赠书 |区块链和物联网也能擦出火花？

转载

区块链大本营 于 2020-07-17 19:15:11 发布 991 收藏
文章标签： 网络 分布式 编程语言 区块链 java

点击上方蓝字关注“区块链大本营”

来源 | 《深度区块链：用技术重构世界》

作者 | 庞宇雄

责编 | Carol

封图 | CSDN 付费下载自视觉中国

* 文末有赠书福利

物联网作为一项飞速发展的技术，在**智能电网、智能供水网络、智能家居、智能交通**等各项领域已有广泛的应用。不久的将来，物联网应用将深入生活的方方面面，在未来科技生活中担当不可或缺的角色。随着越来越多的智能设备接入网络，物联网应用受到安全威胁的概率大幅增加。根据美国ABI 调查公司的数据，2018 年，大约有**100 亿**台可使用无线网络接入互联网的设备，到2020 年年底，这一数字将超过**300 亿**。

可以预见的是未来将会有更多拥有廉价传感器的物联网设备进入人们生活，分享消费者的敏感信息。物联网设备的安全管理问题将成为物联网产业可持续发展的核心问题之一，人们必须对此高度重视。**区块链去中心化、去信任和高安全隐私性的特点，为物联网应用提供了点对点直接进行数据传输的解决方案。**

01

区块链物联网初级实验案例

要实现基于区块链系统的物联网平台应用，应该主要关注能够使区块链保持数据一致性的方法，这种方法一般被称为**共识算法**，它起源于分布式一致性算法。其核心思想是引导系统上的所有不可靠的节点达成如何产生下一个区块的一致性算法，但是这种分布式一致性算法在实现技术细节上有很大的区别。从人们开始使用比特币并进行技术上的积极探索，区块链技术得到了蓬勃发展，并衍生出各种新技术和产品，成功地证明了其在不同领域的**高安全性、灵活性、隐私性和容错性**，人们开始将分布式共识基于不同的目的，进行更加准确和专业的使用。

共识算法是分布式应用软件中特有的算法机制，而如果没有一个好的算法理论作为支撑，将根本无法实现一个好的分布式应用。这是因为在中心化的软件设计中，复杂问题设计的解决方案可以通过不使用复杂的算法逻辑实现，但是在分布式软件开发中，节点间的互操作和节点行为的统一管理都会因为分布式而变得十分的复杂多样，无法通过普通的方式去预先设定运行产生的结果，所以需要使用共识算法来完成应用并维持分布式一致性。

常用的区块链下的共识机制主要有PoW、POS、DPOS、Paxos、PBFT 等，基于区块链技术所需要应用到的不同场景和各种共识算法自身的特性，人们一般通过以下 4 个标准来评价各种共识算法的适用性。

合规监管：可否支持设定某些权限节点对全网节点、数据进行监管。

性能效率：在交易达成共识后被确认的效率。

资源消耗：在一次共识过程中，耗费的计算能力、存储和网络带宽等计算机资源。

容错性：是否具有防攻击、防欺诈的能力。

一般来说，**区块链的类型可分为两种，一种是公众所熟知的公有区块链**，其代表者是比特币系统，在该系统中，所有节点享有同等的权利和义务，每一个节点根据自己的能力参与并作为区块链共识的一部分。在目前的公有区块链中，所采用的共识算法通常是由内在的经济激励制度通过引导所有区块达成共识获取相关奖励的工作量来证明PoW 共识算法。

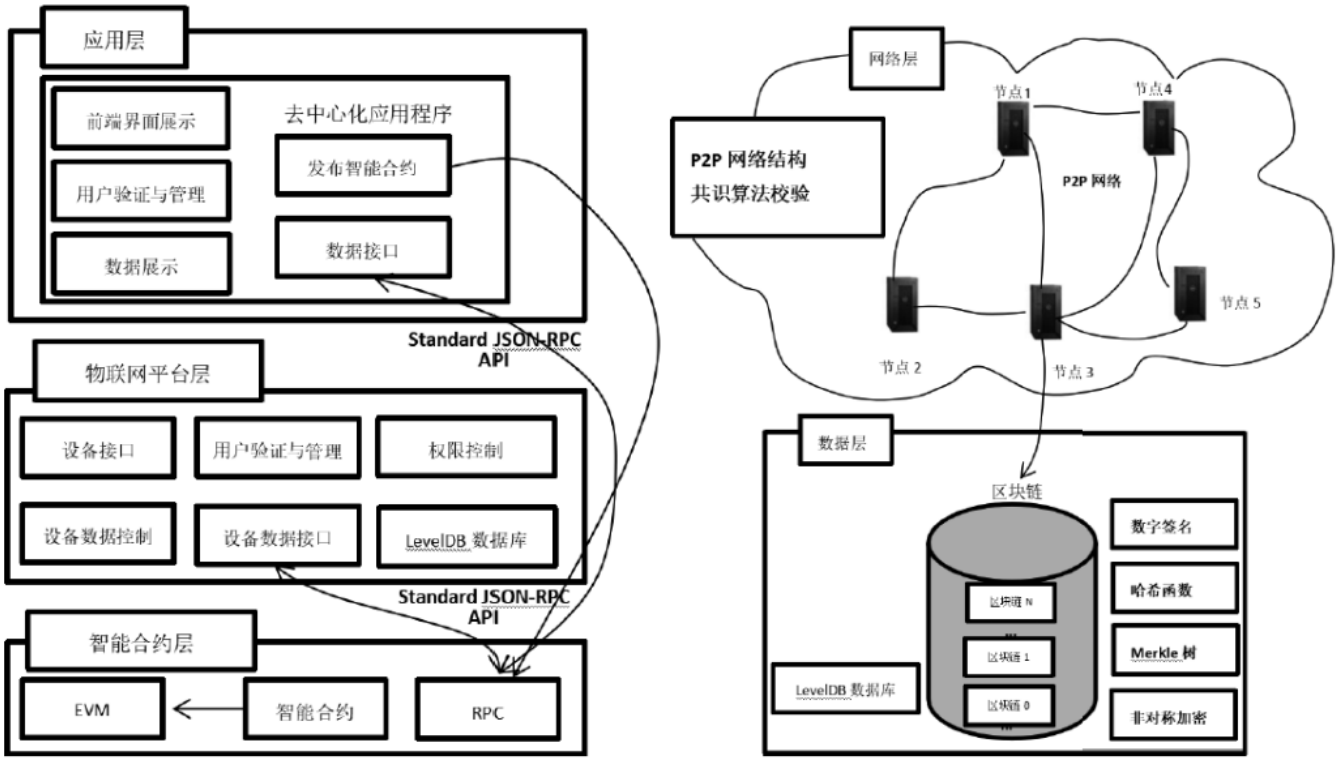
另一种是私有区块链，可用于运行环境完全只对内部开放的私有链，或系统跨越几个网络彼此连接，并能够互相通信和操作的部分私有链系统，为作进一步区分，人们通常把这种区块链系统称为联盟区块链。在物联网系统中，私有链场景是最为适合物联网使用的场景，其安全许可的严格限制和设置特权节点的灵活性可用于更明确地设定设备、用户的管理权限和优先级别，解决当前系统无法完全满足的需求。

在初步测试实验中，**人们利用以太坊区块链作为底层的技术支持，基于已有的物联网平台，建立了一个能够在用户与其他用户设备之间或用户与物联网平台之间获得数据、达成购买数据和设备服务的不可篡改的契约交易关系的区块链应用平台。**

整个区块链系统由多个客户端节点组成，各节点都是完整的数据节点，每个节点内都有整个区块链数据地址的完整备份。这些节点可以分别由不同的机构或一个机构内部的多个数据中心来分别维护。实验中的区块链系统不需要相互竞争去产生新的区块，在获得竞争权后对这段时间的区块进行打包，然后分发给其他节点。所有节点达成一致后各自对区块进行存储。区块链的区块之间通过哈希值连接在一起，此哈希值由区块头部字段组合计算而成。

区块中的交易通过Merkle 树的数据结构组织在一起，其中Merkle 树的根节点存放在区块的头部中。用户或平台制定自己能够提供数据或服务的条件，应用将条件编译为智能合约脚本再发布到系统，然后系统通过审核和编译，形成去中心化的应用提供给其他用户，其他用户如果有需求并且能够满足条件响应，智能合约通过在区块链上的执行来完成合约内容，通过所有其他全节点的验证达成合约。**系统上的去中心化应用是通过与物联网平台约定好的JSON-RPC API 进行调用和验证，获取远端物联网平台的数据和服务，提供给区块链去中心化应用的用户。**

整个系统从架构设计上来说，可以分为**数据层、网络层、智能合约层、物联网平台层和应用层** 5 个层次，如下图所示。下面根据系统总体的架构图来分别描述各层的设计。



物联网区块链架构图

（1）**最底层的是数据层**，主要负责存储区块链数据，包含区块数据和事务交易数据HASH 地址的存储。一些通用的基础模块，如网络通信库、流处理、线程封装、消息封装与解码、系统时间、基础加密算法和数据存储技术等，采用改进的以太坊区块链系统对区块数据的存储进行了优化设计。

（2）**第二层是系统的网络层**，主要包括共识算法、P2P 网络及验证机制。这层一般包含了区块链的主要逻辑，如共识模块、交易处理模块、嵌入式数据库处理模块等，难点在于点对点网络的实现和并发处理。在本系统中，针对物联网平台下的节点承载能力与应用需求，用基于Tendermint 共识机制的Ethermint 替换了传统以太坊上的工作量证明共识机制。

（3）**第三层是智能合约层**。系统基于Json Standard RPC 的交互RPC 模块与EVM（以太坊虚拟机）模块，基于EVM 模块运行智能合约交互处理区块链与共识的相关事务，基于JSON－RPC 通过网络从远程计算机程序上请求服务，进行区块节点的一致性处理和网络层事务的交互，从而实现各种交易转账等具体商业活动的完整过程。人们可以通过类似JavaScript 编程语言的Solidity语言，灵活编写，在区块链中严格执行适用于各种应用的智能合约脚本。

（4）**第四层是物联网平台层**。系统通过基于Json Standard RPC 的交互RPC 模块，通过物联网平台已有的接口，调用物联网数据信息、操控指令和发布智能合约到智能合约层与区块链节点进行交互处理相关的事务，应用层去中心化应用用户通过底层区块链平台能够间接获取交易物联网平台设备的数据和控制权。

（5）**最上层的是去中心化应用层**。它通过封装以太坊Json RPC API 的Web3.js 接口库与智能合约层、物联网平台层进行数据信息交换。在去中心化应用中，所有的智能合约在经过编译后都以二进制代码的形式运行在区块链系统的EVM 上，并用到了RPC API 的调用。区块链上的智能合约可提供自治的服务，通过在平台中去中心化的应用程序提供物联网设备信息或操作为用户服务。

基于安全的区块链物联网试验案例

现在的物联网管理平台基本有集中式管理和分布式管理两种管理方案。其中集中式系统对物联网物体进行集中化管理，进行统一的分配调度和权限管理。然而随着物联网的迅速发展，接入网络的物体迅速增加，网络结构也变得越来越复杂多样，导致集中式系统的管理和维护压力巨大。更为重要的是集中式系统中存在的单点信任问题，由于集中式系统的统一控制和中央裁决，当主机出现故障或被攻击时，可能会导致整个系统停止工作，甚至出现整个系统的信息泄露，这对于系统安全是一个致命的影响。

研究人员在试验中拟通过两个方面的研究实现分布式平台的搭建。

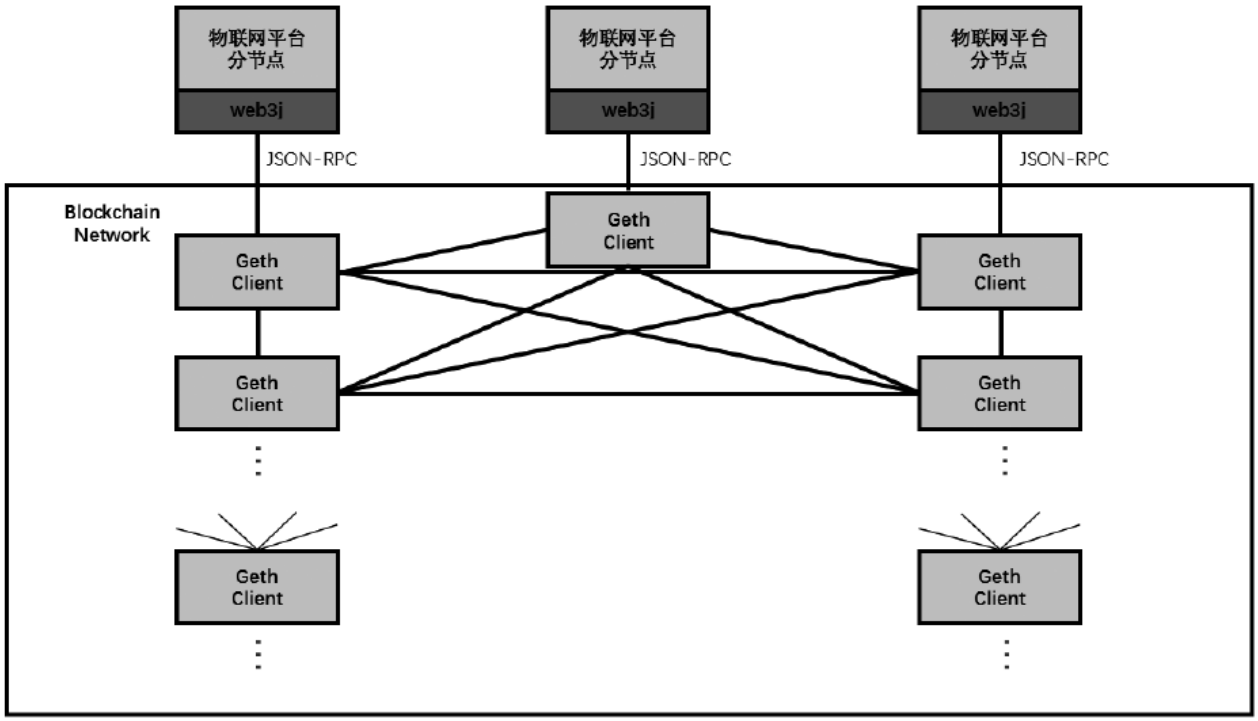
> **通过Geth 客户端搭建出私有的区块链网络，**该区块链网络负责平台节点的信息通信、对裁决方案进行表决、对平台信息进行账本存储，私有网络上的节点需要提供API 供平台节点进行信息访问和结果反馈。
>
> **设计分布式平台的架构，**设计平台与私有区块链网络的信息交流方式、为设备提供的功能及在Web 端的展现形式。

为了实现分布式平台对物联网设备的管理能力，人们在使用平台设备之前需要在平台进行设备注册，只有**注册后的设备才能被用于在平台上进行信息交互**。为了保证物联网设备之间信息交互的安全可靠，平台设备的合法性必须得到保障。接入认证功能能够在设备注册时对设备进行合法身份的鉴定，认证过程需要通过区块链的智能合约去完成，以保证每个平台分节点都参与到认证之中，以此来解决单点故障问题，保证认证的可信度。认证成功后的设备认证信息也需要存储在平台进行备案，认证信息会被存储到区块链账本中，以保证认证信息不被轻易篡改。

物联网设备需要频繁地对自身的运行信息进行记录，接入平台的设备可以将自己的运行信息上传到平台上。在上传信息之前，平台端会对设备的权限进行验证，判断其是否具有上传信息的权限，权限验证过程也需要通过区块链的智能合约去完成，从而使每个平台分节点都参与到权限验证的过程中，以保证验证的可信度。平台在对设备进行权限验证后，验证通过的设备便可以将运行信息存储到平台上，由其再存储到区块链账本中，以备将来进行信息的统计和历史追溯。设备的上传请求需要受到容忍入侵机制的监督，以防止某些恶意设备进行频繁的错误请求以损耗系统的性能。和前面使用智能合约的原理一样，对容忍入侵模型中的恶性事件的判定也要通过区块链的智能合约去完成，以保证判定的可信度。

设备在接入平台之前，需要进行设备注册的操作，设备注册信息被上报到平台，注册信息包括**生产厂商、设备型号等设备详细信息，以及设备安全凭证信息**。平台对设备上报的注册信息进行接入认证，接入认证过程会触发智能合约，该项工作由所有平台分节点共同完成。对于认证通过的设备，平台会将信息存储在区块链账本中，进行永久备份。设备认证通过后即可接入平台，进行设备登录操作，平台读取区块链账本中的注册设备表，与登录设备信息进行比对，对已经注册的设备进行上线处理。在平台中运行的设备可以进行信息交互，包括设备信息上传和数据信息获取。设备定期上传自己的运行信息到平台，平台会在权限验证通过后将上传信息存储到区块链账本中永久存储。另外，设备也可以根据所拥有的权限获取平台上其他设备的信息，或者进行**信息追溯和信息统计**，在此过程中平台会读取区块链账本中的相应信息，进行分析并返回结果。平台也会对设备信息交互过程进行容忍入侵检测，警告和排除出现故障的设备或恶意设备。

平台的节点需要处理平台与物联网设备的信息交互、设备信息统计分析、设备信息的数据可视化及平台对外的服务封装，还需要接入认证机制、权限管理机制和入侵检测机制的逻辑管理功能。而区块链网络完成的功能比较纯粹，只需要关注对于决策的多数表决和对于信息的永久存储。所以，在平台的总体设计中，需要将平台节点和区块链网络节点在结构上分离开来，让**平台节点专注于数据处理、服务封装和管理逻辑，区块链网络节点专注于决策表决和信息存储**，具体平台架构设计如下图所示。



物联网络结构图

平台的下层是由Geth 客户端节点相互连接构建的区块链网络，它们负责**交易的验证、信息存储备案及执行智能合约并返回执行结果**。下层的Geth 客户端节点之间相互连接，能保证上层平台节点的信息传递，下层网络的所有节点会对上层的裁决请求进行多数表决，给出上层裁决结果，其区块链账本会对信息进行永久存储，并对上层节点数据进行备份。

平台的上层是分布式物联网平台的分节点，每一个分节点对应着一个底层的Geth 客户端节点。上层平台节点负责与物联网设备的信息交互，对物联网设备信息进行统计分析，将物联网设备信息数据进行可视化展示，将平台服务对外封装，提供服务接口，并完成设备接入认证、设备权限管理和平台入侵检测的逻辑功能。

平台分节点与Geth 客户端节点之间通过JSON-RPC 进行信息通信，平台分节点通过Web3.js 进行接口调用，将信息传递给Geth 客户端节点，也可以请求Geth 客户端节点返回区块信息。分节点安全机制中的仲裁判定都是与区块链网络合作完成的，包括设备接入时进行的身份认证，设备权限控制中进行的权限判定，以及负责入侵检测的事件分析器对事件的分析判定。当分节点需要进行仲裁判定时，分节点将仲裁请求及仲裁信息通过JSON-RPC 传送给Geth客户端，触发区块链网络中的智能合约，启动对信息的仲裁判定，区块链节点执行智能合约并返回合约运行结果，在区块链网络形成仲裁结果后，Geth 客户端再将仲裁结果通过JSON-RPC 返回给平台分节点，从而完成仲裁判定。

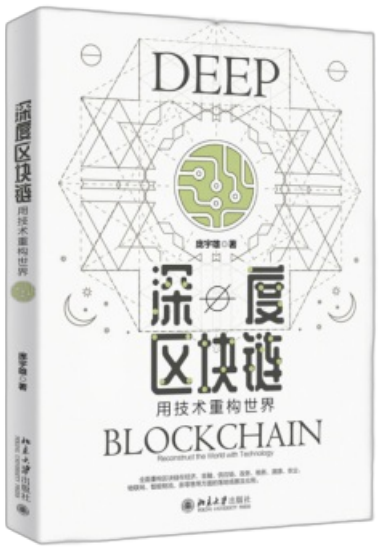
#欢迎留言在评论区和我们讨论#

区块链和物联网结合的应用

对此，你怎么看？

我们将在 **7 月 22** 日精选出 3 条优质留言

赠送《深度区块链》纸质书籍一本哦！



THE END

推荐阅读

黑客悬赏活动第二期 | 10万美金悬赏全球黑客，aelf 跨链转账标准协议CCTP等你挑战！

以太坊2.0究竟何时落地？V神这样说……

解读领跑全国的区块链发展“北京方案”：设专项基金，构建开源生态

“自由主义教皇”、Linux 之父的封神之路

5G：新基建的压舱石，如何为新基建按下“加速键”？