DOI:10.16644/j.cnki.cn33-1094/tp.2018.01.006

基于Hyperledger的自交易共享平台解决方案*

陈 德[1]，姜新旺[1,2]，王艳霞[2]，马永进[2]

(1. 浙江师范大学经济与管理学院，浙江 金华 321004；2. 区块链实验室(浙江师范大学))

摘 要：提出采用Hyperledger超级账本，对网络节点数据从采集到自交易的应用场景及业务逻辑进行分析建模，给出节点及其数据的可信验证方法，构建一个以区块链及智能合约为基础的去中心化的自交易共享平台解决方案。该方案可用于实现低成本网络节点数据的自主管理和商品资产化的增值服务，从而衍生出新型的商业形态。

关键词：超级账本；区块链；智能合约；自交易共享平台

中图分类号：R197.1 文献标志码：A 文章编号：1006-8228(2018)01-20-03

Building a shared discretionary trading platform with Hyperledger

Chen De[1], Jiang Xinwang[1,2], Wang Yanxia[2], Ma Yongjin[2]

(*1. College of Economics and Management, Zhejiang Normal University, Jinhua, Zhejiang 321004, China;*
2. Blockchain Laboratory(Zhejiang Normal University))

Abstract: This paper introduces Hyperledger technology. The application scenarios and business logic of discretionary trading are analyzed and modeled, the trusted verification method for the node and its data is given, and a scheme of shared discretionary trading platform with blockchain technology and smart contract is put forward. The scheme can be used to realize the low cost self management of network node data and value-added service of commodity assets, and thus derive a new commercial form.

Key words: Hyperledger; block chain; smart contract; shared discretionary trading platform

0 引言

人类最原始交易是物物交换，随后经历法币、信用卡交易等阶段。目前，互联网的支付方式是一种基于第三方信用背书的电子支付(如：支付宝等)，存在第三方中介的信任问题，根源在于，基于TCP/IP的互联网只是解决了点对点可靠、近乎零成本的信息传递，而非价值传递，其应用模式只是在数据传递这条技术主线上演变。互联网金融作为金融创新模式，要想真正实现健康可持续发展，面临着网络技术漏洞、消费者权益保护法律缺失、金融监管体制不健全、信用体系不完善、消费者维权难等一系列问题[1]。

基于密码学原理的区块链，是一种去中心、去信任、集体维护的分布式账本技术[2]。它由一串使用密码学产生的数据区块有序链接而成，无需信任单个节点，依靠共识机制确保交易的真实和不可逆，可实现方便快捷、安全可靠、近乎零成本的价值传递，从而构建不同于以往人类社会的“信任”生态的价值互联网，建立了去中心化的价值体系，其核心特征是实现资金、合约、数字化资产等价值传递和交易[3]。

超级账本Hyperledger汇集金融、银行、物联网、供应链、制造等各界开发人员心血，目的是为了打造一个跨领域的区块链应用[4]。本文采用Hyperledger Fabric开源项目，提出一种从数据采集到自交易的应用场景解决方案，方案仅限交易对象提供实时数据，交易双方通过合约实现灵活交易，交易达成后，允许买方主动读取(或被动收听)特定的节点数据；卖方可以对节点的私有钱包进行资金归集等操作。

收稿日期：2017-10-18

*基金项目：国家自然科学基金(61272007)

作者简介：陈德(1992-)，男，浙江金华人，硕士研究生，主要研究方向：互联网金融。

通讯作者：马永进(1976-)，男，副教授，硕士生导师，主要研究方向：区块链技术。

1 基于 Hyperledger 的开发环境[5]

1.1 Hyperledger 简介

超级账本 Hyperledger 是 Linux 基金会于 2015 年发起的推进区块链数字技术和交易验证的开源项目，30 家初始成员（包括 IBM 等）共同宣告 Hyperledger 项目成立。由于其点对点网络的特性，分布式账本技术是完全共享、透明和去中心化的，非常适合于在金融行业应用。其中 Fabric 项目是目前比较活跃的一个开源项目，在 Hyperledger Fabric 基础上又衍生出一些其他相关的应用项目。Fabric 是区块链技术的实现，比特币可以作为一种简单的应用在 Fabric 基础上构建。Fabric 采用了模块化的构架，允许不同的组件在实现协议的基础上即插即用。可以使用强大的容器技术来运行主流编程语言以进行智能合约的开发。Fabric 项目的构架由成员服务（Membership）、区块链服务（Blockchain）和链码服务（Chaincode）三个主要类别构成。Hyperledger 具有身份识别与可审核性、私下交易及保密合约、用户可自行选择共识算法、能够通过主流编程语言编写链上代码 chaincode（也称：智能合约）、性能绩效以及可扩展性等特点。

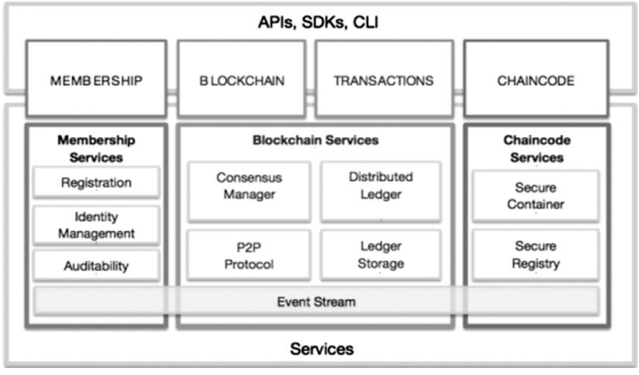

图 1 Hyperledger 架构图

1.2 搭建开发环境

在区块链应用项目研发中，共识算法的研究和改进十分重要。因此，基于 Hyperledger 的开发环境，不仅可供企业级应用项目的编程开发，而且可用于相关共识算法、智能合约等内容的性能分析测试。开发环境的技术路线是在 Linux 系统下搭建测试环境，构建测试网络，分析共识源码，测试算法效率。搭建的工作步骤如下。

步骤 1：在 Linux 系统下搭建测试环境。根据官方网站给出的 4 个验证节点的网络环境搭建方案，虚拟机内利用 Docker 安装测试环境。

步骤 2：构建测试网络。在一台 PC 上安装多个 docker 以承载多个验证节点；在多台 PC 上安装多个 docker，实现 docker 之间通讯，以扩充网络规模。

步骤 3：查看共识模块，分析源码。分析实用拜占庭 PBFT 算法源码，了解共识代码的书写规范格式；找到相关事件接口。

步骤 4：确定共识模块的启动接口和共识事件流程。找到启动共识算法接口函数；跟踪该函数了解共识事件流程；找到系统中所有对于共识算法参数设置变量及相关参数。

步骤 5：更改原有 PBFT 共识代码，更换并测试共识算法的有效性。

2 自交易业务逻辑

目前互联网金融平台是一种中心化的组织架构，采用基于第三方信用背书的交易模式，不仅交易成本高，而且容易出现信任危机等交易纠纷。在一个去中心化、去信任的分布式环境中，因为没有传统的交易中心环节，任何人在任何时间任何地点都可以发起交易，实现了自主 C2C 交易，区块链的共识算法保证了交易流程的不可抵赖性、各种交易模型的安全设置使得安全性大大提高，整个交易过程操作简单，无技术门槛，交易成本低。

本文提出建立一个基于区块链的网络节点数据自交易共享平台，利用 P2P 支付奖励机制，鼓励数据拥有者开放分享数据，实现节点数据自盈利。

平台运行机制如下：

⑴ 软件运行在多个节点，以 P2P 方式通信，一个节点数据的变化会通知同步到其他所有节点；

⑵ 在通信过程中必须验证其真实性，验证机制为共识算法；

⑶ 采用代币对算力的奖励；

⑷ 根据一段时间内交易的信息计算 hash 值，打上时间戳，成为链中的一个区块，计算 hash 值通过特定机制由某个节点完成（即该节点提供算力），并给予奖励；

⑸ 如果需要修改交易信息，必须得到所有算力的 50%以上的认可；

⑹ 通过这种运行机制，解决了认证、存储、防攻击三个问题。

自交易平台的业务流程如下：

⑴ 区块链保存交易信息，购买方自行保存数据，出售方提供数据的访问接口及特定的访问机制；

⑵ 用户的注册本质是私钥的生成；

⑶ 目前仅考虑实时数据的交易；

⑷ 合约应由发起方决定合约内容，如传节点类型、数量、时长等；

⑸ 交易时先锁定交易金额，然后按日转账到对应的传感器账户；

⑹ 平台必须考虑节点及其数据的真实性，以及运行状态。

自交易业务流程如图2所示，其中角色分为两类：一类是网络节点，其私有钱包由owner管理；另一类是普通用户。在本文，节点主要以卖方身份出现，普通用户以买方出现。

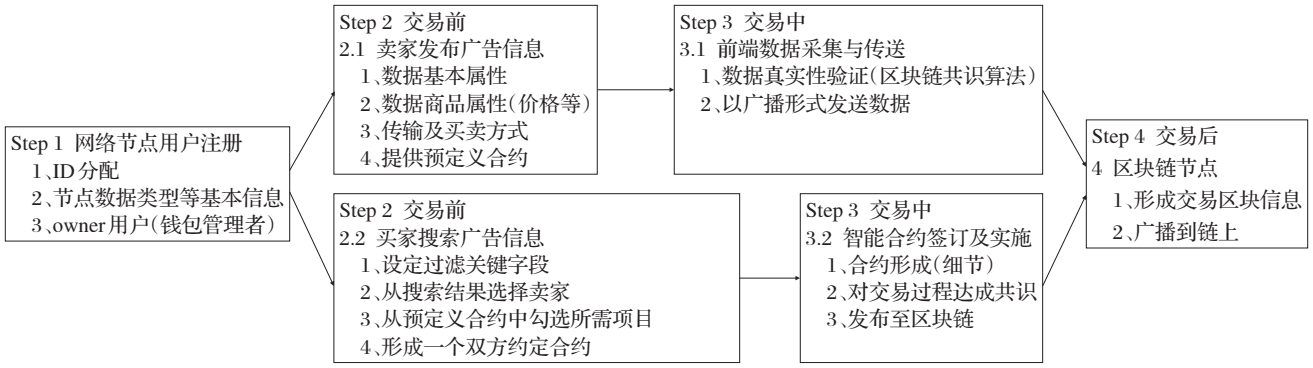

图2 自交易业务流程

3 节点及其数据的可信验证

在去中心化条件下，网络节点数据涉及两个方面：一是如何证明节点用户真实可信；二是如何验证实时数据真实可靠。在去中心化条件下，让节点数据卖方自己证明自己真实可信，理论上相当于程序正确性证明，相当于图灵机的停机问题，而已知图灵机停机问题是不可判定的。尽管如此，在实际应用中，可以为网络节点及其数据的真实性给出定义或制定相关标准，使得买方用户可以凭借这些标准来自行判定节点数据的真实性。如此，节点数据是否“正确”的理解可以有以下四个层次：

⑴ 节点数据中不含明显低级的错误数据；

⑵ 节点对于几组探测需求能够得出满足要求的数据；

⑶ 节点对于精选、典型苛刻且带有刁难性的几组探测要求能输出满足要求的数据；

⑷ 节点对于一切合法的探测要求都能得出满足要求的数据。

通常以第⑶层意义上的正确性作为衡量一个节点提供数据是否真实的标准。根据第⑶层定义的标准，为了完成对节点数据正确的验证，在不引入第三方的情况下，可采取如下三种可能的方法。

方法1：仅由交易系统来验证节点数据的正确性。若由交易系统验证节点数据正确性，则当节点用户注册时，由系统根据节点用户的类型、特征和作用等，自动产生上述标准⑴–⑶的要求，根据节点返回的结果与系统自身理论上的结果进行比较，如若一致，则证明该节点用户是真实、可信的，准予注册；否则不允许注册。

方法2：仅由数据买方用户来验证节点数据的正确性。若由数据买方用户来验证节点数据正确性，则节点用户注册时，交易系统并不验证其真实性，而当买方用户欲购买节点用户数据时，由买方用户根据节点用户类型和作用，发出如上述标准⑴–⑶中要求，并根据节点返回的结果与客户自身理论分析的结果进行比较，如若一致，则该用户认为该节点用户是真实可信的，可以进行购买；否则不可信不产生交易。

方法3：先由交易系统验证再由普通用户自行选择验证。该方案是结合上述两种方案，进一步增强了可信性，首先当节点用户注册时由系统验证，在一定程度上保障了注册节点用户的真实性，而当买方用户的再次验证，则可进一步保障该节点用户的可信性。

4 结束语

本文通过对网络节点及其数据自交易业务逻辑进行分析建模，提出采用Hyperledger超级账本，给出了网络节点及其数据的可信验证方法，构建一个去中心化的自交易平台解决方案，方案中的区块链只记录

（下转第26页）

⑶ 推进垂直化和细分化。由于每个产业的供应链模式，盈利模式，资金需求的强弱、周期都是不同的，因此供应链金融应用于不同的行业，必然催生出不同的行业特征，这将促使供应链金融平台向更垂直细分、更精准、更专业的方向发展。以服装行业为例，厂商门店多、供应商多，产品更新快，去库存需求强烈；融资主体散、资金需求短平快、安全性相对较差、收益较高；钢贸行业为例，资金需求较大应收账款额度大，利润低，年化收益率不高，安全性较高，因此，各供应链金融参与主体需要根据不同行业、不同企业的具体需求来为其量身定做金融服务，提供更加灵活和个性化的供应链融资产品。可以预见，各供应链金融参与主体只有不断深耕各自所经营的一条或几条产业链，在充分了解行业属性和特征的基础上，结合自身的专业分析与研判能力，才能为各垂直细分供应链上的企业提供个性化的供应链金融产品服务。

5 结束语

本文阐述了我国供应链金融发展的现状，剖析存在的主要问题，对互联网背景下供应链金融如何创新和发展提出了思路。供应链金融是商业银行转型的重要领域，是银行对公业务的重要产品，是服务企业客户的重要模式，宏观上，可以推动产业链升级，服务实体经济；中观上，可以推动金融创新，促进产融结合；微观上，可以推动银行经营转型，夯实业务基础。供应链金融需不断创新求变，探索更多的新模式、新市场、新领域，使得金融能真正服务于整个供应链的各类主体并推动商业生态的发展。

参考文献**(References):**

[1] 网贷天眼研究院．互联网+供应链金融创新模式[M]．中国铁道出版社，2017．

[2] 何丹，陈酋．我国供应链融资的现状分析及发展展望[J]．中国市场，2016.32:51-52

[3] 吴琼．供应链金融的发展现状及问题分析[J]．中国管理信息化，2016.2:135-136

[4] 李德莉，周永强．我国汽车产业线上供应链金融现状与发展分析[J]．中国市场，2016.19:40-41

[5] 王泰川．互联网+时代的商业银行变革之道[J]．现代商业银行导刊，2015.8(344):17-19

(上接第22页)

通过合约实现的交易细节，达成交易合约后，只为给购买者提供节点数据的访问权限或者将数据广播给购买者，至于购买者什么时候读取或者使用数据，是购买者自己的事情，与交易平台无关。

随着物联网的发展，更多智能设备及产品实现入网互联，每个物体都将拥有惟一数字身份识别码，在万物互联的体系中，平台解决方案可用于实现低成本网络节点数据的自主管理和商品资产化的增值服务，从而衍生出新型的商业形态，如：金融服务和保险、新制造业和零售、智慧城市与交通、智慧家居和能源、环境检测与保护、个性化服务、共享经济等。

参考文献**(References):**

[1] 邵燕．互联网金融交易中的消费者风险及对策[J]．现代经济探讨，2016.4:39-43

[2] 郭艳，王立荣，韩燕．金融市场中的区块链技术：场景应用与价值展望[J]．技术经济，2017.7:110-116

[3] 温晓桦．区块链-金融场景应用[J]．金融博览(财富)，2016.11:38-41

[4] 超级账本 Fabric 的架构与设计[EB/OL].2017 [2017-9-7]. http://blog.csdn.net/

[5] Hyperledger[EB/OL]. 2017[2017-01-17]. https://www.hyperledger.org/