部攻击。

5.3.2 构建物联网共识网络

通过改造区块链的共识验证机制，可以构建应用于物联网的共识网络。在物联网环境下，智能设备节点不承担数据计算工作，不参与工作量机制证明，只进行数据的加密和传输，同时把数据传输作为区块链交易向整个网络广播。另外，部署特定的验证节点进行 POW 计算，验证节点不保存交易数据，起到了数据安全与隐私保护作用。

5.3.3 物联网设备追踪

区块链技术可以通过记录设备与用户或是网络服务之间数据交换的账本以此构建一个新的方式来追踪单个设备的唯一历史记录。区块链也可以让智能设备成为独立代理并单独管理各种交易。比如，连接一台自动贩售机能够追踪其用户的购买历史记录，利用这一点来自动支付交付的新物品。通过设备追踪，实时了解设备的使用状态，一旦出现异常，立即响应，能够最大限度地保护设备安全，从而保证整个物联网网络的安全。

总的来说，区块链技术应用于物联网，可以为海量的物联网设备之间建立了低成本的彼此直接交流的桥梁，同时通过去中心化的共识机制提高了系统的安全性和私密性，基于智能合约将智能设备变成了可以自我维护和

调节的独立个体，便于对智能设备进行跟踪管理，提高智能设备的安全性和使用率。希望本文能够为区块链技术提升物联网安全方面提供研究参考。

参考文献

[1] Nakamoto S. Bitcoin: A peer—to—peer electronic cash system[J]. Consulted, 2009.
[2] Melanie Swan M. Blockchain: blueprint for a new economy[M]. USA: O'Reilly, 2015.
[3] 谭磊，陈刚. 区块链2.0[J]. 中国信息化，2016(8).
[4] 袁勇，王飞跃. 区块链技术发展现状与展望[J]. 自动化学报，2016,42(4):481—494.
[5] Antonopoulos A M. Mastering Bitcoin: Unlocking Digital Crypto—Currencies[J]. Oreilly Media Inc Usa, 2015.
[6] S Li, LD Xu, S Zhao. The internet of things: a survey[J]. 《Information Systems Frontiers》, 2015,17(2):243—259.
[7] 李德全. 拒绝服务攻击[J]. 电子工业出版社，2007(2):13—15.

A summary of research on block chain technology in the security field of IoT

HE Yu-jun, GONG Guo-cheng
(China Mobile IoT Company Limited, Chongqing 401336, China)

Abstract The block chain is the underlying technology of the digital currency - Bitcoin. Block chain is a distributed database system that participates in nodes. It has the characteristics of de-centering and unforgeability, which is highly regarded by the financial world.This paper expounds the advantages of the block chain technology in the network security from the aspects of the technical architecture and key technology of the block chain technology, and puts forward the thinking of the application of the block chain to the security of the IoT, which aims to help the research of block chain technology in the security field of IoT.

Keywords block chain; distributed; de-centering; security of IoT

DOI:10.13992/j.cnki.tetas.2017.05.005

News

中国移动通信集团设计院组建雄安新区规划工作组全力支持规划建设

2017年4月19日，中国移动通信集团设计院召开雄安新区规划工作组成立会议，组建并落实规划层面的技术支撑保障组织架构。

高鹏副院长就成立雄安新区规划工作组的重大意义和历史使命进行了概括和说明，并指出，设立河北雄安新区，是以习近平同志为核心的党中央作出的一项重大的历史性战略选择，是千年大计、国家大事，具有重大现实意义和深远历史意义。高鹏副院长要求我院迅速行动起来，贯彻落实集团公司精神，并积极参与、全力支持雄安新区的规划建设。

张同须院长在最后的总结发言中指出，雄安新区规划工作是设计院发展的又一个重要机遇，既是展示中国移动通信集团设计院整体实力的机会，也是实现高新技术超前布局的平台，做好规划具有战略意义。

通过此次会议，全院统一了思想，明确了目标，建立了组织，为中国移动通信集团设计院更好的承接雄安新区的有关规划任务奠定了基础。（本刊讯）