**·栏目· 文章编号：1000-3428(20xx)0x-00xx-xx 文献标志码：A 中图分类号：**

基于区块链的物联网云服务质量可信认证模型

谈玉胜1，柳毅2

(1.广东工业大学，计算机学院，广州 510006；2. 广东省大数据安全与服务工程技术研究中心，广州 510000)

**摘 要：**在物联网云服务质量评价体系中，现行的物联网云服务模型缺少完善自动执行的机制来维护客户的权益，现利用区块链技术不可篡改的技术特性，用户难以找到物联网供应商在服务期间存在缺陷的证据。因此，将服务质量缺陷的事件记录到区块链中。扩展现有的物联网服务评价模型，利用无偏向随机选择方法引入证人模型，用于检测和报告服务质量是否达到标准。引入了证人池机制，提出了一种无偏向排序算法保证了证人池中选择证人的随机性。同时，引入证人审计机制检测潜在的恶意证人。最后，利用以太坊智能合约创建系统原型，最终实验结果表明该模型可行，性能符合设计要求。

**关键词：**区块链；物联网；服务质量；以太坊；智能合约

Internet of Things Cloud Service Quality Authentication Model based on block chain

TAN Yusheng1, LIU Yi2

(1.Guangdong University of Technology, Guangzhou 510006, China；2. Guangdong Big Data Security and Service Engineering Technology Research Center,Guangzhou 510000,China)

**【Abstract】**In the Internet of Things cloud service quality evaluation system, the current Internet of Things cloud service model lacks a perfect automatic execution mechanism to safeguard the rights and interests of customers. With the immutable technical characteristics of blockchain technology, it is difficult for users to find evidence of defects of Internet of Things suppliers during service.Therefore, quality-of-service defect events are logged to the blockchain.The existing iot service evaluation model is extended, and the unbiased random selection method is used to introduce witness model, which is used to detect and report whether the service quality meets the standard.The mechanism of witness pool is introduced and an unbiased sorting algorithm is proposed to ensure random selection of witnesses in witness pool.At the same time, witness audit mechanism is introduced to detect potential malicious witnesses.Finally, ethereum smart contract is used to create a prototype of the system, and the final experimental results show that the model is feasible and the performance meets the design requirements.

**【Key words】**Block chain; The Internet of things; Service quality; Ethereum; Intelligent contract

# 概述

当前大多数的物联网云服务业务模型是：普通用户通过使用物联网服务商提供的计算、存储和api服务，共享服务器资源。这种共享模式给用户带来极大的便利，使得小规模或初级用户也能以较低的价格获取便捷完善的物联网服务体验；同时也带来了一些挑战，如物联网服务供应商在服务期间出现宕机，用户从供应商获取相应的赔偿，存在一定的困难。业内普遍的处理方案是共同执行服务水平协议（SLA，Service Level Agreement）,这是一个商业概念，定义了客户与供应商之间的合同和财务协议。如果在服务期间内服务方出现了故障，客户可以向服务方索取赔偿或抵消部分费用；如果在服务期间内，服务方没有出现故障，则客户正常支付全部费用。以此保障双方的合法权益。

现阶段,区块链技术与物联网技术进行结合，是一种发展趋势[1]。区块链技术的不可篡改特性，为物联网设备接入后的数据共享和协同工作提供了良好的保障。以太坊[2]中的智能合约提供了一种可行的方式来自动化执行服务水平协议。使用预言机[3]（Oracle）作为可信第三方，为智能合约提供可信的链外信息和数据，以验证触发智能合约的条件。

物联网服务水平协议出现的问题主要有以下三种：

1. 对于用户的补偿方面，缺少一种自动的机制来执行物联网服务水平协议。
2. 在当前的模型中，服务提供者拥有更多权利，特别是在验证物联网服务质量缺陷和决定是否对用户进行赔偿方面。
3. 用户难以提供证据证明物联网服务商确实存在质量问题。

物联网服务质量可信认证模型需要解决的问题:如何保证物联网服务水平协议服务商与用户的权益；由哪一方检测和证明违反了服务水平协议；如何实现支付流程的自动化执行，包括补偿流程的自动化。

本文在已有云服务水平协议的基础上，针对物联网云服务场景下用户权益的缺陷问题展开研究。主要贡献包括以下两个方面。

1. 引入了证人审计机制（WAM，Witness Audit Mechanism）
2. 结合区块链技术，制定了证人管理方案和无偏向随机选择方法（WMURS，Witness Management and Unbiased Random Selection）

# 1 相关理论与研究

## 1.1 SLA协议

SLA是云服务服务提供者与用户之间的服务质量协议[4]，可以适用于物联网云服务背景下，在协议被违反时保护用户的合法权益。SLA是连接用户与物联网服务提供者的桥梁，包含参数表示、参数映射、 违约惩罚三个方面。

SLA模型功能框架如图1所示。



图 1 SLA功能框架

一个典型的SLA生命周期由多个实施阶段组成，包含协商、建立、监控、违规报告和终止。研究工作主要集中在SLA参数的语法定义，便于系统的在线处理；优化资源分配算法，减少SLA冲突；根据云服务SLA的系统调查报告[5]，表明大部分的工作集中在监控和部署阶段，小部分工作集中在协商和建立阶段。目标是是的供应商和用户的利益最大化。在业界，Amazon推出了CloudWatch服务用于自动监控和通知SLA服务。但是，作为受信任的第三方执行监控和违规报告，用户没有别的选择，只能假定该服务是可信的。为了解决可信问题，还需要引入其它技术方案。

## 1.2 以太坊与智能合约

以太坊（Ethereum）是由比特币开发商Vitalik Buterin在2013年设计的[6]，用于促进区块链上分布式应用程序的开发。以太坊是一个开放的区块链平台可以建立和使用去中心化应用。以太坊是从2015年开始的第二代区块链，提出了以太坊虚拟机（Ethereum Virtual Machine）,这是一组表示虚拟机状态的字节值。在以太坊上运行的程序被称为智能合约（Smart Contract）。智能合约的工作流程如图2所示。



图 2 智能合约工作流程

智能合约是区块链上以计算机程序的方式定义的和自动执行的各种合约，用于开发分布式应用。 通过计算机协议促进、验证和执行合约。将智能合约与服务质量协议结合起来，重点注重语义的表达，实现协商阶段的不可篡改与自动化执行，具有一定的实用价值。区块链作为执行平台，链上的交互是不可变的，因此可以保证只能合约的可信度。

## 1.3 相关研究

国内外学者对物联网服务质量协议已有较多研究成果。这些方案都有其优势与不足。适用于不同的应用环境与网络模型。目前，物联网服务质量协议的可信模型还没有得到完全解决，还需要做进一步的深入研究。

文献[7]分别从硬件和传输协议角度保证了可信赖的执行环境。提出了一个认证的数据反馈系统：Town Crier，使用可信硬件后端，依靠智能合约提供源认证数据。该方案存在的问题是需要特殊的基础设施支持，实际应用环境中需要的是通用性与普适性的解决方案。文献[8]引入了一个服务器性能监视器的角色来检测违规并通知用户。提出了基于构建在区块链上的公共SLA契约方法，实现了SLA合同平台原型，并将其应用到实例中。然而提议的解决方案缺乏对已识别违规行为的可信性分析，并且仍然面临在区块链之外发生事件的共识挑战。

对于基于区块链的系统当事件发生在区块链之外时，如何可信地将随机事件上链。文献[3]的解决方案是使用预言机充当区块链的数据载体代理。Oraclize作为可信赖的第三方机构提供预言机服务。但是它可能会存在单点故障，这就偏离了区块链的去中心化思想。为了解决这个问题，文献[9]提出了在分布式预言机上工作，其工作方式是：只有在预言机之间达成协议时，事件的结果数据才会上链并触发事务。但是这个理念也存在一定的不足，对于预言机而言，如果没有足够的激励机制，预言机自身的可信问题并不能得到解决。

# 2 基于智能合约的证人模型

本节将介绍基于区块链的认证模型，具体介绍证人的角色和功能，如何检测和报告违规行为，以及在区块链上如何使用智能合约实施服务质量协议的系统架构。

## 2.1 引入证人池机制的SLA协议

证人是区块链的正常参与者，它们是自愿参与到系统中并且通过监控服务获取自身收入。证人角色默认是自私的，以获得自身收益最大化为目标。

对于传统的物联网服务质量协议，主要参与的两个角色是物联网云服务提供商Provider和物联网客户Customer。使用一个基础示例来演示SLA协议的工作流程。假设一个物联网云服务提供商根据客户的请求，提供一个具备公网IP地址并定义了数据节点类型的服务器Virtual Machine。在有效服务时间Tservice内，客户Customer可以通过透传连接到服务器。服务质量协议SLA可以做出承诺：在有效服务时间Tservice内，Provider提供的服务器始终是可访问的，如果满足条件，在服务结束后Customer必须支付费用Fservice，否则在违反SLA的情况下，Customer必须获得一笔补偿费用Fcompensation。这里我们假设Fservice＞Fcompensation，也就是说Customer需要给Provider支付的费用为Fservice - Fcompensation。此外，对于Customer自身的网络问题引起的无法访问服务器不属于违反SLA协议。

为了确认是否真的违反了SLA协议，需要在传统SLA协议角色的基础上，再引入一个新的证人角色Witness，利用以太坊交易平台创建一个可信的交易环境。这些Witness也是区块链的一般参与者，自愿参数SLA协议，通过提供监控服务获得收入。为了解决SLA协议中的信任问题，创建一个由n个Witness组建的证人委员会{w1,w2,w3,…,wn}来参与SLA协议，它们一起监控SLA协议中的违规事件。并从Provider和Customer双方获得证人费作为回报。这里对证人角色做一个假设，证人都是自私的，都以自身收益最大化为目标。对于不符合假设的证人则视为懒惰证人，会通过下文算法将其排除在证人委员会之外。

## 2.2 系统架构

系统由两类智能合约构成，第一类是证人池智能合约，是系统的基本智能合约；第二类是特定的物联网服务质量协议智能合约，用于SLA的自动执行。证人池智能合约主要有三个功能，分别是证人管理、具体SLA的生成和证人委员会的选举。区块链的任何用户都可以通过钱包地址在证人池中注册，成为证人。用户可以保持在线状态，等待被选中执行SLA协议。所有的证人参与这个系统的动机都是获得收益，系统中的证人越多，系统越可信。系统整个架构如图3所示。



图 3 系统架构图

物联网服务供应商Provider利用证人池智能合约为自己生成SLA智能合约，Provider与Customer协商详细的SLA条款，服务时间Tservice、服务费用Fservice、补偿费用Fcompensation以及确定执行本SLA协议的证人Witness的数量。证人越多违规检测的结果越可信，同时Provider与Customer也要共同额外支出更多的费用。系统可以根据Customer表单提交的结果，Provider传入这些参数在证人池智能合约中生成新的SLA智能合约。同时利用公正和随机的无偏向排序算法，从证人池中选举证人委员会。证人委员会中的成员是独立公正的无偏袒的，监控SLA协议的执行，于此同时，Provider提供物联网服务器给Customer使用，并且在SLA中发布服务细节。接着，证人委员会开始监测服务，并将服务器公网IP通知给证人委员会成员。服务期间Customer可以正常使用服务器，证人委员会中的证人也可以不断ping服务器的ip地址，如果在Tservice内服务器出现故障，证人立即向智能合约报告违规事件。

具体的SLA工作机制为：当系统收到证人委员会中的第一个举报时，开始计时，此后，SLA智能合约接收来自委员会中其它证人的举报。直到没有其它证人举报了为止。如果SLA收到证人委员会中举报的人数X，证人委员会的人数为Y，当前仅当X/Y > 1/2时，Tservice期间内的违规行为将会被自动确认。例如，证人委员会中有三个成员参与监控SLA协议，只有其中至少两个证人报告该事件时，才能确认服务违规。同时，该SLA智能合约也定义了如果同一证人在Tservice时间内只有一次报告机会，预防恶意证人多次汇报扰乱机制。每一个证人都想要最大化自己的收益，他们都是诚实的参与者根据实际情况报告违规情况。最后SLA智能合约存在两种执行结果：一种是Tservice时间后，没有违反协议，Customer正常支付的费用为Fservice；另一种是Tservice时间后，报告违反了协议，Customer需要获得补偿，所需支付的费用为Fservice - Fcompensation；不论哪种情况，证人委员会都会从智能合约中获取报酬。

# 3 核心算法

物联网服务质量可信认证模型所采用的关键技术是对SLA违规行为进行自动检测，得到使Customer和Provider的都信服的检测结果。使用无偏向排序算法，确保被选入证人委员会的证人都是随机且独立的。同时也使用了证人审计算法，分析了来自恶意证人的欺诈行为，确保参与者必须诚实才能利益最大化。

## 3.1 无偏向随机选择算法

从证人池中选举证人委员会的方法使用的是无偏向随机选择算法，针对特定的SLA合同证人的选择必须是公正的，引入以太坊作为模型的可信方，在证人池智能合约中实现该算法，对于Customer或者Provider都不能有偏向。算法伪代码如算法1所示。

**算法1** 无偏向随机选择算法

**输入**：

已注册的证人集合set\_registered；

在线证人数量online\_witness;

证人委员会中需要的人数N；

第b个区块链的哈希值

生成的新区块链长度

证人的在线状态state

证人的信誉度：reputation

证人的地址witness\_address;

**输出**：

1.seed = 0; // 初始化随机数种子

2.for():

3. seed += ; // 将个区块哈希值累加

4.end for // 结束循环获取随机种子

5. for(int j = 0; j < N; j++):// 选择证人

6. index = seed % len(set\_registered)+1;

7. check(set\_registered[index].state)

&& check(set\_registered[index].reputation)

//判断证人在线状态与信誉度

8. set\_registered.add(witness\_address)

//将证人添加到证人委员会集合中

9.end for //证人满足数量结束循环

10. return set\_registered;//返回证人委员会集合

在证人池智能合约中，开放了提供注册接口，区块链用户都可以注册到证人池中，同时区块链用户可以将自身状态切换为“在线”或“离线”，表明当前是否愿意加入证人池选举活动。证人池中存储的是地址列表记录了区块链用户注册的顺序。 为了从证人池中选择N个证人委员会成员，证人池智能合约定义了两个接口：请求和排序。利用区块的哈希值生成随机数种子，新的种子是根据前一个种子的哈希值生成的，这个过程重复进行，直到选定出N个证人委员会成员。这样既保证了算法的输出，又保证了算法的随机性，无论是对于Customer还是Provider都不能随意操纵排序结果，从而控制证人委员会的选举结果。

## 3.2 证人审查选择算法

无偏向排序算法保证了选举的证人的公平独立，但是仍然需要一种审计机制来保证系统能够检测到恶意或者懒惰证人，并将其从证人池中开除。由于智能合约中的交易是公开并永久存储在链上的，因此可以通过目击者的行为历史来审查证人的声誉，而不是根据其它人的反馈来评估证人的信誉度[10]。

**算法2** 证人审查算法

**输入**：

恶意证人集合set\_malicious；

默认声誉值reputation;

证人委员会set\_registered；

**输出**：

1. flag = event.isValid;//获取SLA结果

//获取证人委员会中所有投赞成票的集合

1. setYes = set\_registered.getYes();

//获取证人委员会中所有投反对票的集合

1. setNo = set\_registered.getNo();

//对证人委员会的每一个地址进行遍历

1. for(String address : set\_registered):

// 如果最终结果为违规

1. if(flag==false):

// 所有赞成票的地址扣除声誉

1. for(String address:setYes):

address.reputation--;

else:

// 否则所有反对票的地址扣除声誉

1. for(String address:setNo):

address.reputation--;

// 如果证人声誉小于0

8. if(address.reputaion < 0):

// 将证人地址加入恶意地址集

set\_malicious.add(address);

一般情况下，恶意证人主要分为两类：懒惰证人和牺牲证人。懒惰证人是指不愿意举报违规行为的证人，或者举报违规行为的收益不足以激励证人工作，他们选择不真正监视的策略总是保持沉默，从不报告违规行为，使用这种策略后。即使SLA最终状态被违反，懒惰证人也不会付出代价。同时，整个系统中由于总体报告违规的的次数应小于正常的次数导致懒惰证人仍然能够通过参与多轮服务总体获得收益。牺牲证人是指总是在特定时间点报告的证人，例如证人总是在SLA启动1分钟内报告违规，虽然一开始可能由于自己的恶意行为受到惩罚，但是可以在以后的历史中向他人展示自己的行为模式，从而获得最大利益。为了审查这些恶意证人，系统需要为我设计声誉值参数，当违规行为被证实时，没有做出举报行为的证人声誉扣除1点，举报违规行为，最后系统并没有违规的证人同样扣除1点声誉值。当证人的声誉值降至为0时，证人的选举流程也被终止，提出证人池，系统恶意地址表中记录恶意证人的地址，恶意证人无法再次加入证人池。这种算法的设计能有效减少懒惰证人与牺牲证人的参与，提高了SLA系统的稳定性与安全性。

×××××××××分析结果如表1所示。

表1 各协议每轮全网发送能耗分析比较

|  |  |  |  |
| --- | --- | --- | --- |
| 协议 | 短距离 | 中长距离 | 长距离 |
| LEACH | 95 | 0 | 5 |
| PEGASIS | 99 | 0 | 1 |
| COSEN | 95 | 4 | 1 |
| 改进分层链路路由 | 99 | 0 | 1 |
| MSLR | 99 | 0 | 1 |

对于论文中表的相关内容要求如下：

1）表用阿拉伯数字依序连续编号，如表1、表2、表3等。

2）表序号和表题，置于表的上方，表格用三线表形式，必要时可加辅线。

3）文前表后，表应紧跟在正文描述后面。

4）表中文字须为中文，特定英文缩略语首次出现时需括号备注中文含义。

5）表题要与正文描述一致，正文提及表必须明确指出，如“如表1所示”、“见表2”等，不可简单写作 “见下表”等。

6）同一类数据的有效数字需保持一致。

## 3.2 二级标题

××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××

代码、伪代码不要以图和表的形式插入文中。具体示例如下：

**算法1** 伪代码的算法1名称

**输入** ……

**输出** ……

1.算法步骤1的语句//注释

2.算法步骤2的语句//注释

3.算法步骤3的语句//注释

4.算法步骤4的语句//注释

……

## 1.1.1 三级标题

××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××

## 1.1.2 三级标题

××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××××

# 4 结束语

对全文进行总结并指出下一步研究方向，勿简单重复摘要和概述。不要以1）、2)、3）形式简单罗列前文已经写出的结论。结束语中不出现图、表、公式。

参考文献

1. Ali M S, Vecchio M, Pincheira M, et al. Applications of blockchains in the Internet of Things: A comprehensive survey[J]. IEEE Communications Surveys & Tutorials, 2018, 21(2): 1676-1717.
2. Buterin V. A next-generation smart contract and decentralized application platform[J]. white paper, 2014, 3(37).
3. (2014) Ethereum and Oracles. [Online]. Available: https://blog.ethereum.org/2014/07/22/ethereum-and-oracles/
4. 周胜利,陈光宣,吴礼发. 基于隐私的云计算SLA违规检测模型[J]. 计算机科学,2016,43(12):146-151.
5. Faniyi F, Bahsoon R. A systematic review of service level management in the cloud[J]. ACM Computing Surveys (CSUR), 2015, 48(3): 1-27.
6. Wood G. Ethereum: A secure decentralised generalised transaction ledger[J]. Ethereum project yellow paper, 2014, 151(2014): 1-32.
7. Zhang, Fan, et al. "Town crier: An authenticated data feed for smart contracts." Proceedings of the 2016 aCM sIGSAC conference on computer and communications security. 2016.
8. Nakashima H, Aoyama M. An automation method of sla contract of web apis and its platform based on blockchain concept[C]//2017 IEEE International Conference on Cognitive Computing (ICCC). IEEE, 2017: 32-39.
9. Ellis S, Juels A, Nazarov S. Chainlink: A decentralized oracle network[J]. Retrieved March, 2017, 11: 2018.
10. Wang X, Su J, Hu X, et al. Trust model for cloud systems with self variance evaluation[M]//Security, Privacy and Trust in Cloud Systems. Springer, Berlin, Heidelberg, 2014: 283-309.
11. 作者. 技术报告名:编号[R]. 出版地：出版者，出版年：起止页码.
12. 作者. 技术报告名:编号[R]. 出版地：出版者，出版年：起止页码.
13. 作者. 技术报告名:编号[R]. 出版地：出版者，出版年：起止页码.
14. 作者. 技术报告名:编号[R]. 出版地：出版者，出版年：起止页码.
15. 作者. 技术报告名:编号[R]. 出版地：出版者，出版年：起止页码.
16. 作者. 技术报告名:编号[R]. 出版地：出版者，出版年：起止页码.

参考文献应按顺序在正文中逐条引用，从文献1开始，具体格式要求参考本刊官网“下载中心”的《参考文献著录规则》文档）

请在文章最后给出前3位作者的联系方式(长期有效的手机、电话及E-mail。