基于区块链的实验教学经费可信任回溯机制研究

曲广强 孙 斌
(东北电力大学教务处 吉林 132012)

摘 要 文中提出了一种基于区块链技术的实验教学经费系统的解决方案,其主要分为两部分:核心数据网络和信息公开网络。核心数据网络是由一系列具有平等核心的权力节点组成的分布数据库,主要负责数据的存储与录入;信息公开网络是一个对外开放的网络,任何人都可以读取核心数据网络中的完整数据,实现对实验相关信息的监督,但不具有写权限。实验结果表明,在传统的基于道德教育方法基础上,去中心化的算法和数据能够增加更好的检测机制。

关键词 网络拓扑,区块链,信任机制,去中心化
中图法分类号 TP311.52 **文献标识码** A

Study on Trustworthy Backtracking Mechanism of Experimental Teaching Fund Based on Blockchain

QU Guang-qiang SUN Bin
(Northeast Dianli University Academic Administration, Jilin 132012, China)

Abstract This paper proposed a solution for experimental teaching fund system based on blockchain technology, it is divided into a core data network and an information disclosure network. The core data network is a distributed database composed of a series of core nodes with equal power, which is mainly responsible for data storage and input. The information disclosure network is an open network where anyone can read the complete data stored in the core data network and supervise the experimental related information, but does not have write permission. Experimental results show that decentralized algorithm and data can add a better monitoring mechanism to the traditional methods based on moral education.

Keywords Network topology, Blockchain, Trust mechanism, Decentralization

自 19 世纪 70 年代到 20 世纪初,以电能的突破、电气技术的应用及内燃机的出现为标志,在德国和美国掀起了近代史上的第二次工业革命,自此科学技术的发展越发成为促使人类社会向前发展的重要推动力,而只有在教育科研领域不断地投入资金才能满足科学技术的发展需求,教育科研经费的投入力度大小直接影响着国家科学技术的发展。中国对教育科研的投入力度是相当大的,2012 年国家财政性教育经费支出占国内生产总值的比例如期实现了 4%的目标,此后,中央财政保障教育发展的投资额度也在不断增加[1]。然而,大力度教育科研经费的投入并没有得到相应的预期成果。统计数据表明,每年的科研成果能产生规模效益的仅占 15%,科技成果转化率仅占 25%,而产业化率仅占 5%[2]。我国科研教育经费的腐败问题愈演愈烈,自 2012 年中央颁布"八项规定"至 2016 年,仅中纪委监察网公布的教育经费违规案件就高达 404 起,由此可见教育经费腐败问题的严重性[3]。

教育经费腐败有虚假劳务费用、虚假发票套现以及收受厂商回扣等惯用手段。教育理论界一致认为,教育腐败是指掌握与行使公共教育权力的主体滥用公职权力以谋取私利的行为。腐败的主体是公职人员,其手中掌握一定的权力;腐败的目的是谋取私利,私利包括金钱、其他物质、精神层面的欲望。所以,腐败问题的深层次原因就是滥用权力以及相关的信息不够透明化。从经济学角度看,人们在拥有权力的情况下能够获得大于风险的收益时,会铤而走险而违背规则的几率就大大增加。在科研教育经费的管理上更是如此,许多公职人员存在着伪造发票、设备耗材高价上报低价买入以及吃回扣等腐败行为。其中,实验经费,如实验耗材、实验设备等,在管理过程中出现这些问题是因为实验经费系统存在不透明、中心化(权力集中)等问题。如果实验经费的使用能够做到公开、透明并受公众监督、不可篡改,那么在面对巨大风险的情况下,实验经费的腐败会减少许多。

Satoshi nakamoto 于 2008 年发布了比特币白皮书——《Bitcoin: A Peer-to-Peer Electronic Cash System》[4]。支撑比特币运行的主要技术包括哈希函数、分布式账本、区块链、非对称加密、工作量证明等。它最大的特点是去中心化、公开透明且几乎不可篡改,这正好可以解决目前实验经费系统中存在的一些不透明、腐败问题。本文提出了一种新的基于区块链技术的实验经费系统,探索了区块链技术减少实验经费腐败的可能性。

1 去中心化与实验经费系统

1.1 信任系统

英国演化理论学者里查德·道金斯在他的一本著作《自

本文受吉林省高等教育教学研究重点课题项目(ST201605)资助。
曲广强(1977—),男,硕士,副研究员,主要研究方向为计算机应用技术,E-mail:630665545@qq.com(通信作者)。

私的基因》[5]中持有这样的观点:人们生来就是自私的,生物一切行为的原动力均来自于基因赋予的两大任务——生存和繁衍。生存和繁衍的首要条件是能量,于是围绕着获取能量便产生了生活中最普遍也是最重要的行为——交易。交易背后的本质都是为了利益(获取能量)而交易,而交易的核心前提就是信任。个体与个体、个体与组织之间如果没有信任,便不存在交易成功的可能。

信任问题一直是困扰人类的一大难题,为了更大的利益而敲诈勒索、背叛朋友、经费腐败等事件屡出不穷。为了解决交易中的信任问题,人们想方设法。当人类还是小规模部落的时候,人们选择信任的村长或者部落首领作为记录信用、资产的人;当规模再大一点的时候,就出现了钱庄、银行等中介记录人们的交易或者信用[6]。但是这些模式始终存在一个弊端,首领或者银行等是中心化系统,人们虽然有了中介做担保,但这是在人们信任中心系统的情况下条件才成立,假如在中心系统信用也存在问题从而违约对数据库进行数据的修改,那么整个交易网络将会失效。对于整个实验经费管理系统来说也是如此,如果某人掌握了该系统数据库的修改权限,那么经费腐败是很容易发生的。

1.2 教育经费研究现状与管理问题

教学科研经费腐败是一个普遍性的问题,如中国工程院院士用空壳公司捞钱,涉案 2500 万元;北京航空航天大学主任贪污 260 万元科研经费;交通部违规使用 1.86 亿元科研经费发工资补贴等[2]。针对不同的腐败行为,不同的机构采取了不同的处理措施。万丽华等提出了应对科研机构经费腐败可以从法制建设、道德教育方面和制度建设、管理机制方面采取措施[7];杨柳等提出了用"智力补偿费"来防治科研经费腐败[8]。

对于教学实验经费的管理,许多教育机构通过采取思想道德教育和法制建设的方法来解决教学、科研经费腐败的问题卓有成效,但是现在的教学、科研经费管理仍然存在着许多问题:

1)思想道德教育只是一种精神契约上的约束,一旦腐败行为能够获取的利益远超所承担的风险,那么道德约束有很大的可能性会失效。

2)法制建设是一种有效的方法,它能够对公职人员起到一定的约束作用。但是传统的实验经费系统是一个中心化的系统,信息不够透明而且数据可篡改程度也较高,即公职人员暴露风险较低。

3)传统的实验经费系统是一个中心化系统,数据库容灾能力较低,一旦中心数据库受到攻击或者出现异常情况,那么整个系统都将会崩溃。

1.3 区块链技术概述

区块链技术的概念最早起源于密码学学者对电子货币的探索,其中最早大获成功的电子货币当属于比特币,比特币于 2009 年左右首次成功在大众中传播。由于比特币是一个去中心化的分布式数据库系统,它拥有不可篡改、匿名、政府监管难度高等特点,但比特币有了一些不好的名声,原因在于比特币多用于敲诈勒索、黑市买卖毒品与枪支弹药、雇佣杀手等,如 2018 年初的美国对叙战争就曾导致比特币价格大涨,可见比特币在黑市中的受欢迎程度。2015 年,经济学人刊登了一篇文章——《区块链:信任的机器》[9],从此人们的注意力逐渐从比特币转向比特币的底层技术区块链,世界各地的研究机构纷纷开始研究区块链的内在价值。从比特币的另一方面来看,可以发现比特币背后所隐藏的区块链技术其实是有希望解决人类社会中的许多问题。区块链技术站在一个全新的角度通过分布式的去中心化系统建立一个数学模型巧妙地解决了人类社会中的中央权威信任问题。在区块链中,一切的信任基础都是基于数学模型而不是第三方中介或者中央权威的信用。区块链的去中心化、不可篡改特性是信任问题天然的解决方案。

区块链的本质是一个去中心化的分布式数据库,该数据库由一串使用密码学方法产生的区块有序连接而成,区块中包含一定时间内产生的无法被篡改的数据信息。区块中包含数据记录、当前区块根哈希(Hash)、前一区块根哈希、时间戳等信息。数据记录可以是任意数据,如交易数据、资产数据、实验教学经费数据等。区块哈希值指的是当前区块通过 SHA-256 等哈希算法计算出的哈希值。整个区块链是通过哈希值从上一块到下一块有序连接而成,如果在整个区块链中的某个区块数据被修改了,哈希值相应地发生了改变,所以整个区块链就会断掉[10]。区块链将密码学、数学、经济学、网络科学等技术组合到一起,形成了一个去中心化的分布式数据库,网络中的每一个用户节点既是客户端也是服务端,每一个节点都存有整个数据库的完整备份,所有节点都通过特定的共识算法进行数据的插入。如果某个节点不诚实的对自己的数据库进行修改,只要整个数据库网络中大多数节点都是诚实的,那么它的修改就不会影响其他节点。所以区块链信任基础本质上是建立在数学模型和相信大多数人可靠的前提下,而不是建立在信任某一个组织或者政府的前提下,这样就使得系统的信任度大大提高。这类似于如今的政府选举,只要大多数人在某一时刻认可某一届政府,那么它在这一时刻对于大多数人而言就是可信任的。

由于区块链的完全可信任、高度冗余等特性,使得区块链可以应用于许多场景。目前区块链主要应用于数字货币、数据鉴证、选举投票、公证、信息公开等领域。特别是区块链在信息记录与公开的应用,这将会大大减少真实性证明方面的成本。对于实验经费系统来说,信息的完全可信任、公开透明、不可篡改等特性不仅减少了证明成本,也大大增加了经费腐败暴露的风险,这在一定程度上减少了腐败的发生。

2 实验经费系统设计

2.1 网络拓扑架构

图 1 是基于区块链技术的实验经费系统,由核心数据网络和外部信息公开网络两部分组成。

核心数据网络是整个系统的核心组成,它由一系列可靠的计算机节点组成,主要任务是创造新的区块和存储区块数据,每个节点都拥有高速处理器和大容量存储空间并且存有完整的区块链数据。根据研究机构不同的组织情况,这些节点可由不同的机构部门组成。比如高等学校可由不同的部门或学院组成,如纪委办、科技产业处、图书馆、马克思学院等。每个部门控制一个节点,并通过数字签名赋予一定的权重,并按照一定的机制产生新的区块和存储区块链。

外部信息公开网络是一个开放的网络,任何人和组织均可按照一定的规则接入外部信息公开网络,但是只有读取完

整区块链数据并验证真伪的能力，而没有写入权限。与此同时，核心数据网络是按照一定的共识机制在不同的核心节点之间存储和更新数据，这种机制是所有新产生的区块数据均需要通过一半以上的核心节点认可。在某种程度上，核心数据网络所存储的信息可信任度是远远大于传统的中心化实验经费系统，因为它把信任基础平摊给了各个部门，而不仅仅依赖于某一个部门，因此公众可以放心地信任核心数据网络上的区块数据并通过此网络对实验经费数据进行一定的监督。由于区块链数据的开放性，任何公职人员对实验经费的使用情况都需要面对公众的监督。

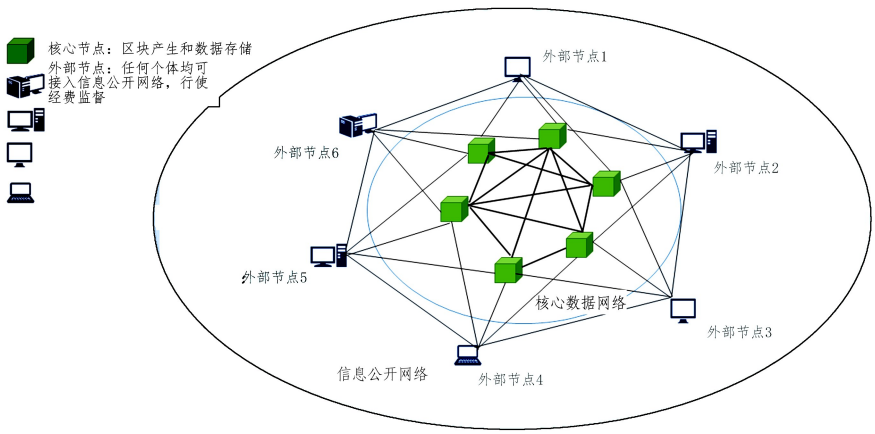

图 1　基于区块链技术的实验经费系统网络拓扑架构

2.2　区块链结构

实验经费系统最重要的两个模块是实验耗材和仪器设备的管理，这两部分是最容易发生经费腐败的地方。如图 2 所示，以实验耗材为例，我们可以将实验耗材的名称、单价、购买数量、购买人以及购买日期等重要数据记录到区块链中。区块数据则由若干实验耗材数据、前一个区块哈希数值（选择 SHA256 算法）、随机数 Nonce 等组成。每当需要记录新的耗材时，我们通过一个相对公平的共识机制在核心数据网络中选定一个代理节点，来行使记录权力将一定大小的耗材记录打包到某一个新开辟的区块中，然后代理节点将新区块数据在网络中进行广播，收到区块数据的节点在验证数据合法性后，将其添加到自己区块链的最末尾；如果区块数据非法则终止操作。

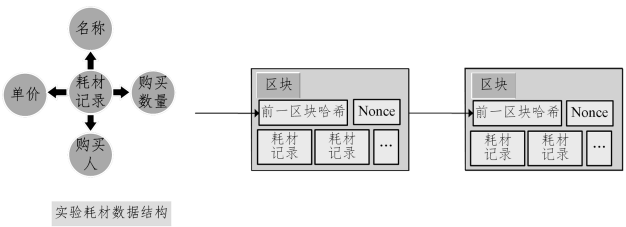

图 2　实验耗材区块链结构

2.3　共识机制

选择某一个节点行使数据记录权力并保证区块链数据库分布的一致性的机制称作共识机制，共识机制最早是由拜占庭将军问题[11]演化而来的。最常见的共识机制的特点如下[12]：

1）工作量证明（PoW）机制：通过 CPU 算力竞争解决难题，但浪费资源、确认时间过长；

2）权益证明（PoS）机制：具有权益最高的节点拥有区块记账权，不存在算力浪费问题；

3）股份授权证明（DPoS）机制：类似于“董事会决策”，系统中每个股东节点根据所占股份获得投票权。

由于实验经费系统中只有少量核心节点拥有记录数据的权力而不存在大量算力浪费的情况，并且记录实验经费数据不需要具有很高的时效性，因此我们选择 PoW 机制。本文采用的工作量证明机制是基于一定难度的哈希计算，算法步骤如下：

```
difficult=6 //难度
    block.nonce=1 //区块随机数
    block.hash=sha256(block) //计算哈希数值
    while !block.hash.startswith(difficult * "0") //如果哈希数值
          不是以 difficult 个'0'开头
Block.nonce=block.nonce+1 //随机数自加 1
Block.hash=sha256(block) //重新计算哈希数
```

其中，difficult 代表工作量的大小，即区块哈希值从第一位开始连续的零的个数，零越多难度越高，意味着新创造一个区块的时间就越长。

2.4　工作步骤

1）系统管理员通过实验经费系统在核心数据网络对全网所有节点广播一个数据录入请求的数据包；

2）核心数据网络的所有正常节点在收到录入请求数据包时，在内存中开辟一个新的区块，并将相关信息填入区块中，其中随机数 Nonce 初始化为 1；

3）通过 SHA256 算法计算区块数据哈希数值；

4）判断哈希数值是否满足难度要求，如果不满足，则将随机数 Nonce 加 1，并转至 3），否则转到下一步；

5）向全网中广播扩散当前的新区块；

6）所有节点收到区块后，验证该区块是否合法，如果合法，则将其连接到区块链的最后一块区块之后，否则中止行为；

7）所有需要获取完整区块链的节点只需要在网络中广播获取数据请求，收到请求的节点会将自己的区块链数据发送出去，而该请求节点也可以根据区块链哈希链的特性来验证数据的真伪。

3　实验及结果分析

3.1　实验环境

本文用 python 语言对区块链实验经费系统进行了编程建模，实验环境为 CPU：AMD A8-5550M（2.10GHz）；RAM：12GB；OS：Windows 10；Program Language：Python 3.5；IDE：

Visual Studio Code。

3.2 数据篡改难度分析

假如某个不诚实的节点想要篡改数据，由于散列函数的强混淆性，它不仅得有能力控制网络中的大部分节点，而且需要花费大量的时间来重新计算更改区块后的所有区块哈希值。设成功计算一个区块的哈希值所需时间为 t，所需篡改的区块之后的区块个数为 n，那么总共所需时间为：

$$T=\sum_{i=1}^{n}t_i$$

其中，t_i 为计算第 i 块区块哈希值所需的时间。如图 3 所示，随着区块链越来越长，所需成本将快速增长，这种篡改的可能性将越来越低。由于数据的真实性，如果有人涉嫌贪污经费，那么真实性证明成本将变得很低，反之，由于贪污经费暴露风险的增加，这将会减少公职人员贪污经费的可能性。

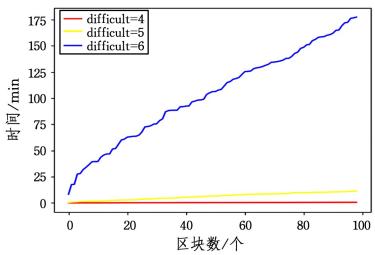

图 3 篡改时间增长曲线

3.3 可靠性分析

由于每个核心数据网络的节点都有整个数据库的完整备份，这有助于提高整个系统的容灾能力，即使某几个节点受到了不可恢复的破坏，其他完好的节点也仍然存有完整的系统数据，我们可以通过网络随时恢复数据。假设整个系统有 n 个节点，并且整个系统的网络是完美的无向完全图，那么整个网络系统的边的条数为：

$$E=\frac{n*(n-1)}{2}$$

边的条数为节点个数的二次函数，边越多系统就越稳定。

结束语 传统计算机科学所追求的目标往往是时间复杂度和空间复杂度尽可能高效，但是区块链的设计理念却反其道而行之，它通过尽可能的拖延新区块的产生时间来决定谁拥有记录权力和尽可能多的数据冗余来解决去中心化的问题。这种做法看似不明智，但是却是一种解决信任问题的巧妙方法。基于区块链的实验经费系统正是充分利用了区块链的去中心化、可信任、不可篡改的特性，才能达到在一定客观程度上抑制实验经费腐败案件的发生。

更进一步的是，我们可以完全消除传统的购买、开发票报销的流程，只需将实验设备、耗材等商家与教育机构交易网络连通，公职人员与商家交易时便通过此区块链网络进行交易，整个交易记录也记录在区块链上，这样一来经费管理会变得更加科学有效。

参 考 文 献

[1] 国家数据. 研究与试验发展经费支出[Z]. http://data.stats.gov.cn/easyquery.htm?cn=C01&zb=A0N02&sj=2016.

[2] 曾丽. “科研经费腐败”有多严重？[Z]. 廉政瞭望，2015-08：9-9.

[3] 杨蓉，刘婷婷. 我国教育经费腐败现状和趋势分析[J]. 教育财会研究，2017，28(3)：3-11.

[4] NAKAMOTO S. Bitcoin：A Peer-to-Peer Electronic Cash System[R]. https://bitcoin.org/bitcoin.pdf，2008.

[5] 里查德·道金斯. 自私的基因[M]. 吉林：吉林人民出版社，1998.

[6] 长铗，韩锋. 区块链：从数字信用到社会[M]. 北京：中信出版社，2016.

[7] 万丽华，龚培河. 高校科研经费腐败的形式、根源与对策研究[J]. 科学管理研究，2014，32(5)：40-43.

[8] 杨柳，王义杰. 用“智力补偿费”防治科研经费腐败[N]. 检察日报，2012-03-10(8).

[9] BERKELYE J. The promise of the blockchain ： The trust machine[N]. The Economist，2015-8-31.

[10] 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.

[11] GRAMOLI V. From blockchain consensus back to Byzantine consensus[J]. Future Generation Computer Systems，2017，9(23)：1-10.

[12] 夏清，张凤军，左春. 加密数字货币系统共识机制综述[J]. 计算机系统应用，2017，26(4)：1-8.

(上接第 547 页)

[8] IDELBERGER F，GOVERMATORI G，RIVERET R，et al. Evaluation of logic-based smart contracts for blockchain systems[C]// International Symposium on Rules and Rule Markup Languages for the Semantic Web. Cham：Springer，2016：167-183.

[9] ANDROULAKI E，BARGER A，BORTNIKOV V，et al. Hyperledger fabric：a distributed operating system for permissioned blockchains[C]// Proceedings of the Thirteenth EuroSys Conference. ACM，2018.

[10] LIANG G，SOMMER B，VAIDYA N. Experimental performance comparison of Byzantine fault-tolerant protocols for data centers[C]// INFOCOM，2012 Proceedings IEEE. IEEE，2012：1422-1430.

[11] CASTRO M，LISKOV B. Practical Byzantine fault tolerance[C]// Symposium on Operating Systems Design & Implementation. 1999，99：173-186.

[12] 韩璇，刘亚敏. 区块链技术中的共识机制研究[J]. 信息网络安全，2017(9)：147-152.

[13] 沈鑫，裴庆祺，刘雪峰. 区块链技术综述[J]. 网络与信息安全学报，2016，2(11)：11-20.

[14] 袁勇，倪晓春，曾帅，等. 区块链共识算法的发展现状与展望[J]. 自动化学报，2018，44(11)：93-104.

[15] DINH T T A，LIU R，ZHANG M，et al. Untangling blockchain：Adata processing view of blockchain systems[J]. IEEE Transactions on Knowledge & Data Engineering，2018，30(7)：1366-1385.

[16] DINH T T A，WANG J，CHEN G，et al. Blockbench：A framework for analyzing private blockchains[C]// Proceedings of the 2017 ACM International Conference on Management of Data. ACM，2017：1085-1100.

[17] LO S K，XU X，CHIAM Y K，et al. Evaluating suitability of applying blockchain[C]// International Conference on Engineering of Complex Computer Systems. IEEE Computer Society，2017：158-161.

[18] CLEMENTA，WONG E L，ALVISI L，et al. Making Byzantine fault tolerant systems tolerate Byzantine faults.[C]// Usenix Symposium on Networked Systems Design & Implementation，2009，9：153-168.