doi:10.3772/j.issn.2095-915x.2018.03.004

面向工业互联网场景的新型分布式账本技术

张正[1] 杨睿哲[1] 金凯[1] 杨兆鑫[1] 林波[1] 张延华[1] 于非[1,2]

1. 北京市未来网络高精尖创新中心，北京工业大学信息学部 北京 100124；
2. 卡尔顿大学，渥太华，加拿大

摘 要 分布式账本是一种在网络成员之间共享、复制和同步的数据库，它记录网络参与者之间的交易，如资产或数据的交换。本文提出一种不同于传统区块链链式结构的新型分布式账本技术，通过采用有向无环图分布式账本结构，克服了传统链式结构的分布式账本在面对工业互联网场景下高频密集信息时会出现交易确认缓慢、网络拥塞等问题。

关键词： 分布式账本技术；有向无环图；工业互联网
中图分类号： G35
开放科学（资源服务）标识码（OSID）

A New Distributed Ledger Technology For Industrial Internet Scenarios

ZHANG Zheng[1] YANG Ruizhe[1] F. Richard Yu[1,2] JIN Kai[1]
YANG Zhaoxin[1] Lin Bo[1] ZHANG Yanhua[1]

1. Beijing Advanced Innovation Center for Future Internet Technology, Beijing University of Technology, 100124, China;
2. Carleton University, Ottawa, ON K1S 5B6, Canada

Abstract The distributed ledger is a database that is shared, replicated, and synchronized among network members. It records transactions between network participants, such as the exchange of assets

基金项目： 国家自然科学基金资助项目（61571021）；北京工业大学基础研究基金项目 (040000546317525)。
作者简介： 张正 (1993–)，博士研究生，研究方向：分布式账本技术和人工智能；杨睿哲（1982–），讲师，研究方向：无线通信技术与移动边缘计算技术等方面的研究；金凯（1994–），硕士研究生，研究方向：区块链技术及智能合约应用；杨兆鑫（1993–），博士研究生，研究方向：区块链技术与数据挖掘技术；林波 (1993–)，硕士研究生，研究方向：移动边缘计算技术及区块链技术应用；张延华（1960–），教授，研究方向：信号及信息处理、智慧无线通信网络方面的研究，E-mail: zhangyh@bjut.edu.cn；于非 (1974–)，教授，IEEE Fellow，研究方向：分布式账本技术、车联网及绿色通信等方面的研究。

doi:10.3772/j.issn.2095-915x.2018.03.004

or data. This paper proposed a new distributed ledger technology that is different from the traditional blockchain chain structure. It overcomes the infrequent transaction confirmation problem when the high cost of distributed ledgers with traditional chained architectures in the industrial Internet scenarios by adopting a directed acyclic graph distributed ledger structure.

Keywords：Distributed ledger technology; directed acyclic graph; industrial internet

1 引言

随着我国将“中国制造 2025”上升到国家战略层次，工业互联网作为实现这一宏伟目标的主攻方向，已经开始引起越来越多人的关注。在工业互联网场景中，数据通过智能设备被收集、共享，然后储存至数据中心进行大数据处理，最终分析出有用的“智能决策”以推动各设备之间更好的进行协作，对于工业互联网来说，海量数据是让控制中心做出智能决策的基础[1-4]。然而，在工业互联网的体系中，产品制造往往涉及多个工厂或企业，如何保证各方之间的互相信任，不同公司涉及安全隐私的数据不被泄露，产品问题追踪时数据不被恶意修改，伴随着每时每刻大量的工业数据在网络中流通，如何保证工业互联网中数据的安全和可靠成为了一个重要的问题[5]。传统的解决方案一般会将数据托管于有良好信誉的第三方机构，但是随之而来的是昂贵的中介费用。

另一方面，随着比特币这类加密数字货币的兴起，作为其支撑技术的分布式账本技术得到越来越多的关注。分布式账本技术具有的防篡改、不可抵赖、强一致性和去中心化等特性，可以在不依赖第三方机构的前提下为工业互联网场景下多方企业提供一个可靠的协作平台[6]。

本文基于分布式账本技术（Distributed Ledger Technology，DLT），针对传统区块链链式结构的不足，提出一种适用于工业互联网场景的新型分布式账本设计框架，通过采用有向无环图的分布式账本结构，克服了传统区块链链式结构下分布式账本在面对高频密集信息记录时可能出现的交易确认缓慢和网络拥塞等问题。

2 传统分布式账本技术的优势与局限

2.1 分布式账本技术的特性

分布式账本技术（Distributed ledger Technology，DLT）是一种在网络系统中各成员之间共享、复制和同步的数据库。DLT 记录网络参与者之间的交易，如智能制造环节中涉及的零部件或数据的交换，可以有效降低因调度不同账本所产生的时间和成本开支[7]。

分布式账本的特性主要包括以下几点：

1. 去中心化：

数据库中的数据可以通过多个站点、不同地理位置或者多个机构组成的网络进行分享。所有网络成员都可以获得与其他成员内容一致的唯一、真实账本副本。账本里的任何改动都会在所有的其他网络成员的副本中被反映出来。

2. 共识机制

分布式账本中所存储数据信息的安全性和可靠性是通过公钥、私钥以及签名来保证，从而实现密码学层次上的一致性维护。根据网络中达成共识的规则，账本中的数据可以由一个、部分或者全部参与者共同进行更新。网络中的参与者根据共识原则来制约和协商对记录的更新，不需要将信任托付给中间的第三方机构。

3. 不可篡改

分布式账本中的每条记录都有唯一的时间戳和唯一的密码签名[11]，这使得账本成为网络中所有交易的可审计历史记录。任何网络成员对数据的修改必须根据共识机制与其他网络成员达成一致方可以完成。

2.2 工业互联网场景下分布式账本的优势

在工业互联网场景中，所有设备是高度自动化的。设备采用蓝牙、ZigBee、WiFi、Lora等通信技术发送数据，然后控制中心对这些数据进行数据分析，通过机器学习算法推导出最优的“智能决策”，最终发出指令保证各设备之间高效的协同运作。这一过程中，不需要依靠工作人员的人工干预，实现完全的机器对机器（MachinetoMachine，M2M）。

不少文献已经证明[6-9]，数据是影响工业互联网中智能决策好坏的重要因素。机器学习算法接受训练数据的量级和维度越多，最终训练的效果就越好。换而言之，就是说采用一个工厂所有车间的数据训练处的智能决策模型一定优于只采用单个车间数据所训练的模型。同样而言，也就是说如果数据采集自不止一个工厂，那理论上会得到更准确的优化模型。因此，海量、多方面、跨企业间的数据共享是工业互联网中的必要需求。

为了消除企业对数据共享过程中安全、隐私的顾虑。现有的工业互联网大多选择将数据托管给中心化的第三方数据中心（比如公有云）[7]，但是这种解决方案往往纯在高成本、低效率和数据储存不完全等问题[10]。

于是，分布式账本作为一种去中心化架构的分布式储存式数据库技术，为多方之间的数据安全共享提供看一个新的选择。在工业互联网场景下，我们希望其可以有效的解决协同制造各企业之间的协调和信任问题，提高多方合作的沟通效率。

与传统的将数据托付给中心化的第三方数据中心方法相比，分布式账本采用去中心化的网络结构，提高了交易的透明度，避免权力过度集中的数据中心结构发生腐败和欺诈的可能性。同时因为账本由所有网络成员共同维护，所以单一网络节点受到攻击并不会对账本本身造成重大影响，有利于保护整个分布式网络稳定性和安全性[8-10]。

所有接入分布式网络的设备，可以借助分布式账本的共识机制确认交易对方的信任度。通过执行储存于分布式账本中的智能合约，设备相互之间数据资源访问和验证不再需要人类参与。由此可知，应用于产业链的分布式账本所建立的机器之间的信任，使得整个产业生态内所有的机器都可以基于工业互联网实现自我维持、自我服务。

2.3 传统分布式账本技术的局限性

目前，大部分的分布式账本都是基于区块

doi:10.3772/j.issn.2095-915x.2018.03.004

链（BlockChain）结构的，所以分布式账本技术在很大程度上被等价于区块链技术[12]。作为一种典型的分布式账本，区块链具有上文所说的分布式账本去中心化、不可篡改等诸多优点，理论上可以满足工业互联网对数据共享安全隐私保护的要求。但是在面对工业互联网中数据共享高频次、密集上传的产业场景时，传统区块链往往存在一定的局限。

区块链中的账本由其所组成的区块通过链式结构连接而成，每个区块包括产生时间、当前区块根哈希值、前一区块根哈希值和所包含的若干交易记录[13]。如果基于区块链技术构建一个产品信息录入系统，其规则往往如下[14-15]：产品的信息根据产品的流通顺序被依次添加入区块链中，产品的一个环节信息添加入到区块链的一个区块，作为区块中的一笔交易记录。在将产品信息加入区块链的同时，会为产品生成唯一的 ID，同时将唯一 ID 也作为产品的详细信息被添加到区块链的一个区块中。基于区块链技术的产品信息查询步骤中，在区块链中查询产品的详细信息，并确认产品的 ID 的唯一性。各个区块链参与者都持有全部区块链，任何参与者添加的新的合理交易信息都会被同步到其他参与者所持有的区块链中。同样，参与者也能在区块链中查看其他参与者所添加的产品信息，完成产品信息查询操作。

但是在区块链账本中，单个区块所能储存的数据有限且无法扩展，如果短时间所需要上链的数据过多，在单个区块所储存的信息已经达到上限的情况下，溢出的数据信息必须排队等到下个区块产生才能被添加上链[15]。

然而，现代工业中产品流通环节复杂多样，机器与机器之间的交易记录非常频繁，这就意味着在短时间内所需要记录的产品数据的数量巨大。大量的产品数据信息需要被记录入区块而又不能被及时添加入区块，就会处于排队状态并不断堆积，最终造成区块链网络的拥堵[8]。

3 面向工业互联网的新型分布式账本技术

为了满足工业场景下的短时间频繁数据交换的需求，本文提出并设计了一种新型的基于有向无环图（Directed Acyclic Graph，DAG）的分布式账本系统。

3.1 新型分布式账本结构

有向无环图来自数学图论中的概念，若一个有向图无法从某顶点出发经过若干条边回到该点，则称该图为有向无环图。在本文提出的新型分布式账本中，账本不再是按照定时生成的区块经过链式结构构建成，而是基于有向无环图，因此工厂机器所发送的信息数据不再需要等待新的区块产生后才能被打包合并添加到分布式账本中，而是直接将数据本身作为节点进行数据上传。所有的节点构成了有向无环图的集合。物联网设备要将新的数据上传至有向无环图，必须先验证有向无环图中的两个节点，验证通过后形成有向无环图中新的有向边，新旧数据之间验证关系通过有向边来表示。在本文提出的账本中，所有网络成员都可以积极的参与共识。分布式账本网络中其他成员对有向无环图的变动进行同步时，会先对新存入有向无环图的数据进行验证操作，如果发现数据存

在冲突，其他成员将不会通过验证。随着交易不断的增加，如果数据不被多数成员验证，那这笔数据记录不会被分布式账本系统所承认[15-17,19]。基于这种机制，交易验证是并行的，网络完全分散，不需要像传统区块链一样将信任托付给矿工。

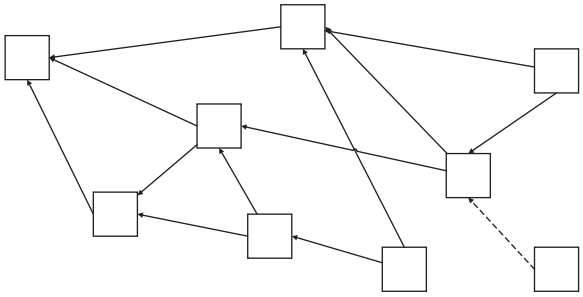

图 1 有向无环图账本结构图

图 1 为有向无环图账本的结构图。图 1 中方块代表所记录的交易信息，工业互联网设备所上传的数据信息以交易的形式被记录在账本之中，方块之间的有向边代表新旧数据之间验证关系，实线代表已被确认的数据验证关系，虚线代表尚未得到多数确认的验证关系。

3.2 基于新型分布式账本的工业产品溯源系统

本文基于有向无环图分布式账本架构设计并实现了一个面向工业产品溯源的 DLT 系统。

1) 系统架构

本系统从架构上可以分为应用层，网络层，数据层和物理层，其中，基于有环无环图的 DLT 应用于数据层和通信层。而从功能上，生产商执行产品数据上传，分销商执行物流数据录入，客户则可以根据产品 ID 查询产品生产环节的详细信息。

物理层主要包括工业物联网传感器，负责采集工业产品流通过程中的相关信息，例如工厂环境数据和产品的规格参数，并将信息通过网络层转发到数据层。

网络层主要包括网络结构和协议，执行传感器上传数据的通信协议（例如蓝牙，Zigbee 和 Lora 等传统物联网通信协议）、分布式账本节点之间的同步通信（P2P 协议）、客户向溯源系统进行溯源请求的通信协议（HTTP）。

数据层主要指记录产品信息的数据库，由有向无环图结构分布式账本承担储存功能。产品信息通过交易事务的形式储存在分布式账本中，交易一旦被添加到有向无环图中并得到验证，会立即同步到其他网络成员的有向无环图账本中。即便对单一节点中的以前交易记录进行篡改，只要大多数成员所储存的分布式账本正确，错误的交易记录将不会被承认，所以储存于分布式账本中的产品数据可以做到唯一和不可篡改[8]。

应用层实现给组织或个人提供访问分布式账本的接口和应用，服务对象主要包括产品的生产商、分销商和客户。

产品溯源系统的物理层采集到产品信息后，通过网络层将产品信息转发至数据层进行储存，由应用层向溯源过程中的所有参与者提供接口，使其通过网络层访问数据层，进行产品溯源信息数据的访问。

2) 系统成员

在本文所涉及的产品溯源系统中，所有网络成员都需要在分布式账本中注册唯一账户，从职责功能上参与者分为以下几类：

1、生产商：负责生产产品，记录产品的生产数据。数据来源主要通过传感器采集，数据

doi:10.3772/j.issn.2095-915x.2018.03.004

包括但不限于产品加工信息，产品唯一识别编号、质检认证信息、生产负责人 ID、产品特征描述等。

2、分销商：负责将产品销售给消费者，记录产品的销售数据，包括但不限于产品发货信息、配送物流信息等。

3、客户：从经销商购买产品，具有访问产品特定信息的权限。平时只能查看产品的销售物流信息，产品发生安全问题后，可以访问关键的生产信息。

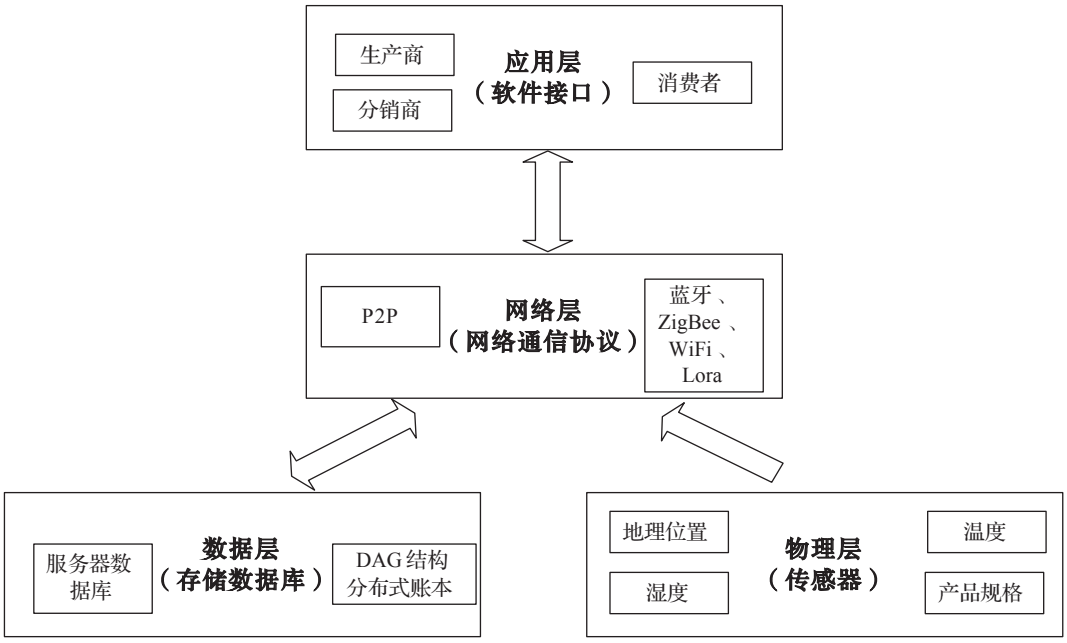

图 2 产品溯源系统的技术架构图

3) 产品识别

产品信息在记录到有向无环图中之前会先获取产品的唯一标示编号（例如通过条码、RFIC 等），将产品信息与编号一同发送至分布式节点。分布式节点收到编号会先确认账本是否已为该产品创建检索编号，如果没有，则先为产品注册检索编号；如果有，则为检索编号增加新的产品信息。为了防止产品信息被分布式账本中其他无关人员获取，节点会对交易信息详情（即产品信息）进行加密。

4) 加密机制

根据溯源功能需求，加密可选择对称加密和非对称加密方法。对称加密方法即所有参与溯源过程的参与者采用同一个加密密钥，所有参与者均可以通过密钥查看其它用户所添加溯源信息的全部内容，非溯源参与者因为没有所述密钥即便得到有向无环图中消息也无法获得溯源内容。非对称加密方式即溯源过程的所有参与者均获得一个公钥和私钥，公钥对所有参与者开放，可以对产品信息进行加密，私钥决定该用户的信息读取权限，据私钥权限查看溯源内容数据 [20]。

5) 数据处理

基于以上定义的系统架构、成员及产品识别和加密机制，给出数据上传和数据查询机制如下。

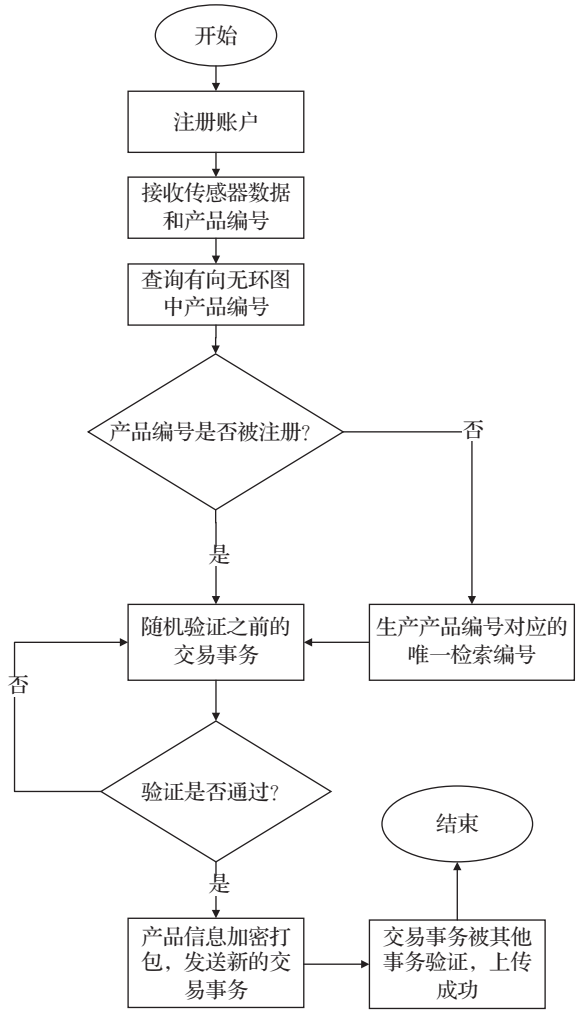

图 3 产品溯源系统数据上传流程图

产品溯源系统数据上传流程如图 3 所示，产品溯源系统中存储产品信息的流程步骤包括：

1、网络成员在分布式账本中注册账户，同时从其他网络成员处同步完整的分布式账本。

2、网络成员采集需要上传的产品数据。

3、网络成员对所上传产品进行注册，获得唯一产品编号。

4、网络成员检查分布式账本中是否已存在产品编号对应的检索编号，如果存在则执行步骤 5，否则，生成唯一的检索编号。

5、网络成员随机对有向无环图中的交易进行验证，如果验证通过，则执行步骤 6，否则继续寻找其他交易进行验证。

6、网络成员以检索编号为交易接收地址发送一笔新的交易事务，其中包含加密后的产品数据。

7、网络成员发起的交易被其他节点验证通过，产品数据上传完成。

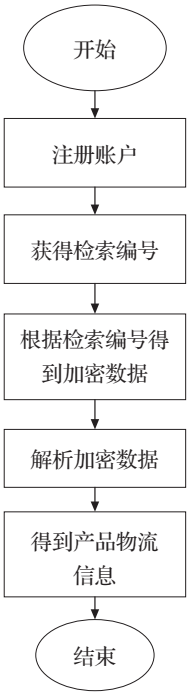

图 4 产品溯源系统数据查询流程图

产品溯源系统数据查询流程如图 4 所示，产品溯源系统中读取产品信息的流程步骤包括：

1、客户在分布式账本中注册账户，通过电商平台（账本节点之一）访问分布式账本。

2、客户得到产品编号对应的检索编号和可以访问部分产品信息的私钥。

3、客户依据检索编码对分布式账本的交易事务进行检索，得到加密后的信息数据。

4、客户通过私钥解析加密数据。

5、客户得到产品的销售物流信息。

doi:10.3772/j.issn.2095-915x.2018.03.004

4 结语

本文提出一种新型的分布式账本机制，通过采用有向无环图分布式账本结构克服了传统区块链链式结构在面对高频密集信息记录场景时会出现交易确认缓慢、网络拥塞等的不足，在工业互联网智能制造、物联网应用等领域具有广泛的应用价值。

参考文献

[1] 通用电气公司. 工业互联网:打破智慧与机器的边界[M]. 北京: 机械工业出版社, 2015.

[2] 沈苏彬, 杨震. 工业互联网概念和模型分析[J]. 南京邮电大学学报(自然科学版), 2015, 35(5):1-10.

[3] Sadeghi A R, Wachsmann C, Waidner M. Security and privacy challenges in industrial internet of things[C]. Proceedings of the 52nd annual design automation conference. ACM, 2015:54.

[4] 吴文君, 姚海鹏, 黄韬,等. 未来网络与工业互联网发展综述[J]. 北京工业大学学报, 2017, 43(2):163-172.

[5] 王继业, 高灵超, 董爱强,等. 基于区块链的数据安全共享网络体系研究[J]. 计算机研究与发展, 2017, 54(4):742-749.

[6] Wang H, Osen O L, Li G, et al. Big data and industrial internet of things for the maritime industry in northwestern norway[C]. TENCON 2015-2015 IEEE Region 10 Conference. IEEE, 2015:1-5.

[7] 姬广鹏. 基于工业互联网的大数据中心建设探索[J]. 中国新通信, 2014(18):66-66.

[8] JaredDean. 大数据挖掘与机器学习: 工业4.0时代重塑商业价值[M]. 北京: 人民邮电出版社, 2015.

[9] Hestness J, Narang S, Ardalani N, et al. Deep Learning Scaling is Predictable, Empirically[J]. 2017.

[10] Azaria A, Ekblaw A, Vieira T, et al. MedRec: Using Blockchain for Medical Data Access and Permission Management[C]. International Conference on Open and Big Data. IEEE, 2016:25-30.

[11] 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.

[12] Kshetri N. Can Blockchain Strengthen the Internet of Things?[J]. IT Professional, 2017, 19(4):68-72.

[13] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[EB/OL]. [2018-02-13]. https://bitcoin.org/bitcoin.pdf.

[14] Tapscott D, Tapscott A. Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world[M]. London: Penguin Books, 2016.

[15] Skwarek V. Blockchains as security-enabler for industrial IoT-applications[J]. Asia Pacific Journal of Innovation and Entrepreneurship, 2017, 11(3):301-311.

[16] Lakshman A, Malik P. Cassandra: a decentralized structured storage system[J]. ACM SIGOPS Operating Systems Review, 2010, 44(2):35-40.

[17] Sikorski J J, Haughton J, Kraft M. Blockchain technology in the chemical industry: Machine-to-machine electricity market[J]. Applied Energy, 2017, 195:234-246.

[18] Divya M, Biradar N B. IOTA-Next Generation Blockchain[J]. International Journal of Engineering and Computer Science, 2018, 7(4):23823-23826.

[19] Mills D C, Wang K, Malone B, et al. Distributed ledger technology in payments, clearing, and settlement[EB/OL]. [2018-03-11]. http://www.istein.org/component/flexicontent/weblink/25/21144/1.html.

[20] Pinna A, Ruttenberg W. Distributed Ledger Technologies in Securities Post-Trading Revolution or Evolution?[EB/OL]. (2016-04-27) [2018-02-15]. https://publications.europa.eu/en/publication-detail/-/publication/b90e4bb8-0dcc-11e6-ba9a-01aa75ed71a1/language-en.

[21 CHURYUMOV A. Byteball: A Decentralized System for Storage and Transfer of Value[EB/OL]. [2018-03-15]. https:/byteball.org/Byteball.pdf.

[22]. Huckle S, Bhattacharya R, White M, et al. Internet of things, blockchain and shared economy applications[J]. Procedia computer science, 2016, 98(C):461-466.