软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software, [doi: 10.13328/j.cnki.jos.000000]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

异构联盟系统中基于二层区块链的用户信任协商模型

杨 敏[1], 张仕斌[1], 张 航[1], 刘宁[1], 黄圆圆[1]

[1](成都信息工程大学 网络空间安全学院, 四川 成都 610200)

通讯作者: 张仕斌, E-mail: cuitzsb@cuit.edu.cn

摘 要: 为打破传统孤立、分散的系统形成的“信息孤岛”效应，确保异构联盟系统中用户相关信息的可信性和安全性，本文提出了异构联盟系统中一种基于二层区块链的用户信任协商模型。该模型借助于区块链技术对用户行为数据进行防篡改保护，形成用户行为数据区块链（即第一层区块链）；以这些行为数据为基础，计算出用户的信任值，形成用户信任区块链（即第二层区块链）。通过仿真实验及安全性分析，若存在恶意用户以及恶意联盟系统，通过区块链的特征均能够被检测。表明该模型能实现用户行为、信任值不可篡改以及信任信息在联盟系统成员间协商。

关键词: 异构联盟系统；二层区块链；信任协商；可信评估

中图法分类号: TP311

User Trust Negotiation Model Based on Two-layer Blockchain in Heterogeneous Alliance System

Yang Min1, Zhang Shibin1, Zhang Hang1, Liu Ning1, Huang Yuanyuan1

[1](School of Cyber-Security, Chengdu University of Information Technology,Chengdu 610200,China;)

Abstract: In order to break the 'information island' effect formed by traditional isolated and decentralized systems, and ensure the credibility and security of user-related information in heterogeneous alliance systems, an alliance system user trust negotiation model based on two-layer blockchain is proposed. The model uses the blockchain technology to protect the user behavior data from tampering, and forms a user behavior data blockchain (ie, the first layer of blockchain). Based on these behavioral data, the user's trust value can be calculated to form a user trust blockchain (ie, the second layer of blockchain). Through simulation experiments and security analysis, it demonstrates that the user behavior data and trust value cannot be falsified through the proposed model, as well as the related information can be safely shared in the heterogeneous alliance system.

Key words: heterogeneous alliance systems; two-layer blockchain; trust negotiation; trust evaluation system

近年来，随着传感器、嵌入式产品、消费电子等设备的大量介入，网络规模日益拓展，系统与系统间常常需要彼此交换信息而变得不再孤立分散，网络系统逐渐呈现出复杂异构的特征。侯明星等指出同一环境中经常存在多种不同类型的物联网互联以共享数据，因而形成了异构网络系统[1]。王志虎针对不同的电子政务系统间的信息交换及安全管理技术问题，提出了在异构信息系统之间实现电子政务有效共享和通用的数据交换平台架构[2]。Steve H 等将不同的物联网系统通过区块链技术有效的组合联盟系统，提出了‘共享经济’的概念[3]。上述研究表明，由不同的物联网系统，电子政务系统等形成的联盟系统可以有效的进行资源整合分配，信息共享，提升交互效率，降低成本，符合当前互联网的发展。但是随之而来的安全问题也成为技术难点，比如各联盟系统身份管理平台多样[4]，平台间的数据孤立分散；跨域用户的可信评估缺失；多态跨域网络实体行为监管困难等问题。

为了解决异构联盟系统中的信任问题,本文从最关键的用户因素入手，给出了异构联盟系统中用户行为的定义，然后在此基础上引入了区块链技术，提出如何运用区块链技术解决异构系统中实体的信任问题，

* 基金项目: 国家重点研发计划(2017YFB0802302)Foundation item: National Key Research and Development Project of China (2017YFB0802302)

收稿时间: 0000-00-00; 修改时间: 0000-00-00; 采用时间: 0000-00-00; jos 在线出版时间: 0000-00-00

CNKI 在线出版时间: 0000-00-00

最后通在线社交网络的应用场景验证了本文所提方法的有效性和可行性。本文的主要贡献在于：(1)对异构联盟系统的安全性研究，从用户层面出发，给出了异构联盟系统中用户行为的定义；(2)提出了二层区块链模型，确保用户行为的真实性以及用户自身的可信性；(3)提出改进的拜占庭共识机制，将用户信任信息在联盟系统中共享；(4)将本文所提模型应用于在线社交网络中，为在线社交网络用户可信研究提供了一种新思路。本文组织结构如下:第 1 部分介绍了相关的定义和问题描述。第 2 部分详细介绍本文提出的模型框架和实施思路。第 3 部分基于所提模型进行实验仿真与安全性分析.第 4 部分对全文的研究工作进行总结。

1 相关问题的研究

自 2008 年中本聪发表了题为《比特币：一种点对点式的电子现金系统网络身份管理》一文以来[5]，研究者们开始利用区块链去中心化、去信任、以及消息不可篡改性等特点，相继将其应用于物联网、医疗、金融等网络系统的数据共享中[6-11]。区块链技术利用哈希函数的单向性、抗碰撞特性验证数据，实现数据的不可篡改，利用加密链式区块结构存储数据，利用分布式节点共识算法更新数据及利用零知识证明、智能合约等选择性共享数据以保护用户的隐私。本文从用户层面的安全性出发，设计了一种在异构联盟系统下基于区块链的用户信任协商模型，解决了传统的网络系统间数据不互联、不互通，网络用户统一监管困难的难题，同时实现用户对其历史行为不可赖账，评估信任值不可篡改的去中心化用户管理。为了更好的理解异构网络下基于区块链的用户信任协商模型，下面将对用户行为以及区块链相关知识进行详细介绍。

1.1 用户行为相关问题研究

用户行为是指在异构联盟系统中，用户发生的包括物理行为、空间行为，或两者的结合在内的所有可通过设备、网络观测记录的行为。物理行为又指用户的身体行为，如说话、面部表情、走路等能够在物理领域内被客观地观察或间接推断。例如，用户 A 未经授权走进某管理中心这一行为能够被电子设备监测，叫做物理行为。空间行为指的是用户在网络空间中发生的一切可被客观观察的、直接或间接推断出的行为，如用户在网站上浏览网页时，其浏览网页这一行为将会被该网站服务器以及本地浏览器记录。鉴于人们当今处于互联网时代，大多数的人都是通过网络获取信息、完成业务，因此本文将重点关注用户在网络中的行为，即空间行为，把发生在同一网络环境下的用户空间行为称为 “横向行为”，发生在跨域网络环境下的用户空间行为称作“纵向行为”。不管是物理行为或者空间行为，用户的一个行为通常包含了多个行为属性，由这些行为属性一起构成了一个有意义的行为。例如，用户 A 想要登录系统 1，必须输入相关的个人信息，像用户名、密码等，输入用户名和密码这两个行为属性就构成了一次有意义的登录行为，A 在系统 1 中所操作的一切行为都是横向行为，若 A 要与系统 2 中的用户 B 通信，那么就称用户 A 和用户 B 之间的交互行为为纵向行为。

2.2 区块链及应用相关问题研究

目前，区块链技术的发展分为 3 个阶段。第一个阶段是区块链 1.0，代表的是以比特币为首的公有链的应用。区块链体系由大家共同维护，不需专门消耗人力物力，去中心化结构使安全性大大提高，同时，数据存储在加密链式的区块中，对所有节点公开透明，数据的公开性使得在其中做假账几乎不可能，节点间主要通过 POW 共识机制实现数据的生成和更新。但是由于挖矿所产生的资源浪费使得区块的生成过程较为缓慢，依靠代币，数据的完全透明性等缺点使得区块链 1.0 技术无法普及到除货币体系以外的行业中。第二个发展阶段是区块链 2.0，主要是在以太坊平台之上，各节点参与撰写智能合约，无须彼此信任，合约中的代码在一定条件下会自发执行。节点可以通过智能合约选择性地共享数据以保护隐私，同时，POS、DPOS 等新的共识机制的出现使区块链 2.0 的应用领域从最初的货币体系拓展到金融的其他应用领域。但是由于 POS、DPOS 等共识机制仍然需要挖矿，交易速度受到限制，无法实现商用。第三个发展阶段是区块链 3.0，代表的是以 Hyperledger 为首的联盟链，其采用的共识机制是拜占庭容错协议（PBFT）。区块链 3.0 架构是超越货币、金融范围的区块链应用，是商用化的一个里程碑阶段，它能够构建如游戏币、电子发票、虚拟货币、数据资产等‘虚拟资产’的可信安全生态，实现虚拟资产全生命周期监管。

用户在网络中的行为可能受到生理、心理、环境、时间等因素的影响，具有随机性、多样性等复杂特

征，传统的单一系统下对用户横向行为可信监管研究卓有成效。然而在当今数字化时代下，各行各业都开通了网上营业系统，一个用户在不同的系统中扮演的角色各异，导致其在网络中的行为也更加复杂难以管控，多态跨域行为监管已经成为研究的热点和难点。若把若干个相互关联的系统组成联盟系统，用户在不同网络中产生的行为看作是数据资产，那么将区块链 3.0 应用到异构联盟系统用户行为监管问题将能够解决用户行为数据的全生命周期管理，同时通过无代币存在的共识机制实现联盟系统中用户的信任协商，构建可信安全架构。

为了更好的理解区块链 3.0 技术，下面将涉及到本文应用过程中的相关概念逐一介绍。

共识机制[11-13]是区块链技术的最重要的部分，目标是使所有节点能够在互不信任的前提下，基于各自的利益最大化自觉的保存由诚实节点发布的信息。区块链技术发展的不同阶段产生的共识机制特点各异，目前常见的共识机制总结如表 1 所示：

Tab. 1 Consensus mechanism categories and characteristics

表 1 共识机制类别及特点

共识机制	优点	缺点	应用对象
工作量证明机制（POW）	算法简单，容易实现，节点间无需交换额外的信息	资源消耗高，区块产生速度慢,拥有强大算力的节点一直拥有记账权，中心化程度高	比特币、ZCash、以太坊为代表的公有链
股权证明机制（POS）	通过持有币的数量和时间长短来决定记账的节点，一定程度上减少了竞争记账造成的资源浪费	记账节点的选取仍然需要挖矿，中心化现象仍存在	比特币、ZCash、以太坊为代表的公有链
股份授权证明机制（DPOS）	公平竞选记账权，参与验证和记账节点的数量受限，可以达到秒级的共识验证	整个共识机制还是依赖于代币，而大多数商业应用不需要代币，商业化难	比特币、ZCash、以太坊为代表的公有链
实用拜占庭容错机制（PBFT）	系统的运作脱离代币，可商用，共识的时延大约在 2~5 秒钟	当有 1/3 或以上记账人联合作恶，且其它所有的记账人被恰好分割为两个网络孤岛时，恶意记账人可以使系统出现分叉	R3、Hyperledger、金链盟为代表的联盟链
授权拜占庭容错机制（dBFT）	通过投票决定共识参与节点，记账节点需要数字签名，最大限度地确保系统的最终性，使区块链能够适用于真正的金融应用场景	当有 1/3 或以上记账人停止工作后，系统将无法提供服务	R3、Hyperledger、金链盟为代表的联盟链

本文在对比了表 1 涉及到的 5 种共识机制的优缺点以及适用范围后，针对应用场景，提出了一种基于改进的授权拜占庭容错协议的共识机制，称为 IdBFT，其工作过程是：

（1）假设有 M 个联盟系统，联盟成员根据社会影响力、服务质量等多个维度对其所在的联盟系统进行初始投票，选出 F 个成员作为受托节点又叫做授权代表，由它们共同签署（生产）新区块，剩下的成员作为审计节点，轮流检验每个被签署的新区块是否真实有效，其中F满足$3F+1 \leq M$；

（2）如果 F 个授权代表节点中的的某一个或几个错过了签署新区块或者产生了错误的区块，客户端会自动将他的选票移走，因此错过签署区块的“董事们”将会被投出董事会，由剩余的审计节点作为替补，充当授权代表；

（3）联盟成员要想成为代表，必须拥有一个能表征其真实身份的数字证书。并且在每笔交易数据的“头部”引用。

联盟链：本质上仍然是一种私有链，只不过它比单个小组织开发的私有链更大，却又没有公有链那么大的规模，可以理解为它是介于私有链和公有链之间的一种区块链。联盟区块链的每个区块生成由所有的预选节点共同决定，其他接入节点可以参与交易，但不过问记账过程。例如，有 10 个金融、电商、政府、银行等异构网络组成的联盟系统，每个系统都运行着一个节点，为了使每个区块生效需要获得其中 5 个系统的确认（1/2 确认）。一般而言，联盟链的共识节点都需要生成一个数字证书，使得他们的身份可以验证。如果出现异常状况，可以启用监管机制和治理措施做出跟踪惩罚或进一步的治理措施，以减少损失。

联盟成员：联盟链上所包含的所有成员系统，本文指的是价值、利益具有关联性的同行业或跨行业间

的机构或组织所形成的异构网络系统，可以由集合 M 表示，定义为：$M = U_{i=1}^{m} M_i, 1 < i < m$，一个网络系统都包含一定数量的用户，可以由集合 N 为其编号，$N = U_{i=1}^{m} U_{j=1}^{n} N_{ij}, 1 < i < m, 1 < j < n$，其中，m 表示联盟成员个数，n 表示每个成员系统中的用户数。N_{22}表示联盟成员 2 系统中的第 2 个用户的编号，其他编号以此类推。

2 异构联盟系统中基于二层区块链的用户信任协商模型

2.1 用户信任协商模型的思路

传统的网络系统对用户的信任数据都是孤立分散的，用户在某一个系统中的数据不能在其他系统中共享，然而随着互联网的不断发展，系统间的联系逐渐加强，如果用户的信任信息能够在各个系统之间协商，则会为用户管理带来极大的便利，区块链的出现在提供安全保障的基础上使数据共享成为可能。本文提出的信任协商模型包含了 3 个重要的组件，即用户行为区块链、可信评估系统、用户信任区块链，具体架构如下图所示。

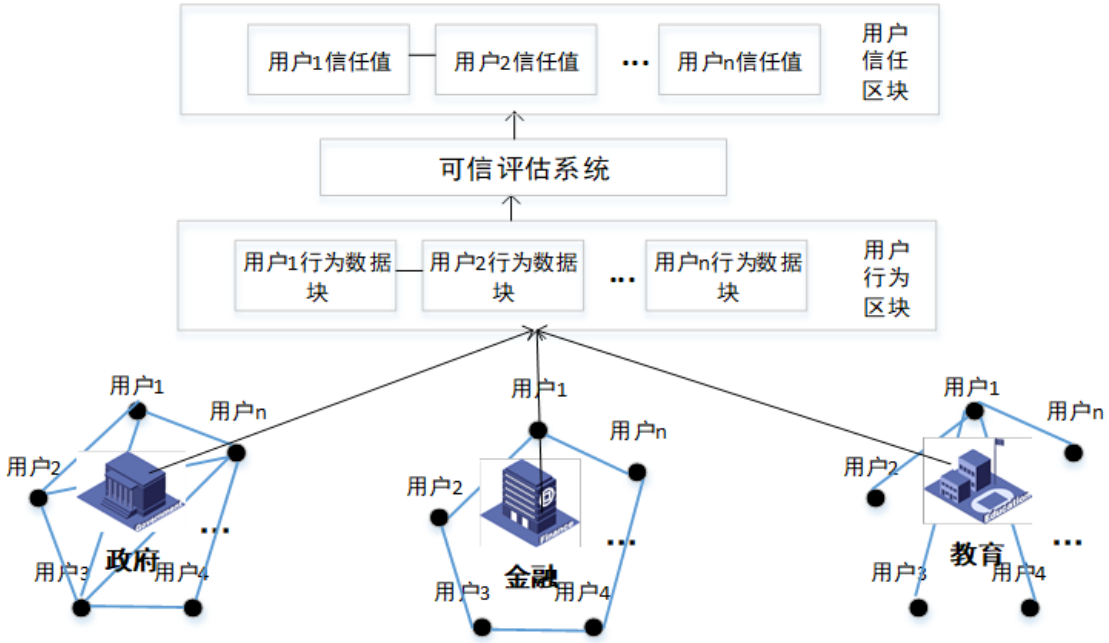

Fig. 1 The basic framework of trust negotiation model based on blockchain

图 1 基于区块链的信任协商模型的基本框架

图 1 中用户行为区块是第一级区块链，保障用户行为可追溯，将用户行为经由可信评估系统后，得到用户信任值，形成的第二级区块链，保证用户可信值不可篡改，对用户在网络中的行为起到一定监管的作用。可信评估系统则是利用数学理论与方法对用户行为建模，由于用户在网络中的行为具有随机性、模糊性、复杂性等特殊性质，因此可以借助云模型理论对网络系统下用户行为所具有的不确定性问题进行定量描述，借助模糊综合评价理论构建网络用户行为可信评价模型，后文将详细阐述这 3 个组件。

信任协商模型的具体工作步骤：

步骤 1. 假设联盟系统的注册格式一致，某一用户向某一联盟系统S_i提交注册请求，并提交用户的公钥作为标识，系统S_i作为主节点广播用户的注册请求，并给请求编号，此时除S_i以外的成员，由系统中存在该用户且社会影响力排名靠前的 3 个节点分别作为从 1、2、3 节点，S_i发送预准备类型信息给从节点，同时进入准备阶段；

步骤 2. 从节点 1 收到信息后，查看其信任评估值，若信任值正常，则返回准备类型信息给主节点和其他 2 个从节点，若低于阈值则丢弃该消息；

步骤 3. 若从 1 节点收到另外两个从节点都发出的同意主节点分配的编号的准备类型的消息，则 3 个

从节点都进入确认阶段；若从节点 2、3 中该用户的信任值低于阈值，则不发送任何消息给从 1 节点；

步骤 4. 若S_i收到了这 3 个从节点的确认消息，则同意该用户的注册请求，将用户的公钥信息记录到 item，并用主节点以及所有从点的私钥签名，S_i广播 item 确认消息，剩余节点轮流校验签署的区块是否真实有效，并更新数据；

步骤 5. 返回步骤 1。

2.2 用户行为数据区块链（即第一层区块链）

用户在网络上产生的行为数据作为 item 块，一个数据块由多个 item 块组成，包含了一个用户在某段时间内在网络中产生的所有行为，通过层层计算哈希值生成 Merkle 树，由联盟系统中的授权代表提交 Merkle 根到联盟链上，剩余节点完成校验工作，形成类似于比特币区块链上的一笔交易，交易公开透明，可追溯，通过这种方式，实现用户行为不可篡改，用户对已发生的行为不可抵赖，对用户在网络中的行为规范起到监管控制的作用。

一个用户行为 item 块包含了用户编号N_{ij}、用户数字签名、用户在网络中产生的行为、时间戳，如图 3 所示：

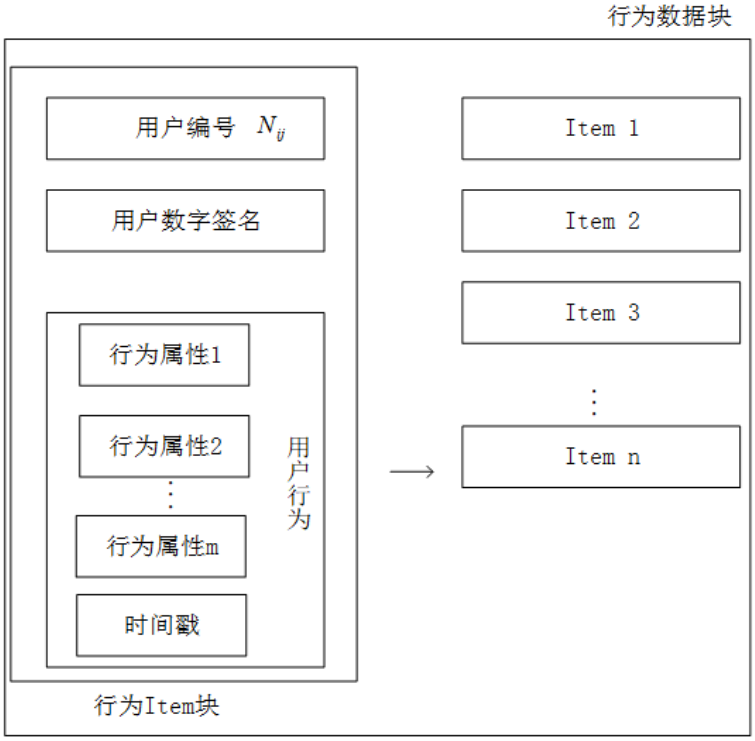

Fig. 2 User behavior data block

图 2 用户行为数据块

行为数据块经过层层哈希算法，生成 Merkle 树，由当值代表节点将 Merkle 根锚定到联盟链上，其生成区块的过程采用 IdBFT 共识机制，稳定在每 3-5 秒生成一个区块，其数据处理速度足以满足用户在网络中产生行为的速度。用户行为区块链如下：

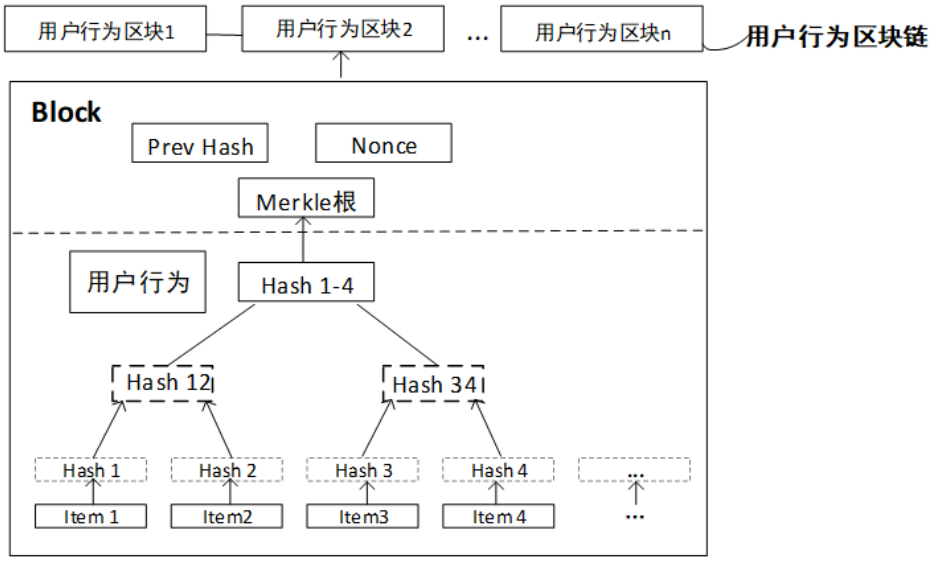

Fig. 3 User behavior blockchain

图 3 用户行为区块链

2.3 用户信任区块链（即第二层区块链）

用户行为经过评估系统后，会得到一个信任值，将用户编号、数字签名、时间戳、信任值存放到数据块中，形成信任 Item 块，产生区块链的过程与行为区块链类似，此处不再赘述。下图为示意图：

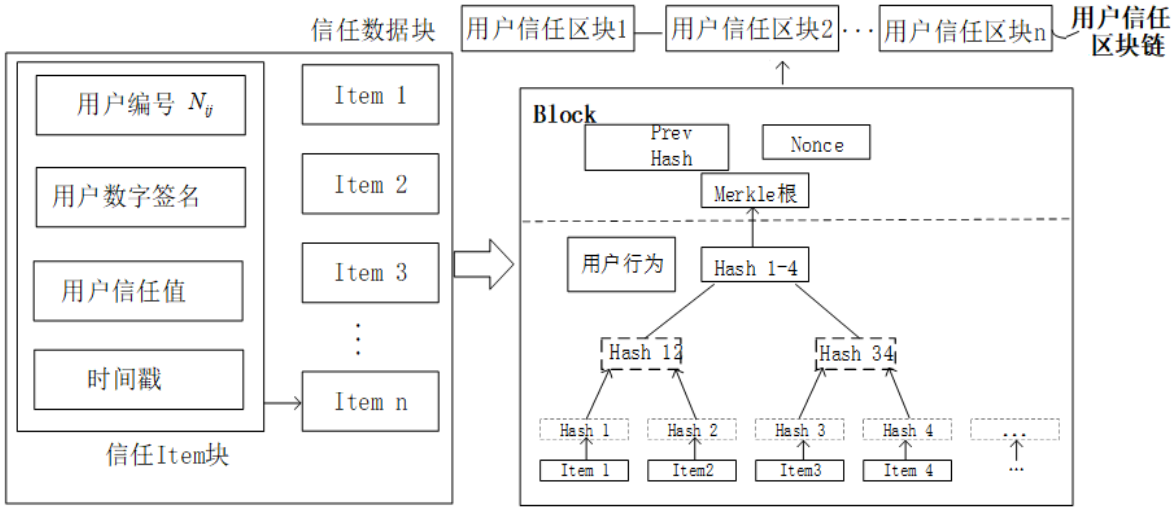

Fig. 4 User trust blockchain

图 4 用户信任区块链

3 基于二层区块链的用户信任协商模型的应用及安全性分析

3.1 基于二层区块链的用户信任协商模型的应用

近年来，随着社交网络的迅速发展，随之而来的用户安全问题也引起了广泛的关注，特别是用户间跨社交网络通信、交换数据等行为，在方便用户的同时，也使得恶意用户窃取、篡改信息更加容易。因此本文将二层区块链的用户信任协商模型应用在跨平台社交网络中，将若干个有关联的在线社交网络平台组成联盟系统，实现用户信任信息在联盟系统间共享，同时在用户注册某一社交网络时，联盟系统间通过共识机制来核实用户的信任值是否超过可信阈值，进而决定是否同意该用户的注册请求，防止恶意用户登录系

统，实现跨社交网络平台下用户行为监管。其中，用户的信任值是通过评估系统产生的，本文采用一种基于云模型理论[14]和模糊综合评价法相结合的可信评估系统，如下图所示：

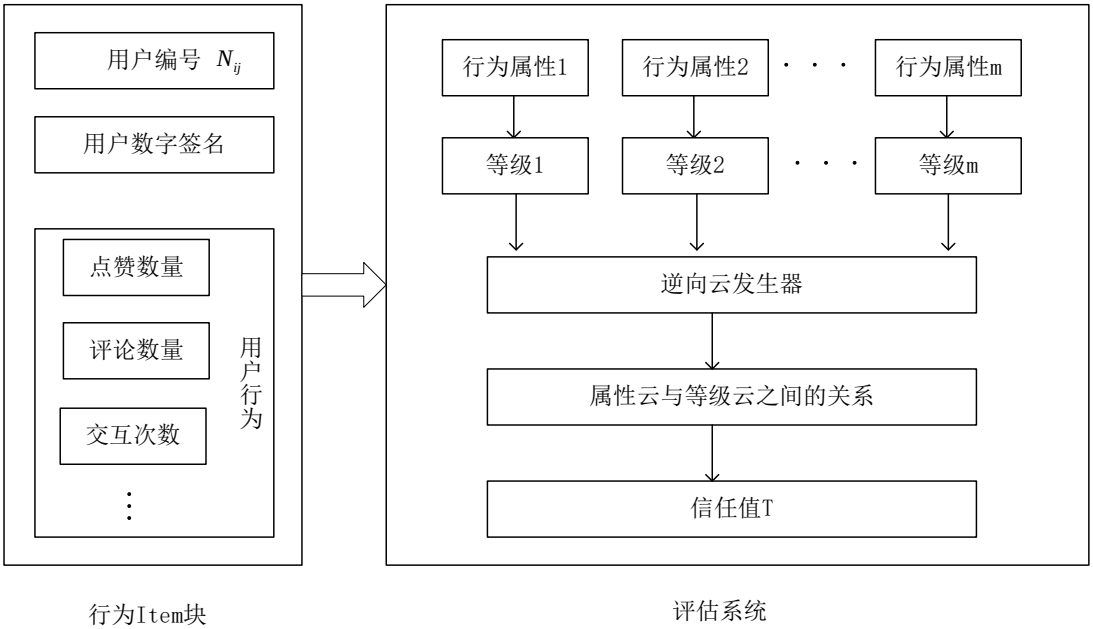

Fig. 5 User behavior assessment system

图 5 用户行为评估系统

其中，用户行为属性是对原始行为数据进行预处理后，从不同维度对其分类而定义的最能够体现用户行为特征的元素，在社交网络这个特定情境下，用户行为属性包：点赞数量、评论数量、交互次数、交互频率等。对用户综合行为信任评估时，应当将用户行为属性分为两个部分，一部分是同一社交网络平台下，收集用户所有横向行为，提取出用户行为属性，另一部分是跨社交网络平台下，提取出用户纵向行为的行为属性，然后将这两部分分别作为可信评估系统的输入，输出 2 个部分的信任值，再通过加权求和的方式，最终计算出用户综合信任值。信任评估系统的具体工作过程如下：

步骤 1. 建立行为属性云。对横向行为数据按其行为特征提取成 m 个行为属性。根据每一个行为属性的样本数据，利用样本均值代替总体均值，得到期望，样本方差代替总体方差的方法，得到熵和超熵，还原出云的数字特征。从而得到 m 个行为属性云。

步骤 2. 建立等级云。事先给出 n 个评价等级，设每个等级区间范围为$[\gamma_{\min},\gamma_{\max}]$，根据文献[15]中的方法确定每一个等级云的数字特征，进而得到 n 个等级云。

步骤 3. 通过计算 m 个行为云对 n 个等级云的隶属度得到模糊关系矩阵矩阵。根据模糊熵权法[16]得到每一个行为属性的权重。

步骤 4. 将隶属度矩阵与权重向量相乘得到横向行为数据的信任值T_1。

用相同的步骤计算纵向行为数据的信任值T_2，用户的综合信任值$T = \alpha * T_1 + \beta * T_2$（$\alpha,\beta$分别表示横向行为和纵向行为对整体信任值的影响，其取值视具体情况而定）。

计算出用户信任值后，经过层层哈希，形成 Merkle 根，由当值的在线社交网络系统将 Merkle 根锚定到区块链，形成用户信任区块链。

3.2 基于二层区块链的用户信任协商模型的安全性分析

本文所提的基于 2 层区块链的用户信任协商模型能从以下 2 个方面保障社交网络环境的安全性：

1）如果存在恶意用户：当某一用户或某一群体企图在社交网络中发起 Spam，Sybil，谣言攻击，首先，在第一层用户行为区块链上，用户的每一个发生过的行为都存在区块体中，形成 Merkle 根被锚定到区块链上，由于 Merkle 根是通过哈希算法生成，由于哈希函数具有单向性、抗碰撞性的特征，使得任意一个行为

被修改都能够使 Merkle 根的值发生改变，这意味着用户行为可被追溯，且不可篡改，因此用户行为区块链保障了用户行为的真实性，但是仅仅通过第一层区块链，不能判定该用户是否是恶意用户，因此，便需要将用户行为经过可信评估系统，得到的用户的信任值，形成第二层区块链，即用户信任区块链，用户的信任值能被所有联盟系统查看，一旦发现可疑用户便立即做上标记，联盟系统则根据可信值对该用户设置访问权限，或者禁止该用户加入系统。综上，通过 2 层区块链能从用户层面保障网络环境的安全。

2）如果存在恶意代表节点：考虑最坏的情况，若提交数据的 f 个授权代表节点共同发起恶意篡改数据攻击，由于采用的是 IdBFT 共识机制，只要满足$3f+1<M$，便可以抵御攻击。举例如下，若 10 个网络系统组成联盟系统，则在授权代表系统最多为 2 个前提下能确保系统的安全，因为在这种情况下，即使这 2 个代表节点都是恶意节点，整个系统的安全性能也不受影响。

4 结束语

本文主要针对价值、利益具有关联性的同行业或跨行业的机构或组织所形成的异构网络系统，用户数据难以共享导致多态跨域网络实体行为监管困难等问题，利用改进的 dBFT 共识机制，提出了基于 2 级区块链的用户信任协商模型，对用户行为起到一定监管规范的作用，同时也能防止恶意用户注册。此模型为跨域用户管理提供了一种新思路，同时区块链去中心化的特点为 web3.0 的到来打下了基础。

References:

[1] HOU Mingxing,QI Hui.Research on Heterogeneous Internet of Things Security Solution Based on SDN[J]. Internet of Things technology, 2017, 7(12).

[2] WANG Zhihu. Asia-Pacific Conference on Information Network and Digital Content Security. 2011.

[3] Bendiab K, Shiaeles S, Boucherkha S. A New Dynamic Trust Model for "On Cloud" Federated Identity Management[C]// Ifip International Conference on New Technologies, Mobility and Security. 2018:1-5.

[4] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[J]. Consulted, 2008.

[5] XUE Tengfei, FU QunChao, WANG Cong. A Medical Data Sharing Model via Blockchain[J]. Acta Automatica Sinica, 2017, 43(9):1555-1562.

[6] Zhang Y, Wen J. The IoT electric business model: Using blockchain technology for the internet of things[J]. Peer-to-Peer Networking and Applications, 2017, 10(4):983-994.

[7] Walker M A, Dubey A, Laszka A, et al. PlaTIBART: a Platform for Transactive IoT Blockchain Applications with Repeatable Testing[J]. 2017:17-22.

[8] Kuo T T, Kim H E, Ohno-Machado L. Blockchain distributed ledger technologies for biomedical and health care applications[J]. J Am Med Inform Assoc, 2017, 24(6):1211-1220.

[9] Kim S. Blockchain for a Trust Network Among Intelligent Vehicles[J]. Advances in Computers, 2018.

[10] Castro M, Liskov B. Practical Byzantine fault tolerance[C]// ACM, 1999:173-186.

[11] SHE Wei,YANG Xiaoyu,HU Yue,et al. Transaction certification model of distributed energy based on consortium blockchain[J]. J ournal of University of Science and Technology of China, 48(4): 307-313.

[12] Nguyen G T, Kim K. A Survey about Consensus Algorithms Used in Blockchain[J]. Journal of Information Processing System-s, 2018, 14(1).

[13] LI Deiyi, LIU Changyu. Artificial intelligence with uncertainty[C]// International Conference on Computer and Information Technology. IEEE, 2004:2-2.

[14] ZHANG Shibin, XU Chunxiang. Study on the Trust Evaluation Approach Based on Cloud Model[J]. Journal of University of Electronic Science & Technology of China, 2013, 42(1):92-97.

[15] Mosadeghi R, Warnken J, Tomlinson R, et al. Comparison of Fuzzy-AHP and AHP in a spatial multi-criteria decision making model for urban land-use planning[J]. Computers Environment & Urban Systems, 2015, 49:54-65.

附中文参考文献:

[1] 侯明星, 亓慧. 基于 SDN 的异构型物联网安全解决方案研究[J]. 物联网技术, 2017, 7(12).

[3] 王志虎. 电子政务异构系统数据安全策略分析[C]// Asia-Pacific Conference on Information Network and Digital Content Security. 2011.

[6] 薛腾飞, 傅群超, 王枞,等. 基于区块链的医疗数据共享模型研究[J]. 自动化学报, 2017, 43(9):1555-1562.

[12] 佘维, 杨晓宇, 胡跃,等. 基于联盟区块链的分布式能源交易认证模型[J]. 中国科学技术大学学报, 2018(4).

[14] 李德毅, 刘常昱, 杜鹢,等. 不确定性人工智能[J]. 软件学报, 2004, 15(11):1583-1594.
[15] 张仕斌, 许春香. 基于云模型的信任评估方法研究[J]. 计算机学报, 2013, 36(2):422-431.