基于区块链的去中心化信贷系统及应用

王明生[1,2]，曹鹤阳[1,2]，李佩瑶[1,2]
（1. 中国科学院信息工程研究所信息安全国家重点实验室，北京 100093；2. 中国科学院大学网络空间安全学院，北京 100049）

摘 要：提出了去中心化信贷系统，并给出了其构造应用。通过扩展基于区块链的“数字货币商品”的交易结构、扩展共识协议的功能和增加特定账户的方法，来构造去中心化信贷系统。同时，将去中心化信贷系统应用到基于区块链的 PKI 增强与监督系统 IKP，从而使 IKP 系统在运行中不需要全局基金，并且通过在去中心化信贷系统中引入分层“虚拟货币商品”供应量调节机制缓解基于区块链的“数字货币商品”在“虚拟货币商品”供给量上难以调节的问题，实现精确调节“虚拟货币商品”供应量。

关键词：区块链；“数字货币商品”；信贷系统；去中心化
中图分类号：TP302
文献标识码：A
doi: 10.11959/j.issn.1000−436x.2019126

Decentralized credit system based on blockchain and its application

WANG Mingsheng[1,2], CAO Heyang[1,2], LI Peiyao[1,2]
1. State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
2. School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China

Abstract: A decentralized credit system was proposed and its construction application was given. Decentralized credit system could be constructed by expanding the transaction structure of “digital currency commodity” based on block chain, expanding the function of consensus protocol and adding specific accounts. Also, the decentralized credit system was applied to the PKI enhancement and supervision system IKP so that IKP system did not need global fund in operation. Moreover, by introducing the hierarchical “virtual currency commodity” supply adjustment mechanism in the decentralized credit system to alleviate the difficulty of regulating the “virtual currency commodity” supply of “digital currency commodity” based on block chain, the precise “virtual currency commodity” supply regulation can be achieved.

Key words: block chain, “digital currency commodity”, credit system, decentralization

1 引言

自 2008 年基于区块链技术的比特币[1]产生之后，去中心化“数字货币商品”技术及其所依托的区块链技术得到了广泛关注和迅猛发展。与此同时，大量相同类型的“数字货币商品”随之出现。区块链是一个去中心化存储结构，在基于区块链的“数字货币商品”系统中，每一个区块包含若干交易信息，系统通过共识协议实现网络节点之间的数据一致，应用密码学工具实现不可篡改性和认证性，从而实现“虚拟货币商品”系统的功能[2]。

在传统信贷系统中，银行为借贷人提供信贷服务。当借贷人进行借贷时，借贷人向银行发出借贷请求，银行对借贷请求进行响应，将货币转给借贷人同时保存借贷凭证。借贷人应按期偿还贷款并支付一定利息。

有些基于区块链的“数字货币商品”如 BalanceCoin、BFEX（Banking Future Exchange），在去中心化“数字货币商品”的基础上引入了传统

收稿日期：2019−02−14；**修回日期**：2019−06−24
通信作者：曹鹤阳，caoheyang@iie.ac.cn
基金项目：国家重点研发计划基金资助项目（No.2017YFB0802202）
Foundation Item: The National Key R&D Program of China (No.2017YFB0802202)

信贷机制，实现了传统信贷系统的功能。

然而，在传统信贷系统中，需要银行对借贷人每次的借贷请求都进行实时响应并保存借贷凭证，因此，在传统信贷系统中，提供借贷服务的银行为系统的中心[3]。

针对以上问题，本文通过扩展基于区块链的“数字货币商品”的交易结构、扩展共识协议的功能和增加特定账户来构造去中心化信贷系统。在去中心化信贷系统中，“数字货币商品”的拥有者可以成为担保人，为借贷用户提供担保，借贷用户的借贷过程不需要中心机构对借贷请求进行响应与确认，从而实现去中心化的信贷系统。

在去中心化信贷系统中，“虚拟货币商品”更加便于使用和流通。对于基于区块链的“数字货币商品”，当未持有“虚拟货币商品”的新用户需要使用“数字货币商品”，且具体需求量不定时，需要分次进行兑换。每次兑换均需要“虚拟货币商品”交易所对兑换请求进行响应。而在去中心化信贷系统中，未持有“虚拟货币商品”的新用户可以通过借贷高效快捷地使用“数字货币商品”。

“虚拟货币商品”的一个重要功能是作为价值尺度，然而，基于区块链的“数字货币商品”通常出现巨大的价值波动，而巨大的价值波动的“虚拟货币商品”显然无法作为交易的一般等价物。

针对这个问题，本文通过在去中心化信贷系统引入分层“虚拟货币商品”供应量调节机制，实现了根据经济活动对“虚拟货币量”的需求调节“虚拟货币商品”的供给量，从而强化“数字货币商品”作为价值尺度的能力。

近年来，出现了一些支持信贷功能的基于区块链的“数字货币商品”，如 BalanceCoin 通过募集“虚拟货币商品”后对借贷用户进行借贷；BFEX 通过智能合约实现匹配借款用户和贷款用户，这种方式类似于 P2P（peer-to-peer）网络信贷平台。然而以上的方式实现的信贷系统均需要中心机构，未能实现去中心化。

当前基于区块链的“数字货币商品”的功能的优化工作主要包括增加链的结构和扩展共识协议。2014 年，Back 等[4]针对“数字货币商品”系统在金融领域需要更丰富的功能的问题，引入了侧链（sidechain），其核心技术为双向锚定（two-way peg）。通过在主链（主流“数字货币商品”）上锚定不同的侧链，在侧链上实现衍生功能，比如 BTC Relay 将以太坊与比特币通过双向锚定连接起来。BTC Relay 通过使用以太坊的智能合约功能使用户在以太坊区块链上验证比特币交易。以太坊应用程序开发者可以从智能合约向 BTC Relay 进行应用程序接口（API, application program interface）调用来验证比特币的交易。多链技术是侧链的进一步扩展，它将多条链连接到一起，实现多条链上资产的转移、交易。从共识协议出发的工作主要包括 Kiayias 等[5]提出的 Ouroboros 协议，Ouroboros 协议是可证安全的基于权益证明（PoS, proof-of-stake）算法的共识协议，应用 Ouroboros 协议可以优化基于区块链的“数字货币商品”的功能。

本文的主要贡献如下。

1) 通过扩展基于区块链的“数字货币商品”的交易结构、扩展共识协议的功能和增加特定账户来构造去中心化信贷系统。

2) 基于区块链的 PKI（public key infrastructure）增强与监督系统 IKP（instant karma PKI）[2]中需要全局基金（GF, global fund），本文将去中心化信贷系统应用到 IKP 系统中，从而使 IKP 系统不需要全局基金就能运行。

3) 针对基于区块链的“数字货币商品”在“虚拟货币商品”供给量上难以调节的问题，基于去中心化信贷系统引入分层“虚拟货币商品”供应量调节机制，从而精确地实现“虚拟货币商品”供应量调节。

2 预备知识

本节将简要介绍区块链和比特币的预备知识。特别地，将详细描述共识机制、交易结构和未消费交易输出（UTXO, unspent transaction output）模型。关于比特币的更多细节见文献[6-7]。

2.1 区块链

区块链是由 Hash 连接的区块构成的链式数据结构，每个区块包含前一个区块的 Hash。区块可以记录交易、版权、财产等信息。区块链是一个公开的、去中心化的数据库，能以一种可验证和永久的方式有效地记录双方之间的交易。本文将区块链看作 P2P 网络中的去中心化账本，网络中的所有节点共同维护账本。链中的每个记录或区块都是公开的，并且能够抵抗数据的篡改。下面简要介绍区块链所应用的关键技术。

1) 数字签名

基于区块链的“数字货币商品”系统应用数字签名实现交易的认证，数字签名的公钥通常作为用户的地址，当用户发起交易时，用户使用私钥对交易信息进行签名。本文使用符号 $\mathrm{sig}_{\mathrm{A}}(m)$ 表示用户 A 使用私钥对消息 m 的签名。

2) 共识协议

区块链是 P2P 网络中的去中心化系统，因此需要一种机制来保证网络中节点维护数据的一致性，这种机制是共识协议。共识协议主要包括传统的拜占庭容错算法、工作量证明（PoW, proof-of-work）算法、PoS 算法等[8]。传统的拜占庭容错算法在安全性和去中心化方面较好，但效率较低。PoW 算法使系统达到共识的方式是每个参与共识的节点提供计算能力来尝试解决计算问题（puzzle），成功解决计算问题的节点获得记账权并创建一个新的区块，PoW 算法可以完全实现去中心化，但会造成能耗方面的巨大浪费。PoS 算法通过要求节点证明其所持股份的所有权，且系统中实体创建区块的概率与其所持股份成正比。在系统中拥有更多股份的实体更愿意维护系统的安全性，以确保他们自己的股份不会贬值，所以 PoS 算法是合理的。然而，PoS 算法在某种程度上会导致系统的中心化。其他新提出的共识机制往往是这些传统机制的结合和改进。

3) 智能合约

智能合约是当某些条件满足、系统被触发时自动运行的计算机程序。智能合约也可以作为常规用户来发送和接收事务，甚至控制其他智能合约。它们由系统的用户（或其他智能合约）创建，并存储在区块链中[9]。智能合约中的代码通常用某种高级语言编写，比如 Solidity 语言或 Go 语言。

2.2 比特币

比特币是区块链技术最重要的应用。比特币是最受欢迎的去中心化“数字货币商品”，可以在 P2P 网络上从一个用户发送到另一个用户，而不需要“中间人”。比特币使交易匿名，保护用户隐私。交易是比特币的关键组成部分，能实现比特币的主要功能，UTXO 模型在比特币中也发挥着关键作用。

1) 交易

比特币交易由一个或多个输入和一个或多个输出组成。当用户 A 要向用户 B 转入比特币时，用户 A 首先创建一个交易，该交易包括用户 A 未花费交易的交易索引、转入用户 B 的 ID、转入金额及用户 A 对交易信息的数字签名。其中交易索引通常是交易的 Hash 值。为了防止“双重花费（double spend）”攻击，交易的输入必须是未在其他交易中使用过的交易（即在 UTXO 中），且输入总额不少于输出总额，创建区块的矿工验证交易的合法性并将合法交易写入区块，此过程称为打包上链。因为在去中心化系统中没有中心来维持精确的时间同步，所以通常应用区块数（block number）作为时间度量。

2) UTXO 模型

UTXO 是所有未经过转出的转入交易所组成的集合，只有 UTXO 中的交易才能作为交易的输入[10]。当一笔交易被矿工打包到一个新的区块写入区块链后，则这笔交易的输入交易将在 UTXO 集合中删除，同时将这笔交易添加到 UTXO 集合中，这种方式结合共识协议便可防止“双重花费”。比特币使用 UTXO 模型，与之对应的还有账户/余额模型、以太坊使用账户/余额模型。不难发现，只需将一个用户在 UTXO 集合中的所有输入相加便可得到这个用户的账户余额。

2.3 PKI 系统

PKI 系统是一种遵循标准的密钥管理系统，能够为公钥密码系统的用户提供加密和数字签名所需的密钥和证书管理。PKI 系统由认证中心（CA, certificate authority）、证书库、证书作废系统、客户端证书处理系统等组成。

CA 为每个使用公开密钥的用户发放一个数字证书，数字证书的作用是证明证书中列出的用户合法拥有证书中列出的公开密钥。CA 机构的数字签名使攻击者不能伪造和篡改证书。

CA 是数字证书的签发机构，也是 PKI 的核心[11]。CA 负责签发证书、认证证书及管理已颁发证书，制定政策和具体步骤来验证、识别用户身份，并对用户证书进行签名，以确保证书持有者的身份和公钥的拥有权。

当需要验证一个证书的有效性时，验证者使用 CA 的公钥对证书上的签名进行验证，验证通过则该证书就被认为是有效的[12]。

3 去中心化信贷系统

基于区块链的“数字货币商品”系统有 2 个特

点。1) 基于区块链的“数字货币商品”系统中每个用户都能成为“虚拟货币商品”的铸造者。2)在基于区块链的“数字货币商品”系统中，“虚拟货币商品”的销毁可以是公开可验证的。事实上，如果一个账户的私钥丢失，这个账户中的“虚拟货币商品”将无法被花费，那么将“虚拟货币商品”转入这个账户，就相当于“虚拟货币商品”的销毁过程。

应用基于区块链的“数字货币商品”系统的以上特点，去中心化信贷系统的设计思想如下。

1) 在担保人的担保下，借贷人通过铸造“虚拟货币商品”实现借贷。

2) 在借贷周期内，借贷人通过销毁“虚拟货币商品”实现还贷。

3) 如果在借贷周期内借贷人未还款，发生贷款逾期，则销毁担保人的一部分“虚拟货币商品”实现债权转移。

接下来，给出去中心化信贷系统的总体描述。

在去中心化信贷系统中，担保用户通过向系统中一个具有特殊功能的账户转账来建立担保资格，担保用户为借贷用户提供担保，当具有担保资格的担保用户为借贷用户提供担保之后，借贷用户可以发起借贷交易，矿工验证担保用户的担保资格和借贷交易的有效性，并将有效借贷交易打包上链之后，借贷过程完成。之后借贷用户可以使用贷款进行支付和流通。

在贷款周期内，借贷用户通过向去中心信贷系统中一个特定的只能转入无法转出的账户转入“虚拟货币商品”实现还贷。

当出现贷款逾期，即贷款周期内借贷用户没有还贷时，矿工将担保用户的一部分“虚拟货币商品”转到无法转出的账户实现债权转移，并得到一笔费用作为发现逾期贷款的奖励。

以上为去中心化信贷系统的设计思想，值得注意的是，去中心化信贷系统的构造通过扩展区块链的共识协议实现，而这种扩展方式不依赖于特定的共识算法，可以在任何底层共识协议上实现。

接下来，定义去中心化信贷系统的交易结构和实现特殊功能的账户，然后详细给出去中心化信贷系统的构造。

3.1 交易结构与特殊账户

去中心化信贷系统由普通交易和借贷交易 2 种不同类型的交易组成。普通交易可以表示为

$$\left|y,\mathrm{A}\to\mathrm{B},v,\mathrm{sig}_{\mathrm{A}}(y,\mathrm{B},v)\right\rangle$$

其中，y 为输入交易 T_y 的交易索引，该符号表示用户 A 向用户 B 转入数量为 v 的“虚拟货币商品”。

借贷交易具有不同的结构，可表示为

$$\left\langle z,\mathrm{B},u,\mathrm{sig}_{\mathrm{A}}(z,\mathrm{B},u,\mathrm{st}),\mathrm{sig}_{\mathrm{B}}(z,u,\mathrm{st})\right|$$

其中，A 为担保用户，B 为借贷用户，u 为借贷数额，z 为输入交易 T_z 的交易索引，st 为区块数，表示担保有效期。

与比特币系统中的 UTXO 类似，定义所有未被偿还的借贷交易所组成的集合为未被偿还的借贷交易集合（UPL, unpayback loan）。

为实现去中心化信贷系统，有 2 个需要解决的主要问题：担保用户如何建立担保资格和借贷用户如何还款。针对这 2 个问题，本文在去中心化信贷系统中引入抵押账户（MA, mortgage account）和黑洞账户（BA, black-hole account）。

抵押账户为系统中的一个特殊账户，这个账户没有私钥，只有当特定情况满足时，才能发起抵押账户向其他账户转账的交易。担保用户 A 通过发起一笔普通交易 $\left|y,\mathrm{A}\to\mathrm{B},v,\mathrm{sig}_{\mathrm{A}}(y,\mathrm{B},v)\right\rangle$ 来建立担保资格，此交易被称为担保交易，定义所有有效担保交易构成的集合为有效担保交易集合（VMT, valid mortgage transaction）。当担保交易被矿工打包上链之后，担保用户 A 可以为借贷用户 B 提供担保。

在比特币系统中，如果一个账户的私钥丢失，那么该账户中的“虚拟货币商品”将无法被花费。BA 为系统中的一个特殊账户，此账户只可以转入，不可以转出，即转入 BA 的“虚拟货币商品”将无法被花费。借贷用户 B 的还贷过程为发起交易向 BA 转入“虚拟货币商品”，当这笔还贷交易被写入区块链之后，还贷过程完成，同时借贷用户 B 的借贷交易将被移出 UPL。

3.2 系统构造

去中心化信贷系统由 4 个部分组成：抵押、借贷、按期还贷和逾期贷款。下面给出系统的详细描述。

1) 抵押

对于担保用户 A，首先 A 发起普通交易 $\left|y,\mathrm{A}\to\mathrm{MA},v,\mathrm{sig}_{\mathrm{A}}(y,\mathrm{MA},v)\right\rangle$ 来建立担保资格。当该普通交易被矿工打包上链，并将其存入 VMT 中，此时担保资格建立完成。需要注意的是，此交易不

放入 UTXO 中。

担保用户 A 为借贷用户 B 提供担保，其过程为生成签名 $\mathrm{sig_A}(p,\mathrm{B},s,\mathrm{st}_i)$，其中 p 为担保交易的交易索引，s 为用户 B 的贷款额度，st_i 为担保有效期，即 B 的借贷交易只能被写入区块数小于或等于 st_i 的区块。

2) 借贷

当用户 B 进行借贷时，B 发起借贷交易

$$\left\langle p,\mathrm{B},s',\mathrm{sig_A}(p,\mathrm{B},s,\mathrm{st}_i),\mathrm{sig_B}(p,s',\mathrm{st}_i)\right|$$

矿工对借贷交易的有效性进行验证，验证算法如下。

① 验证 $\mathrm{sig_A}(p,\mathrm{B},s,\mathrm{st}_i),\mathrm{sig_B}(p,s',\mathrm{st}_i)$。

② 验证担保交易 p 在 VMT 中且 $\mathrm{st}_i>\mathrm{st}$，其中 st 为当前区块数。

③ 计算 UPL 中担保交易 p 所担保的借贷交易的借贷数额的总和 v_0，验证条件 $v_0+s'<v$。

④计算 UPL 中用户 B 所有的借贷交易的借贷数额的总和 s_0，验证条件 $s_0+s'<s$。

若以上条件均满足，返回借贷交易有效的验证结果。

矿工将有效借贷交易打包上链，同时将这个交易存入 UTXO 和 UPL 中，借贷过程完成。借贷用户 B 便可使用贷款发起普通交易向其他用户进行转账。设借贷交易的交易索引为 q，用户 B 使用借贷交易 p 向用户 C 转账的交易为

$$\left|q,\mathrm{B}\to\mathrm{C},s',\mathrm{sig_B}(p,\mathrm{C},s')\right\rangle$$

抵押与借贷过程如图 1 所示。注：在系统的实现中为避免重放攻击，应在交易的签名中加入时间戳，此处为了简洁予以省略。

3) 按期还贷

首先在系统中设置统一借贷期限的上限 r_0。设用户 B 的借贷交易 $\left\langle p,\mathrm{B},s',\mathrm{sig_A}(p,\mathrm{B},s_i,\mathrm{st}_i),\mathrm{sig_B}(p,s',\mathrm{st}_i)\right|$ 的交易索引为 q，借款交易所在区块的区块数为 st_1。

若当前区块数 $\mathrm{st}<\mathrm{st}_1+r_0$，则借款交易未逾期，否则为逾期借款交易。当用户 B 发起还款时，B 发起交易

$$\left|z,q,\mathrm{B}\to\mathrm{BA},s',\mathrm{sig_B}(y,q,\mathrm{BA},s')\right\rangle$$

矿工检查借款交易 q 是否逾期，若借款交易未逾期，则将此交易打包上链，同时将借贷交易 q 移出 UPL，还贷过程完成。

4) 逾期贷款

如果借款用户未在还贷期限内还贷，即 $\mathrm{st}\geqslant\mathrm{st}_1+r_0$，则贷款逾期。此时将由发现逾期贷款的矿工，从抵押账户进行扣款，具体过程如下。

对于逾期贷款，设借贷交易的交易索引为 q，借贷数额为 s，借贷交易的担保交易 $\left|y,\mathrm{A}\to\mathrm{MA},v,\mathrm{sig_A}(y,\mathrm{MA},v)\right\rangle$ 的交易索引为 p。矿工 C 发起普通交易为

$$\left|p,q,\mathrm{MA}\to\mathrm{MB},s_1\right\rangle$$

$$\left|p,q,\mathrm{MA}\to\mathrm{MB},s_2\right\rangle$$

其中，$s_1+s_2=s$，s_2 为矿工发现逾期贷款的奖励。逾期贷款的处理过程如图 2 所示。

当担保交易 $\left|p,\mathrm{MA}\to\mathrm{A},v',\mathrm{sig_A}(p,v')\right\rangle$ 担保的

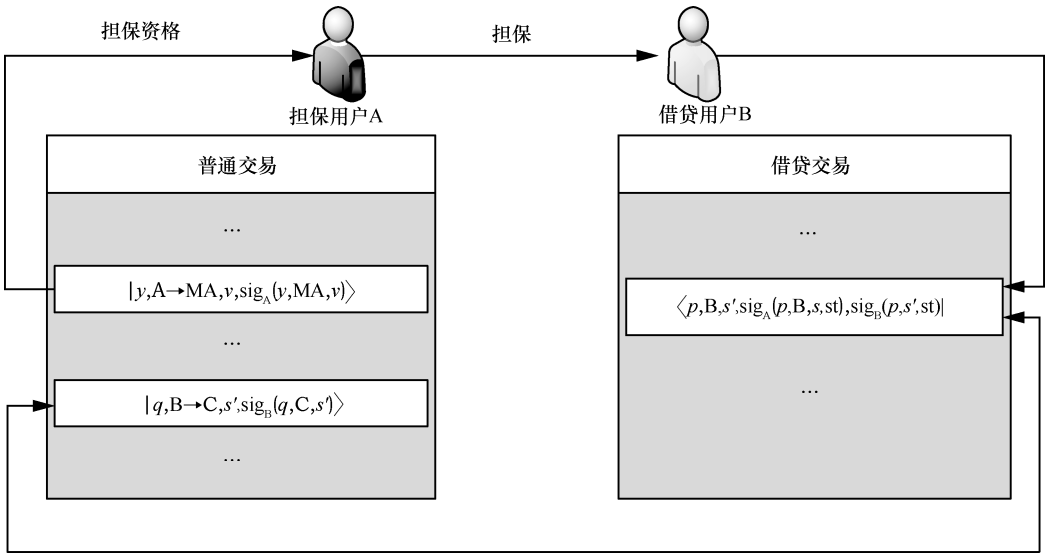


图 1　抵押与借贷过程

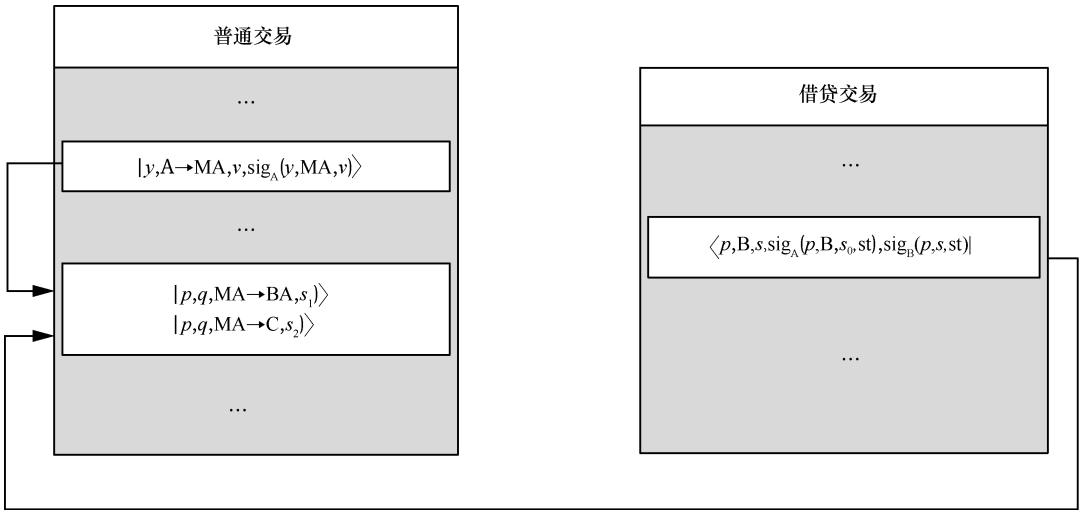


图 2　逾期贷款的处理过程

在 UPL 中的所有的借贷交易中没有未逾期交易时，担保用户可以撤回担保金，过程为发起交易

$$\left|p,\mathrm{MA}\to\mathrm{A},v',\mathrm{sig}_{\mathrm{A}}(p,v')\right\rangle$$

矿工验证以下条件。

①担保交易 p 在 UPL 中担保所有借贷交易中没有未逾期交易。

②计算担保交易 p 担保的所有逾期借贷交易借贷数额的总和 v_0，验证 $v_0=v-v'$。

若以上条件均满足，则将此交易上链，同时将担保交易移出 VMT。

综上，只有在贷款逾期时和担保用户撤回担保金时，才能发起从 MA 转出的交易。

以上为去中心化信贷系统的详细描述，在实现时，还有许多实现细节需要补充。

在系统中，担保用户为借贷用户提供担保，借贷用户借贷的计费规则由担保用户制定，担保用户可将计费规则通过智能合约写入区块链中，通过调用智能合约来计算借贷用户所需向担保用户支付的费用。

对于担保交易 $\left|y,\mathrm{A}\to\mathrm{MA},v,\mathrm{sig}_{\mathrm{A}}(y,\mathrm{MA},v)\right\rangle$，在系统中其在 UPL 中所担保的所有借贷交易的借贷数额的总和 v_0 不能大于 v。若在某一时间段内 v_0 与 v 相等，则会出现在这个时间段内这笔担保交易所担保的借贷用户无法进行借贷。所以担保用户需要通过设置合理借贷计费规则来减少这种情况的发生。计费规则可以通过智能合约部署在区块链上，借贷用户调用智能合约就能计算出贷款所需支付的费用。

对于逾期贷款，担保用户的一部分担保金被转入黑洞账户，从而发生了债权转移，逾期的借贷交易将作为担保用户的债权凭证。

4　去中心化信贷系统在 IKP 系统中的应用

4.1　IKP 系统

IKP 系统由 Matsumoto 等[2]提出，它是一种基于区块链的 PKI 增强机制，通过智能合约对证书 CA 的错误行为自动响应，并为那些帮助检测错误行为的人提供激励。IKP 系统的去中心化和智能合约系统允许任何人公开地参与对 CA 行为的检测。IKP 系统的总体架构如图 3 所示。

IKP 是标准 TLS（tansport layer security）体系结构的扩展，它引入了 2 个新实体：IKP 权威机构和探测器。IKP 权威机构负责 IKP 的核心功能，具体包括维护 CA 的信息、存储域证书策略（DCP, domain certificate policie）和响应策略（RP, reaction policie）。DCP 和 RP 由智能合约实现，域证书策略由域提出，可以用于计算性地确定一个给定的证书对某一个域是否被授权；RP 由 CA 提出，在一个未授权的证书被发现时自动触发。IKP 权威机构中还有一个全局基金，负责响应 IKP 系统中的赔偿。探测器监视 CA 颁发的证书，并报告它们认为未经授权的任何证书，如果报告是正确的，它们将获得金钱的奖励。系统中的任何实体都可以作为探测器，包括 CA、域和客户端。

IKP 中的操作包括如下几项。

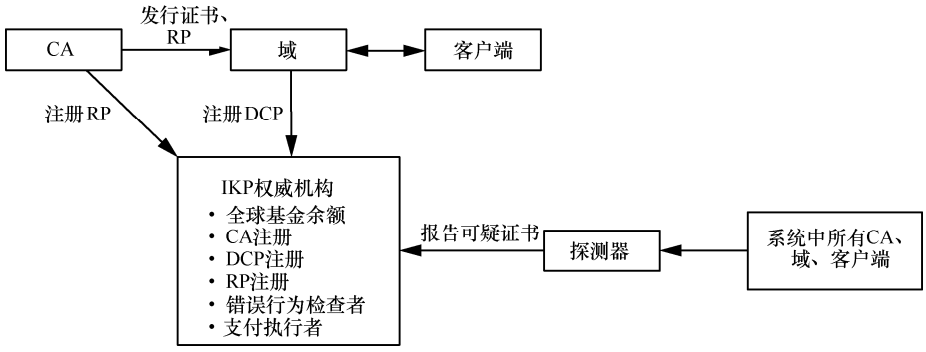


图 3　IKP 的总体架构

1) CA 注册：CA 在 IKP 权威机构中注册自己的信息，包括标识符、金融账户信息、一个或多个公钥和一个更新策略。

2) 域注册：域向 IKP 权威机构注册 DCP。具体地说，域注册其域名系统（DNS, domain name system）名称、一个或多个公钥、金融账户信息和一个检查程序，该检查程序决定给定的证书对这个域是否授权。

3) 发行 RP：一个注册过的域与一个注册过的 CA 商谈 RP 的条款，包括域名、CA 标识符、有效期、对域的 DCP 的引用，以及包含响应 CA 不当行为所触发的支付的响应程序。域向 CA 支付费用来购买一个 RP，保障自己不受未授权证书的危害，一旦购买过 RP 的域接收到不符合自己的 DCP 的证书，这个证书将被认定为未授权证书，这会触发 RP，启动相应的赔偿行为。

4) 发行证书：CA 向域发送证书。

5) 错误行为报告：探测器向 IKP 权威机构发送 CA 错误行为的证据，同时附上自己的账户信息用来接收奖励。为了防止探测器不断产生错误行为报告，每发送一个错误报告，就要支付报告费。

6) 响应：IKP 权威机构收到报告后认定这个报告是否正确，如果报告正确，那么 CA 确实有不符合相应域的 DCP 的错误行为，则触发该域的 RP 对域进行赔偿，该 RP 执行指定的交易，向相应的 CA、域、探测器支付指定好的金额。

值得注意的是，CA 在注册时会向全局基金支付一笔费用，相当于它的保证金，之后 IKP 系统中的所有转账交易都是转入全局基金或从全局基金转出的，这样就需要全局基金账户的管理者对 IKP 系统中的请求进行实时响应。

4.2　在 IKP 系统中使用去中心化信贷系统

接下来，将去中心化信贷系统引入 IKP 系统中，从而实现不需要全局基金账户的 IKP 系统。

1)设 CA 为系统中 CA 的账户，初始化 RP 的过程为 CA 发起担保交易

$$\left|y,\mathrm{CA}\to\mathrm{MA},v,\mathrm{sig}_{\mathrm{A}}(y,\mathrm{MA},v)\right\rangle$$

设担保交易的交易索引为 p，系统中购买 RP 的域为 $\mathrm{B}_1,\mathrm{B}_2,\cdots,\mathrm{B}_n$。

2)当担保交易被矿工打包上链之后，CA 为购买 RP 的域 $\mathrm{B}_1,\mathrm{B}_2,\cdots,\mathrm{B}_n$ 生成 n 个签名 $\mathrm{sig}_{\mathrm{A}}(p,\mathrm{B}_i,s_i,\mathrm{st}_i)$，$i=1,2,\cdots,n$。其中，$s_i$ 为 DCP 所确定的赔偿额度，st_i 为 RP 的有效期。

3) 当探测器 D 发现 CA 的错误行为时，将错误行为报告给 IKP 权威机构，IKP 权威机构对错误行为进行认定，生成错误行为证据 w，并对证据签名。然后将 w 和 $\mathrm{sig}_{\mathrm{IKP}}(w)$ 发送给 $\mathrm{B}_1,\mathrm{B}_2,\cdots,\mathrm{B}_n$。

4) B_i 使用证据 w 生成借贷交易

$$\left\langle p,w,\mathrm{B}_i,s_i,\mathrm{sig}_{\mathrm{IKP}}(w),\mathrm{sig}_{\mathrm{A}}(p,\mathrm{B},s_i,\mathrm{st}_i)\right|$$

矿工对借贷交易的有效性进行验证，验证算法如下。

① 验证签名 $\mathrm{sig}_{\mathrm{A}}(p,\mathrm{B},s_i,\mathrm{st}_i)$ 和 $\mathrm{sig}_{\mathrm{IKP}}(w)$。

② 验证担保交易 p 在 VMT 中且 $\mathrm{st}_i>\mathrm{st}$，其中 st 为当前区块数。

若以上条件均满足，返回借贷交易有效的验证结果。矿工将有效借贷交易打包上链完成赔偿过程。

5) 通过去中心化信贷系统中的逾期贷款过程完成 CA 对域的赔偿。

6) 若 CA 在 RP 有效期内未出现错误行为，则可通过交易 $\left|p,\mathrm{MA}\to\mathrm{CA},v,\mathrm{sig}_{\mathrm{A}}(p,v)\right\rangle$ 撤回担保金。

5　分层“虚拟货币商品”供应量调节机制

5.1　基于区块链的“数字货币商品”所存在的问题

以比特币为代表的基于区块链的“数字货币商

品”的一个显著特征就是“虚拟货币商品”总量固定，系统通过调节共识算法的参数（如工作量证明中的难度值）来调节一个时间段内的“虚拟货币商品”供应量，但是这样的调节机制会带来 2 个问题，具体如下。

1) 如果一种“虚拟货币商品”的总量固定，从长期的角度看一定会带来通货紧缩[13]。因为“虚拟货币商品”总量恒定，系统中的用户会更倾向于将这样的“虚拟货币商品”用作储值工具，而不是流通手段，会导致市场上流通的“虚拟货币商品”减少，进一步导致通货紧缩。而“虚拟货币商品”制度建立的初衷并不是让持有“虚拟货币商品”的人变得更加富有，而是让交易和流通等经济活动更加便利。

2) 通过调节共识算法参数来调节一段时间内新“虚拟货币商品”的产生量很难实现精确和有效[14]。以比特币为例，比特币需要根据所有参与的矿工的计算能力来调节工作量证明的难度值，首先，矿工的计算能力的估计并不能做到完全准确，其次，这样的调节方式对“虚拟货币商品”供应量的影响具有一定的滞后性。

针对现有“加密货币商品”系统中这样的问题，接下来，在去中心化信贷系统引入分层“虚拟货币商品”供应量调节机制。

5.2 分层“虚拟货币商品”供应量调节机制

去中心化信贷系统模型中，引入第一级调节用户 $\{\mathrm{A}_1,\mathrm{A}_2,\cdots,\mathrm{A}_i\}$，对应现实经济系统中的政府机构。第二级调节用户 $\{\mathrm{B}_1,\mathrm{B}_2,\cdots,\mathrm{B}_s\}$，对应现实经济系统中的各大银行。

在去中心化信贷系统中，担保交易所担保的借贷交易的借贷额度的总和小于或等于担保交易转入抵押账户 MA 的额度。分层“虚拟货币商品”供应量调节机制通过允许第一级调节用户超额担保，第二级调节用户的借贷无时间期限来实现“虚拟货币商品”供应量的增加。即当系统需要增加“虚拟货币商品”供应量时，首先确定一组系统参数 $\big((s_1,v_1),(s_2,v_2),\cdots,(s_t,v_t)\big)$，在实际应用中，这组参数可以由经济系统中的变量（如生产总量、消费量等）来确定。其中 (s_i,v_i) 表示用户 A_i 发起的数额为 s_i 的担保交易可以担保第二级调节用户 $\{\mathrm{B}_1,\mathrm{B}_2,\cdots,\mathrm{B}_s\}$ 发起总额小于 s_i+v_i 的借贷交易，$\sum_{i=1}^{t}v_i$ 表示系统通过分层调节机制增加的货币量的最大值。设 A_i 的担保交易 $|y,\mathrm{A}_i\to\mathrm{MA},v,\mathrm{sig}_{\mathrm{A}}(y,\mathrm{MA},s_i)\rangle$ 的交易索引为 p，其中 A_i 为 B_j 生成签名 $\mathrm{sig}_{\mathrm{A}}(p,\mathrm{B}_j,u_j)$。

B_j 发起借贷交易

$$\left\langle p,\mathrm{B}_j,u,\mathrm{sig}_{\mathrm{A}_i}(p,\mathrm{B},u_j),\mathrm{sig}_{\mathrm{B}_j}(p,u)\right|$$

矿工对借贷交易的有效性进行验证，验证算法如下。

1) 验证签名 $\mathrm{sig}_{\mathrm{A}_i}(p,\mathrm{B},u_j)$ 和 $\mathrm{sig}_{\mathrm{B}_j}(p,u)$。

2) 验证担保交易 p 在 VMT 中且计算 UPL 中担保交易 p 所担保的借贷交易的借贷数额的总和 v_0，验证条件 $v_0+u<s_i+v_i$。

3)计算UPL中用户B所有的借贷交易的借贷数额的总和 s_0，验证条件 $s_0+u<u_j$。

若以上条件均满足，返回借贷交易有效。

不难验证，系统通过分级调节机制所增加的“虚拟货币商品”供应量由 $\{\mathrm{A}_1,\mathrm{A}_2,\cdots,\mathrm{A}_t\}$ 和 $\{\mathrm{B}_1,\mathrm{B}_2,\cdots,\mathrm{B}_s\}$ 共同决定，且总量小于或等于 $\sum_{i=1}^{t}v_i$。

6 结束语

本文提出了去中心化信贷系统，并给出了其构造应用。首先，通过扩展基于区块链的“数字货币商品”的交易结构，引入特殊账户并扩展共识协议实现了去中心化信贷系统，实现“虚拟货币商品”的持有者可以为借贷用户提供担保，借贷用户可以通过借贷交易使用“虚拟货币商品”进行交易，且借贷用户的还贷过程以及贷款逾期均能通过协议处理，从而使“数字货币商品”作为流通手段更加高效便捷。

对于基于区块链的 PKI 增强机制 IKP 系统，系统中的所有转账交易都是转入全局基金或从全局基金转出的，这样就需要全局基金账户的管理者对 IKP 系统中的请求进行实时响应。本文通过将去中心化信贷系统引入 IKP 系统，实现 IKP 系统在使用时不需要全局基金。针对基于区块链的“数字货币商品”的价格浮动剧烈和“虚拟货币商品”供应量不易控制的问题，本文在去中心化信贷系统中引入分层调节机制，实现对“虚拟货币商品”供应量的调节。

对于去中心化信贷系统，其中还有许多实现细节部分需要进一步确定与优化，比如担保用户提供担保的费用设置，借贷用户的信用评估方法。另外，

可将普通交易与借贷交易通过侧链技术分别放入 2 条区块链中，从而提高交易的效率。

参考文献：

[1] ELBAHRAWY A, ALESSANDRETTI L, KANDLER A, et al. Evolutionary dynamics of the cryptocurrency market[J]. Royal Society Open Science, 2017, 4(11):170623.

[2] MATSUMOTO S, REISCHUK R M. IKP: turning a PKI around with decentralized automated incentives[C]//2017 IEEE Symposium on Security and Privacy. IEEE, 2017:410-426.

[3] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[J]. 2008: 1-9.

[4] BACK A, CORALLO M, DASHJR L, et al. Enabling blockchain innovations with pegged sidechains[R]. (2014-10) [2019−02−14].

[5] KIAYIAS A, RUSSELL A, DAVID B, et al. Ouroboros: a provably secure proof-of-stake blockchain protocol[C]//International Cryptology Conference. 2017: 357-388.

[6] NARAYANAN A, BONNEAU J, FELTEN E, et al. Bitcoin and cryptocurrency technologies: a comprehensive introduction[M]. Princeton: Princeton University Press,2016.

[7] KARAME G. On the security and scalability of bitcoin's blockchain[C]//The 2016 ACM SIGSAC conference on computer and communications security. ACM, 2016: 1861-1862.

[8] RUFFING T, MORENO-SANCHEZ P, KATE A. Coinshuffle: practical decentralized coin mixing for bitcoin[C]//European Symposium on Research in Computer Security. Springer, 2014: 345-364.

[9] EYAL I. Blockchain technology: transforming libertarian cryptocurrency dreams to finance and banking realities[J]. Computer, 2017, 50(9): 38-49.

[10] STOSIC D, STOSIC D, LUDERMIR T B, et al. Nonextensive triplets in cryptocurrency exchanges[J]. Physica A Statistical Mechanics & Its Applications, 2018(505): 1069-1074.

[11] GARAY J, KIAYIAS A, LEONARDOS N. The bitcoin backbone protocol: analysis and applications[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, 2015: 281-310.

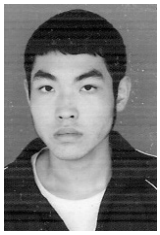
[12] GARAY J A, KIAYIAS A, LEONARDOS N, et al. Bootstrapping the blockchain, with applications to consensus and fast PKI set-up[C]//IACR International Workshop on Public Key Cryptography. Springer, 2018: 465-495.

[13] EYAL I, GENCER A E, SIRER E G, et al. Bitcoin-ng: a scalable blockchain protocol[C]//13th USENIX Symposium on Networked Systems Design and Implementation. USENIX, 2016: 45-59.

[14] SWAN M. Blockchain: blueprint for a new economy[M]//SWAN M. Blockchain: Blueprint for A New Economy. Sebastopol: O'Reilly, 2015.

[作者简介]

王明生（1967− ），男，四川遂宁人，博士，中国科学院信息工程研究所研究员、博士生导师，主要研究方向为轻量密码学、大数据密码和密码相关的困难问题等。



曹鹤阳（1993− ），男，河北承德人，中国科学院信息工程研究所硕士生，主要研究方向为密码学、信息安全。

李佩瑶（1994− ），女，河南焦作人，中国科学院信息工程研究所硕士生，主要研究方向为密码学、区块链。