基于区块链的商户间账本管理模型

李 卫[1] 王腾宇[2] 刘乾隆[2] 刘克猛[2] 范永刚[2]
(国家工业信息安全发展研究中心 北京 100040)[1] (大连理工大学软件学院 辽宁 大连 116620)[2]

摘 要 随着互联网经济的不断发展,越来越多的商户选择利用互联网终端进行账本管理。但是,常常会由于人为因素导致账本丢失、数据被篡改、商户双方信任危机等一系列问题。通过梳理当前社会上常见的账本管理问题发现,数据的分布式存储、可追溯性和不可篡改性成为了解决账本管理问题的关键,而这恰恰是区块链技术的主要特性。鉴于账本对于交易双方的重要性以及区块链技术与账本管理的高契合度,文中提出了基于区块链的商户间账本管理模型并加以实现。首先,在介绍区块链特性与账本管理联系的基础上,提出基于区块链的账本管理模型架构;其次,分析交易文本格式设计、区块成链方式、智能合约设计与共识算法设计;最后,对模型进行安全性分析和性能测试,并对模型性能方面存在的缺点进行分析。结果证明了基于区块链的账本管理模型符合商户间账本管理的安全性与性能要求。该模型为建立安全、可靠的交易账本管理提供了新思路与新方法。

关键词 区块链,账本管理,去中心化,可追溯性
中图法分类号 TP391 **文献标识码** A

Inter-merchant Account Management Model Based on Blockchain

LI Wei[1] WANG Teng-yu[2] LIU Qian-long[2] LIU Ke-meng[2] FAN Yong-gang[2]
(China Industrial Control Systems Cyber Emergency Response Team, Beijing 100040, China)[1]
(School of Software Technology, Dalian University of Technology, Dalian, Liaoning 116620, China)[2]

Abstract With the continuous development of the internet economy, more and more merchants choose to use internet terminal for account management. However, there are a series of problems such as loss of account books, tampering with data, and crisis of trust between merchants due to human factors. By sorting out the common accounting management problems in the current society, distributed storage, traceability and non-defor mable of data, which are precisely the main features of blockchain, become the keys to solve the problems of account management. In view of the importance of the account books on transaction partners and the high degree of fit between blockchain technology and account book management, this paper proposed an inter-merchant account management model based on blockchain technology. Firstly, based on the introduction of blockchain characteristics and link between blockchain and ledger management, a structure of ledger management model is explained. Secondly, the design of transaction text format, block, smart contract and consensus are analyzed. Finally, the model is analyzed for safety and performance, and the shortcomings of model performance are analyzed. It is proved that the account book management model based on blockchain technology meets the security and performance requirements of account book management between merchants. This model provides new ideas and methods for establishing a safe and reliable transaction account management.

Keywords Blockchain, Account management, Decentralization, Traceability

1 引言

随着互联网商业技术的不断进步,在各行各业,信息管理系统都已经是人们不可或缺的组成部分,越来越多的商户选择使用移动终端进行在线收支和账本管理。然而,由于一些人为因素,商户间的账本经常出现错误,如记账错误、双方账本不一致、历史账目丢失、账本被篡改等。由于账本及交易数据对于商户的重要性,业内采用各种各样的方法来减少账本的错误,最常见的方式便是商户双方进行对账:商户双方拿出自己计算清分后的账本与对方进行核对,确认无误后进行结算。一旦出现双方清分结果不一致的情形,则需要商户双方互相核对出错部分;若为账目不同,则需拿出交易时的记录进行对比。但这种方式增加了成本与耗时,扩大了不必要的交易规模,若出现双方交易记录均丢失的情况,便只能服从信用更好的一方,安全性与便利性就变得很差。

区块链的发展,让账本保护问题有了新的解决方法。区块链是一种具有普适性的去中心化的网络模型,具有去信任、集体维护、可追溯性、不可篡改等特性[1-3],受到了众多公司,尤其是金融公司的大力追捧。区块链技术经历了以可编程数字加密货币体系为主要特征的区块链 1.0 模式、以可编程金融系统为主要特征的区块链 2.0 模式和以可编程社会为主要特征的区块链 3.0 模式[4]。

李 卫(1981—),男,硕士,工程师,主要研究方向为区块链;范永刚(1974—),男,硕士,主要研究方向为区块链,E-mail:yonggang_fan@dlut.edu.cn(通信作者)。

区块链的区块 hash 加密方法可以保证数据不可被修改,即数据内容一旦写入区块,就不能被篡改。如果系统中某一方用户篡改了账本数据,将会被及时检测出来。此特性可以保证交易一旦达成,则数据无法被篡改,从而达到对账本安全有效的保护。同时,区块链系统内多个节点共同组成一个网络,其中的数据库和区块文件由各个节点共同维护。写入数据时,为了保证各节点的数据一致和内容同步,可以采用 PBFT(Practical Byzantine Fault Tolerance)或者 SBFT(Speculative Byzantine Fault Tolerance)算法等。这就保证了各商户之间的原始记录一致,避免了双方账目不一致时无法判定真伪的情况。这就为场景之中的商户结算提供了一种新的思路:多家商户可以组成一个区块链网络,在这个网络中,每家商户都可以将自己的交易记录放在系统中,并通过区块链算法来保证各商户账本的一致性,从而避免数据不一致带来的风险和沟通成本。同时,由于区块链的不可更改性和可追溯性,商户既避免了交易记录被不法分子更改的风险,又可以防止交易账单不慎丢失的情况。

本文第 2 节描述了基于区块链的账本管理模型的核心架构;第 3 节阐述了模型的功能和详细设计;第 4 节对模型安全性与性能进行了分析;最后总结全文。

2　模型架构

基于区块链的账本管理模型主要分为 4 个模块:用户交互、智能合约处理,区块链服务、数据库。其中,智能合约处理属于区块链服务,但由于其特殊性与重要性,本文将单独讲解。具体模型架构如图 1 所示。

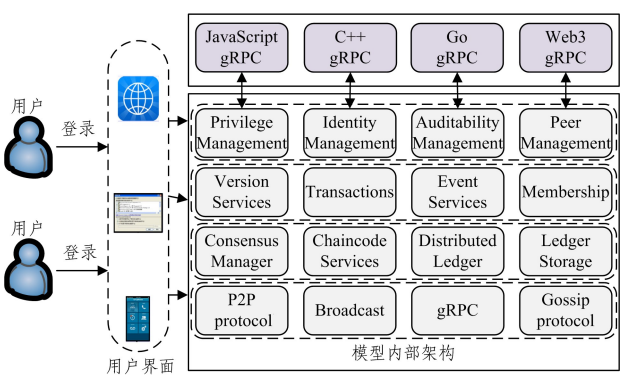

图 1　系统模型架构

模型使用联盟链作为基础,以若干个频繁发生交易、账目繁多的可信商户形成联盟,联盟中各商户信息记录在数据库中,并通过读取数据库中的商户账号、密码进行登录。

商户间每次发生交易或发生数次交易后,需要在前端界面将账目信息发送到区块链网络中,区块链网络收到后,会将其保存。同时,系统会根据用户要求通过智能合约实现账目收入、账目支出、账目查询和账目清算功能。在账本管理系统中,存储交易信息而非双方交易金额,此存储方式可以精准查询到每一次的交易信息而不仅是交易金额。

在区块打包上,有两种方式可以选择:1)选定时间间隔打包,即在选定的时间间隔后对交易记录进行链式打包;2)选定数据大小打包,即当交易记录总大小达到指定大小后,将数据打包成区块相连。鉴于基于联盟链的账本管理模型中的交易记录量并不巨大,为防止出现某一区块内无交易内容,本模型选用第二种方案[5-6]。

在共识服务模块,本模型使用 PBFT 共识算法。用户发送交易请求后,各个节点使用 PBFT 算法进行验证,通过验证的信息按时间顺序进行排序,当数据大小达到指定要求时,由 order 节点进行区块的打包,并在达成共识后将区块广播给各个节点,并将区块与前一区块相连。同时,每隔一段时间间隔,区块链系统会进行定时交流,检测是否存在恶意节点或改变的区块,当检测到节点与其他节点的区块不一致时,使用共识算法将区块进行更新。

3　模型设计

3.1　文本格式设计

基于区块链的商户间账本管理模型主要包括 3 种存储格式:用户信息存储、交易信息存储和交易请求。

(1)用户信息存储格式,本系统模型采用外接的 Mysql 数据库进行存储。这是基于 Mysql 数据库的整齐性与便于管理的特性决定的。具体格式设计为:

[client String][password String][property Int]

其中,client 为用户账户名,password 为账户密码,property 为账户所存在的金额。通过 client 和 password 来登录系统,property 表示余额,当通过智能合约清算得到交易所需金额时,修改余额。

(2)交易记录的存储格式,我们使用 fabric 自带的 CouchDB 数据库。格式为:

[client String][account Byte]

其中,由于 CouchDB 数据库是 K-V 数据库,本模型将交易发起者与接受者作为 K 值 client,将进行的所有交易内容如交易时间、交易内容、交易金额皆归于 V 值 account。

(3)交易请求格式,用户需要将交易请求发送给区块链网络,同时选择执行节点、调用函数等。因此,我们将交易请求格式设计为:

[CID Int][Chain_ID Int][Data String]

其中,CID 为通道标识符,相同通道内的账本相同。ChainID 为链码标识符,即选择对应的智能合约的版本号,实现对应的功能。Data 为选择的智能合约中调用的具体函数以及所带的参数,是实现用户账本管理功能的主要内容。

3.2　区块链接方式

"账本管理"模型收到交易请求后,通过共识服务对交易进行验证,验证通过后将结果发给 order 节点,交易内容达到一定数量后,按时间顺序打包生成区块,而区块根据前一区块的块头进行 hash 得到 hash 值,从而将区块相连,格式如图 2 所示。最后,各节点之间达成共识,将连接后的区块广播给各个节点。

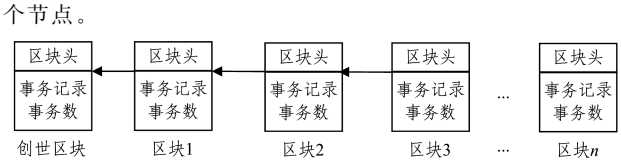

图 2　区块链接方式

在区块链中每个打包形成的区块由两部分组成:区块头和区块体[5]。区块体包括区块 ID、区块内各个交易事务记录、事务数,如表 1 所列。

表 1 区块体结构

子结构名称	说明
区块 ID	每个区块的唯一标识符
区块头	区块头部信息,其 hash 值作为下一个区块的参数
事务记录	当前区块存储的所有交易事务
事务数	当前区块存储的事务交易数

在区块中,区块 ID 是每个区块的唯一标识符,用于区分区块,事务记录是通过共识算法,将事务按时间排序并记录在区块之中;区块事务数则是记录本区块中事务的个数。而对防篡改和可追溯性起到巨大作用的是区块头,通过对本区块内容进行 hash 运算,得到区块的 hash 值;同时,与上个区块的 hash 值相连。如果上个区块的数据改变,那么它的 hash 值会发生巨大变化,将无法与后续区块相连,这也是区块链不可篡改性和可追溯性的原因之一。区块头的结构信息如表 2 所列。

表 2 区块头结构

子结构名称	说明
区块大小	记录本区块的大小
父块 hash 值	记录上一个区块的 hash 值
默克尔树根植	当前区块中所有事务的默克尔根节点 hash 值
时间戳	记录区块生成时间

3.3 基于智能合约的账本管理功能

基于区块链的账本管理模型设计了以智能合约[7-8]为中心的账本管理协议,该协议主要由交易上链、交易账目查询、交易清算 3 个模块构成。

3.3.1 交易上链

用户完成一次交易后,需要将交易内容存储到区块链节点中。我们使用 invoke 函数输入交易发起方、接收方、交易时间、交易金额以及交易内容。而系统在得到函数后,将内容保存到 CouchDB 数据库中。在区块链中,我们使用的 CouchDB 数据库为 K-V 数据库,其中 K 值为 string 字符串型,而 V 值为 Byte 型,因此我们保存时,须将交易记录的 V 值(此情形下为交易时间、交易金额、交易内容)转换为 Byte 型。具体合约伪代码如下。

```
Input:用户 a、交易对象 b、交易时间 t、交易事项 f、交易金额 s
1. K=a+b V=t+f+s /* 合并存储格式 */
2. if K is exist then
3.    for i< length(V1)
4.       if V1[i]==V
5.          show repeat record/* 验证是否重复 */
6.       end if
7.    end for
8.    store V /* 无重复则存储 */
9. else store V /* 无交易对象直接存储 */
```

3.3.2 交易账目查询

存储了若干交易后,当用户需要进行清算时,往往不仅仅需要一个清算结果,还需要账单记录中的内容,因此,系统提供了交易账目查询。用户需要输入交易双方及交易的起止时间,通过交易起止时间来查询 CouchDB 数据库中所有符合要求的交易记录并显示出来。具体合约伪代码如下。

```
Input:用户 a、交易对象 b、起始时间 t1、截止时间 t2。
1. K=a+b /* 合并 K 值 */
2. if K is exist then
3.    for i< length(V)
4.       if t1 <t. V[i] < t2
5.          output V/* 遍历符合要求的交易记录 */
6.       end if
7.    end for
8. else output 无交易记录
```

3.3.3 交易清算

用户需要进行清算时,用 calculate 函数输入交易发起方和接收方,而系统使用函数进行清算,最终得到发起方应给接收方的金额。系统先提取出 K 值对应的 V 值中每一条交易记录,同时根据交易时间范围进行筛选,得到交易记录后筛选出交易的金额并进行汇总。但需要注意的是,清算时,不仅要计算 k1 值(用户+交易对象)对应的内容,同时还要计算 k2 值(交易对象+用户)对应的内容,两个计算结果汇总后才是最终的结果。具体伪代码如下。

```
Input:用户 a、交易对象 b、起始时间 t1、截止时间 t2
1. K1=a+b K2=b+a
2. if K1 is exist then
3.    for i1 < length(V1)
4.       if t1 <t. V1[i] < t2
5.          sum1=sum1+s. V1[i] //累加符合要求的交易记录金额
6.       end if
7.    end for
8. end if
9. if K2 is exist then
10.  repeat 3 to 7 get sum2 //重复 3 到 7 行操作,得到 K2 的金额
11. end if
12. sum=sum1+sum2
13. output sum//输出本次清算总额
```

3.4 共识服务设计

由于本模型采用区块链分布式系统,因此如何保持所有节点内数据一致性是本系统要解决的问题之一。因此,“账本管理”模型中使用共识服务模块进行消息的验证、区块的统一。

本文采用 PBFT 算法[9-11]实现节点自行与其他节点进行数据同步和对比,在 PBFT 算法中,每个 client 的请求为了达成数据一致性需要完成 5 个阶段[12-14]。当 client 发送请求时,网络内节点使用两次交互,达成一致后再执行 client 请求。如果提交消息后一段时间内都没有结果返回,说明系统数据未达成一致,需要 client 重新提交数据。

如图 3 所示,PBFT 系统中共有 5 个节点,分别为 client 节点和 4 个 peer 节点(分别标号为 0,1,2,3)。其中,client 节点为用户请求节点,4 个 peer 节点中的 3 节点为错误节点,即发生了数据错误或者无法使用。PBFT 算法可分为 5 个阶段:

1) Request 阶段,用户选定提交节点,如图 3 的 0 节点即被用户选中的节点。在选定节点后,用户会向 0 节点发送交易请求,而 0 节点收到请求后会进行签字,并选取节点进行背书签名。

2) Pre-prepare 阶段,提交节点在签名后,通过通道广播,向所有节点发送背书请求。

3) Prepare 阶段,其余节点在收到背书请求后,为了验证

请求的真实性，会在请求上签名，之后向其他节点发送背书验证请求。

4）Commit 阶段，其他节点收到背书验证请求后，会对验证请求进行拜占庭验证，如果认为请求合法、有效，则在请求上签字，并将交易即 commit 消息发送给其余节点。

5）Reply 阶段，每个背书节点收到超过总背书节点 2/3 的 commit 消息后，可认为请求有效，确认本轮交易完成并反馈给 client 节点。

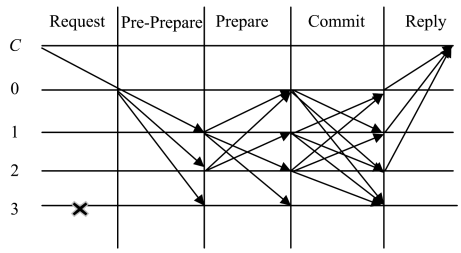

图 3　PBFT 算法流程图

在 PBFT 系统下，即使 3 节点是发送错误消息或不发消息的失效节点，仍然可以保持每个阶段正确的操作（当然，失效节点不超过 1/3）。同时节点使用 Gossip 协议来广播账本和通道数据。

4　实验与结果分析

本模型实验环境为 16 台 4 核处理器，RAM 为 16 GB 的主机搭建的节点网络，操作系统均为 Ubuntu16.04，区块链模型为单链结构、单通道、单片，并满足一次交易进行一次签名的要求。

4.1　安全性分析

对于安全性能，本模型在信息加密上，采用哈希函数加密和非对称加密。通过哈希散列算法形成固定二进制的输出，从而实现区块链的不可篡改性。公私钥加密则通过节点签名实现，加强了共识服务中 PBFT 算法的安全性[9]。

同时，由于本模型采用区块链分布式存储结构，因此大量针对传统数据库的攻击（如强力（非强力）破解弱口令、特权提升、SQL 注入、窃取备份磁带等攻击）即使通过特有的方法攻击了某个节点，使节点成为了无效节点，但依然可以通过区块链中的共识服务来保证系统的正常运行。

当账本被他人恶意修改时，常规的中心化数据库无法识别，从而造成用户的损失。但是，由于链的区块结构，当某一节点的区块内容改变，hash 值也将发生改变，节点间的连接将会断开。这样系统就可以在定时监测时发现某个节点的区块发生了改变，并通过 PBFT 共识算法来重新达成共识，将区块广播给有问题的节点进行修改，从而避免了账本内容被他人修改的情况。

由于本模型采用了 PBFT 算法，因此只能在 $N \geqslant 3F+1$ 时解决数据一致性问题（N 为结点总数，F 为失效节点数）。即只要系统有 2/3 的节点正常工作，就可以保证数据一致性。由于本模型建立在联盟链中，自身要求节点内部信任度较高，因此 1/3 的容错量符合容错要求。

4.2　性能测试与分析

对于性能测试，本模型分别在 4 节点、8 节点、16 节点搭建的区块链网络中进行 24 小时稳定运营，并测试吞吐量，结果如图 4 所示。

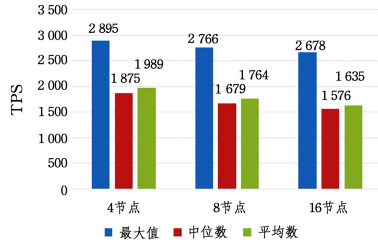

图 4　吞吐量测试

在 24 小时运营中，模型在 4，8，16 节点环境中均达到 2 600/s 以上交易量的最大值，并达到了 1 600/s 以上交易量的平均值，符合日常商户间账目记录的需求。但与常见中心化账本管理系统相比，本系统的吞吐量仍显示出明显的不足。这是由于本模型使用了 PBFT 的共识算法，在商户发起交易时，节点之间需要达成共识，这一阶段是影响吞吐量的主要原因。同时，随着节点数量的增多，达成共识所需时间增加，吞吐量也降低，这是 16 节点下吞吐量最低的原因[15-18]。

结束语　本文基于区块链技术设计了一种去中心化的“账本管理”模型。该模型通过对区块的设计、共识服务的选取以及智能合约的撰写实现了区块链的可追溯性和不可篡改性。同时，将区块链技术与账本管理相结合，实现了对用户账本的保护，防止了账本丢失以及账目被篡改的情况发生。同时，由于采用了用户登录模式，每个用户只能查询与自己相关的账本，也保护了联盟中其他用户的隐私安全。最后，通过对本模型的安全性分析，再次证明了模型的实用性。未来的研究中，需要解决区块链环境中由于频繁的交易验证而造成的吞吐量低下的问题，以加强“账本管理”模型的实用性。

参 考 文 献

[1] SWAN M. Blockchain：blueprint for a new economy[M]. Sebastopol：O’Reilly Media，2015.

[2] SASSON E B，CHIESA A，GARMAN C，et al. Zerocash：Decentralized anonymous payments from Bitcoin[C]// Security & Privacy. 2014：459-474.

[3] KOSBA A，MILLER A，SHI E，et al. Hawk：the blockchain model of cryptography and privacy-preserving smart contracts[C]// Security and Privacy. 2016：839-858.

[4] 刘秋万. 区块链技术发展与银行业应用[J]. 金融电子化，2016(6)：11-13.

[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] WATANABE H，FUJIMURA S，NAKADAIRA A，et al. Blockchain contract：Securing a blockchain applied to smart contracts[C]// 2016 IEEE International Conference on Consumer Electronics (ICCE). IEEE，2016：467-468.

[7] WATANABE H，FUJIMURA S，NAKADAIRA A，et al. Blockchain contract：A complete consensus using blockchain[C]// 2015 IEEE 4th Global Conference on Consumer Electronics (GCCE). IEEE，2015：577-578.

（下转第 556 页）

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。

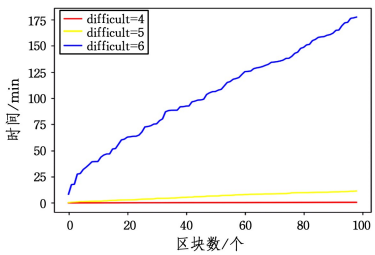

图 3 篡改时间增长曲线

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.