基于区块链的供应链动态多中心协同认证模型

朱建明[1]，付永贵[1,2]
（1.中央财经大学信息学院，北京 100081；
2.山西财经大学信息管理学院，山西 太原 030031）

摘 要：比特币的成功证明了区块链技术的价值。在分析了区块链的特点、局限性以及其链式结构散列原理的基础上，研究了区块链技术的应用，提出了基于区块链的 B2B+B2C 供应链各交易主体交易结构简图及动态多中心协同认证模型。实证分析了区块链在 B2B+B2C 供应链电子交易中的产生过程，指出了区块链在 B2B+B2C 供应链企业进行推广使用所面临的问题。其研究成果对于密码学与区块链的应用提出了新的思路。

关键词：区块链；散列原理；供应链电子交易；多中心协同认证
中图分类号：TP 309.7
文献标识码：A
doi: 10.11959/j.issn.2096-109x.2016.00019

Supply chain dynamic multi-center coordination authentication model based on block chain

ZHU Jian-ming[1], FU Yong-gui[1,2]
(1. School of Information, Central University of Finance and Economics, Beijing 100081,China;
2. School of Information Management, Shanxi University of Finance and Economics, Taiyuan 030031,China)

Abstract: The value of block chain technology is proved by the success of Bitcoin. The characteristics, limitations and its chain structure Hash principle of block chain were analyzed, the applications of block chain technology were researched, the B2B+B2C supply chain each transaction subject transaction structure diagram and dynamic multi-center coordination authentication model based on block chain were proposed. Then the producing process of block chain in B2B+B2C supply chain electronic transaction with example was analyzed, and the facing problems that block chain spreading use in B2B+B2C supply chain enterprise were pointed out. The research results have proposed a new idea for the application of cryptography and block chain.

Key words: block chain, Hash principle, supply chain electronic transaction, multi-center coordination authentication

1 引言

近年来，区块链（block chain）[1]技术引起了学术界和产业界的高度重视，许多学者认为区块链技术是未来互联网技术的革命，是信息基础技术的巨大创新。区块链技术的主要特点是去中心化，是基于密码学算法建立的一个全球信用的基础协议。具体来说，区块链是基于互联网的分布式账本技术，由于账本由多方共享，保证了账本的不可篡改性，比特币（Bitcoin）是区块链技术的一个成功应用。2015 年 12 月 30 日，美国纳斯达克 Linq 系统通过其基于区块链的平台完成了

收稿日期：2016-01-01；**修回日期**：2016-01-05。**通信作者**：朱建明，zjm@cufe.edu.cn
基金项目：国家自然科学基金资助项目（No.61272398）；北京市哲学社会科学重点基金资助项目（No.14JGA001）
Foundation Items: The National Natural Science Foundation of China (No.61272398), The Key Projects of Philosophy and Social Sciences of Beijing (No.14JGA001)

首个证券交易，标志着区块链技术在主流金融系统中的成功应用。本文将区块链技术应用于供应链管理过程中，提出了基于区块链的供应链动态多中心协同认证模型。

比特币最早出现于 2008 年中本聪（Satoshi Nakamoto）的白皮书，其中作者给出了比特币的概念：一种点对点的电子现金[2]系统，这一系统允许交易双方不通过金融机构而实现一方对另一方的在线支付[3,4]。学术界及产业界公认这一概念的发布时间为 2009 年 1 月 9 日，它是最早也是最大的去中心化数字货币。比特币使用加密技术实现点对点交易的安全性，比特币网络系统使用计算机解决复杂数学问题的形式（俗称“挖矿”）来产生新的比特币，该系统构建一定的算法呈递减的速度产生新的比特币，以确保比特币在整个系统中不会严重“通货膨胀”。自比特币产生以来，虽然得到了学术界及产业界的广泛关注，其应用仍处于初级阶段，但关于比特币和区块链技术的应用和研究越来越引起人们的重视，更有学者认为区块链将是改变世界的互联网新技术。在比特币系统中，区块链表示所有已经发生的比特币交易的记录账本，显然随着交易的不断进行，这一账本的长度一直延伸。

区块链作为一种信息技术，使用随机散列并对全部交易加上时间戳的方法，其链式结构散列原理如图 1 所示[3]。

在图 1 中，对于 U2 来说，首先 U2 使用 U1 的公钥验证 U1 通过 U2 公钥发给 U2 的使用 U1 私钥签名的先前交易信息及 U1 与 U2 的交易信息，确认 U1 的身份，然后将交易信息进行重新组合或者分解，使用 U2 的私钥对重新组合或者分解后的先前交易信息及 U2 与 U3 的交易信息签署一个随机散列的数字签名[5]，并将这一签名通过 U3 公钥发送给 U3，U3 按照 U2 的方式进行验证、签名和进一步处理，如此区块包含的交易信息就产生了。

其中，对区块进行随机散列时要加上时间戳，并将随机散列在网络中进行广播，这样加了时间戳的区块就是其存在的一个有力证明，每一个时间戳对前一时间戳的信息纳入其随机散列值中，用以对上一时间戳信息进行增强。

通过分析区块链链式结构散列原理可以发现，如果大多数的所有者是诚信的，则随着区块链的增长，区块链的信用会相应快速增长，如果攻击者企图对已经形成的区块进行篡改，则必须篡改所有诚信者的区块以及其后交易区块的信息，对于一个长度不断增长的区块链来说，攻击者要完成相应区块信息的修改几乎是不可能的，区块链的去中心化及区块所有者互相证明的机制实现了交易的有效证明。

2　区块链的研究进展及应用综述

2015 年是区块链应用研究最为活跃的一年，主要研究成果如下。

1) 解决了计算性难题“拜占庭将军问题”。“拜占庭将军问题”是指战场上多个将军在彼此互不信任的情况下的一种沟通协调机制。

2) 改造众筹模式。基于区块链技术的众筹平

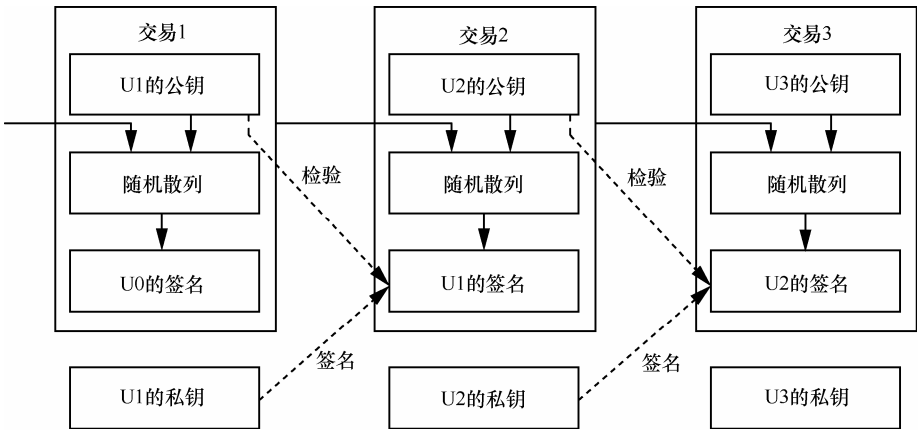

图 1　区块链链式结构散列原理

台支持初创企业创建自己的数字货币，用以实现资金的筹集或者“数字股权”的分发，比较有代表性的数字货币众筹平台有 Swarm、Koinify 等，在比特币应用领域实现众筹目前还有很大的争议，需要相应的制衡机构参与和监管措施。

3) 构建去中心化的政府治理服务体系。区块链去中心化、便宜、有效和个性化的特点，使政府部门之间可以借助区块链的技术优势构建政府治理服务体系[6]，这样的体系体现了公平、透明、诚信的特点，其服务内容将包括在线合约认定、法律法规的登记、选举投票[7]、冲突的解决等，建立在区块链技术上的政府治理服务体系会更加有据可查，便于责任的认定和问题的解决。

4) 信息的快速传播及真实性认定。通过区块链可以使各类事件、活动在全世界范围快速传播，同时对传播对象，信息内容的变更进行追溯，因为区块链所包含的数据具有个性化，这就为解决一些科学难题及进行预测提供了可靠的依据。

总之，区块链的核心技术是加密技术[3,8,9]，使用区块链协议可以解决交易信用问题[3,9]，因此区块链与传统的以金融系统为中介的交易相比其交易费用是很低的[10]。以比特币网络为依托，交易者只要安装相应的软件进入这一系统按照相应的协议就可以进行自由交易，因此其交易是跨时空的交易；由于没有金融中介机构的参与，交易者只需等待区块产生即可使用比特币进行支付，因此与跨地域的传统交易相比，其交易更加便捷[3]。区块链技术以“以太坊（ethereum）”为基础架构平台，这一平台包括了文件管理、信息加密传输以及建立交易信用证明的功能[8,11]。由于区块链应用的包容性，使任何进入区块链的人都可以访问相应的记录，也可以提交记录；同时由于所有的交易会被全网记录，使得区块链记录是可追溯的和不可抵赖的；区块链以数学算法为基础，摒弃了不同国家文化、经济的差异，使全世界人民在此基础上建立信用体系成为可能；同时由于区块链运行于互联网，这也使区块链的通用性和扩展性成为可能；区块链可以与大数据进行结合，使得通过大数据分析获取的知识更加精准；同时由于区块链技术与传统技术融合及应用的发展，促使大数据的量级向更高一级发展；区块链的去中心化及不可抵赖性，使区块链为解决合同冲突提供了更加有力的证据，其发展有助于实现社会的公平正义；区块链使用散列算法加时间戳（timestamping），既可以保证交易信息的真实性、独立性和保密性，又为交易提供时间上的证明；基于区块链的交易每一新的交易信息都会向全网广播，每一个加入系统的节点都将收到的交易信息纳入区块，节点始终将最长的链条作为正确的链条，并不断地延伸链条[3]。区块链不仅可以用于经济领域，对于文件信息真实性认证、财产公证、合约的订立等，都可以使用区块链来实现。

另外，区块链作为一种信息技术，目前也存在着有待解决的一些问题。

1) 操作壁垒。区块链作为一种经济体出现于网络中是中立的，即所有接入这一系统的人都可以自由地进行交易，因此区块链是面向全世界数十亿人的一种经济体；然而区块链本身又是一种信息技术，一种以网络为依托，以加密算法为核心的技术，因此就目前来说还有很多技术问题需要解决，对于网络安全知识不太多的用户来说，其操作还不是十分友好。

2) 交易区块链处理速度较慢。目前，每一交易区块处理大约需要 10 min，对于通过网络实现的小额电子商务交易来说，这样的处理速度显然会失去很多客户。

3) 容量较大。从 2014 年到 2015 年，区块链的容量从 14 GB 增长到 25 GB，这样大的容量需要交易用户有很高的网络带宽，使其广泛应用受到很大的影响。

4) 技术及应用融合问题。区块链技术目前一直都在发展过程中，其技术标准有待完善，这就使未来要创造一个如同互联网一样的统一区块链完整应用体系成为未知数，可想而知，随着区块链的蔓延性发展，这样的完整应用体系的构建是相当困难的。

目前，区块链的应用项目也很多，国外比较有代表性的项目主要有 Ripple、Counterparty、Ethereum、Mastercoin、NXT、BitShares 等，国内有代表性的项目主要有万向区块链实验室、布比、莱特币、太一系统、精灵天下、安存正信等，这些项目产品在应用中受到了学术专家的广泛关

注，同时也在不断地更新和发展中。因为区块链对经济交易信用的革命性，未来的区块链产品会继续加速产生。

3 区块链技术在 B2B+B2C 供应链交易认证中的应用

近年来，互联网用户的信用问题引起全社会的关注。区块链技术的高可靠性证明机制给人们解决交易双方信用问题带来了新的方向和希望。区块链的主要特点是可信、透明、高安全、低成本、去中心化等，这些都是对现有互联网交易体系基础架构及原理的巨大变革，尤其区块链不需要信用数据的信任证明机制，彻底解决了传统信用体系的可抵赖问题。本文基于区块链的基本理论与技术，提出 B2B+B2C 供应链各交易主体交易结构和动态多中心协同认证模型。

3.1 B2B+B2C 供应链各交易主体区块链交易结构

B2B 与 B2C 交易是网络交易的主要模式，在现实生活中面临着严重的交易信用问题，虽然大数据技术的发展给 B2B 与 B2C 交易信用问题带来了契机，交易双方可以借助大数据技术遍历对方交易大数据以获取对方交易数据信息的证明。但由于有时数据来源受限，导致无法获取完善的交易信用证明数据，同时由于数据源及数据信息的独立性，大数据技术也为不法分子修改、破坏、盗窃、交易数据提供了更高的可能，所以从根本上来说，大数据技术仍然不能彻底解决 B2B 与 B2C 交易的数据证明问题。

B2B+B2C 供应链是从原材料到产成品全部交易所经历的整个链条，其间涉及供应商、生产企业、销售商、客户等多个交易主体，整个供应链条的一部分蕴含在企业的企业资源计划（ERP，enterprise resource planning）之中，而 ERP 是生产企业的一个复杂的管理信息系统，所以对于一个具有一定规模的企业来说，其 B2B+B2C 供应链的整个交易关系也是复杂的，这也同时导致了 B2B+B2C 供应链各交易主体之间交易行为认证的难度，区块链技术的产生恰恰可以解决 B2B+B2C 供应链各交易主体之间交易行为认证困难的问题。

在对区块链技术及 B2B+B2C 供应链结构进行分析研究的基础上，本文构建了基于区块链的 B2B+B2C 供应链各交易主体交易结构如图 2 所示。

在图 2 中，供应商、企业内部交易主体、销售商与客户的交易关系结构构成了供应链，各交易主体交易的过程是在区块链技术的基础上实现的，这样可以确保 B2B+B2C 供应链这一包含庞大交易主体的交易过程是有证据可以查询的。

3.2 区块链技术在 B2B+B2C 供应链中的认证模型

在传统的交易中，通常使用单一的中心机构实现交易行为的认证，认证中心需要具有一定的独立性、权威性和固定性，B2B+B2C 供应链传统独立中心认证模型如图 3 所示，有关独立认证中

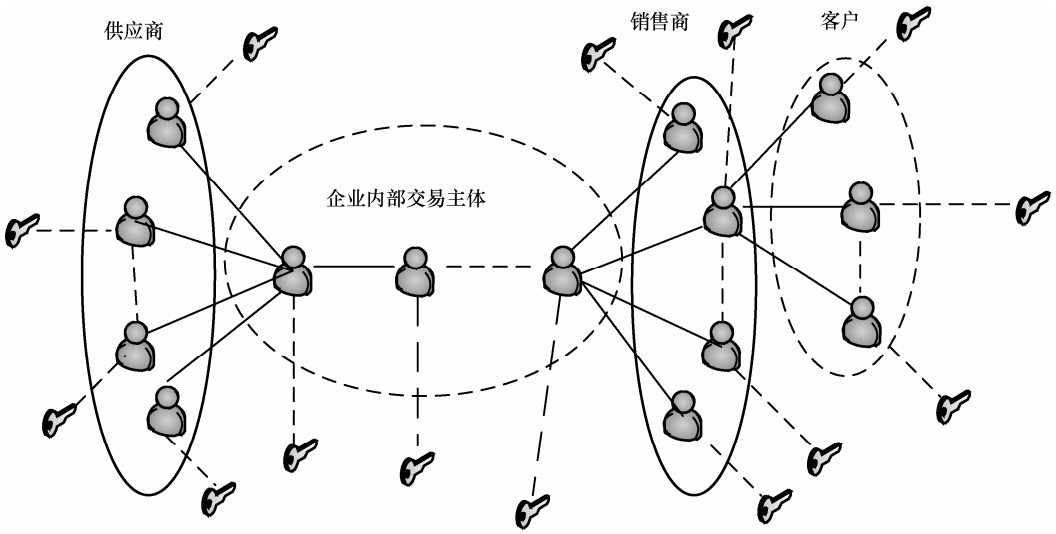

图 2 基于区块链的 B2B+B2C 供应链各交易主体交易结构

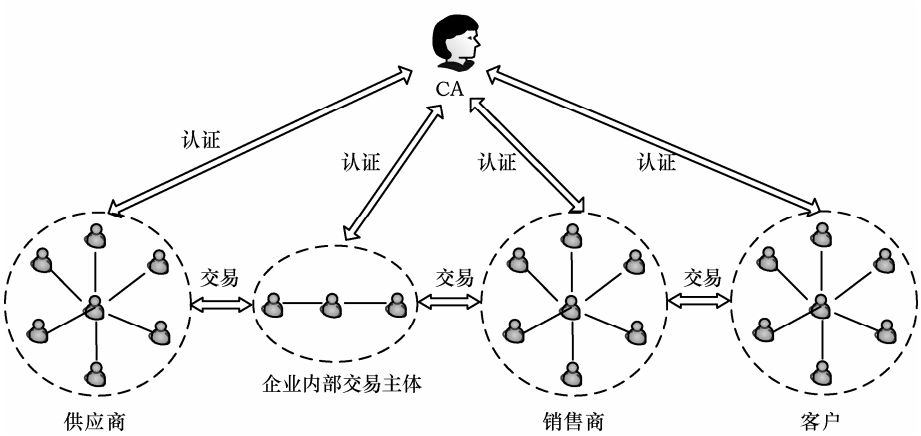

图 3　B2B+B2C 供应链传统独立中心认证模型

心的缺点本文不做过多阐述。

通过对 B2B+B2C 供应链各交易主体的交易行为进行分析可以看出，B2B+B2C 供应链各交易主体是动态变化的，尤其客户的流动性更大，而且具有很大的随机性，但是 B2B+B2C 供应链企业内部交易主体基本上是固定的，而且上游的供应商和下游的销售商在一定的时间内也体现了较大的固定性，而在基于区块链的交易行为认证机制下，企业内部交易主体、供应商、销售商又是区块链的认证主体，这样可以考虑构建集内部交易主体、供应商、销售商为认证集体的基于区块链的供应链动态多中心协同认证模型，同时客户作为区块链交易的一个主体也进行交易行为认证，但不再作为认证中心，客户参与认证的作用是在多中心协同认证仍不能实现交易行为证明的情况下进一步作出证明。

与传统的独立中心认证相比，基于区块链的 B2B+B2C 供应链动态多中心协同认证模型不需要委托第三方作为独立的认证中心，由多交易主体作为不同认证中心共同来认证供应链交易行为。从长期来说，上游的供应商与下游的销售商是动态变化的，这样可以确保参与认证交易主体构成的认证中心的数量并防止共谋的形成。各认证中心是 B2B+B2C 供应链的交易行为主体，受利益博弈会主动遵守信用机制，因此基于区块链的 B2B+B2C 供应链动态多中心协同认证模型具有高的交易行为证明性和稳定性。基于区块链的 B2B+B2C 供应链动态多中心协同认证模型如图 4 所示（在图 4 中，CA 表示认证中心）。

由图 4 可以看出，企业内部交易主体、供应商、销售商之间任何一个交易主体都有交易行为证明的能力，如果某一个交易主体单独或者联合其他交易主体试图篡改交易记录，其他交易主体可以根据自己对交易的记录证明其不法行为，并将其踢出供应链。如果销售商中的一个或者多个交易主体试图欺诈客户，由于客户本身也具有交易证明的能力，客户可以向其他作为认证中心的交易主体反映，经多个认证中心核实情况后将不

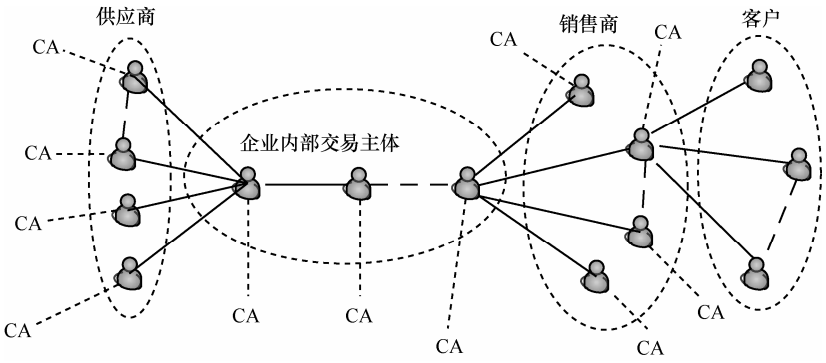

图 4　基于区块链的 B2B+B2C 供应链动态多中心协同认证模型

法销售商踢出供应链。如果客户试图欺诈销售商，经多交易中心协同认证后将不法客户进行记录，取消其交易资格。

基于区块链的 B2B+B2C 供应链动态多中心协同认证模型可以保证多个交易中心组成的整体认证机构具有一定的稳定性，这样便于企业内部交易主体、供应商、销售商共同掌握商品的销售情况和客户行为情况，共同经营供应链，保证交易信息的高度透明性、一致性和真实性，促进企业内部交易主体、供应商、销售商集体作出决策。

4 实例分析

近几年以来，我国煤炭销售一直供过于求，煤炭行业处于低迷状态，而长期以来我国大型煤炭企业原材料采购、产成品的销售一直沿用着在政府参与情况下由集团公司统购统销的经营模式，在市场经济高速发展的情况下，我国大型煤炭企业目前的经营模式对于其参与国际竞争，走出困境显然是不利的。随着电子商务的发展，我国很多大型煤炭企业也建立了自身企业采购、销售的电子商务平台，但在现实中由于交易双方信用没法得到保障，使得我国大型煤炭企业的电子商务平台事实上只是起到了采购需求发布、产品展示宣传的一个媒介，电子商务平台没能发挥其应有的效用。

基于我国大型煤炭企业传统交易模式成本高昂，现有的电子商务平台下又体现出与供应商及销售商、客户交易效率低下的现状，提出基于区块链技术构建我国大型煤炭企业的电子交易平台，以最大程度地开拓我国大型煤炭企业的交易市场，提高交易效率。基于区块链的大型煤炭企业电子交易平台由集团公司随时统计二级矿井的原材料需求状态及产成品待销状况，并将信息发布于集团公司的电子交易平台，上游的原材料供应商可以在集团公司的 B2B 电子交易平台与集团公司进行原材料的交易，下游的销售商也可以在集团公司的 B2B 电子交易平台与集团公司进行产成品的交易，然后销售商将产成品在自己的基于区块链的 B2C 电子交易平台进行销售。由于基于区块链的 B2B 与 B2C 电子交易平台交易主体的交易行为将是完全证明和无可抵赖的，所以供应商、煤炭企业、销售商受利益驱使将会共同经营整个供应链，给顾客提供可靠的产品和真诚的服务；对于客户来说，由于交易的不可抵赖性，客户也将真诚地与销售商进行交易，以免受到不必要的惩罚。

基于区块链的大型煤炭企业 B2B+B2C 电子交易流程及其交易认证过程如下：

1) 煤炭企业构建自己的 B2B 电子交易平台，销售商构建自己的 B2C 电子交易平台，所有的 B2B 与 B2C 电子交易平台加入 internet；

2) 构建煤炭企业基于区块链技术的网络系统并接入 internet，将煤炭企业的 B2B 电子交易平台接入基于区块链技术的网络系统，将销售商的 B2C 电子交易平台接入基于区块链技术的网络系统；

3) 供应商通过煤炭企业的 B2B 电子交易平台与煤炭企业进行网络交易；

4) 供应商与煤炭企业的网络交易在整个基于区块链技术的网络系统中进行全网广播；

5) 所有的供应商、煤炭企业、销售商、客户将收到的电子交易信息纳入到一个区块中；

6) 所有的供应商、煤炭企业、销售商、客户都尝试在自己的区块中找到一个证明交易信息真实性的工作量；

7) 当供应商、煤炭企业、销售商、客户中的任何一个找到工作量证明以后，就会向全网进行广播；

8) 所有的供应商、煤炭企业、销售商、客户认同该新的交易是有效的且是最新的，接受该交易信息，认同区块的有效性，否则对该交易的真实性提出疑问；

9) 其交易区块链接到上一区块末尾，延长区块链一个区块；

10) 交易继续进行，煤炭企业通过自己的 B2B 电子交易平台与销售商进行网络交易；

11) 煤炭企业与销售商的电子交易及区块链认证过程参照 4)~9)执行；

12) 交易继续进行，销售商通过自己的 B2C 电子交易平台与客户进行电子交易；

13) 销售商与顾客的电子交易及区块链认证过程参照 4)~9)执行。

大型煤炭企业 B2B+B2C 电子交易的区块链产生过程如图 5 所示（这里假设一次交易形成一个区块）。

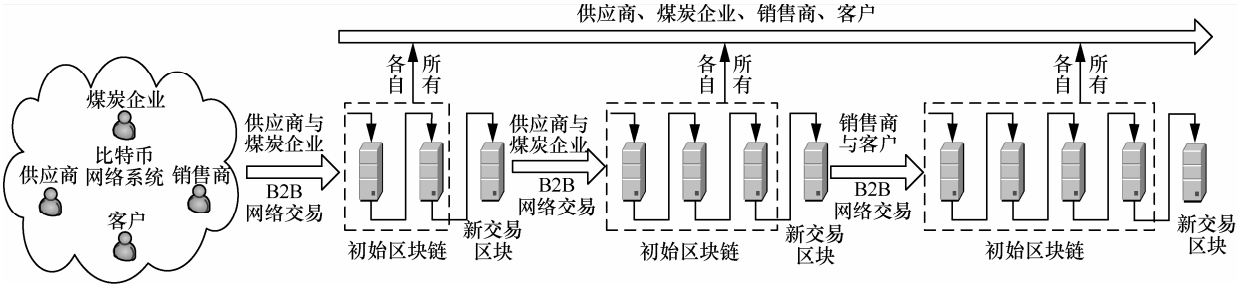

图 5　大型煤炭企业 B2B+B2C 电子交易的区块链产生过程

显然，区块链技术的交易可证明性促进了大型煤炭企业电子交易的应用，为促进煤炭企业与供应商、销售商之间的交易以及销售商与客户的交易提供了有力的行为证据保障。对于我国中小煤炭企业来说，也可以通过联合组成虚拟组织的形式构建基于区块链的电子交易平台，提高其市场竞争力，本文不再累述。

5　结束语

在比特币以及区块链受到学术界及产业界关注的情况下，本文分析了区块链的特点、局限性及其链式结构散列原理，分析了区块链的研究进展及应用现状；探索了基于区块链的 B2B+B2C 供应链各交易主体交易结构并提出了基于区块链的 B2B+B2C 供应链动态多中心协同认证模型，结合我国大型煤炭企业现状，分析了大型煤炭企业 B2B+B2C 电子交易的区块链产生过程，其研究对于其他企业电子交易平台交易证明体系的构建具有一定的参考价值。

目前，由于区块链容量、处理速度、操作壁垒的限制，对于 B2B+B2C 交易主体知识水平、个体特性多样化的现实情况来说，区块链短时间之内在 B2B+B2C 供应链交易中得以推广使用还是不现实的；区块链技术需要不断完善，建立全球统一的交易体系架构及协议，提高操作的便利性、界面的友好性以及处理速度，降低区块链运行存放所需的容量空间，才能推进其在 B2B+B2C 供应链交易中应用的速度。

参考文献：

[1] KAVANAGH D, MISCIONE G. Bitcoin and the block chain: a coup d'état in digital heterotopia?[C]//The 9th International Conference in Critical Management Studies: Is there an alternative? Leicester. c2015.

[2] ALI R, BARRDEAR J, CLEWS R, et al. The economics of digital currencies[J]. Social Science Electronic Publishing, 2014(54): 276-286.

[3] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system [EB/OL]. https://bitcoin.org/bitcoin.pdf.

[4] KUMARESAN R, MORAN T, BENTOY I. How to use bitcoin to play decentralized poker[C]//ACM Sigsac Conference on Computer & Communications Security. c2015: 195-206.

[5] 孙文高. 数字签名技术研究[D]. 西安: 西安电子科技大学, 2010.
SUN W G. The Digital Signature Technology Research[D]. Xi'an: Xidian University, 2010.

[6] PRISCO G. Bitcoin governance 2.0: let's block-chain them [EB/OL]. https//www.cryptocoinsnews.com/bitcoingovernance-2-0-lets-block-chain/.

[7] LANN G L. Distributed systems-towards a formal approach[C]// IFIP Congress. Toronto, c1977: 155-160.

[8] BUTERIN V. Ethereum white paper[EB/OL]. https://github.com/ethereum/wiki/wiki/White-Paper.

[9] Blockchain: the next big thing[EB/OL]. http://www.economist.com/news/special-report/21650295-or-it-next-big- thing.

[10] BUTERIN V. Scalability, part 1: building on top[EB/OL].http://blog. ethereum.org/2014/09/17/scalability-part-1-building-top/.

[11] WOOD G. Ethereum yellow paper[EB/OL]. http://gavwood.com/paper.pdf.

作者简介：

朱建明（1965-），男，山西太原人，中央财经大学信息学院教授、博士生导师，主要研究方向为信息安全、经济信息分析。

付永贵（1976-），男，山西广灵人，中央财经大学信息学院博士生，山西财经大学信息管理学院副教授，主要研究方向为经济信息分析。