江西省研究生创新专项资金项目

申　　请　　表

项　目　名　称：基于区块链技术的物联网传输层安全智能交互协议的研究

申　　请　　人：范　末　婵

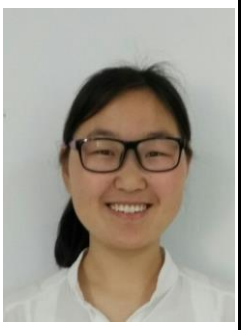
指　导　教　师：杨义先　教授、张小红　教授

培养单位(签　章)：江　西　理　工　大　学

填　报　时　间：2017 年 05 月 09 日

江西省教育厅制

一、项目申报人基本情况

<table>
<tr><td>姓　　名</td><td>范末婵</td><td>性别</td><td>女</td><td rowspan="4">  </td></tr>
<tr><td>出 生 年 月</td><td>1991.02</td><td>籍贯</td><td>江苏 徐州</td></tr>
<tr><td>在读学历层次</td><td>硕士研究生</td><td>入学日期</td><td>2016.09.09</td></tr>
<tr><td>在 读 专 业</td><td colspan="3">电子与通信工程</td></tr>
<tr><td>身份证号码</td><td colspan="4">320381199102146343</td></tr>
<tr><td>指导教师姓名</td><td>杨义先
张小红</td><td>研究方向</td><td colspan="2">信息安全</td></tr>
<tr><td>本科(硕士)毕业学校</td><td colspan="2">苏州科技大学</td><td>专 业</td><td>通信工程</td></tr>
<tr><td>所 在 院 系</td><td colspan="2">电子与信息工程学院</td><td>E-mail</td><td>946942303@qq.com</td></tr>
<tr><td>联 系 电 话</td><td colspan="2">0797-8312029</td><td>手机</td><td>15607072778</td></tr>
</table>

二、项目基本情况

项目主要研究内容（2000 字以内。文科包括：研究的主要问题、目的、意义、研究方法、对策建议、创新点等；理工科包括：主要问题、关键技术、解决方案、研究方法、创新点等）：

一、研究背景

在信息迅猛发展的时代，“物联网”作为新一代信息技术的重要组成部分获得了人们的广泛而深入的认识。**区块链(BlockChain)是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式。**区块链技术具有分布式去中心化、无须信任系统、不可篡改和加密安全性、集体维护等特点，为物联网应用中“设备民主”、“去中心化”、“自制的物联网”等核心问题提供了有效的解决方案。区块链作为应用于物联网的新型技术，利用其去中心化优势，**给数以亿计的物联网传感器和硬件设备升级，可以帮助物联网中的设备理解彼此，并且帮助设备知道不同设备之间的关系，通过寻址和权限控制，实现对分布式的物联网的去中心化控制，**其应用市场也随着物联网技术的发展而不断扩大，在将来会发挥越来越重要的作用。国际权威杂志《经济学人》、《哈弗商业周刊》、《福布斯杂志》等相继报道**区块链技术将影响世界**[1]。

本申请由国家自然科学基金项目“无源 RFID 系统自同步防碰撞和可信认证协议研究”(编号：61363076，在研)提供项目资助。

1、区块链技术的发展

区块链技术的发展[2,3]可分为以下这几个阶段，如表 1 所示。

表 1　区块链技术的发展历程

时间	区块链技术发展
1982-1984 年	Leslie Lamport 等人提出拜占庭将军问题
1985-1997 年	椭圆曲线密码学、椭圆曲线数位签章演算法、用时间戳确保数位文件安全的协议及 Hashcash（杂凑现金）等技术相继被提出。
1998-2004 年	发表的分散式电子现金系统 B-money 及中心化的数位货币系统 Bit Gold 为比特币区块链奠定基础。
2005-2007 年	可重复使用的工作量证明机制（RPOW） Hal Finney 提出可重复使用的工作量证明机制，结合 B-money 与 Adam Back 提出的 Hashcash 演算法来创造密码学货币。
2008-2011 年	Blockchain 1.0：加密货币 数位货币与支付系统去中心化、比特币：Satoshi Nakamoto（中本聪）发表一篇关于比特币的论文，描述一个点对点电子现金系统，能在不具信任的基础之上，建立一套去中心化的电子交易体系。
2012-2013 年	Blockchain2.0：智慧资产、智慧契约 市场去中心化，可作货币以外的数位资产转移，如股票、债券。如 Colored Coin 便是基于比特币区块链的开源协议，可在比特币在区块链上发行多项资产

2014-2015 年	Blockchain 3.0：更复杂的智慧契约 更复杂的智慧合约，将区块链用于政府、医疗、科学、文化与艺术等领域。
2016 年至今	Blockchain 2.5：金融领域应用、资料层 Blockchain2.5：强调代币（货币桥）应用、分散式帐本、资料层区块链，及结合人工智慧等金融应用 Blockchain 3.0：更复杂的智慧契约

2、区块链的结构

以物联网中智能设备为例，区块链技术中每一个数据块**由区块体和区块头构成[4]，**区块体包含了过去十分钟内所有的物联网中智能设备的交互信息，区块头存储前一个区块的引用，区块以类似链表的数据结构存储起来，形成从创世区块到当前区块的一条最长的主链，从而记录了所有智能设备交互记录。因此有人也将区块链技术看做一种分布式去中心化的公共总账本。区块链的基础架构[5]如图 1 所示：

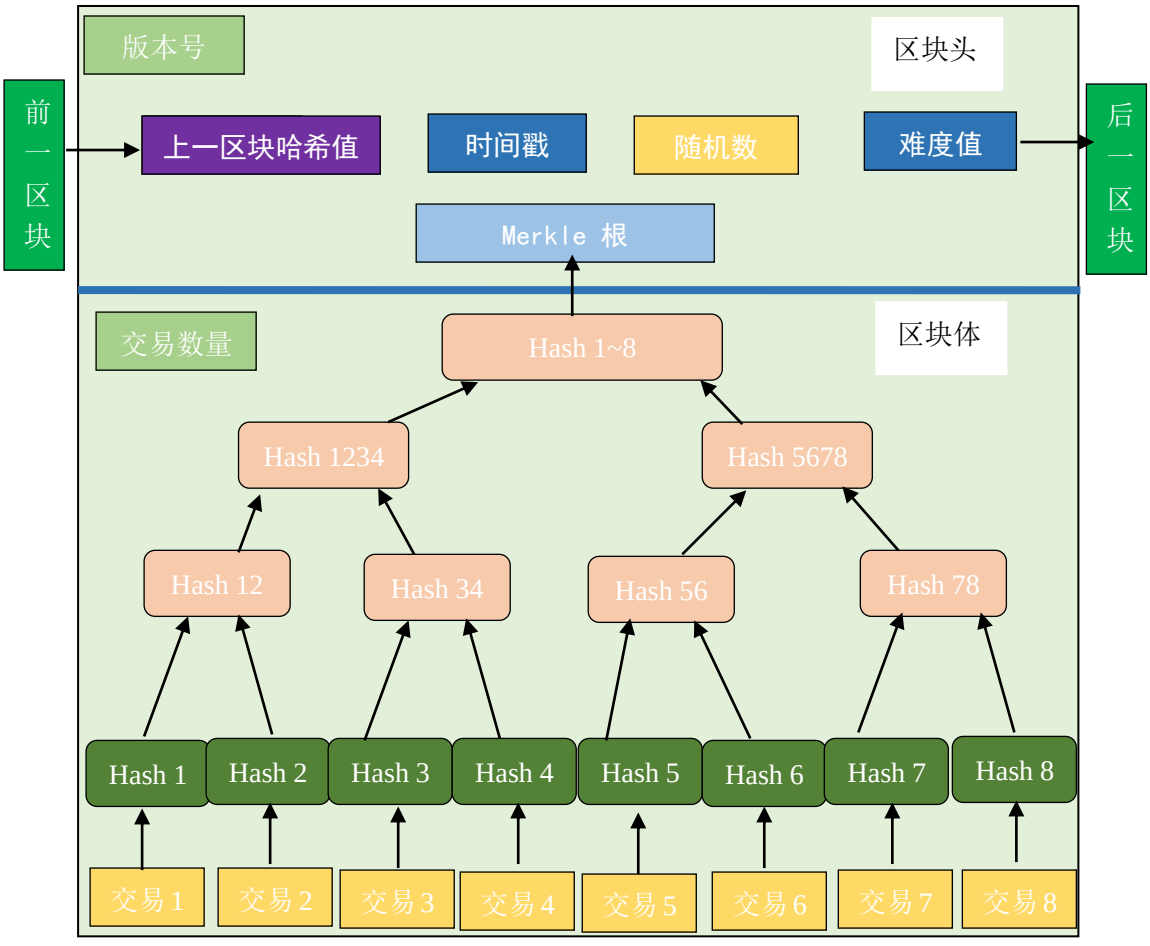


图 1　区块结构

区块体记录了网络中更新的数据信息，记录了一段时间内区块的交互、新产生智能设备的登记以及经过验证的区块创建过程中生成的所有交互记录，这些交互以及登记记录将构建成 Merkle 二叉树这样的结构。如果记录是奇数，则由二叉树自己填补，二叉树的两个交易记录的哈希值串联作为下一个二叉树的输入，最终生成唯一的

Merkle 根节点并写入区块头。

区块头中最为关键的字段是 hashPrevBlock，该字段使得 Block 之间链接起来，形成一巨大的“链条”。Block 本是稀松平常的数据结构，但以链式结构组织起来后却使得它们具有非常深远的意义：

(1) 形成分支博弈，使得算力总是在主分支上角逐；

(2) 算力攻击的概率难度呈指数上升（泊松分布）。

每个 block 都必须指向前一个 block，否则无法验证通过。追溯至源头，便是高度为零的创世纪块(Genesis Block)，这里是 Block Chain 的起点，其前向 block hash 为零，或者说为空。区块链头部信息的构成如表 2 所示。

表 2　区块链头部信息的构成

字 段 名	含　　义	大 小（字节）
Version	版本号	4
HashPrevBlock	上一个 Block Hash 值，当前区块的 Hash 值一定比它小	32
HashMerkleRoot	上一个 block 产生之后至新 block 生成此时间内，交易数据打包形成的 Hash	32
Time	Unix 时间戳	4
Bits	当前区块生成所达成目标值的特征，用于旷工的工作量证明	4
Nonce	随机数，当前区块工作量证明的参数	4

3、区块链的工作原理（以比特币为例）

(1) 广播比特币网络中的每一笔交易，使每个参与者（指矿工）都记录下这笔交易；

(2) 每个参与者接收到交易信息后，都要将该笔交易盖上时戳，收入区块；

(3) 由于每个矿工都做了工作，谁赢了获得奖励呢？此时参与者们要通过一个计算游戏，谁能最快解出 SHA256 运算的值，谁就将赢得打包区块的权利，并获得系统的 12.5 个比特币奖励。这个数量的设定是每四年减半；

(4) 获得记账权的矿工将向全网广播这十分钟内区盖了时戳的交易，其他参与者将核对这些账目；

(5) 当其他参与者都确认无误后，该区块就确认合法，就进入了下一轮的区块争夺战，多个区块逐渐形成区块链[6]。

区块链作为一种信息技术，使用随机散列、非对称加密并对全部交易加上时间戳的方法[7]，其非对称加密结构如图2所示。

在图 2 中，对于 U2 来说，首先 U2 使用 U1 的公钥验证 U1 通过 U2 公钥发给 U2 的使用 U1 私钥签名的先前交易信息及 U1 与 U2 的交易信息，确认 U1 的身份，然后将交易信息进行重新组合或者分解，使用 U2 的私钥对重新组合或者分解后的先前交易信息及 U2 与 U3 的交易信息签署一个随机散列的数字签名，并将这一签名通过 U3 公钥发送 U3，U3 按照 U2 的方式进行验证、签名和进一步处理，如此区块包含的交易信息就产生了。

其中，对区块进行随机散列时要加上时间戳，并将随机散列在网络中进行广播，这样**加了时间戳的区块就是其存在的一个有力证明，每一个时间戳对前一时间戳的信息纳入其随机散列值中，用以对上一时间戳信息进行增强。**

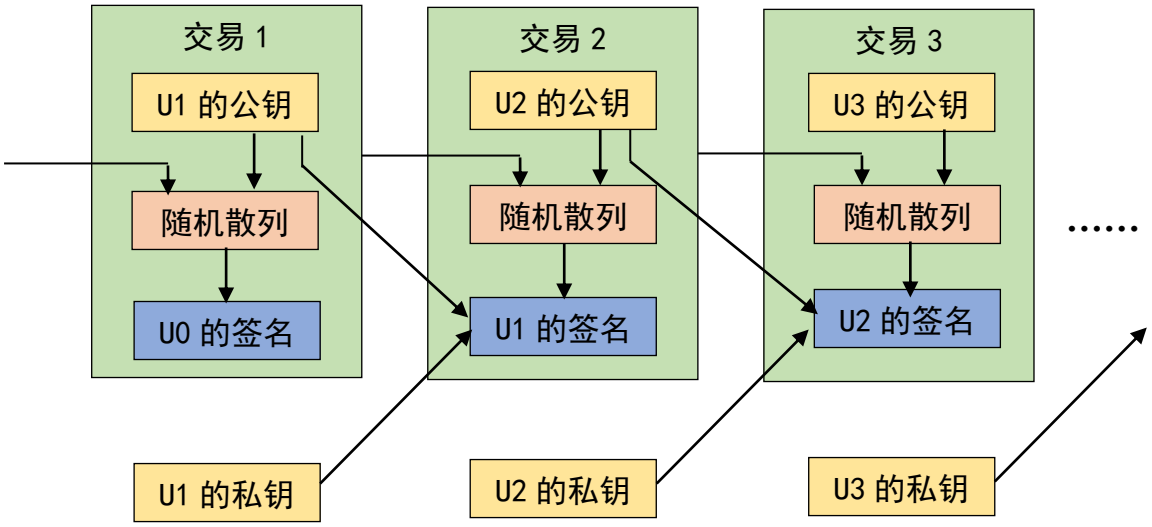


图 2　非对称加密在区块链中应用

通过分析区块链链式结构散列原理可以发现，如果大多数的所有者是诚信的，则随着区块链的增长，区块链的信用会相应快速增长，如果攻击者企图对已经形成的区块进行篡改，则必须篡改所有诚信者的区块以及其后交易区块的信息，对于一个长度不断增长的区块链来说，攻击者要完成相应区块信息的修改几乎是不可能的[8,9]，区块链的去中心化及区块所有者互相证明的机制实现了交易的有效证明。

4、区块链技术的出现重新定义了智能合约

当智能设备进行交互时触发智能合约[10]来执行操作，通过在区块链上写入类似 if-then 语句的程序，使得当预先编好的条件被触发时，程序自动触发支付及执行合约中的其它条款。**方便了物联网的设备维护、自动升级等。**从安全的角度来看，智能合约首先是同一般区块链数据一样，具有分布式、存证、一致完整、不可篡改删除等特性；其次，智能合约也是作为保证区块链安全的一种技术手段。在智能合约里规定了参与方的权利义务，合约执行的触发条件以及对应结果，一旦该智能合约被加入到区

块链中就可以不受任何一方影响，客观、准确地执行。在提供了安全的区块链环境之后，智能合约的安全很大程度上取决于合约代码。如果合约代码里的实现逻辑存在问题就严重影响到区块链的安全，因此，有必要对上链的智能合约进行慎重检查。一种效率较高的解决办法就是提供智能合约模板，智能合约模板经过了专业审核、试用验证，用户在使用智能合约模板时只需要填写相关输人数据即可。**智能合约可以由一个计算系统自动执行。**智能合约的运作机理如图 3 所示：

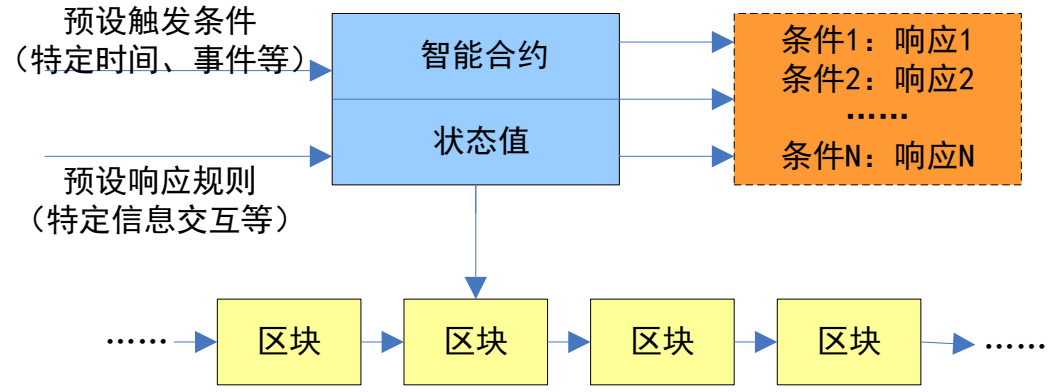


图 3　智能合约的运作机理

通常情况下，智能合约经各方签署后，以程序代码的形式附着在区块链数据上，经 P2P 网络传播和节点验证后记入区块链的特定区块中。智能合约封装了预定义的若干状态及转换规则、触发合约执行的情景(如到达特定时间或发生特定事件等)、特定情景下的应对行动等。区块链可实时监控智能合约的状态，并通过核查外部数据源、确认满足特定触发条件后激活并执行合约。

如果区块链是一个数据库，智能合约就是能够使区块链技术应用到现实当中的应用层。传统意义上的合同一般与执行合同内容的计算机代码没有直接联系。纸质合同在大多数情况下是被存档的，而软件会执行用计算机代码形式编写的合同条款。**智能合约在区块链 2.0 中得到长足发展，以以太坊为代表的区块链将智能合约的应用推向了更高水平。**

(1) 多方之间的定期交付合同被以代码的形式写入区块链。其中的个体是匿名的，但合同记录在公共账本中。

(2) 当扳机事件触发时，比如到期、执行价格达到，合约按照编程的条款自动执行。

(3) 监管者可以通过这个区块链了解市场上的活动，同时维护个体成员的隐私。

5、由物联网中不同的实际需求对区块链进行分类

根据物联网中的实际需求对区块链进行了分[11]，公有链是任何节点都是向任何人开放的，每个人都可以参与到这个区块链中参与计算，而且任何人都可以下载获得完整区块链数据（全部账本）。但是有些区块链的应用场景下，并不希望这个系统任何人都可以参与，任何人都可以查看所有数据，只有被许可的节点才可以参与并且查看

所有数据。那么这种区块链结构我们称为**私有链**。

联盟链是指参与每个节点的权限都完全对等，大家在不需要完全互信的情况下就可以实现数据的可信交换，R3 组成的银行区块链联盟要构建的就是典型的**联盟链**。区块链解决了囚徒困境中的背叛选项，能够实现强制执行，相比于跨国之间信任度很弱的合作来说是进步的。

但是随着区块链技术的快速发展，不排除以后公有链和私有链的界限会变得比较模糊。因为每个节点的可以有较为复杂的读写权限，也许有部分权限的节点会向所有人开放，而部分记账或者核心权限的节点只能向许可的节点开放，那就会不再是纯粹的公有链或者私有链。

6、区块链与物联网相结合

物联网中智能设备多达数百万，交互高达数十亿，仅靠中心化的模式运行会产生问题，其安全性也越来越引起人们的关注。区块链采用分布式账本技术、非对称加密算法、智能合约等使得安全的网状网络得以建立，这其中物联网设备将以可靠的方式互相连接，从而避免设备欺骗和假冒的威胁[12,13]。

当智能设备每发生一次交互，其交互信息会被物联网中其他节点们看到，它们会将这些信息临时放到自己各自维护的一个临时的信息池中，当矿工创建出一个区块以后，便可以把这些交互信息从信息池中拿出放到这个新区块中，然后通过解决一个双哈希问题去证明这个区块的合法性。当每一项物联网中智能设备交互信息被区块收录的时候，可以被认为是一次确认。在此区块之后每产生一个区块，此项交互的确认数就再加一。当确认数目到达六次以上的时候，通常就能认为此项设备交互比较安全并且不可逆转，当确认数达到 120 次时说明此次物联网中智能设备之间进行的信息交互是绝对安全和绝对不可逆转的。与此同时，此次设备的信息交互已经在物联网上传播开来，但只有通过验证且成功加入到一个区块中的时候，这笔交互才能成为区块链的一部分。

区块链中的工作量证明机制[14]使得生成下一个区块的节点和矿工几乎无法被被攻击预测到，同时，通过计算双 Hash 问题且输出的 Hash 值以特定数量的 0 开头，保证了节点和旷工的随机性，所以删除物联网中交互记录几乎不可能。**中本聪在论文中写道：“工作量证明本质上是一 CPU 一票(Proof-of-work is essentially one-CPU-one-vote)”。**

区块链技术与物联网相结合，可以实现物联网中智能设备的智能交互、自动升级、智能维护等，**帮助物联网中的设备理解彼此，并且帮助设备知道不同设备之间的关系，通过寻址和权限控制，实现对分布式的物联网的去中心化控制。**研究区块链技术在物联网中的应用，为智能设备安全及隐私保护提供解决技术方案具有重要的科学意义和社会意义。

主要问题

物联网(Internet of things IoT)是一个迅速发展的产业，其注定将改变住所、城市、农场、工厂以及几乎其他所有的物体，使它们智能化并更具有效率。但是，物联网的混乱发展也将面临诸多挑战，因为要对那么多设备进行识别、连接、保护及管理。区块链，即比特币及以太坊等加密货币背后的分布式记账技术[15]，可以解决这些问题。区块链已经在包含物联网在内的其他诸多领域体现了它的价值。区块链可以使得物联网生态体系挣脱传统基于经纪人的网络工作模式[16,17]，即使得设备不再依赖于通过中央云服务器来识别和鉴定单个设备。

1、物联网的安全问题

物联网的安全形态主要体现在其体系结构的各个要素上。第一是**物理安全**，主要是传感器的安全，包括对传感器的干扰、屏蔽、信号截获等，是物联网安全特殊性的体现；第二是**运行安全**，存在于各个要素中，涉及到传感器、传输系统及处理系统的正常运行，与传统信息系统安全基本相同；第三是**数据安全**，也是存在于各个要素中，要求在传感器、传输系统、处理系统中的信息不会出现被窃取、被篡改、被伪造、被抵赖等性质。物联网除面临一般信息网络所具有的安全问题外，还面临物联网特有的威胁和攻击，物联网系统中主要面临的安全和隐私威胁是**物理俘获、传输威胁、自私性威胁、拒绝服务威胁、感知数据威胁。**

目前物联网的安全威胁主要来自以下几个方面：**阻塞干扰、碰撞攻击、耗尽攻击、非公平攻击、选择转发攻击、陷洞攻击、女巫攻击、洪泛攻击、信息篡改等。**

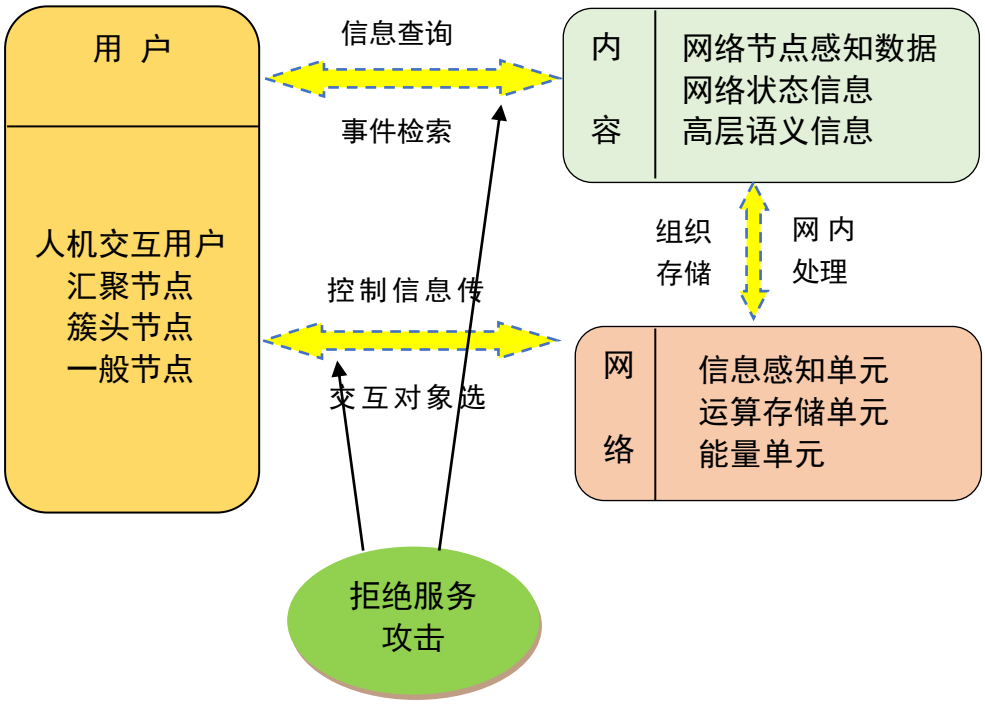


图4　物联网信息交互威胁

物联网的重要特征是智能处理，包括如何从网络接收信息，并确定哪些信息是真正有用的信息，哪些垃圾邮件甚至是恶意的信息。智能处理过程中有拒绝服务攻击(DOS)，分布式拒绝服务(DDoS)等其他攻击。由于目前物联网的混乱发展，使其在系统逻辑设计上存在缺陷和漏洞，这种缺陷或错误可以被攻击者利用，通过阻塞干扰、碰撞攻击、耗尽攻击、非公平攻击、选择转发攻击、陷洞攻击等来攻击或控制整个系统，从而窃取重要信息和信息，甚至破坏系统。这些攻击会影响到一个大范围，包括系统本身及网络中相交互的智能设备等。

2、物联网的安全隐患

(1) 网络节点日趋庞大。随着网络节点增至数百万，交易高达数十亿，就会产生问题。因为这将几何数地提高计算要求，进一步讲就是增加成本。

(2) 针对服务器的攻击。单独一个点的问题将导致物联网非常易于遭受拒绝服务攻击(DoS/DDoS)，这些攻击专门瞄准服务器和将其淹没在盗用设备流量中。这将周期性地影响物联网生态体系，特别在运行更多的敏感任务时。

(3) 中心化网络难以建立。因为物联网节点需要遍布在缺乏连接装置的广泛区域内例如大农场中，这使得建立中心化网络的成本增加，且维护困难。

3、物联网的安全机制

针对物联网中存在的安全隐私问题，国内外的研究人员给出了许多不同的安全对策。典型的解决方案是针对物联网不同的分层采用不同的处理方案，但由于物联网标准尚未发布，对物联网的分层并不统一，只是初步搭建了物联网的安全架构体系[18]。本项目中我们将区块链技术应用到物联网中，下面我们针对物联网安全攻击和安全风险所采取的安全机制和方法从这以下两个方面分析。

(1) 基于分层的安全机制

物联网的核心可划分为三个逻辑层，分别为感知层、传输层和处理应用层。总体上，感知层的作用是获取原始数据，传输层的作用是将这些原始数据传输到远程的处理平台进行处理，而处理应用层的作用无疑是对来自不同感知节点的信息进行存储、处理和应用。

物联网感知层包括 RFID[19]安全措施、无线传感网络安全措施等。传输层安全机制可综合利用点到点加密机制和端到端加密机制。应用层安全措施，在数据智能化处理的基础上加强数据库访问控制，加强不同应用场景的认证机制和加密机制，加强数据溯源能力和网络取证能力，完善网络犯罪取证机制。虽然目前已提出一些轻量级加密、认证算法，但是还没有提出完整的适用于大规模传感网的整体安全方案。而且**即使保证物联网感知层安全、传输层安全和处理层安全，也保证终端设备不失窃，仍然不能保证整个物联网系统的安全。**

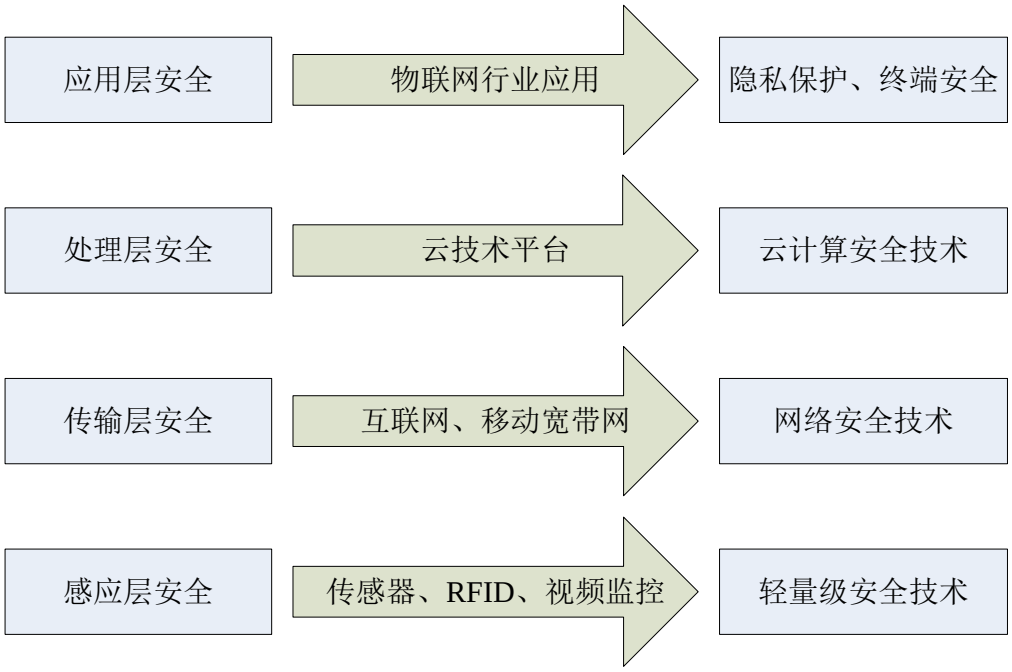


图5　物联网安全架构和关键技术示意图

(2) 基于区块链的安全机制

区块链技术以其去中心、去信任、分布式存储等特点可以使得安全的网状网络得以建立，其中物联网设备将以可靠的方式互相连接，从而避免设备欺骗和假冒的威胁。每一个合法节点都在区块链中登记，且每个智能设备都有一个相同的区块链账本，**设备将非常容易地识别和鉴定其他设备，不需要中间经纪人或者认证机构，网络将具有扩展性地支持数十亿设备，而且不需要额外资源。**

由区块链构建起的物联网社会，让我们的所有智能终端都成为网络的一分，没有任何的企业可以掌握我们的信息，所有的控制权都掌握在我们每个人的手上。同时，区块链的存在又大大降低了集中存储、使用、运算的成本，智能设备将会通过区块链加密之后分享自己的运算资源、网络带宽，从而让分享成为一种可能。区块链带来的万物互联正在让互联网从线上走到线下，真正让物联网成为可能。

在区块链中采用数字签名、SHA256 和 Merkle Tree 可以保证隐私安全。数字签名涉及到一个哈希函数、发送者的公钥、发送者的私钥。**ECDSA** 是基于椭圆曲线的公钥密码体制上实现的数字签名方案，其安全性依赖于基于椭圆曲线的有限群上的离散对数难题。与基于 RSA 的数字签名和基于有限域离散对数的数字签名相比，在相同的安全强度条件下，EDCSA 方案具有如下特点：**签名长度短，存储空间小，计算速度快，特别适用于计算能力和存储空间有限、带宽受限、要求高速实现的场合。**

Hash 函数因其具有单向性将其与数字签名及 Merkle Tree 相结合应用到区块链中防止签名的伪造和对数字签名的抵赖，并且对每笔交易都进行 hash 运算保证了数据安全。在本文中我们采用 SHA256 算法[20]，目前 SHA 系列有多种算法其相关属性区别如表 3 所示：

表 3　SHA 相关属性比较

	SHA1	SHA256	SHA384	SHA512
消息摘要长度	160	256	384	512
消息长度	$<2^{64}$	$<2^{64}$	$<2^{128}$	$<2^{128}$
分组长度	512	512	1024	1024
字长度	32	32	64	64
步数	80	64	80	80

当发生数据交互时将数据进行分组哈希，并将生成的新哈希值插入到 Merkle 树中，如此递归直到只剩最后一个根哈希值并记为 Merkle 根，在区块链的数据结构中可以快速归纳和校验区块数据的存在性和完整性。同时**采用同态加密技术进行加密保证了明文的安全。**因此，本项目提出的**基于区块链技术的物联网传输层安全智能交互协议在解决智能设备交互中具有更好的优势。**

关键技术

本项目主要是设计一种基于区块链技术的物联网安全智能交互协议，下面对采用的关键技术进行详细介绍。

1、同态加密 Paillier

同态加密[21,22]是基于数学难题的计算复杂性理论的密码学技术。**对经过同态加密的数据进行处理得到一个输出，将这一输出进行解密，其结果与用同一方法处理未加密的原始数据得到的输出结果是一样的。**Paillier 算法对密文进行同态操作减少了大量的加解密次数，避免了读取用户明文形式的密钥份额，这样**不影响明文数据的机密性。**当有多个节点离开或加入时，基于同态技术的批处理密钥分发方案以其较少的加解密开销将更具优势。

Paillier 加密算法是一种加同态加密算法，它有三个算法组成：密钥生成算法(Key Generation)、加密算法(Encryption)和解密算法(Decryption)。

(1) Paillier 同态性分析

密钥生成：

① 随机地选取两个素数 p 和 q，且满足 $\gcd=(pq,(p-1)(q-1))=1$。

② 计算 $N=pq$ 和 $\lambda=lcm(p-1,q-1)$。

③ 选取随机数 g $(g\in Z^{*}_{N^2})$，且满足 μ=（L（$g^{\lambda}\bmod N^2$））$^{-1}\bmod N$ ，其中定义函

数 L 为 $L(u)=\frac{u-1}{N}$ 。

④ 公钥为 $PK=(N,g)$，私钥为 $SK=(\lambda,\mu)$。

加密算法： 给定消息 $M\in Z_N$，随机选择 $r\in Z_N^*$，计算密文 $C=E(M)=g^M\bullet r^N \bmod N^2$。

解密算法： 给定密文 $C\in Z_{N^2}^*$ 对应的明文为 $M=D(C)=L(C^\lambda \bmod N^2)\bullet\mu \bmod N$。

同态性分析：paillier 密码体制是具有加法同态性的加密方案。对其加法同态性证明如下：对明文 m_1 和 m_2 加密后，可以得：$E(m_1)=g^{m_1}\bullet x_1^N \bmod N^2$，

$E(m_2)=g^{m_2}\bullet x_2^N \bmod N^2$。此时，$E(m_1)\bullet E(m_2)=g^{m_1}x_1^N\bullet g^{m_2}x_2^N \bmod N^2=E(m_1+m_2)$。

(2) 各种同态性质的定义

① **加法同态：** 如果从 $E(x)$ 和 $E(y)$ 通过运算可以计算出 $E(x+y)$，而不需要知道 x，y 的值，$C(E(x),E(y))=E(x+y)$，此处 C 代表任意运算。

② **乘法同态：** 如果从 $E(x)$ 和 $E(y)$ 通过运算可以计算出 $E(x\times y)$，而不需要知道 x，y 的值，$C(E(x),E(y))=E(x\times y)$，此处 C 代表任意运算。

③ **混合乘法同态：** 如果从 $E(x)$ 和 y 通过运算可以计算出 $E(x\times y)$，而不需要知道 x 的值，$C(E(x),y)=E(x\times y)$ 此处 C 代表任意运算。

④ **全同态加密**方案：如果一个同态加密方案 E 对于所有的布尔电路都满足一致性，则称方案 E 为全同态加密方案。

2、椭圆曲线数字签名的生成和验证算法

本节阐述基于椭圆曲线的公钥密码体制(简称 ECC)在数字签名中的一个实现方案 ECDSA[23,24]，这个方案的**基本思想就是在椭圆曲线有限域上实现 DSA 算法。**与普通的离散对数问题和大数分解问题不同，椭圆曲线离散对数问题(ECDLP)没有亚指数时间的解决方法。因此椭圆曲线密码的单位比特强度要高于其他公钥体制。ECDSA 是基于椭圆曲线的公钥密码体制上实现的数字签名方案，**其安全性依赖于基于椭圆曲线的有限群上的离散对数难题。**与基于 RSA 的数字签名和基于有限域离散对数的数字签名相比，在相同的安全强度条件下，ECDSA 方案具有如下特点：**签名长度短，存储空间小，计算速度快，特别适用于计算能力和存储空间有限、带宽受限、要求高速实现的场合。**ECDSA 在安全性方面的目标是能抵抗选择明文或密文攻击。而攻击 A 的攻击者的目标是在截获 A 的签名后，可以生成对任何消息的合法签名。尽管 ECDSA 的理论模型很坚固，但是人们仍研究很多措施以提高 ECDSA 的安全性。在 ECDLP 不可破解及哈希函数足够强的前提下，DSA 和 ECDSA 的一些变形已被证明可以抵抗

现有的任何选择明文（密文）攻击。在椭圆曲线所在群是一般群并且哈希函数能够抗碰撞攻击的前提下，ECDSA 本身的安全性已经得到证明。

下面详述 ECC 签名方案的实现过程。

(1) 生成 ECDSA 密钥对

ECDSA 密钥对与 EC 域参数的特定集相关联。公钥是基点的随机倍数；而私钥则是用来生成这个倍数的整数。

为了生成 ECDSA 密钥对，每个成员 A 都要做如下操作：

a) 在区间$[1,n-1]$中选择一个随机或伪随机整数d；

b) 计算$Q=dG$；

c) A的公钥是 Q，私钥是d。

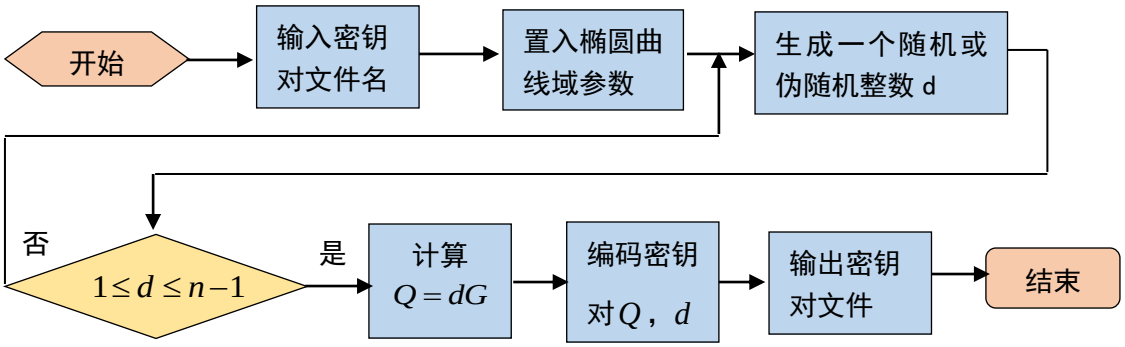


图 6　密钥对生成流

（2）生成 ECDSA 签名

为了签署消息 m，具有域参数$D=(q,FR,a,b,G,n,h)$及其相关密钥对(d,Q)成员 A 作如下操作：

a) 选择一个随机或伪随机整数k满足$1\le k\le n-1$；

b) 计算$kG=(x_1,y_1)$，且将x_1转换成整数$\overline{x_1}$；

c) 计算$r=x_1 \bmod n$，如果$r=0$则回到第a步；

d) 计算$k^{-1} \bmod n$；

e) 计算$SHA-256(m)$，并将该位串转换成整数e；

f) 计算$s=k^{-1}(e+dr) \bmod n$，如果$s=0$则回到第a步；

g) A对消息m的签名为(r,s)。

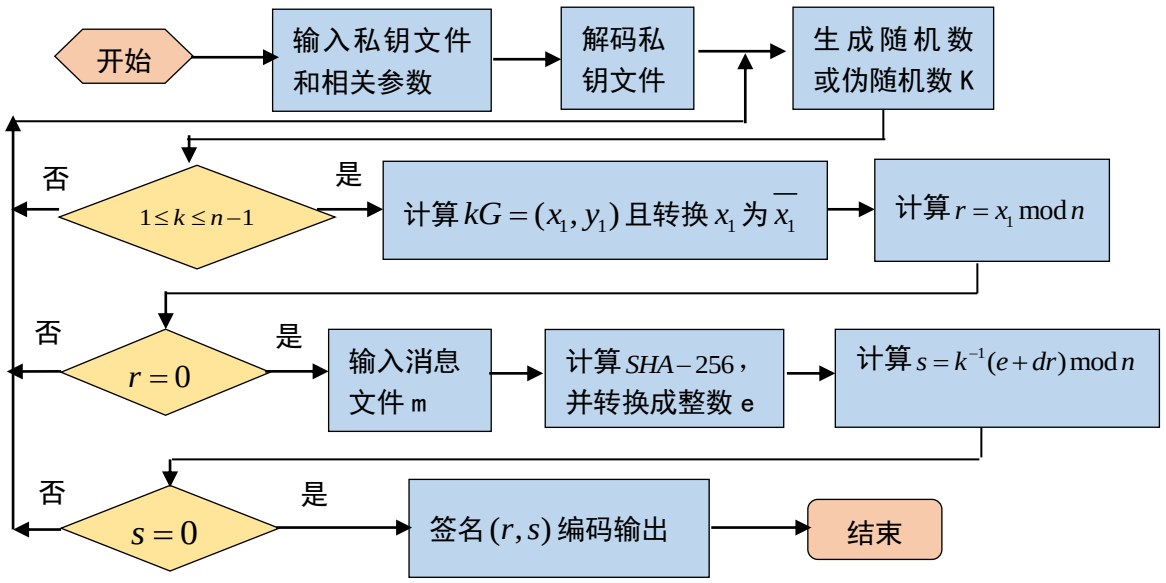


图 7　签名流程

（3）验证 ECDSA 签名

要验证 A 在消息 m 上的签名为 (r,s)，B 取得 A 域参数 $D=(q,FR,a,b,G,n,h)$ 的可信副本和相关公钥 Q，推荐 B 也验证 D 和 Q 的有效性，然后 B 做以下的操作：

a) 验证 r 和 s 是区间 $[1,n-1]$ 内的整数；

b) 计算 $SHA-256(m)$，并将该位串转换成整数 e；

c) 计算 $w=s^{-1} \bmod n$；

d) 计算 $u_1=ew \bmod n$ 和 $u_2=rw \bmod n$；

e) 计算 $X=u_1G+u_2Q$；

f) 如果 $X=0$ 则拒绝签名；否则转换 X 的 x 坐标 x_1 为整数 $\overline{x_1}$，并计算 $v=\overline{x_1} \bmod n$；

g) 当且仅当 $v=r$ 时接受签名。

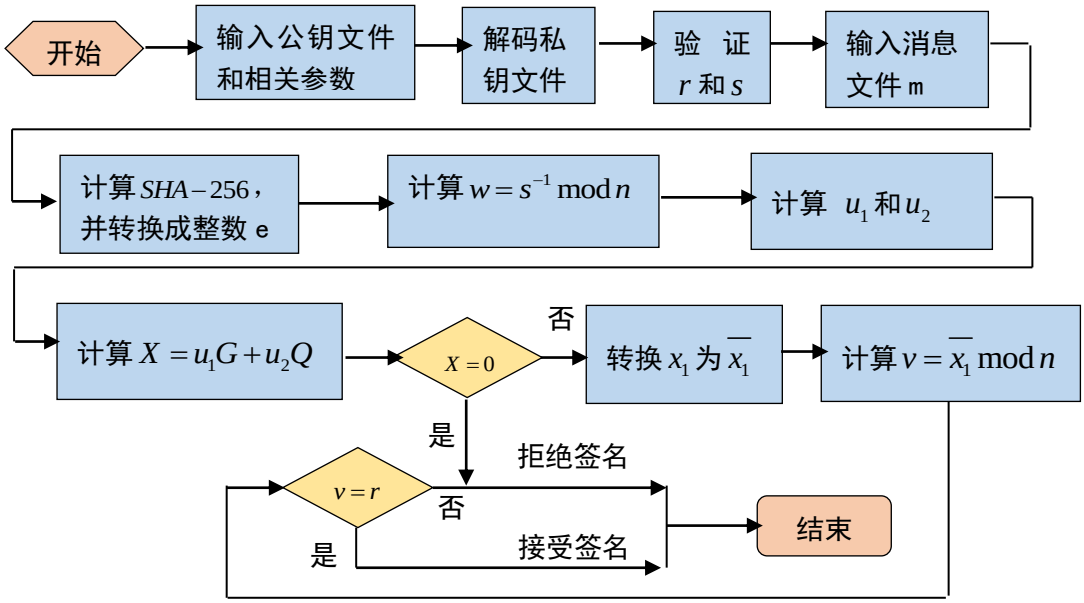


图 8　验证流程

3、基于以太坊的 Merkle Tree

Merkle 树[25]是区块链的重要数据结构，**其作用是快速归纳和校验区块数据的存在性和完整性。**如图 9 所示，Merkle 树通常包含区块体的底层(交易)数据库，区块头的根哈希值(即 Merkle 根)以及所有沿底层区块数据到根哈希的分支。Merkle 树运算过程一般是将区块体的数据进行分组哈希，并将生成的新哈希值插入到 Merkle 树中，如此递归直到只剩最后一个根哈希值并记为区块头的 Merkle 根。最常见的 Merkle 树是比特币采用的二叉 Merkle 树，其每个哈希节点总是包含两个相邻的数据块或其哈希值，其他变种则包括以太坊[26,27]的 Merkle patricia tree 等。Merkle 树有诸多优点：首先是**极大地提高了区块链的运行效率和可扩展性，使得区块头只需包含根哈希值而不必封装所有底层数据，这使得哈希运算可以高效地运行在智能手机甚至物联网设备上。**

梅克尔树最为常见和最简单的形式，是二进制梅克尔树(binary Merkle tree)，其中一个 bucket 单位的数据块总是包含了两个相邻的块或哈希，它的描述如下：

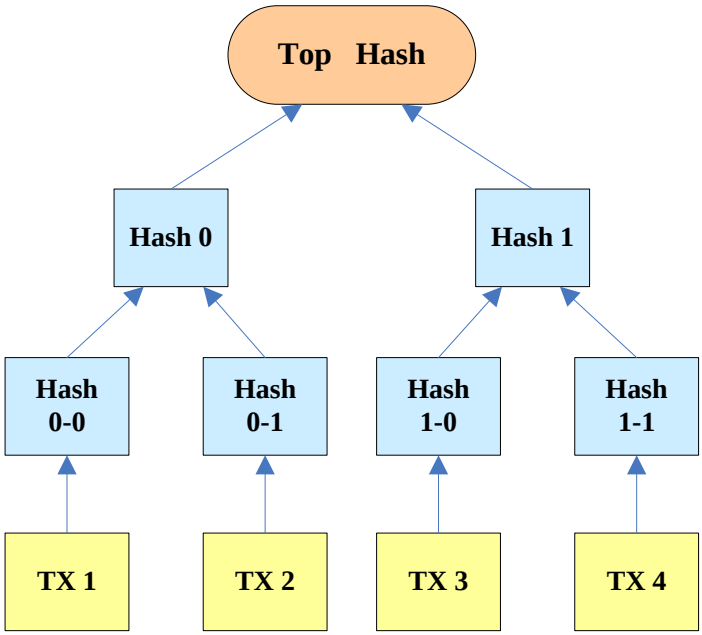


图 9　Merkle 树

上图中 TX1~TX4 为物联网中智能设备的交互信息，采用这样的哈希算法它允许了一个整齐的机制，我们称之为梅克尔证明(Merkle proofs)。

帕特里夏树（PATRICIA TREES）

最为简单的一种梅克尔树是二进制梅克尔树。然而，以太坊所使用的梅克尔树则更为复杂，我们称之为“梅克尔.帕特里夏树”[28]（Merkle Patricia tree）。二进制梅克尔树对于验证“清单”格式的信息而言，它是非常好的数据结构，本质上来讲，它就是一系列前后相连的数据块。而对于交易树来说，它们也同样是不错的，**因为一旦树已经建立，花多少时间来编辑这颗树并不重要，树一旦建立了，它就会永远存在。**

以太坊的每一个区块头，并非只包含一颗梅克尔树，而是包含了三颗梅克尔树，分别对应了三种对象：**交易**(Transactions)、**收据**(Receipts，基本上它是展示每一笔交易影响的数据条)、**状态**(State)。这使得一个非常先进的轻客户端协议成为了可能，通过 Merkle 树计算查询是相当简单的。服务器简单地找到了对象，获取梅克尔分支，并通过分支来回复轻客户端。而对状态树来说，情况会更加复杂些。以太坊中的状态树基本上包含了一个键值映射，其中的键是地址还有各种值，包括账户的声明、余额、随机数、代码以及每一个账户的存储(其中存储本身就是一颗树)。然而，不同于普通的交易历史记录，状态树需要经常地进行更新：账户余额和账户的随机数 nonce 经常会更变，更重要的是，新的账户会频繁地插入，存储的键(key)也会经常被插入以及删除。而这样的数据结构设计，**我们可以在一次插入、更新编辑或者删除操作之后，快速地计算出新的树根(tree root)，而无需重新计算整颗树。**此外，它还有两个非常好的次要特性：

(1) 树的深度是有限制的，即使考虑攻击者会故意地制造一些交易，使得这颗树尽可能地深。不然，攻击者可以通过操纵树的深度，执行拒绝服务攻击(DOS attack)，使得更新变得极其缓慢。

(2) 树的根只取决于数据，和其中的更新顺序无关。换个顺序进行更新，甚至重新从头计算树，并不会改变根。

而帕特里夏树，简单地说，或许最接近的解释是，我们可以同时实现所有的这些特性。**其工作原理，最为简单的解释是，一个以编码形式存储到记录树的“路径”的值。**每个节点会有 16 个子(children)，所以路径是由十六进制编码来确定的。在实践中，当树稀少时也会有一些额外的优化，我们会使过程更为有效。

解决方案

区块链技术以其去中心化、去信任、分布式存储、开放性、不可篡改和加密安全性被广泛应用于各个领域，它是通过**去中心化和去信任**的方式集体维护一个可靠数据库的技术方案。通俗一点说，区块链技术就指一种全民参与记账的方式。所有的系统背后都有一个数据库，可以把数据库看成是就是一个大账本。研究区块链技术在物联网等领域的应用具有深远的实际意义。**本方案中我们通过以下四个步骤实现基于区块链技术的物联网传输层安全智能交互协议的设计与研究。**

1、首先分析了典型物联网中智能设备交互协议

本项目首先**针对**物联网中碰撞攻击、信息篡改、选择转发等常见的攻击形式和信息交互协议的安全需求，详细研究了目前主流的 RFID 的安全认证协议，RFID 通过无线射频方式进行非接触、双向数据通信对目标加以识别。可以快速读写、长期跟踪管理。但是 RFID 标签无需直接与收发器接触，使用者会在不知情的情况下被他人读取标签内存的信息，构成安全隐患。因此本项目**提出**一种新的基于区块链技术的物联网智能交互协议，该协议具有更高的安全性和执行效率。

2、其次提出基于区块链技术的物联网传输层安全智能交互协议

在分析了典型物联网安全交互协议及安全需求后，**对提出的新协议的安全性进行详细研究。**

(1) 详细的阐述了区块链技术的运作机制，其**分布式账本技术、非对称加密算法和智能合约**等技术保证了物联网中各个智能设备都独立的拥有全网统一的数据账本。对于物联网，智能设备数量呈指数级增长，区块链技术在这些设备之间**建立了低成本的互相直接沟通桥梁，**同时又通过去中心化的共识机制提高系统的安全私密性。区块链叠加智能合约技术将智能设备变成可以自我维护调节的独立个体，这些个体可在事先规定或植入的规则合约基础上执行类似和其他个体交换信息或核实身份等功能。在我们的项目中智能设备一经生产就通过 Merkle 树将其登记到区块链中并同时设定其安全等级，当一智能设备向另一智能设备提出请求服务时**触发智能合约**来同其他智能设备交互信息。

(2) 采用椭圆曲线数字签名技术实现数据完整性和不可否认性。ECDSA 是基于椭圆曲线的公钥密码体制上实现的数字签名方案，其安全性**依赖于基于椭圆曲线的有限群上的离散对数难题。**在本项目的 ECDSA 中我们采用 SHA256 散列函数，进行 64 轮操作，输出 256 bit 的消息摘要。与其它基于有限域离散对数的数字签名相比，在相同的安全强度条件下，ECDSA 签名方案其**签名长度短，存储空间小，计算速度快，适用于物联网中智能设备信息交互时进行签名。**

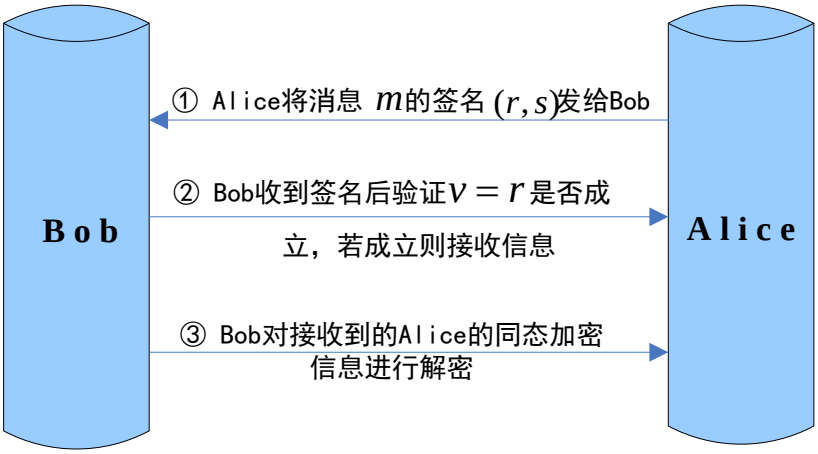


图 10　ECDSA 签名流程

(3) 本项目同时采用同态加密技术来对交互信息进行加密，对经过同态加密的数据进行处理得到一个输出，将这一输出进行解密，其结果与用同一方法处理未加密的原始数据得到的输出结果是一样的。**对密文进行同态操作减少了大量的加解密次数，且不影响明文数据的机密性。**如果用数学方法表述，假设加密操作为 E，明文为 m，加密得 e，即 $e=E(m), m=E^{-}(e)$。已知针对明文有操作 f，针对 E 可构造 F，使得 $F(e)=E(f(m))$，这样 E 就是一个针对 f 的同态加密算法。同态加密与经典的非对称

加密相比算法中多一步 $Eval$， $Eval$ 用于对密文执行再加密。

同态计算算法 $Eval$：公钥 pk，一个算术电路 C，一组 ℓ 个密文 $c=(c_1,c_2,...c_\ell)$ 作为输入值。这里 $c_i=E(pk,m_i)$，输出一个同态计算密文 $c_{Eval}=Eval(pk,C,c_i)$。

同态加密算法在本项目中的应用如图 11 所示。

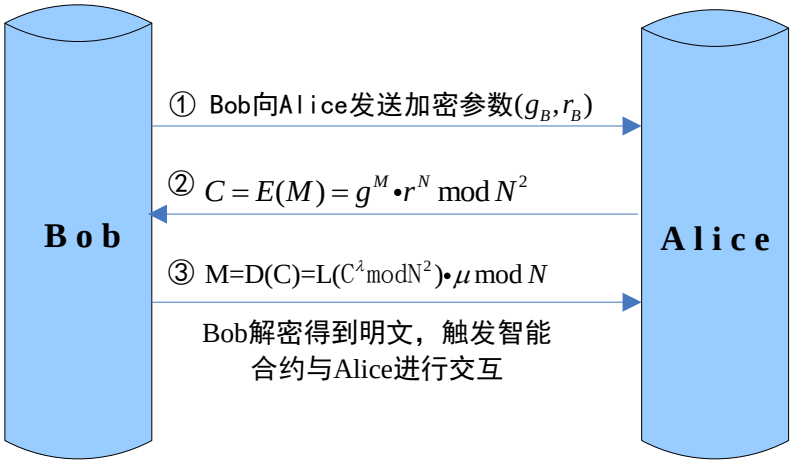


图 11　同态加密算法流程

3、之后对安全交互协议的安全性及可行性分析

本项目提出的基于区块链技术的物联网传输层安全智能交互协议，因区块链是去中心去信任的，所以物联网中智能设备可以实现去中心的智能自我管理、维护。**对本项目的安全及可行性分析如下：**

(1) 将新生产的智能设备的 ID 编号进行 Hash 运算，在区块链中登记 ID 的 Hash 值而不是直接登记 ID 编号，这样实现了对参与节点的匿名保护；

(2) 将智能设备 ID 编号的 Hash 值通过 Merkle 树登记在区块链中，因为 Hash 函数具有单向性和雪崩效应，任一节点的 Hash 值的任意小的变化都将改变 Merkle 树的头部信息。若某一区块头中的 Hash 值与其它区块头中的 Hash 不匹配，则可以认定此区块值为伪造的，则其他区块承认此区块的合法性；

(3) 对交互信息的加密采用同态加密算法，同态加密是对密文进行操作，不直接操作明文，这样保证了明文的安全；

(4) 物联网中设备进行交互时利用 ECDSA 进行签名，其签名长度短、存储空间小且计算速度快很适用于智能设备直接交互信息时进行签名。

经过以上分析，我们提出的基于区块链技术的物联网传输层安全交互协议满足协议的安全性和可行性，可以抵挡重放攻击、篡改攻击、伪装攻击、等常见攻击。能够解决数以亿计的智能设备信息交互的难题，相比于传统的中心控制机制，**我们的方案**

极大的提高了物联网智能信息交互的运行效率和各智能设备的安全性。

4、最后拓展区块链在物联网中的其它应用

在项目的最后我们拓展区块链在物联网中的其它应用，区块链在物联网中的应用不仅仅局限在智能设备之间的信息交互。如对物联网设备制造商和服务提供者而言，允许他们将维护设备的责任转移给一个自我维护设备社区，这使得无论在设备生命周期还是超过生命周期物联网都不会过时，并节省大量的基础设施成本。

本项目通告以上四个步骤解决了物联网传输层安全智能交互存在的安全问题，整体解决方案的流程图如图 12 所示。

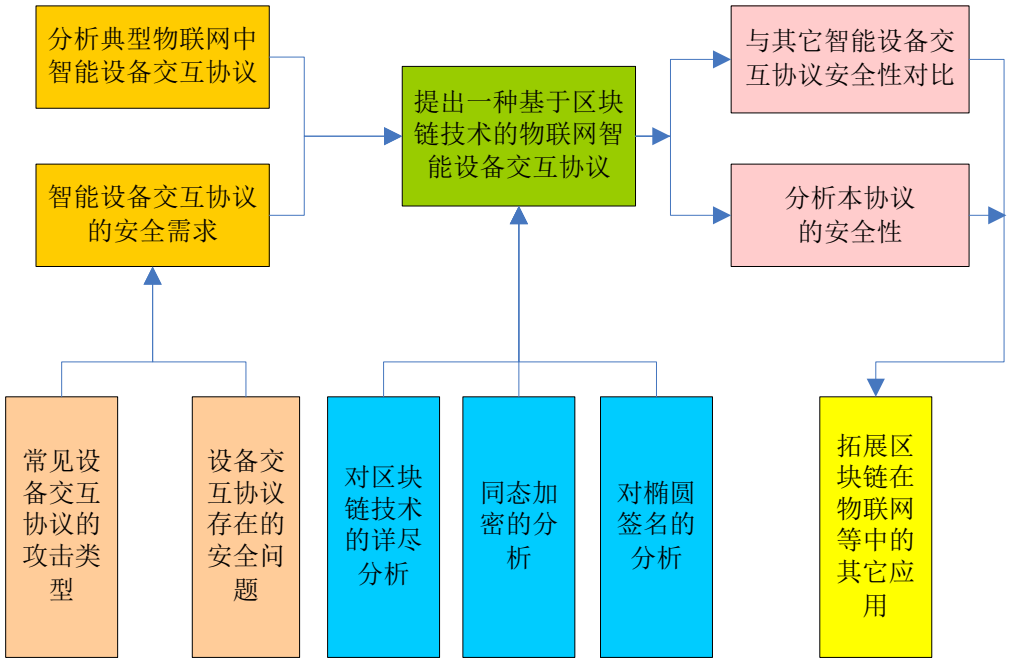


图 12　解决方案的流程图

研究方法

1、协议中的加密及签名

在本协议中需要用到一个同态加密 Paillier 算法，算法中包含加密函数 E 和解密函数 D。显然，作为一个公钥密码算法，F 应该满足以下条件：

(1) 发送方在知道公开密钥 K_{P_u} 和明文 M 的情况下，很容易计算出对应的密文 $C = E_{K_{P_u}}(M)$；

(2) 接收方通过使用私有密钥 K_{P_m} 很容易从密文 C 恢复出密文 $M = D_{K_{P_r}}(C) = DK_{P_r}(E_{K_{P_u}}(M))$；

(3) 攻击者可以获取公开密钥K_{P_u}，但是通过K_{P_u}要得到私有密钥K_{P_r}在计算上是不可行的；

(4) 攻击者在知道密文 C 和公开密钥K_{P_u}的情况下，想要恢复明文 M 在计算上是不可行的；

(5) 加密函数 E 和解密函数 D 的次序可以互换，即：

$$M = E_{K_{P_u}}(D_{K_{P_r}}(M)) = DK_{P_r}(E_{K_{P_u}}(M))。$$

协议中采用基于椭圆曲线的数字签名技术，为了满足身份认证、数据完整性和不可否认性等需求，数字签名应具有一下特点：

(1) 可信性：签名使文件的接受者相信签名者是慎重地在文件上签名的；

(2) 不可重用性：签名不可重用，即同一消息在不同时刻的签名是有区别的；

(3) 不可改变性：在文件签名后，文件不能改变；

(4) 不可伪造性：签名能够证明是签名者而不是他人在文件上签名，任何人都不能伪造签名；

(5) 不可否认性：在签名者否认自己的签名时，签名接收者可以请求可信第三方进行仲裁。

2、协议中的初始化

协议要求在使用前需对每个设备进行初始化操作。设备 Alice 和 Bob 在生产后将它们的 ID 的 Hash 值登记到区块链中，并设定安全等级。

(1) Alice 和 Bob 分别随机选取$x_A \in Z_q^*$，$x_B \in Z_q^*$作为自己的私钥，分别计算$Y_A = x_A p$，$Y_B = x_B p$作为自己的公钥；

(2) Alice 向 Bob 发送交互请求，以及自己的身份信息 ID_A 的 Hash 值；

(3) Bob 在区块链中通过 Merkle Tree 验证 Alice 的合法性以及其安全等级，若合法，向 Alice 返回自己的身份信息 ID_B 的 Hash 值和加密参数(g_B, r_B)，否则丢弃；

(4) Alice 收到 Bob 的 ID 的 Hash 值后在区块链中通过 Merkle Tree 验证 Bob 的合法性，否则丢弃。

3、协议的算法步骤

（1）Alice 向 Bob 发送交互请求以及自己的 ID；

（2）Bob 在区块链中通过 Merkle Tree 验证 Alice 的合法性以及其安全等级，若合

法，向 Alice 返回自己的身份信息 ID_B 和加密参数(g_B, r_B)；

（3）Alice 采用 Bob 返回的 Paillier 加密参数(g_B, r_B)对明文M_A进行加密：$C_A = E(M_A) = g_B{}^{M} \bullet r_B{}^{N} \bmod N^2$，并利用私钥$x_A$生成相应签名$\sigma_A = (R_A, S_A)$，最后将密文和签名打包成报告：$C_A \| ID\_B \| ID\_A \| T \| \sigma_A$，其中 T 为当前时间戳，加时间戳的目的是防止重发攻击；

（4）Alice 将生成的报告发送给 Bob；

（5）Bob 收到 Alice 的数据包后，首先对数据包进行验证，确保收到的数据报是来自合法用户 Alice 且其数据未被篡改或伪造。当且仅当$v_A = r_A$时接受签名；

（6）如果步骤(5)验证通过，Bob 利用 Paillier 解密得到 Alice 的明文信息M_A，$M_A = D(C_A) = L(C_A{}^{\lambda} \bmod N^2) \bullet \mu \bmod N$。Bob 针对此明文信息$M_A$以及 Alice 登记在区块链中的安全等级，启动智能合约向 Alice 提供相应服务；

（7）Alice 接受 Bob 提供服务同时向 Bob 支付一定量的以太币；

（8）Bob 向全网广播与 Alice 的交互信息，全网矿工们将此次交互经过 Hash 运算后加入 Merkle Tree 记录到区块链中。

以上步骤为 Alice 单向的向 Bob 请求提供服务，Alice 与 Bob 可以是对等体，Bob 向 Alice 请求服务时过程与上述相同。

协议算法步骤的示意图如图 13 所示：

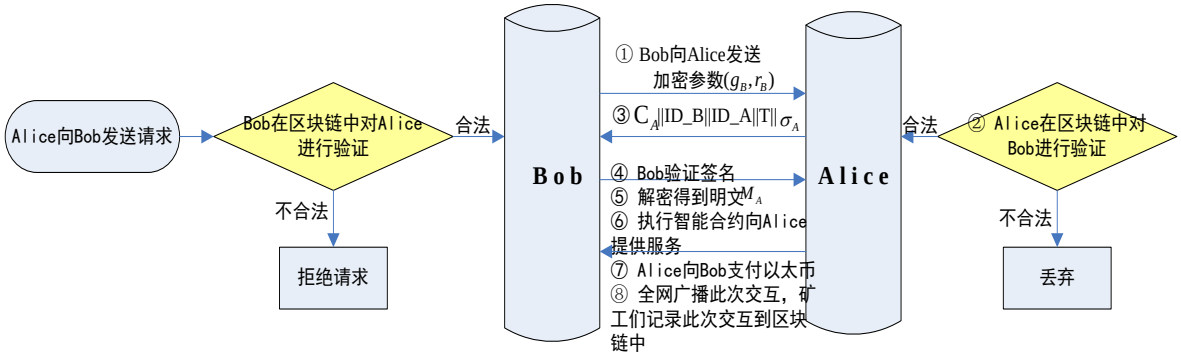


图 13　协议算法步骤

创新点

1、将区块链技术应用到物联网中，保证物联网传输层的安全智能交互。区块链技术以其去中心化、去信任、分布式存储等特性将每一个合法节点在区块链中登记，

使得安全的网状网络得以建立，其中物联网设备将以可靠的方式互相连接，设备将非常容易地识别和鉴定其他设备，从而避免设备欺骗和假冒的威胁。

2、与比特币区块链不同，本项目采用基于以太坊的区块链技术。以太坊的区块链对比特币区块链的应用范围进行了拓展，它可以支持更强大的脚本语言。以太坊区块链可以在物联网中实现智能合约，这些智能设备可在事先规定或植入的规则合约基础上执行类似和其他个体交换信息或核实身份等功能。

3、采用同态加密，在加密时对密文进行操作保证了明文的安全。在本项目中将同态加密技术实现与物联网中，对多个智能交互信息的密文进行计算之后再解密，不必对每一个密文解密从而降低高昂的计算代价，并通过多种计算形式保证了明文的安全。

参考文献

[1] Li Zhengdao, Ren Xiaocong. The Impact of Block Chain on the Internet Finance and its Future Prospects[J]. Technoeconomics Management Research, 2016(10): 397-413 (in Chinese)
(李政道, 任晓聪. 区块链对互联网金融的影响探析及未来展望[J]. 技术经济与管理研究, 2016(10): 75-78).

[2] Ulieru M. Blockchain 2.0 and Beyond: Adhocracies[M]// Banking Beyond Banks and Money. Springer International Publishing, 2016.

[3] Macdonald T J, Allen D W E, Potts J. Blockchains and the Boundaries of Self-Organized Economies: Predictions for the Future of Banking[M]// Banking Beyond Banks and Money. 2016.

[4] Kraft D. Difficulty control for blockchain-based consensus systems[J]. Peer-to-Peer Networking and Applications, 2016, 9(2): 397-413.

[5] Seebacher S, Schüritz R. Blockchain Technology as an Enabler of Service Systems: A Structured Literature Review[J]. 2017.

[6] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[J]. Consulted, 2009.

[7] Reijers W, Coeckelbergh M. The Blockchain as a Narrative Technology: Investigating the Social Ontology and Normative Configurations of Cryptocurrencies[J]. Philosophy & Technology, 2016: 1-28.

[8] Zhao J L, Fan S, Yan J. Overview of business innovations and research opportunities in blockchain and introduction to the special issue[J]. Financial Innovation, 2016, 2(1): 28.

[9] Ouaddah A, Elkalam A A, Ouahman A A. Towards a Novel Privacy-Preserving Access Control Model Based on Blockchain Technology in IoT[M]// Europe and MENA Cooperation Advances in Information and Communication Technologies. Springer International Publishing, 2017.v

[10] Idelberger F, Governatori G, Riveret R, et al. Evaluation of Logic-Based Smart Contracts for Blockchain Systems[M]// Rule Technologies. Research, Tools, and Applications. Springer International Publishing, 2016.

[11] Yuan Y, Wang F Y. Blockchain: The State of the Art and Future Trends[J]. Acta Automatica Sinica, 2016. 42(4): 481-4914 (in Chinese)

(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).
[12] Morabito V. The Security of Blockchain Systems[M]// Business Innovation Through Blockchain. Springer International Publishing, 2017.
[13] Xu J J. Are blockchains immune to all malicious attacks?[J]. Financial Innovation, 2016, 2(1): 25.
[14] Vukolić M. The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication[M]// Open Problems in Network Security. 2016.
[15] Li xin. The distributed ledger for sharing financial development [J]. Rural financial research, 2016, (12): 7-11. (in Chinese)
(李鑫．以分布式账本助推共享金融发展[J]．农村金融研究, 2016, (12): 7-11).
[16] Zhang Y, Wen J. The IoT electric business model: Using blockchain technology for the internet of things[J]. Peer-to-Peer Networking and Applications, 2016: 1-12.
[17] Lee B, Lee J H. Blockchain-based secure firmware update for embedded devices in an Internet of Things environment[J]. Journal of Supercomputing, 2016:1-16.
[18] Park K C, Shin D H. Security assessment framework for IoT service[J]. Telecommunication Systems, 2017, 64: 1-17.
[19] Yuan Bianqing, Liu jiqiang, Provable secure ownership transfer protocol for RFID tag [J]. Journal of communication, 2015, 36(8): 83-90. (in Chinese)
(原变青，刘吉强．可证明安全的 RFID 标签所有权转移协议[J]．通信学报，2015, 36(8): 83-90).
[20] Courtois N T, Grajek M, Naik R. Optimizing SHA256 in Bitcoin Mining[J]. Communications in Computer & Information Science, 2014, 448: 131-144.
[21] Chen Z G, Wang J, Song X X. Survey on fully homomorphic encryption[J]. Application Research of Computers, 2014,31(6): (in Chinese)
(陈智罡，王箭，宋新霞．全同态加密研究[J]．计算机应用研究，2014，31(6): 1624-1630).
[22] Ma C, Li J, Du G. A Flexible Fully Homomorphic Encryption[J]. Wireless Personal Communications, 2016: 1-12.
[23] Chaudhry S A, Farash M S, Naqvi H, et al. A secure and efficient authenticated encryption for electronic payment systems using elliptic curve cryptography[J]. Electronic Commerce Research, 2016, 16(1): 113-139.
[24] Binu V P, Sreekumar A. Secure and Efficient Secret Sharing Scheme with General Access Structures Based on Elliptic Curve and Pairing[J]. Wireless Personal Communications, 2017, 92(4): 1531-1543.
[25] Mao J, Zhang Y, Li P, et al. A position-aware Merkle tree for dynamic cloud data integrity verification[J]. Soft Computing, 2015, 11: 1-14.
[26] Sun J, Yan J, Zhang K Z K. Blockchain-based sharing services: What blockchain technology can contribute to smart cities[J]. Financial Innovation, 2016, 2(1): 26.
[27] Brühl V. Bitcoins, Blockchain, and Distributed Ledgers[J]. Wirtschaftsdienst, 2017, 97(2): 135-142.
[28] Magner A, Szpankowski W. Profiles of PATRICIA Tries[J]. Algorithmica, 2016: 1-67.

项目预期成果（发表本项目有关的学术论文）及考核指标（技术、经济指标和社会效益要具有明确的可考核性，1000 字以内）：

1、对收集的区块链及物联网相关的资料进行详细研读，收悉掌握区块链及物联网的概念、掌握其相关密码技术，了解目前区块链及物联网传输层安全的发展历程及研究现状。根据目前物联网传输层安全存在的不足提出自己的解决方案；

2、根据基于区块链技术的物联网传输层的安全需求构建适宜的实验平台，在本项目的中我们利用以太坊平台来进行研究实验。以太坊是一套完整的去中心化应用平台，其提供了去中心化应用开发、部署和使用的完整工具链，使得基于区块链的应用开发变得极其便利。同时我们采用 MATLAB 软件来进行代码编写；

3、仔细研究前人关于物联网传输层安全协议的研究成果，对目前应用于物联网传输层安全的几种典型的协议进行分析研究，提出基于区块链技术的物联网传输层安全协议，保证物联网中智能设备之间可以进行安全的信息交互。对本项目提出的协议进行安全性及可行性分析；

4、针对本项目的进展情况定期向有关部门汇报，将每个阶段取得的研究成果形成文档提交给有关部门，让相关部门掌握项目研究的及时动态；

5、以本项目提出的基于区块链技术的物联网传输层安全协议为导向进行论文的撰写，发表 2-3 篇论文，其中核心刊物论文或国际会议论文共计 2 篇，且至少 1 篇被 SCI、EI、ISTP 三大检索；

6、采用区块链技术、同态加密及椭圆数字签名等安全信息技术设计物联网传输层安全智能交互协议，提交详细的协议步骤以及实现代码；

7、在江西理工大学信息工程学院向张小红教授、方旺盛教授等进行一到三场学术报告；

8、本项目使得物联网生态体系挣脱传统基于中间人的网络工作模式，即使得设备不再依赖于通过中央服务器来进行设备的信息交互，更加具有经济性。同时本项目还可以应用到给数以亿计的物联网传感器和硬件设备升级等领域。

项目时间进度安排和阶段目标

	考核时间节点（年/月）	阶段目标（阶段考核指标）
1	2017/6 - 2017/12	收集相关资料、了解目前的研究现状
2	2017/12 - 2018/6	对于目前研究现状的不足提出自己的项目方案
3	2018/6 - 2018/12	根据自己的创新点完善项目方案
4	2018/12 - 2019/3	进行协议分析、安全性测试以及论文撰写

预期主要成果形式	√1、论文论著　√2、研究报告　3、新产品（或农业新品种） 4、新装置　5、新材料　6、新技术（新方法、新工艺） 7、计算机软件　8、其他

三、项目人员情况

项目负责人主要科研成果：

项目负责人：范末婵

目前主要从事区块链技术、信息安全等方面的研究。

我在本科学习期间，能熟练使用 Auto CAD, MATLAB, Microsoft Visual C++等软件进行仿真实验，分析数据等技能，对智能设备交互认证及物联网技术很感兴趣。大学期间做过**基于 EPON 组网**的课程设计，我的大学毕业设计论文是**基于 GSM 的无线网络环境监测设计与实现**。

个人获奖情况：

1、专科阶段：

(1) 2011 年 12 月，被评为 2011 年度优秀团员；

(2) 2012 年 6 月，获得校三好学生荣誉称号；

(3) 2012 年 12 月，在校通信百科知识竞赛中荣获一等奖；

(4) 2013 年 5 月，在校脑力风暴竞赛中荣获二等奖。

2、本科阶段：

(1) 2014 年 9 月，被评为校学生工作积极分子；

(2) 2015 年 4 月，被评为校勤学钻研榜样。

3、研究生阶段：

(1) 2016 年 10 月，在校不忘初心，艰苦奋斗主题演讲比赛中荣获三等奖；

(2) 2016 年 11 月，在校第四十九届运动会矿石接力获三等奖；

(3) 2017 年 3 月，在校争做德才兼备，全面发展人才主题演讲，获得三等奖；

(4) 2017 年 4 月，在校女子排球比赛获得一等奖。

项目采取何种方式组织和管理以确保项目完成（200 字以内）：

本项目采用整体与局部统筹协调的方式进行组织和管理，详细安排如下：

(1) 项目成员在项目负责人的组织下，对项目进行积极研究分析，规划项目框架及整体结构，分配各阶段任务；

(2) 本项目以项目负责人为主导同时兼顾各组员进行合理分工，定期开展交流会，各成员积极交流想法，针对不同阶段的项目需求进行积极分析以及实现项目需求；

(3) 项目负责人随时掌控项目的进展动态，协同个项目成员积极研讨项目所遇到的问题，遇到难解的问题向专家老师们请教。对于项目的走向积极参考老师的意见使项目更加完善。

指导教师情况（研究方向、学术地位、代表性成果）（200 字以内）：

杨义先，男，1961 年出生，北京邮电大学教授，博士生导师，兼职江西理工大学硕士研究生导师。在网络信息安全、现代密码学和纠错编码等方面获得了众多在国内外很有影响的成果。担任北京邮电大学学位评定委员会主席，《通信学报》主编等。

代表性成果：获得了众多国家级和省部级科技奖励。包括：一项国家发明三等奖、三项省部级科技进步一等奖、五项省部级科技进步二等奖和其它国家级和省部级重要科技奖励。已经在 IEEE Trans. On AES、 IEEE Trans.On Comm.、IEEE Trans. On EMC 和 Discrete Applied Mathematics 等国际最权威的学术刊物和国内核心刊物上发表了高水平的论文 300 余篇，其中有些成果已经达到国际先进水平，数十次地被国际重要索引刊物 SCI、EI、ISTP 引用收录。已经完成出版了学术专著二十余部，其中包括中国在密码学方面的第一部专著。承担了包括国家杰出青年基金、教育部跨世纪优秀人才专项基金、国家“973”、国家“863”、国家自然科学基金重点项目、国家自然科学基金项目等在内的国家级和省部级重点科研项目四十余项。

张小红，全国优秀教师，江西省新世纪百千万人才工程第一、二层次人选，江西省高等学校学科带头人，江西省教学名师，江西省模范教师，江西省优秀研究生导师，江西省三八红旗手。江西省十二五“计算机科学与技术”重点学科带头人。

近年来主持和完成了国家自然科学基金、中国博士后科学基金等 16 项国家和省部级项目，主持和参与国家重点企业科研项目 9 项。在国际国内学术期刊上发表学术论文 70 余篇，其中 SCI 和 EI 收录 21 篇。以第一发明人身份申请国家发明专利 13 项，授权 6 项。获得江西省高校科技成果奖一等奖、二等奖(排名均第 1)各 1 项，江西省自然科学二等奖(排名第 3)1 项。

主要研究方向：忆阻神经网络、非线性动力学理论、无线射频识别、保密通信。

项目主要人员情况				
	姓名	院　系	专　业	在项目中具体分工
负责人	范末婵	信息工程学院	电子与通信工程	传输协议设计及其可行性分析与论文撰写
项目组成员	孙岚岚	信息工程学院	电子与通信工程	前期调查研究以及协议的安全性测试
	龙克柳	信息工程学院	通信与信息系统	实验平台的搭建
	陈皓琦	信息工程学院	电子与通信工程	相关资料的收集

四、项目经费情况

支出科目	金额（元）	计划根据及理由
调研	1000	项目的前期调查研究
文献资料	1000	项目相关资料的搜集与查阅
实验设备	1000	用于项目中算法的实验和验证平台
论文	2000	论文发表版面、国际会议论文注册等
合计	5000	

五、审查意见	
指导教师意见	指导教师签名：　　年　月　日
培养单位意见	负责人签章：　　年　月　日
专家组评审意见	专家组长签名：　　年　月　日
省级主管部门审核意见	签章：　　年　月　日
备注	