doi :10.3969/j.issn.1671-1122.2018.05.007

基于信誉值创建数字资产的区块链系统

王醒，翁健，张悦，李明

（暨南大学信息科学技术学院，广东广州 510632）

摘　要：区块链上被交易的数字资产类型日渐丰富。非数字货币类的数字资产在创建时，存在创建的真实性和有效性问题。文章利用区块链技术构建信任机制，将数字资产创建视作评估行为的过程，设计处理评估行为的智能合约，搭建基于联盟成员信誉值的区块链系统。智能合约基于联盟成员的信誉值和给出的评估数据来完成数字资产创建。系统借助侧链技术转移创建的数字资产，从而能够为其他交易场景下的区块链增加真实性保证。实验证明该系统的运行具有低成本、存储空间不易扩张的特点。

关键词：区块链；信誉值；数字资产；侧链

中图分类号：TP309　**文献标识码：**A　**文章编号：**1671-1122（2018）05-0059-07

中文引用格式：王醒，翁健，张悦，等. 基于信誉值创建数字资产的区块链系统 [J]. 信息网络安全，2018（5）：59-65.

英文引用格式：WANG Xing, WENG Jian, ZHANG Yue, et al. Blockchain System for Creating Digital Assets Based on Reputation Value[J]. Netinfo Security, 2018 (5) : 59-65.

Blockchain System for Creating Digital Assets Based on Reputation Value

WANG Xing, WENG Jian, ZHANG Yue, LI Ming

(*College of Information Science & Technology, Jinan University, Guangzhou Guangdong* 510632, *China*)

Abstract: The types of digital assets traded on the blockchain are getting richer. When digital assets other than cryptocurrencies are created, the problem of the authenticity and validity of the creation is produced. This paper builds trust mechanism based on blockchain technology, regards digital assets creation as the process of evaluating behaviors, designs smart contracts that deal with assessment behaviors, and builds a blockchain system based on reputation values of alliance members. The system uses sidechain technology to transfer created digital assets, which can increase the authenticity guarantee for blockchains in other trading scenarios. The experimental results show that the system has the characteristics that the cost is low and the storage space is not easy to expand.

Key words: blockchain; reputation; digital assets; sidechain

收稿日期：2018-1-15

基金项目：国家重点研发计划 [2017YFB0802203]；国家自然科学基金 [U173620045]；广东省应用型科技研发专项基金 [2016B010124009]

作者简介：王醒（1992—），男，浙江，硕士研究生，主要研究方向为区块链应用安全；翁健（1976—），男，广东，教授，博士，主要研究方向为密码学与信息安全；张悦（1990—），男，陕西，博士研究生，主要研究方向为智能移动端安全；李明（1987—），男，湖南，博士研究生，主要研究方向为区块链应用安全。

通信作者：翁健 cryptjweng@gmail.com

0 引言

区块链技术是一种分布式账本技术，通过数字签名、哈希算法、非对称加密等保证交易记录和数字资产的不可篡改性[1]。利用该特性，在区块链上被交易的数字资产类型日渐丰富，有能源互联网中的能源、租赁业务中的实体资产和知识产权等。这些系统中被交易的对象都由现实中的资产数字化而来[2,3]。

正是由于区块链的不可篡改性，数字资产在输入时就应当确保真实有效。目前关于区块链的研究主要集中在可扩展性、隐私安全、访问控制和部署各类应用等方面[4]，对数字资产创建的真实性和有效性等问题鲜有提及。区块链中的数字资产可以分为数字货币与非数字货币，均由一份关于该资产的数字文件实现，该文件创建后可在区块链系统中被交易和访问[2]。非数字货币的数字资产创建主要依赖于与之相对应的数字文件，该数字文件的创建方式包括自动或手动，通常通过语义标记[5]、扫描 RFID 和传感器检测等方式输入[6]。但是在此类数字资产的区块链应用方案中，均通过资产持有人直接在区块链上创建数字资产，创建的真实性依赖于区块链输入执行者的自律和区块链外部的审计，因而存在输入虚假或错误数据的可能。例如，TIAN 和 WEBER 等人提出利用区块链技术实现企业间供应链数据集成，数字资产真实性依赖于政府或机构的事后审计[7,8]。BAHGA 等人和 ALI 等人利用传感器向区块链输入数据，但在他们的方案中没有针对传感器的不稳定问题而提出的有效对策[9,10]。CHRISTIDIS[11] 等人提出通过智能合约实现人机交互，但他们的方案只能在传感器输入完成后进行外部审计。Factom 公司的认证报告系统也只能确保数字资产的有序性和不可篡改性，不能保证用户输入信息本身的真实性和有效性。

为提高数字资产的真实性，考虑将区块链上的数字资产由资产持有人单独创建变成由一组联盟成员共同创建。联盟成员的共同创建源于他们公正客观的评估结果，这就起到了外部审计的效果。本文提出基于联盟成员信誉值创建数字资产的方案。联盟成员由不同设备、机构、专家组成。联盟链上运行的智能合约首先收集联盟成员同一时刻对同一对象给出的评估结果，以此计算以信誉值为权重的标准评估结果，再基于该标准评估结果更新各成员信誉值，从而实现基于联盟成员信誉值的区块链系统。该系统采用侧链技术转移数字资产。接收数字资产的区块链称为侧链，侧链只记录被交易对象的流通交易过程，其成员符合可自由加入的公开链特性。

1 相关知识

1.1 区块链技术与智能合约

区块链是一种记录交易相关数据的分布式账本。区块链矿工将一个阶段的交易数据打包成区块，区块头包含时间戳和上一个区块头的哈希值，由此形成区块链。第一个区块称为创世区块。矿工通过校验区块链中的梅克尔树获知交易的真实性，并通过共识机制完成各节点对新增区块的认可[12]。

智能合约是一段存储并运行在区块链可信环境上层的可执行代码，通过在区块链上进行读写数据操作，实现数字资产按既定规则转移。当智能合约预设的信息与资产条件都满足时，智能合约就会被触发执行[13]。智能合约使得区块链系统不再单纯是分布式账本，还能支持编程和数据操作，进一步满足不同场景的应用需求。

1.2 侧链技术与数字资产转移

侧链技术是一种可以使数字资产在多条区块链之间安全转移的技术。当数字资产在主链上被锁定时，该资产可以在侧链内自由转移，不需要与主链进一步交互，从而减少对主链存储与计算资源的使用[14]。数字资产从主链转移到侧链的过程依赖于一种多重签名交易脚本。多重签名交易脚本通过记录 N 个公钥实现锁定，该脚本至少需要得到与公钥对应的 M 个签名才可以满足解锁交易的条件。M 是使多重签名生效的签名数阈值。执行签名的成员称为公证人，而区块链矿工负责执行脚本。

数字资产转移过程如图 1 所示。主链上的一个节

点通过执行脚本发送带有 N 名公证人公钥的锁定交易，锁定交易使得该交易所包含的数字资产不再进入其他智能合约的流程。侧链矿工等待一个确认期，确保锁定交易得到足够多的确认，用以验证其真实存在。在验证锁定交易真实存在后，执行多重签名交易脚本。当其中 M 个公证人执行签名后，数字资产得以解锁并发送给侧链上的数字资产持有人。如果需要将数字资产返回给主链上的节点，则由侧链上的数字资产持有人发送锁定交易，经过同样的过程完成转移。

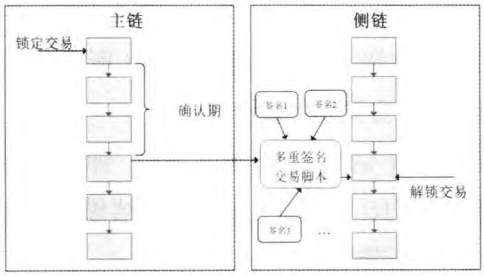

图 1 数字资产转移过程

2 系统设计与算法实现

2.1 系统结构

本文提出一种基于联盟成员信誉值创建数字资产的方案，设计并实现了一个基于联盟成员信誉值的区块链系统。系统结构如图 2 所示，分为区块链层、应用层和存储层。

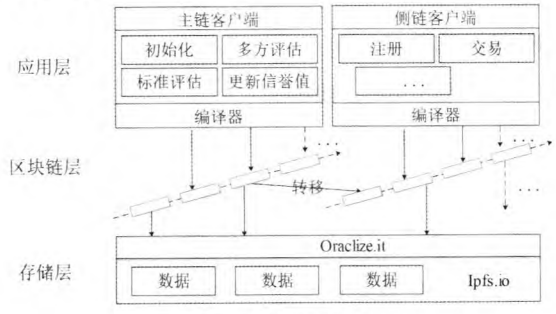

图 2 系统结构图

区块链层分为评估联盟主链和公开交易侧链。两条区块链中的矿工通过确认锁定交易和执行解锁交易完成数字资产的转移。矿工遵守共同的共识协议、通信网络协议和交易规则。矿工可以来自联盟成员或第三方矿池。例如，以太坊的区块链系统可以提供完整的矿工与交易者身份。

评估联盟主链上的应用层包含联盟成员共同开发的主链客户端和 4 个智能合约：初始化、多方评估、标准评估和更新信誉值。联盟成员通过主链客户端与智能合约交互。公开交易侧链上的应用层实现的是公开链普遍具有的注册、交易等功能。两条链上的智能合约均通过对应的区块链平台编译器执行。

存储层用于存储联盟成员提供的评估结果与标准评估结果。可通过生成元数据地址减少区块链数据存储容量的占用，具体实现方式如采用分布式文件存储系统 Ipfs.io 等。智能合约或用户可以通过 Oraclize.it 工具安全地读取并使用数据。

2.2 系统执行流程

系统执行流程如图 3 所示。从评估联盟主链的初始化智能合约开始到转移数字资产于侧链，联盟成员参与方案的 5 个步骤如下：1）初始化智能合约审核具备评估能力的节点，赋予联盟成员身份和初始信誉值；2）一名联盟成员通过多方评估智能合约发起评估事件，持有评估权限的联盟成员在同一时刻对评估对象提供各自的评估结果链接和信誉值；3）标准评估智能合约根据联盟成员各自的评估结果与信誉值计算出标准均值作为标准评估结果，存储于存储层并输出给锁定交易；4）更新信誉值智能合约根据各联盟成员的评估结果与标准评估结果的差异程度，更新各联盟成员的信誉值；5）将标准评估结果输出到公开交易侧链。

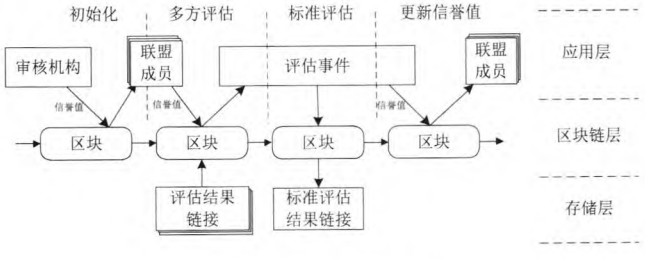

图 3 系统执行流程图

2.3 核心智能合约设计

2.3.1 基本函数说明

定义 1 交易格式 设发起者私钥为 sk_{sender}，接收

者公钥为 $pk_{receiver}$，金额为 *amount*，备注为 *notes*。在一笔交易中，发起者先以私钥解锁持有的资金，再将资金发送给接收者。这一笔交易的交易格式定义为 Sendtouser(sk_{sender}, $pk_{receiver}$, *amount*, *notes*)。

定义 2 多重签名锁定交易 以发起者的私钥解锁，包含资产对象信息，并由 N 个用户锁定的交易称为多重签名锁定交易，标记为 Sendtolock(sk_{sender}, pk_1,pk_2,⋯, pk_N, *index*)。

定义 3 多重签名赎回交易 以接收者的公钥为接收地址，包含资产对象信息，并由 M 个用户解锁的交易称为多重签名赎回交易，标记为 Sendtounlock($pk_{receiver}$, Sig_1, Sig_2,⋯,Sig_M, *index*)。

2.3.2 初始化智能合约

设参与评估事件的总人数为 n。初始化智能合约分发联盟成员（U_i）的公钥（pk_i）和私钥（sk_i），利用审核机构（Auditor）的私钥（sk_A）向满足资质条件的联盟成员赋予信誉值池中的初始信誉值（r_i）。该过程可如下表示。

for i←1 to n **do**

Sendtouser(sk_A, pk_i, r_i, null)

信誉值池中的信誉值来源于创世区块的设定。联盟成员的信誉值会在联盟成员参与一次评估事件后，根据其评估结果质量而调整。

2.3.3 多方评估智能合约

联盟成员均可通过多方评估智能合约发起评估事件来创建一笔数字资产。评估事件发起者（pk_0）可通过发布众包任务 [15] 与其他成员商定评估事件参数。评估事件参数（φ）包括参与评估事件的总人数（n）、惩罚系数（α）和恶意阈值（β）。评估事件发起者将需创建的数字资产作为评估对象，多方评估智能合约生成随机数（*random*）、事件编号（*Enum*）和评估事件的公私钥 {pk_E, sk_E}，并为参与评估事件的联盟成员分发可参与评估的权限（*right*）和事件编号。

持有权限的联盟成员在同一时刻分别给多方评估智能合约上传对评估对象的评估结果链接（$index_i$）和信誉值。多方评估智能合约依据事件编号与对应权限，收集评估结果链接和信誉值，每条评估结果链接都利用 Oraclize.it 工具读取。各联盟成员的评估结果和信誉值被输出给标准评估智能合约。

联盟成员评估结果（c_i）表示为 c_i={x_i,y_{ji}}。其中，布尔型变量 x_i 为结论性指标，表示对评估对象的结论性判断，如商品是否合格；连续型变量 y_{ji} 为描述性指标，表示对评估对象第 j 个描述项的评估结果，评估结果指标数为 m。当 i=0 时，c_0={x_0,y_{j0}} 表示标准评估结果。

多方评估智能合约算法如算法 1 所示。

算法 1 多方评估智能合约

输入：评估事件发起者 pk_0，评估事件参数 φ，联盟成员 {U_i|i=1,2,⋯,n}，评估结果链接 {$index_i$|i=1,2,⋯,n}，信誉值 {r_i|i=1,2,⋯,n}

内部输出：评估事件公私钥 {pk_E,sk_E}，事件编号 *Enum*

输出：信誉值 {r_i|i=1,2,⋯,n}，评估结果 {c_i|i=1,2,⋯,n}

```
1  if pk_0 is registered and φ is complete then
2   get Enum++;
3   {pk_E,sk_E}←keyGenerator(Enum||random);
4   for all i←1 to n
5    giveRightToMembers(U_i.right=1, Enum);
6   for all i←1 to n
7    if U_i.right=1 then
8     Sendtouser(sk_i, pk_E, r_i, index_i);
9     selectMember(U_i.right= 0);
10    c_i←readByOraclize(index_i);
11   else U_i has already assessed;
12 return c_i, r_i;
```

2.3.4 标准评估智能合约

标准评估智能合约根据收集到的评估结果给出评估对象的标准评估结果。首先，标准评估智能合约以信誉值为权重，计算结论性指标 x_i 的加权平均，取整求得标准结论性指标 x_0，见公式（1）。当联盟成

员的结论性指标与标准结论性指标有偏离时，标准评估智能合约会扣除比例为 α 的信誉值，从而求得联盟成员的临时信誉值 r_i^t，见公式（2）。扣除部分的信誉值会被标准评估智能合约发还审核机构。随后，标准评估智能合约以临时信誉值为权重，计算描述性指标 y_{ji} 的加权平均，求得标准描述性指标 y_{j0}，见公式（3）。此时标准评估结果 $c_0=\{x_0,y_{j0}\}$ 被输出到文件存储系统。最后，标准评估智能合约用评估事件私钥 sk_E 对标准评估结果链接 $index_0$ 签名，并将 $index_0$ 发送至锁定交易。该锁定交易需要所有参与联盟成员的公钥参与锁定，以保证标准评估结果不会被任何一个联盟成员单独使用。

$$x_0=\left\lfloor\frac{1}{2}+\left(\sum_{i=1}^{n}r_i x_i\Big/\sum_{i=1}^{n}r_i\right)\right\rfloor \tag{1}$$

$$r_i^t=r_i-\alpha|x_0-x_i| \tag{2}$$

$$y_{j0}=\sum_{i=1}^{n}r_i^t y_{ji}\Big/\sum_{i=1}^{n}r_i^t \tag{3}$$

标准评估智能合约算法如算法 2 所示。

算法 2 标准评估智能合约

输入：信誉值 $\{r_i|i=1,2,\cdots,n\}$，评估结果 $\{c_i|i=1,2,\cdots,n\}$，惩罚系数 α

输出：标准评估结果链接 $index_0$，临时信誉值 $\{r_i^t|i=1,2,\cdots,n\}$

1 x_0=round(average(c_i.x_i,r_i));
2 **init** r_i^t;
3 Set $r_i^t=r_i-\mathrm{Abs}(x_0-x_i)\times\alpha$;
4 **for** all $i\leftarrow$1 to n
5 Sendtouser(sk_E, pk_A, $r_i-r_i^t$,null);
6 **for** all $j\leftarrow$1 to m
7 y_{j0}=average(c_i.y_{ji},r_i^t);
8 $index_0\leftarrow$ipfsDHT(c_0);
9 Sendtolock(pk_E, pk_1, pk_2,$\cdots$,pk_n, $Sig_E(index_0)$){
10 $Scriptpk\leftarrow N<pk_1><pk_2>\cdots<pk_n>N$ OP_CHECKMULTISIG
11 Sendtouser(sk_E, $Scriptpk$, 0, $Sig_E(index_0)$)
12 }
13 **return** $index_0$, r_i^t;

2.3.5 转移数字文件

标准评估结果 $index_0$ 被标准评估智能合约发送至锁定交易后，侧链矿工开始等待一个确认期。在确定锁定交易真实存在后，矿工执行多重签名交易脚本。当脚本得到所有联盟成员的签名后，数字资产在侧链上被创建并发送给数字资产持有人（pk_{owner}）。代码如下所示：

```
Sendtounlock(pk_owner, Sig_1, Sig_2,···, Sig_n, Sig_E(index_0)){
  Scriptsk←OP_0<Sig_1><Sig_2>···<Sig_n>
  Sendtouser(Scriptsk, pk_owner, 0, Sig_E(index_0))
}
```

2.3.6 更新信誉值智能合约

更新信誉值智能合约以标准评估结果比对各联盟成员的评估结果，根据偏离程度，计算并赋予每个联盟成员新的信誉值。更新信誉值智能合约包括计算信誉值子合约和分发信誉值子合约。

1）计算信誉值子合约

计算信誉值子合约首先求得各联盟成员的描述性指标 y_{ji} 相对于 y_{j0} 的标准方差 σ_{ji}，见公式（4），并生成关于各联盟成员标准方差的二维数组，从而求得关于各联盟成员标准方差的总和 σ_y，见公式（5）。

$$\sigma_{ji}=\sqrt{|y_{j0}-y_{ji}|^2} \tag{4}$$

$$\sigma_y=\sum_{i=1}^{n}\sum_{j=1}^{m}\sigma_{ji} \tag{5}$$

接着利用公式（6）求得最终信誉值（r_i^b）。

$$r_i^b=r_i^t+r_i^t\left(\sum_{j=1}^{m}\sigma_{ji}-\frac{\sigma_y}{n}\right)\Big/\sigma_y \tag{6}$$

其中，$\left(\sum_{j=1}^{m}\sigma_{ji}-\frac{\sigma_y}{n}\right)\Big/\sigma_y$ 为临时信誉值（r_i^t）的增减比例。最终信誉值将作为下一次参加评估事件时联盟成员新的信誉值。

2）分发信誉值子合约

分发信誉值子合约计算每个联盟成员损失的信誉值与原信誉值之比，记为降低率（$Rate$）。若降低率大于恶意阈值 β（$\beta\in(0,1)$），该子合约会认为这个联盟

成员是恶意成员，冻结该成员账户，将他的最终信誉值发往信誉值池。审核机构会在冻结期满后，返还该成员最终信誉值，恢复其资格。若判断联盟成员不是恶意成员，最终信誉值则被发送给该联盟成员。

更新信誉值智能合约算法如算法 3 所示。

算法 3 更新信誉值智能合约

输入：临时信誉值 $\{r_i^t|i=1,2,\cdots,n\}$，评估结果 $\{c_i|i=1,2,\cdots,n\}$，标准评估结果 c_0，恶意阈值 β

输出：最终信誉值 $\{r_i^b|i=1,2,\cdots,n\}$

```
1  init σ_ji, σ_y, Rate;
2  for all j←1 to m, i←1 to n
3    σ_ji←standardDeviation(c_i,y_ji,c_0,y_j0);
4  σ_y←sum(σ_ji);
5  for all i←1 to n
6    Rate←calculateRate(σ_ji,σ_y);
7    if Rate>β and (x_0−x_i)=!0 then
8      Sendtouser(sk_E, pk_A, r_i^b, null);
9    else Sendtouser(sk_E, pk_i, r_i^b, null);
10 return r_i^b;
```

3 仿真实验与分析

本文利用区块链技术构建信任机制，为数字资产的创建搭建基于联盟成员信誉值的区块链系统。为验证系统运行的实用性，仿真实验在私有区块链上部署智能合约，并模拟评估事件的全部流程。实验从以太坊燃料消耗（*Gas*）和存储空间占用两个方面进行了测试和分析。

3.1 实验环境

本文实验采用 ubuntu14.04.03 系统，内存为 4 GB，处理器为 Intel Core i5 3.2 GHz；分布式文件系统采用 Ipfs.io，文件读取工具采用 Oraclize.it；区块链操作平台为以太坊开发平台，用于测试的私有区块链的区块难度设置为 0x5ffffa，部署方式为 Web3.js。

3.2 实验过程

1）以太坊燃料消耗与成员数和指标数的关系

实验测试联盟成员数 n 分别为 5,10,15,20,25 时，以太坊燃料消耗（*Gas*）随评估结果指标数 m 增长的变化。实验选取指标数为 5，10，15，20，25，30 时，5 种不同的人数参与这 6 种不同指标数的 30 组评估事件，每组进行 10 次仿真。实验从数字资产锁定交易开始，追溯每个评估事件涉及的所有交易。实验读取交易对应的合约编译文件，统计每组评估事件燃料消耗（*Gas*）的平均数量，如图 4 所示。

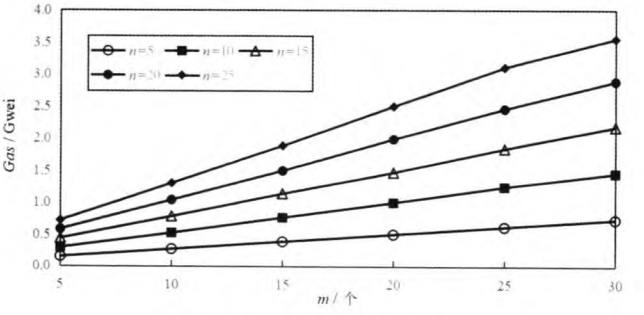

图 4 燃料消耗与成员数和指标数关系图

更新信誉值智能合约在计算信誉值时，为每一个成员的每一个指标开辟了存储空间，这需要消耗大量的燃料。而其他智能合约的燃料消耗主要与成员数呈正相关，和指标数关系不大。因此，在成员数不变的情况下，当指标数单独出现倍数增长时，更新信誉值智能合约的燃料消耗呈倍数增长，其他智能合约的燃料消耗增长则比较缓慢。这样，随着指标数的增加，评估事件的燃料消耗并不呈现倍数增长，呈现的是一条收敛的曲线。

2）存储空间占用与交易笔数的关系

评估事件中发送的交易会在区块链上确认，并占用矿工的存储空间。存储空间占用得越少，越能减轻矿工维护区块链的负担。本文选取实验中的 15000 笔交易，每隔 1000 笔交易取一个点，统计占用的存储空间。实验结果如图 5 所示。

联盟成员递交评估结果时只存储评估结果链接，没有存储完整的数字化结果以及其他不必要的信息，因此减少了存储空间占用。随着交易数量逐渐增加，存储空间占用的收敛趋势更加明显。以 25 名成员参

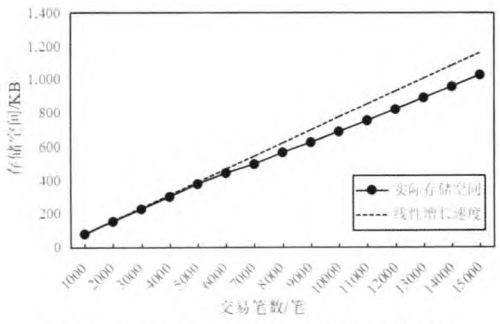

图 5 存储空间占用与交易笔数关系图

与评估为例，记载 30 个评估事件时占用区块链存储空间 216.21 KB，记载 60 个评估事件时占用存储空间 407.93 KB。可见，评估事件总数增加一倍，交易笔数也增加一倍，但是存储空间占用增加不足一倍。

3.3 实验结论

由实验可知，在一个评估事件中，更新信誉值智能合约消耗了大多数燃料。但是随着指标数和成员数的增加，以太坊燃料消耗呈收敛趋势，并未明显增加。此外，随着交易数量的增加，区块链的大小也没有明显膨胀。可见，本文系统的运行具有低成本、存储空间不易扩张等特点。

4 结束语

本文利用区块链技术构建信任机制，搭建基于联盟成员信誉值的区块链系统，以增加数字资产创建的真实性保证。但是，本文系统并不意味着用区块链技术完全取代现实中的审计环节，而是为数字资产的创建提供理论和算法上的支撑和保证。方案主要适用于评价结果主观性强、检测结果稳定性差的区块链应用场景，下一步还需提升系统性能并扩展适用范围。(责编 马珂)

参考文献：

[1] AITZHAN N Z, SVETINOVIC D. Security and Privacy in Decentralized Energy Trading through Multi-signatures, Blockchain and Anonymous Messaging Streams[J]. IEEE Transactions on Dependable and Secure Computing, 2016,PP(99):1.

[2] TAN Lei, CHEN Gang. Blockchain 2.0[M].Beijing: Publishing House of Electronics Industry,2016.

谭磊，陈刚．区块链 2.0[M]. 北京：电子工业出版社，2016.

[3] ZHAO Kuo, XING Yongheng. Security Survey of Internet of Things Driven by Block Chain Technology[J].Netinfo Security,2017(5):1-6.

赵阔，邢永恒．区块链技术驱动下的物联网安全研究综述 [J]. 信息网络安全，2017(5)：1-6.

[4] XU Xiwei, PAUTASSO C, ZHU Liming, et al. The Blockchain as a Software Connector[C]//IEEE. 2016 13th Working IEEE/IFIP Conference on Software Architecture (WICSA), April 5-8, 2016, Venice, Italy. NJ:IEEE, 2016: 182-191.

[5] IDELBERGER F, GOVERNATORI G, RIVERET R, et al. Evaluation of Logic-based Smart Contracts for Blockchain Systems[M]// RuleML.Rule Technologies. Research, Tools, and Applications. Cham: Springer, Cham, 2016: 167-183.

[6] XIE Hui, WANG Jian. Study on Block Chain Technology and Its Applications[J].Netinfo Security,2016(9):192-195.

谢辉，王健．区块链技术及其应用研究 [J]. 信息网络安全，2016(9)：192-195.

[7] TIAN Feng. An Agri-food Supply Chain Traceability System for China Based on RFID & Blockchain Technology[C]//IEEE. 2016 13th International Conference on Service Systems and Service Management (ICSSSM), June 24-26, 2016, Kunming, China. NJ:IEEE, 2016: 1-6.

[8] WEBER I, XU Xiwei, RIVERET R, et al. Untrusted Business Process Monitoring and Execution Using Blockchain[M]//BPM. Business Process Management. Cham: Springer, Cham, 2016: 329-347.

[9] BAHGA A, MADISETTI V K. Blockchain Platform for Industrial Internet of Things[J]. Journal of Software Engineering & Applications, 2016, 9(10):533-546.

[10] ALI M S, DOLUI K, ANTONELLI F. IoT Data Privacy via Blockchains and IPFS[C]//ACM. The 7th International Conference on the Internet of Things, October 22 - 25, 2017 , Linz, Austria. New York:ACM, 2017:542-563.

[11] CHRISTIDIS K, DEVETSIKIOTIS M. Blockchains and Smart Contracts for the Internet of Things[J]. IEEE Access, 2016(4): 2292-2303.

[12] HAN Xuan, LIU Yamin. Research on the Consensus Mechanisms of Blockchain Technology[J].Netinfo Security,2017(9):147-152.

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] BHARGAVAN K, DELIGNAT-LAVAUD A, FOURNET C, et al. Formal Verification of Smart Contracts[EB/OL]. http://antoine.delignat-lavaud.fr/doc/plas16.pdf,2017-12-20.

[14] KIAYIAS A, LAMPROU N, STOUKA A P. Proofs of Proofs of Work with Sublinear Complexity[EB/OL]. http://pdfs.semanticscholar.org/b722/fa7a5c993240f9adf7752fa99b6dc816a49d.pdf,2017-12-20.

[15] LI Ming, WENG Jian, YANG Anjia, et al. CrowdBC: A Blockchain-based Decentralized Framework for Crowdsourcing[EB/OL]. https://eprint.iacr.org/2017/444.pdf, 2017-12-20.