DOI:10.19729/j.cnki.1009-6868.2018.06.007
网络出版地址:http://kns.cnki.net/kcms/detail/34.1228.TN.20181127.1632.006.html

区块链技术在物联网中的身份认证研究

Blockchain Technology for Identity Authentication in Internet of Things

杨惠杰/YANG Huijie
周天祺/ZHOU Tianqi
桂梓原/ GUI Ziyuan
(南京信息工程大学,江苏 南京 210044)
(Nanjing University of Information Science & Technology, Nanjing 210044, China)

中图分类号:TN929.5 文献标志码:A 文章编号:1009-6868 (2018) 06-0035-006

摘要: 基于物联网(IoT)平台的特点,将区块链技术与体域网相结合,提出了应用于体域网身份认证的区块链系统框架,实现用户和传感器、路由器、多服务器间的身份认证,并分析了该框架的安全性。最后,基于研究结果,探讨了在IoT平台中区块链技术可能存在的问题和未来发展方向。

关键词: 区块链技术;体域网;认证;非对称加密算法;共识机制

Abstract: Based on the characteristics of the Internet of things (IoT) platform, a blockchain system framework applied to the identity authentication of the body area network is proposed, which combines blockchain technology with body area network. This framework realizes the identity authentication between users and sensors, routers and multi servers. Then the feasibility and security of the framework are analyzed. Finally, based on the research results, the possible problems and future development directions of blockchain technology in the IoT platform are discussed.

Key words: blockchain technology; body area network; authentication; asymmetric encryption algorithm; consensus mechanism

近年来,随着新一轮经济科技的不断发展,物联网(IoT)平台已被世界发达国家列为重大发展战略。中国也在《"十三五"规划纲要》里明确指出:将物联网作为战略性新兴产业上升为国家发展重点[1]。现如今IoT技术被广泛应用在智能城市、智能家居、智能医疗、车联网、环境监测等实际应用环境中,人们的实际生产生活已经与物联网技术紧密相连,不可分割[2-5]。为实现实时感知环境信息或传输数据给用户,开发人员会将不同种类的传感器嵌入到智能设备或具体物体中,例如:可穿戴设备、传感器和专业工具等智能设备在网络中相互连通,并在网络中完成数据加密、数据传输和数据分析等,协助人们完成IoT平台数据采集和数据分析等工作[6-8]。在上述过程中,无论哪种实际应用场景都需要智能设备能够及时完成对数据的响应或传输,即使数据是在公开信道中传输,也要保证数据传输是不可泄漏的。一旦数据传输速度降低或者数据丢失,将会影响用户的使用效果;一旦数据在传输过程中被恶意敌手篡改或攻击,整个处理数据的过程都会被视为不安全。因此,提高在IoT平台下的数据传输性能和数据安全性,是当前亟待解决的问题。

经过上述的分析,不难发现:传统的IoT技术和中心化的系统框架已经很难满足未来的发展需求。针对IoT平台的特点,区块链技术能解决大量的智能设备数据在中心化的系统框架中会出现的安全和管理问题。区块链是一种集成分布式数据库、共识机制、点对点(P2P)传输和非对称加密算法等新型应用模式,具有去中心化、开放性、自治性、匿名性和信息不可篡改的特点。本文主要对IoT平台之一的体域网展开了详细研究,结合新兴的区块链技术,针对传输的安全性能和数据传输性能差的特点,研究分析了适用于体域网的身份认证技术,利用区块链技术在体域网平台下设计一个新兴的系统框架,主要解决以下问题:

(1)数据的安全问题。由于体域网处于一个公共信道中,因此存在恶意敌手对数据进行攻击、篡改或重放等,造成数据丢失或被窃取的安全性问题。在体域网中,数据一旦受到篡改,则可能酿成医疗事故。

(2)数据的传输问题。在不同网络中传输数据时,需要使用不同的通信协议,导致不同协议之间需要相互转换格式,产生了大量的通信开销,并降低了通信效率。

(3)设备的成本问题。在体域网中需要使用大量的传感器和路由器,

收稿日期:2018-10-23
网络出版日期:2018-11-27
基金项目:国家自然科学基金(61672295,61672290,61772280)、国家信息安全重点实验室(2017-MS-10)、桂林密码学和信息安全重点实验室(GCIS201715)、江苏省研究生科研与实践创新计划项目(KYCX18_1017,KYCX18_1039)

保证数据的采集和传输。在无形中，增加了通信的成本和能源消耗。

1 体域网身份认证现状

无线体域网中收集的都是与人体相关的生理隐私数据，这些数据可被用于医疗、体育、军事和商务社交等方面，并产生各种社会价值。为了保护这些与个人隐私相关的生理数据，首先要进行各个实体间的身份认证，许多研究学者对此展开了研究。这些研究成果大体上可以分为2类：一种是采用人体独特的生物信息进行认证，另一种是利用传统的密码学方式进行认证。

在2003年，CHERUKURI S等人[9]首次利用人体的生物特征信息进行身份认证研究，并提出了可行的Biosec方案。在该方案中，结合纠错码技术以及生物识别技术解决生物特征测量误差和随机性问题，可用于安全通信无线生物传感网络的身份认证。但是其中的生物特征测量方法并不完善，存在缺陷。随后，文献[10-12]对模糊金库算法进行研究并应用于节点间身份认证。模糊金库算法主要利用人体独特的生物特征数据构造一个数据集合，并在数据集合中加入大量的噪声点，用处理后的数据集合对密钥信息进行加密，然后将此加密后的数据用来进行身份认证。如果其他节点想进行解密操作，其自身得拥有与密文中的生物特征数据集合相似的数据集合。但是在模糊金库算法中，网络中通信开销消耗和金库大小有关联，这会导致节点能耗过大的问题。针对此问题，ZAGHOUANI E K等人[13]于2015年利用线性预测编码技术解决了上述能耗过大的问题，并提出了心电图结果线性预测密钥（ELPA）方案。在此基础上，ZAGHOUANI E K等人[14]于2017年将线性预测编码技术与心电图生物识别技术相结合，可在隐藏心电信号隐私数据的同时实现对病人身份的认证。同模糊金库算法相比，该降低了计算复杂性和通信开销。

LAMPORT L[15]于1981年提出了首个远程认证协议，采用了用户密码认证方案，这一方案为今后的远程认证方案奠定了基础。该协议允许节点通过不安全公共信道向服务器进行身份认证。此后也有许多远程认证协议被提出，这些协议都利用了传统密码学方式，需要证书授权中心和公钥基础设施的参与，不适合资源受限的传感器设备。LIU J等人[16,17]对无证书公钥密码进行研究并在无线体域网中首次提出了2个保护隐私的无证书远程匿名认证协议。由于协议中服务器端需要存储认证表来进行身份认证操作，易被篡改和伪造，同时也不满足前向安全性等要求。同时由于使用了双线性对等密码学操作，传感器的计算负担较大，不适合资源受限的客户端。XIONG H[18]则于2014年提出了一种基于无证书加密的远程匿名认证协议，该协议在客户端使用较多的点乘操作并且没有考虑到密钥的撤销问题，同时用户的个人生理数据易被恶意实体收集，因此存在较大的安全问题和计算负担。为了提高无线体域网中认证的安全性并降低计算的成本，SHEN等人[19]于2018年针对无线体域网提出了一种综合认证协议，该协议包括了一种高效的多层认证协议和针对无线体域网的安全会话密钥生成方案。该协议借助个人数字助理和无证书认证技术，可以有效地降低传感器能耗和计算负担，具有一定的实践指导意义。

综上所述，在无线体域网中，全球学者对于身份认证的研究已取得一定的成果，可实现匿名、安全和高效的操作，并在实践中得到应用。采用传统密码学方式进行身份认证虽然可以避开生物信息认证的缺陷，但其本身也存在计算开销较大、传输速度慢、易受共谋攻击和中间人攻击等问题，同时数据易受篡改，对资源受限的传感器节点来说仍然是不小的挑战。

2 区块链概述

区块链技术是使用块式和链式的存储结构来认证和保存数据，使用共识算法实现生成新区块，使用非对称加密算法保证数据在信道中的安全传输，使用智能合约来处理数据的新型分布式技术。区块链分为私有链、联盟链和公有链。从本质上讲，区块链就是一个去中心化的分布式数据库，任何用户都可以参与到区块链中。用户周围的路由器设备就是一个节点，每个节点都拥有一整套数据的备份，并且各个节点间使用相同的共识机制，通过竞争计算来生成或更新区块链。基于区块链结果的特点，如果任何一个节点失败，其他节点仍能进行正常的工作，且能分辨出是哪一个节点失败。因此，区块链技术解决了传统平台易受攻击或篡改的缺陷。

2.1 区块链的基础架构

区块链的基础架构主要分为应用层、合约层、激励层、共识层、网络层和数据层，具体的基础架构如图1所示。

数据层主要封装了区块链的物理结构，该结构中包含诸如哈希函数、时间戳等技术，保证信息的不可篡改性；网络层描述了组网方式、验证机制和传播机制，实现区块链网络节点间的信息交流；共识层选择一种共识记住，用以验证区块的正确性；激励层主要借助设计一些激励策略，保证节点在区块链中参与验证工作，确保共识的稳定；合约层中主要包含各种脚本、算法和智能合约，当其满足触发条件的时候，系统自动执行合约中的命令；应用层为封装的有关区块链应用提供了接口，例如基于区块链的跨境支付平台OKLINK。

2.2 区块链的关键技术

在本节中，我们主要从区块结

◀图1
区块链技术的基础架构

构、非对称加密算法、分布式结构和智能合约4个部分进行阐述。

（1）区块结构

区块链是由2个部分组成：区块和链式，该结构能有效防止恶意用户对数据进行篡改，并能验证新生成区块的合法性。区块链中的网络节点就是区块，每个区块均由2个部分组成：区块头和区块体。

（2）分布式结构

区块链的分布式结构不再让数据集中在服务器上，而是使数据能够分散地存储在不同的节点上。当节点想要写入数据时，需半数以上其余节点通过共识机制确认该节点的身份，才能够将数据写入到节点中。分布式结构能够有效地增强系统的健壮性，即单一节点的失效不会影响整体系统。

（3）智能合约

在智能合约中封装了预先设定的响应条件、触发条件等内容。各个节点就所签署的合约达成一致后将合约内容以代码的形式嵌入区块链中。一旦有满足合约中相应条件或者触发条件时，自动激活并且执行智能合约。

3 适用于体域网平台的区块链身份认证应用设计

由于区块链技术具有去中心化、透明性、高效率和不具名性的特点，因此该技术可以广泛应用到数字货币、征信管理、金融市场、资产管理等相关场景。同时，区块链和IoT均有着去中心化和分布式的特点，有学者提出将区块链技术应用到IoT平台中，用以解决IoT中安全性差和低效率的问题。体域网作为IoT的一部分，可将区块链技术与体域网结合展开研究。目前中国尚无该方向的研究，本文中我们对区块链应用到体域网中进行身份认证展开研究和分析。

智能医疗利用先进的体域网技术，实现患者与医务设备、医疗人员和医疗机构之间的信息沟通，进而达到信息化的效果。智能医疗能够良好地结合区块链技术，实现数据在体域网中安全和高效的传输。

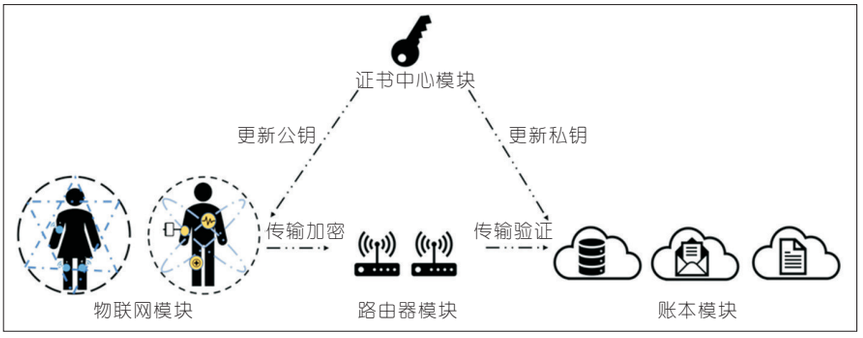
3.1 系统架构设计

本文中我们设计的适用于体域网平台的区块链身份认证系统框架，将传感器、路由器和可信中心构成一个区块网络，如图2所示。由于传感器的资源受限，无法进行数据的计算工作，因此传感器只参与数据的简单加密和传输。然后把数据作为数据交易块发送给路由器，路由器使用验证机制对接受到的数据进行验证。最后，将数据发送给可信中心，可信中心根据共识机制将数据记入帐本。

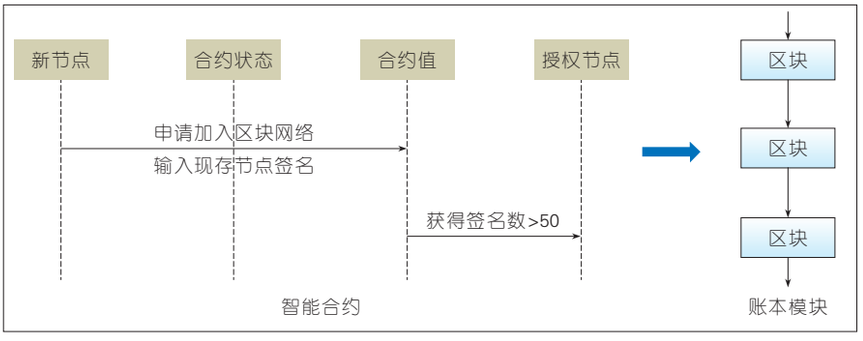
在使用可穿戴传感设备前，每个用户的手机需要与设备借助轻量级认证协议完成用户与传感器之间的身份认证。其次，再利用区块链技术实现体域网中多方身份认证过程。在传感器端生成数据后，使用证书中心生成的公钥将数据加密，传输给路由器。这期间，为保证新加入的节点身份的正确性和真实性，账本端启用共识算法，用于验证新节点身份。新节点需经过智能合约的判断：当有半数以上的节点通过审核时，系统自动认可该节点被记入帐本，并记录到主链上；否则，本次请求视为无效，该节点不被放入主链中。本系统架构能有效地防止恶意节点的加入，确保了节点的正确性和安全性。新节点加入区块的智能合约流程如图3所示。

本文所提的区块链结构如图4所示，区块头包含了版本号、前区块哈希值、时间戳、随机数和该区块哈希值。前一区块哈希值又称为父哈希，用于和前一个区块进行连接，形成链式结构；生成每一个区块的时间就是时间戳；最先找到并正确验证随机数的矿用拥有该区块的记账权；Merkle根中记录了所有交易时所用的信息。

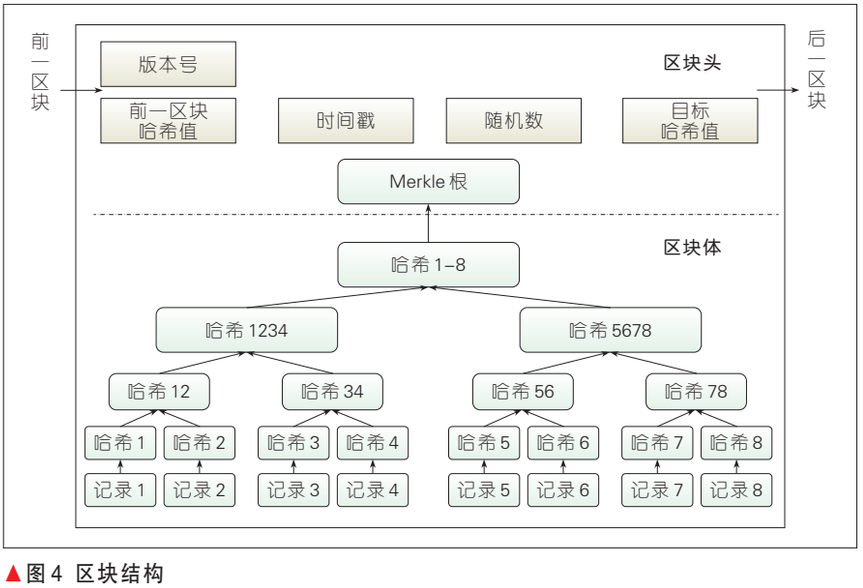
区块链中第一个区块被称为创始区块，起始于创始区块，每一个新生成的区块严格按照时间戳的先后顺序，通过区块哈希地址连接到上一个区块中，形成链式结构。同时，前一个区块的加密结果会被用于当前块的加密，也就是说，任意1个区块数据的改变将会影响2个区块中的信息。所以，区块链技术能够有效地



▲图2 系统框架图



▲图3 智能合约流程图



▲图4 区块结构

防止恶意敌手对数据的篡改，保证了数据的安全性。

3.2 适用于体域网平台的区块链身份认证

在本节，我们提出了2个身份认证的阶段：用户和传感器之间的群组轻量级认证阶段，传感器与证书中心、传感器与路由器之间的基于区块链技术的身份认证阶段。

3.2.1 密钥分配阶段

区块链技术使用的是非对称加密算法。非对称加密是由唯一一对私钥和公钥组成的加密方法。加密算法遵从公钥 K_e 加密，使用其对应的私钥 K'_e 进行解密。在区块链中，区块头中的随机数就是私钥，使用不可逆的加密算法生成其对应的公钥，用公钥的哈希算法生成该区块的哈希地址。为了保证数据的隐私性和密钥的安全性，证书中心的公钥和私钥会定时更新，并对应生成其密钥版本号。与此同时，将密钥的版本号提供给传感器和账本模块，以便于用户对数据进行加解密。

3.2.2 群组轻量级认证阶段

初始化时，在用户使用智能医疗服务前，会分别在用户手机端和其传感器的芯片中添加用户标记 δ_i 和传感器标记 s_i，且两方均可以使用如公式（1）的哈希函数：

$$H_1\{0,1\}^* \rightarrow \{0,1\}^{l_1} 。 \quad (1)$$

在个人可穿戴传感器中，存在资源相对较大的传感器，在该传感器中集成其余设备的信息，用公式（2）进行信息集成：

$$id = id_1 \| id_2 \| ..... \| id_n 。 \quad (2)$$

为验证传感器与用户的身份，用户首先向传感器发送验证请求。该传感器计算如公式（3）—（5），其中 T_i 是时间戳：

$$U_1 = H_1(\delta_i \| T_i) , \quad (3)$$
$$M_1 = U_1 \oplus V_1 , \quad (4)$$
$$V_1 = H_1(id \| T_i) 。 \quad (5)$$

将计算结果 (U_1, M_1, V_1) 发送给用户，用来验证传感器的身份。用户在手机端的计算如公式（6）—（7）：

$$U_1' = H_1(\delta_i \| T_i) , \quad (6)$$
$$V_1' = U_1' \oplus M_1 。 \quad (7)$$

公式（8）如果成立，则完成对传感器身份的验证；否则终止服务：

$$V_1 = V_1' 。 \quad (8)$$

其次，用户端向传感器端发送验证传

感器的身份的请求。用户端的计算公式为(9)—(10),其中 R_1 是随机数,$T_1^{'}$ 是时间戳:

$$M_2=(T_1^{'}\|R_1)\oplus U_1^{'}, \quad (9)$$

$$V_2=H_1(s_i\|T_i^{'}\|R_1), \quad (10)$$

将计算结果 (M_2,V_2) 发送给传感器端,用来验证用户的身份。传感器的计算如公式(11)—(12):

$$M_2^{'}=U_1\oplus M_2, \quad (11)$$

$$V_2=H_1(s_i\|M_2^{'})。 \quad (12)$$

如果传感器端的验证公式(13)成立,则完成对用户身份的验证;否则终止服务。

$$V_2=V_2^{'} \quad (13)$$

3.2.3 区块链身份认证阶段

(1)传感器——证书中心身份认证阶段

在使用传感器前,需要在系统中执行注册阶段。首先,证书中心生成传感器的公钥 K_1,并发送给相应的传感器。其次,传感器使用公钥 K_1 加密其身份信息 id_n 和随机数 R,并将加密结果 E_1 返回给证书中心。最后,证书中心收到加密结果 E_1 后,用其私钥 K'_1 来解密,并对其中的信息进行审核。如果审核通过,则向传感器发送其使用的公钥和私钥(K_s, K'_s)。

在注册阶段完成后,传感器和密钥生成中心进行相互认证。首先,传感器使用加密算法对公钥 K_s、随机数 R_s、时间戳 T 和请求服务内容 M 进行加密,并将结果 E_s 发送给证书中心。然后,证书中心用私钥 K'_s 对加密信息 E_s 进行解密,验证时间戳的准确性并判断传感器的真实性。最后,如果传感器信息为真实可靠的,则再用公钥 K_s 加密请求服务内容 M 和随机数 R_s;否则,终止服务。

(2)传感器——路由器身份认证阶段

在路由器进行数据传输之前,需要在系统中完成注册阶段。首先,路由器将其和传感器的公钥(K_s,K_s)和随机数 R_2 发送给证书中心。然后,证书中心核实2个公钥的身份信息,如果信息真实可靠,则生成路由器和传感器间的会话密钥 K_{KA}。最后,使用传感器公钥对会话密钥和路由器公钥进行加密 E_S,并返回给路由器。

在注册阶段完成后,传感器和路由器进行认证。路由器用其私钥对加密信息 E_S 进行解密,对传感器身份的真实性进行认证。然后,路由器用会话密钥 K_{KA} 对随机数 R_2 加密 $E_{S'}$,返回给传感器。最后,传感器用自己的私钥对 $E_{S'}$ 解密,完成对路由器身份的认证。

使用区块链技术完成身份认证,能够有效地防止恶意用户对数据的篡改。同时,将计算过程进行简化,降低了计算开销,提高了计算效率。

3.3 安全性分析

在本文提出的2个认证阶段中,群组轻量级认证阶段用预先设置随机数的方式,将秘密值提前安全存储在用户移动端和传感器端,并借助发起验证时的时间戳,对用户和传感器群组进行身份认证。无论用户还是传感器群组都无法在自身硬件中篡改或伪造随机数,即使恶意用户对时间戳进行成功伪造,也仅能完成单向认证过程。在该阶段中,用户和传感器群组需要完成双向认证才能证明其身份的真实性。

区块链身份认证阶段使用了区块链的加密方法和结构特征。一个区块中既存有自身的哈希值,也存有前一个区块的哈希值的特征,保证了区块的不可篡改。一旦某一个区块中的数据被篡改或者某一个区块被恶意替换,则会立刻被区块网络所获知。因此,本阶段借助区块的特征对身份进行认证是安全的。

4 结束语

本文主要针对IoT平台中存在的数据安全性差和传输验证效率低的问题展开了研究和分析,并提出使用区块链技术来解决上述问题。体域网作为IoT的一部分,将其与区块链技术相结合实现身份认证,是本文的研究重点。通过研究发现:数据能够有效地实现防恶意用户或者服务器的篡改,保证数据的分散性,符合现实生活对数据存储的需求;数据间的传输、加密、验证过程不再需要过于冗杂的计算,提高了数据操作过程中的计算效率,节约了计算开销。与此同时,如何保护在公共信道中的公钥不被他人用于共谋攻击等问题,仍需要日后解决。此外,随着IoT平台的进一步发展,区块链技术实际应用于智能医疗、智能家居等实际场景中将是未来发展方向。

参考文献

[1] 何渝君,龚国成.区块链技术在物联网安全相关领域的研究[J].电信工程技术与标准化, 2017, 30(5):12–16

[2] SHEN J, ZHOU T Q, CHEN X F, et al. Anonymous and Traceable Group Data Sharing in Cloud Computing [J]. IEEE Transactions on Information Forensics and Security, 2018, 13(4): 912–925. DOI:10.1109/tifs.2017.2774439

[3] 赵阔,邢永恒.区块链技术驱动下的物联网安全研究综述[J].信息网络安全, 2017(5):1–6

[4] SHEN J, ZHOU T Q, HE D B, et al. Block Design–Based Key Agreement for Group Data Sharing in Cloud Computing [J]. IEEE Transactions on Dependable and Secure Computing, 2018: 1–1. DOI:10.1109/tdsc.2017.2725953

[5] 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

[6] XIONG H. Cost–Effective Scalable and Anonymous Certificateless Remote Authentication Protocol [J]. IEEE Transactions on Information Forensics and Security, 2014, 9(12): 2327–2339. DOI:10.1109/tifs.2014.2363553

[7] SHEN J, WANG A X, WANG C, et al. Content–Centric Group User Authentication for Secure Social Networks [J]. IEEE Transactions on Emerging Topics in Computing, 2017: 1–1. DOI:10.1109/tetc.2017.2779163

[8] WANG C, SHEN J, LIU Q, et al. A Novel Security Scheme Based on Instant Encrypted Transmission for Internet of Things[J]. Security and Communication Networks, 2018, 2018: 1–7. DOI:10.1155/2018/3680851

[9] CHERUKURI S, VENKATASUBRAMANIAN K K, GUPTA S K S. Biosec: A Biometric Based Approach for Securing Communication in Wireless Networks of Biosensors Implanted in the Human Body[C]//The Workshop on International Conference on in Wireless Networks of BIOSENSORS Implanted in the Human Body. USA: IEEE, 2003:432–439

[10] BAO S D, POON C C Y, ZHANG Y T, et al. Using the Timing Information of Heartbeats as An Entity Identifier to Secure Body Sensor Network[J]. IEEE Transactions on Information Technology in Biomedicine, 2008, 12(6): 772–779. DOI:10.1109/titb.2008.926434
[11] VENKATASUBRAMANIAN K K, BANERJEE A, GUPTA S K S. PSKA: Usable and Secure Key Agreement Scheme for Body Area Networks [J]. IEEE Transactions on Information Technology in Biomedicine, 2010, 14(1): 60–68. DOI:10.1109/titb.2009.2037617
[12] ZHENG G, FANG G, ORGUN M A, SHANKARAN R. A Comparison of Key Distribution Schemes Using Fuzzy Commitment and Fuzzy Vault within Wireless Body Area Networks[C]//IEEE 26th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications. USA: IEEE, 2015:2120–2125.DOI: 10.1109/PIMRC.2015.7343648
[13] ZAGHOUANI E K, JEMAI A, BENZINA A, ATTIA R. ELPA: A New Key Agreement Scheme Based on Linear Prediction of ECG Features for WBAN[C]//2015 23rd European Signal Processing Conference (EUSIPCO). USA: IEEE, 2015:81–85.DOI: 10.1109/EUSIPCO.2015.7362349
[14] ZAGHOUANI E K, BENZINA A, ATTIA R. ECG Based Authentication for E–Healthcare Systems: Towards a Secured ECG Features transmission[C]//International Wireless Communications and Mobile Computing Conference. China: WiCOM, 2017:1777–1783. DOI: 10.1109/IWCMC.2017.7986553
[15] LAMPORT L. Password Authentication with Insecure Communication [J]. Communications of the ACM, 1981, 24(11): 770–772. DOI:10.1145/358790.358797
[16] LIU J, ZHANG Z, SUN R, KWAK KS. An Efficient Certificateless Remote Anonymous Authentication Scheme for Wireless Body Area Networks[C]//IEEE International Conference on Communications. USA: IEEE, 2012:3404–3408. DOI: 10.1109/ICC.2012.6363786
[17] LIU J W, ZHANG Z H, CHEN X F, et al. Certificateless Remote Anonymous Authentication Schemes for WirelessBody Area Networks[J]. IEEE Transactions on Parallel and Distributed Systems, 2014, 25 (2): 332–342. DOI:10.1109/tpds.2013.145
[18] XIONG H. Cost–Effective Scalable and Anonymous Certificateless Remote Authentication Protocol [J]. IEEE Transactions on Information Forensics and Security, 2014, 9(12): 2327–2339. DOI: 10.1109/tifs.2014.2363553
[19] SHEN J, CHANG S H, SHEN J, et al. A Lightweight Multi–Layer Authentication Protocol for Wireless Body Area Networks [J]. Future Generation Computer Systems, 2018, 78: 956–963. DOI:10.1016/j.future.2016.11.033

作者简介

杨惠杰，南京信息工程大学在读硕士研究生；研究方向包括信息安全、密码学和安全多方计算。

周天祺，南京信息工程大学在读硕士研究生；研究方向包括信息安全和密码学；参与主持江苏省研究生科研与实践创新计划项目、信息安全国家重点实验室项目、桂林密码学和信息安全重点实验室项目等；已发表论文10余篇。

桂梓原，南京信息工程大学在读硕士研究生；研究方向包括信息安全、密码学和轻量级认证；参与主持江苏省研究生科研与实践创新计划项目；已发表论文5篇。

⬅上接第12页

的并且消耗资源量小的信任对象是当前共识机制改进的重要问题。

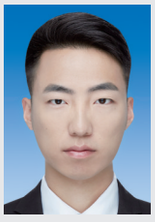
参考文献

[1] NAKAMOTO S. Bitcoin: A Peer–to Peer Electronic Cash System [EB/OL].(2017–06–04)[2018–10–17].https://github.com/GammaGao/bitcoinwhitepaper/blob/master/bitcoin_en.pdf
[2] 袁勇, 王飞跃. 区块链技术发展现状与展望[J]. 自动化学报,2016,42(04):481–494
[3] 袁勇,倪晓春,曾帅,等. 区块链共识算法的发展现状与展望[J/L]. 自动化学报, 2018:1–12. DOI:10.16383/j.aas.2018.c180268
[4] LESLIE L. The Part–Time Parliament [J]. ACM Transactions on Computer Systems, 1998, 16(2): 133–169
[5] ONGARO D, OUSTERHOUT J K. In Search of an Understandable Consensus Algorithm [C]// Proceedings of the USENIX Annual Technical Conference. USA: USENIX ATC, 2014:305–319
[6] CASTRO M, LIISKOV B. Practical Byzantine Fault Tolerance[C]//Proceedings of the 3rd Symposium on Operating Systems Design and Implementation. USA: OSDI, 1999:173–186
[7] DWORK C, NAOR M. Pricing via Processing or Combatting Junk Mail[C]//Proceedings of the 12th Annual International Cryptology Conference on Advances in Cryptology. Germany: Springer–Verlag, 1993:139–147
[8] GIBERT S, LYNCH N. Brewer's Conjecture and the Feasibility of Consistent, Available, Partition–Tolerant Web Services [J]. ACM Sigact News, 2002, 33(2): 51–59. DOI: 10.1145/564585.564601
[9] Proof of Stake [EB/OL].(2017–11–10) [2018–10–17].https://en.bitcoin.it/wiki/Proof of Stake
[10] DUONG T, FAN L, ZHOU H S. 2–Hop Blockchain: Combining Proof–of–Work and Proof–of–Stake Securely [EB/OL].(2016–07–19)[2018–10–17].https://eprint. iacr. org/2016/716
[11] ANTONOPOULOS A M. Mastering Bitcoin: Unlocking Digital Cryptocurrencies [M]. USA: O'Reilly Media Inc
[12] 白帽汇安全研究院.区块链安全分析报告[R/OL].(2018–05–08)[2018–10–17].https://bcsec.org/report
[13] DOUCEUR J R. The Sybil Attack [C]// Revised Papers from the First International Workshop on Peer–to–Peer Systems (IPTPS '01). Germany: Springer–Verlag, 2002. DOI:10.1007/3–540–45748–8_24
[14] Bitcoin Energy Consumption Index [EB/OL]. [2018–10–17]. https://digiconomist.net/bitcoin–energy–consumption

作者简介

王李笑阳，中国人民大学信息学院在读研究生；主要研究领域为区块链技术及其应用。

秦波，中国人民大学副教授；主要研究领域为新兴信息系统安全、数据安全与隐私保护、云计算安全、应用密码学；发表论文近百篇。



乔鑫，中国人民大学信息学院在读研究生；主要研究领域为信息安全、区块链等。