基于区块链技术的电子支付去中心化问题研究

文 / 刘罡　杨坚争

摘要：区块链技术是一种去中心化，去信任化的分布式数据存储技术。其不依赖第三方，运用数学手段保证交易的安全性和不可篡改性的特点针对电子支付领域的痛点，被认为是下一代电子支付技术。但是区块链技术在支付领域的实际应用中暴露出了其无法同时满足“高效低能耗”“支付安全”“去中心化”的“不可能三角”问题。本文通过对“不可能三角”问题和区块链运行机理进行分析后得出结论：“去中心化”是区块链技术的表现形式而不是根本特征，要平衡“不可能三角”需要将“去中心化”变为“多中心化”。依据此结论文章对区块链技术在电子支付领域未来的发展提出了建议。

关键词：区块链，比特币，去中心化，不可能三角

中图分类号：F49

DOI:10.14011/j.cnki.dzsw.2019.09.019

引言

随着近几年中国电子商务迅猛发展，电子支付这种新兴的支付方式也得到了快速普及。据中国互联网信息中心第41次《中国互联网络发展状况统计报告》显示[1]：截至2017年12月，我国使用网上支付的用户规模达到5.31亿。其中手机支付用户规模增长迅速，达到5.27亿，使用比例达70.0%。通过几年的商业布局和市场培育，电子支付已经逐渐从线上交易向线下渗透。据报告显示：在线下消费使用手机网上支付的用户中，更多使用手机电子支付的比例为39.1%，超过了更多使用现金、银行卡支付等传统方式的比例31.1%。

安全问题始终是制约电子支付发展的首要问题。无论是以支付宝和微信支付为代表的第三方支付还是银联主导的闪付，在技术实现方面都是中心化的设计。一旦中心服务器遭受黑客攻击或者通讯连接出现问题将导致整个支付系统的瘫痪。另外大量用户资料存储在中心化的服务器中也增加了用户信息泄露的风险。

效率和成本也是电子支付需要考虑的问题。近年来，随着人们生活水平的提高，对跨境消费的需求也越来越大。目前跨境支付普遍存在支付周期长和费率高等问题。根据世界经济论坛报告 《全球金融基础设施的未来》[2]，汇款人的跨境支付费用一般是汇款金额的7.68%，基于SWIFT①框架的跨境汇款通常需要2~3个工作日才能到账。

以去中心化和去信任化为特点的区块链技术的出现，为解决电子支付存在的问题提供了新的解决方案。

①SWIFT：环球同业银行金融电讯协会，是国际银行同业间的国际合作组织，swift系统为银行提供银行的结算提供了安全、可靠、快捷、标准化、自动化的通讯业务，大大提高了银行的结算速度

1、区块链技术概述

区块链技术，简称BT（Blockchain Technology）起源于2008年由化名为中本聪"（Satoshi nakamoto）的学者在密码学邮件组发表的奠基性论文《比特币：一种点对点电子现金系统》[3]，也被称为分布式账本技术，是一种互联网数据数据库技术。其按照时间顺序将数据区块用类似链表的方式组成数据结构，并以密码学方式保证不可篡改和不可伪造的分布式去中心化账本，能够安全存储简单的、有先后关系的、能在系统内进行验证的数据[7]。区块链技术最显著的特点是去中心化和去信任化。

1） 去中心化

区块链技术的去中心化是指在区块链中各节点之间是完全平等，高度自治的。任意一个节点都可能成为一个区域的中心，但他没有对其他节点的控制功能。在技术实现上，区块链建立了一个分布式数据库，将整个区块链上的交易信息分布式的存储在每一个节点上。去中心化的优势是从根本上解决了少数中心节点出现故障导致整个系统瘫痪的问题。

2）去信任化

区块链技术的去信任化是指在区块链中参与交易的双方无须再进行身份的验证，只需要按照预先设计的程序进行交易，即可建立互信的交易模式。在技术实现上，区块链中每个节点都维护有一套相同的区块链交易信息副本，当新交易产生的时候区块链会应用数学方法向其他节点验证该交易的有效性。去信任化的优势：第一，去除了交易中的可信任第三方的参与，使得交易过程更加简化，减少了可能出错和被攻击的环节；第二，全网所有节点均参与交易账本的验证，使得交易过程更加透明和可追溯，更加不易被篡改。

2、电子支付的特点及区块链技术的应用前景

目前我国主流的电子支付平台为以银行卡为基础的银联支付平台和以支付宝、微信支付为代表的第三方支付平台，这些支付方式均采用中心化模式运行。中心化电子支付最大的优势是支付高效能耗低，最大问题是支付安全。

支付便捷高效是中心化电子支付最大的优势。首先这种支付模式下支付信息的存储和交易都集中在服务器端，对支付终端的性能要求不高，这有利于电子支付的大范围普及；其次一个强有力中心的存在，有利于保持对整个系统的持续投入，保证系统软硬件持续升级，改善用户的使用体验。目前我国的电子支付平台不仅可以满足日常即时支付的需要，还可以满足诸

★基金项目：国家自然科学基金项目“世界市场的虚拟化与我国国际电子商务发展策略研究”基金编号：70973079。

如“双十一购物节”②这种集中爆发式的支付需求。

能耗低是中心化电子支付另一个优势。由于支付信息的处理和存储都集中在服务器端，支付终端所花费的能源几乎可以忽略不计。虽然服务器端集中了海量的数据处理需求需要消耗大量的能源，但其可以发挥规模效应，通过升级和优化软硬件设备来降低单位信息处理的能耗。同时可以通过将中心处理器布置在能源充足，电费相对较低的地区进一步降低信息处理的成本。

支付安全是中心化电子支付所要面临的主要问题。中心化支付系统的服务器，是各种网络攻击的袭击目标。虽然支付平台的中心服务器都有严密的安全保障系统，但面对花样繁多的网络攻击，也无法做到万无一失。一旦中心服务器的安全机制被攻破，整个支付系统将陷入瘫痪。如果存储在中心服务器中的海量用户信息发生泄露，将会造成无法估量的经济损失和社会影响。

区块链技术在电子支付领域的应用正好可以解决支付安全问题。区块链是一种按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构， 并以密码学方式保证的不可篡改和不可伪造的分布式账本。区块链技术赋予了支付过程透明、可追溯、不可更改等特点，可以有效解决电子支付中存在的双重支付问题和拜占庭将军问题[12,13]，被认为是目前最为安全的支付方式。

3、区块链在电子支付领域遇到的“不可能三角”困境

“不可能三角”理论是由克鲁格曼于1999年提出的，原来是指经济社会和财政金融政策目标选择面临诸多困境，难以同时获得三个方面的目标。在金融政策方面，资本自由流动、汇率稳定和货币政策独立性三者也不可能兼得[5]。区块链在电子支付领域的应用也遇到了类似的问题：“高效低能耗”，“支付安全”，“去中心化”三者很难同时满足[6]。如图1所示：

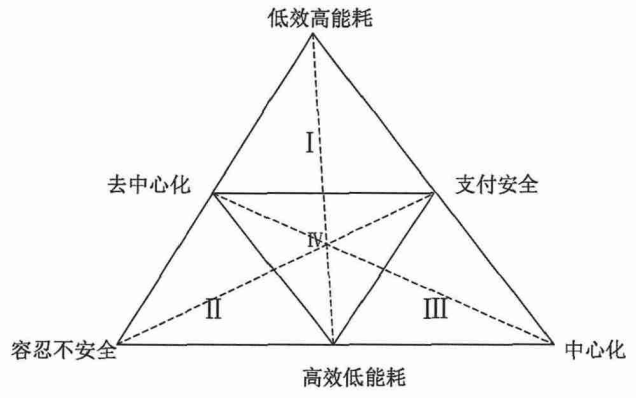

图1 区块链支付的“不可能三角”

按照“不可能三角”理论，区块链技术可以取到图中Ⅰ、Ⅱ、Ⅲ三个区域，区域Ⅳ无法取得。区域Ⅰ表示：要实现支付领域的去中心化和支付安全，就需要舍弃系统的高效低能耗。这正是以“比特币”为代表的数字货币的现状。为了达到去中心化和支付安全的目的，比特币牺牲了高效和低能耗。首先，为了吸引更多人加入比特币区块链中，系统设计了基于工作量证明（Proof of Work）的激励机制。这种机制赋予第一个解决特定数学问题的计算机记录新开辟的区块中交易的权利，并奖励其一定数量的比特币。为了获得奖励，大量算力被用来解决没有实际意义的数学问题，造成了大量电能的浪费；其次，为了实现去中心化的交易验证，所有参与交易的节点中都需要保存全链交易的副本，这对每个参与节点的存储空间提出了较高的要求。截至2018年7月，一个完整的比特币钱包大概需要100G的存储空间，并且还在持续增加；再次，比特币的支付效率无法满足实时交易的需要。根据比特币交易验证规则的设计，一笔交易确认需要60分钟，理论上全链每秒只能处理7笔交易。

区域Ⅱ表示：要想获得去中心化和高效低能耗就需要容忍系统的不安全。在既没有信息中心又要保证交易效率和能耗的前提下，系统无法进行复杂的身份验证，这将给交易安全带来巨大隐患。与之类似的例子如P2P资源下载软件。为了提高可下载资源的数量和下载速度，这类软件一般不对用户的身份进行验证。由于缺少管理中心，造成无人对上传的资源进行审核，这会导致电脑病毒和不良咨询在网络上传播等安全问题。

区域Ⅲ表示：要想获得高效低能耗和安全的支付环境，则无法实现去中心化。这正是目前电子支付系统采用的模式。目前区块链应用中，为了解决支付效率的问题采用了权益证明（Proof of Stack）股份授权证明（Delegate Proof of Stack）等新的区块链奖励机制，并且在公有链基础上发展出了“联盟链”和“私有链”等新的区块链形式，这都是在一定程度上形成了新的“中心”。

4、面对区块链“不可能三角”的对策

区块链“不可能三角”决定了我们必须在“高效低能耗”“安全”“去中心化”三者中至少舍弃一项，这三项内容如何取舍就成了我们需要考虑的问题。首先“安全”不能舍弃。“安全”是电子支付的前提条件，再高效的系统如果没有安全保障都没有人会去使用；其次“高效低能耗”不能舍弃。“高效低能耗”是电子支付区别于传统支付方式的最主要特点，也是电子支付出现的初衷，如果舍弃则是历史的倒退。

由此可见唯有在“去中心化”上做出妥协。有人担心“去中心化”是区块链的主要特征，舍弃“去中心化”就是否定区块链技术在电子支付领域存在的意义，事实并非如此：

1）去中心化是区块链技术的外在表现形式而非根本特征。

区块链是一个开放的、安全的、匿名的、自洽的交易系统[7]。区块链设计的根本思想是设计一个不依赖任何组织和机构，也不受任何组织和机构的控制，完全按照预先设计好的规则和算法来运行的系统，其在目前的技术条件下的外在表现就是“去中心化”。可以看出“去中心化”并不是系统设计的目的，而是满足区块链设计目标现阶段的解决方案，在未来更先进的技术手段和设计方法下完全可能出现其他的解决方案。

2）目前的区块链并非是完全去中心化的。

虽然区块链被设计为一个由数学算法控制的完全“去中心化”的系统，但“去中心化”固有的缺陷使得目前的区块链并无法做到完全“去中心化”。首先区块链的设计是“中心化”的：通过对“比特币”代码的分析显示，绝大部分代码出自几个程序员之手，这种中心化的设计模式导致“比特币”的实际控制权掌握在少数人手中。在区块链发展到以太坊[8]为代表的区块链2.0时代，出现了DAO（Decentralized Autonomous

②“双十一购物节”购物节最早是天猫平台于2009年11月11日发起的商品促销活动，后来发展为一年一度的电商购物节。2017年“双十一购物节”仅仅天猫一个平台营业额超过1682亿元，支付达14.9亿笔。

Organization）。这种以去中心化为名称的组织掌握了智能合约制定和修改的权利，形成了实际上的中心化；其次是区块链运行的“中心化”：以“比特币”为例，系统设计的初衷是每个参与节点获取比特币奖励的几率是相同的，但在实际运行中，为了提高获取比特币的几率，众多节点联合起来形成了一个大的矿区。目前世界上最大的几个矿区的算力总和已经超过了发动51%攻击[9]的要求。

3）去中心化已成为区块链技术推广的障碍。

根据可视化大数据网站HowMuch.net统计，截至2018年2月，全球246个国家中有10个国家（占比4%）认定比特币为非法，7个国家（占比3%）认定比特币为受限制的市场，99个国家（占比40%）对比特币使用不加限制，130个国家（占比53%）对比特币的态度不明确。由此可见，大多数国家对于区块链技术的应用持观望态度，即使是不限制比特币交易的国家，大多也是持着加强监管的态度。各国对区块链技术发展所持的这种谨慎的态度很大一部分原因是源于区块链的去中心化的特点。区块链去中心化的特点使得单个国家很难对区块链支付进行监管，对区块链支付的监管必须进行国际合作，这大大增加了监管的成本和难度。而一个缺乏监管的市场很容易成为洗钱等金融犯罪的工具。所以目前各国只能通过限制代币的交易来控制相应的金融风险，这就大大限制了区块链技术的推广。

5、对区块链支付技术的发展建议

1）强化政府作为推广区块链支付应用的核心地位。

目前区块链支付应用推广的最大障碍是作为支付主体的代币种类繁多且币值波动剧烈。以目前最大的区块链代币“比特币”为例，“比特币”更多的被作为是一种投资产品而不是支付系统，造成这种情况的一个重要原因是“比特币”背后没有国家信用或者实体资产作为背书，其价格完全依赖市场供求关系来决定。解决这个问题最简单的方式是由政府来发行区块链数字货币，用国家信用来保证币值相对稳定，以国家强制力保证数字货币的自由流通。目前世界上已经有几个国家发行了基于区块链技术的数字货币，我国也正在积极研究我国区块链数字货币的发行方案。

2）依托现有银行系统发展区块链支付。

现代银行系统历经数百年的发展已经形成了一个庞大而完善的金融体系，目前主流的电子支付系统也都是基于银行系统的。区块链支付系统完全独立于现有的银行系统，因此在其运行过程中难免会遇到诸如监管、税收、风险控制等一系列法律问题。要解决以上问题，目前最可行的解决方案是应用区块链技术对传统银行系统进行改造，使银行支付系统具有区块链的安全，便捷的特点。目前世界上的主要银行也表现出了进行区块链改造的强烈愿望，许多重要银行加入了R3区块链联盟③，如花旗银行和瑞士银行等还发行了自己的数字货币。

3）转变发展思路，变“去中心”为“多中心”。

区块链技术的核心思想是交易过程的“去干预化”，用数学的方法来保证交易各个环节的安全，将人为的干预将至最低限度，在现阶段表现为“去中心化”。但随着区块链应用的深入，“去中心化”表现出来的效率低下、对使用终端的性能要求高等问题纷纷暴露了出来，一味坚持“去中心化”只能使得区块链技术陷入缺少用户的困境。我们可以借鉴“联盟链”的思路，设计若干个区域中心节点，将数据存储和交易验证工作交给区域中心节点，从而保持用户节点的“轻载”，最大限度得在保留区块链优点的基础上减少用户的使用成本。

③R3CEV是一家总部位于纽约的区块链创业公司，由其发起的R3区块链联盟，至今已吸引了42家巨头银行的参与，其中包括富国银行、美国银行、纽约梅隆银行、花旗银行、德国商业银行、德意志银行、汇丰银行、三菱UFJ金融集团、摩根士丹利、澳大利亚国民银行、加拿大皇家银行、瑞典北欧斯安银行（SEB）、法国兴业银行等。

参考文献

[1] 中国互联网信息中心. 第41次《中国互联网络发展状况统计报告》[EB/OL].[2018-1-31]. http://www.cac.gov.cn/2018-01/31/c_1122346138.htm

[2] The future of financial infrastructure: An ambitious look at how blockchain can reshape financial services: Report of WEF[R]. Deloitte:WEF,2016

[3] Nakamoto S. Bitcoin: a peer-to-peer electronic cash system[EB/OL]. available: https://bitcoin.org/bitcoin.pdf, 2009

[4] coinmarketcap[EB/OL].[2018-08-15].https://coinmarketcap.com/

[5] 保罗.克鲁格曼.萧条经济学的回归[M].北京：中国人民大学出版社,1999

[6] 陈一稀，区块链技术的“不可能三角”及需要注意的问题研究[J].浙江金融，2016,2:17-20

[7] 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

[8] Ethereum White Paper. A next-generation smart contract and decentralized application platform [EB/OL],available: https://github.com/ethereum/wiki/wiki/White-Paper, November 12, 2015

[9] 沈鑫.区块链技术综述[J]. 网络与信息安全学报,2016,11:107-117

[10] D. Leung,A. Dickinger.Use of Bitcoin in Online Travel Product Shopping : The European Perspective[J]. Information and Communication Technologies in Tourism 2017, 2017, 741 – 754.

[11] Blockchain Luxembourg S.A.Bitcoin Stats[EB/OL]. Available: https://blockchain.info/en/stats,2018

[12] SWAN M. Blockchain thinking: the brain as a decentralized autonomous corporation [J].IEEE Technology and Society Magazine,2015, 34(4):41-52.

[13] FAN J, YI L T, SHU J W. Research on the technologies of Byzantinesystem[J]. Journal of Software, 2013, 24(6):1346-1360

作者简介：

刘罡、博士研究生、上海理工大学管理学院，研究方向：电子商务，电子支付，跨境贸易；

杨坚争、教授、上海理工大学管理学院，研究方向：电子商务发展政策、电子商务交易安全、电子商务法律。