DOI:10.13878/j.cnki.jnuist.2019.05.001

高峰[1]　祝烈煌[1]　丁凯[1]　巩国鹏[2]　戴庆祝[3]

区块链稳定代币研究进展

摘要

作为一种具有价值稳定属性的特殊加密货币,稳定代币不仅能够成为链接区块链加密资产和现实世界资产的桥梁,而且有潜力降低金融行业的中介成本、提高资金转移的效率.自摩根大通、Facebook 等国际知名企业宣布其稳定代币计划后,稳定代币成为监管机构、企业界和科研机构的研究热点.本文通过对比法币、加密货币与稳定代币,深入分析了稳定代币的特征,然后从区块链基础设施、价值稳定机制、运营机制 3 个方面详细介绍了稳定代币的系统架构和运行机制.最后结合稳定代币的技术特点,分析了稳定代币系统面临的缺陷和可能的解决方案.

关键词

区块链;加密货币;稳定代币;共识机制;隐私保护

中图分类号 TP309;TP311.13

文献标志码 A

收稿日期 2019-08-18

资助项目 广东省重点领域研发计划项目(2019B010137003)

作者简介

高峰,男,博士,主要研究领域为区块链数字货币监管、网络与信息安全.gaofengbit@foxmail.com

祝烈煌(通信作者),男,博士,教授,主要研究领域为密码学、网络与信息安全.liehuangz@bit.edu.cn

1　北京理工大学 计算机学院,北京,100081

2　临沂冠奇信息科技有限公司,临沂,276000

3　杭州链大科技有限公司,杭州,310012

0　引言

自从中本聪发表论文《Bitcoin:a peer-to-peer electronic cash system》[1]以来,一种新型的去中心化技术范式——区块链得到快速发展和推广,成为学界、企业界、甚至普通民众耳熟能详的热点话题.比特币作为区块链技术的第一个成功应用受到广泛关注,随之产生了以太币、门罗币等大量基于区块链技术的加密货币.之后,为加密货币项目提供融资的 ICO、STO 等新机制更是将加密货币行业变成大众关注的热点,被认为是改革传统融资模式、变革世界经济体系的新技术.然而,从 2017 年开始,由于 ICO 导致的加密货币泡沫带来了巨大的金融风险,各国颁布了严厉的监管政策,导致加密货币行业陷入寒冬时期.区块链技术的研究重点从加密货币领域转移到以“无币区块链”为口号的其他行业.然而,随着著名跨国互联网公司 Facebook 推出了基于区块链技术的稳定代币项目 Libra,全世界的目光重新聚焦到区块链加密货币领域.

稳定代币是一种基于区块链技术的特殊的加密货币.相比比特币等典型的加密货币,稳定代币不仅具备了区块链技术去中介信任、安全可靠的核心优势,而且具备与现实资产稳定挂钩的特点.例如,GUSD、PAX 稳定代币与美元保持 1:1的兑换比例,DGD 稳定代币与 1 g 黄金保持 1:1的兑换比例,此外还存在与日元、人民币、石油等多类型现实资产保持稳定兑换比例的稳定代币项目.通过与现实资产挂钩,稳定代币解决了传统加密货币价值剧烈波动、市场操控严重的问题,不仅可以作为加密货币与现实世界的纽带,推进加密货币领域的发展.而且稳定代币具备了解决现实世界资产流动问题的潜力,能够减少中介环节、提高流动效率,有望成为推动金融行业改革的核心技术.

稳定代币最早的目的是解决加密货币领域的兑换问题.随着加密货币的快速发展,加密货币的种类快速增加,截止到 2019 年 7 月,全球加密货币种类超过 2 391 种.这些加密货币之间存在大量的交换需求.如果直接使用法币作为交换的中间媒介,则会受限于现实金融业务的性能瓶颈,造成严重的性能延迟和巨大的中介费用.因此,一种基于区块链技术并且和法币锚定的加密货币应运而生.2014 年,Tether 公司推出了基于比特币架构、和美元挂钩的稳定代币 USDT[2-3],迅速占据了加密货币交换领域的市场,目前市值超过 40 亿美元,占据稳定

代币市场的80%以上的份额.2018年,世界上首批受到地方政府授权的稳定代币GUSD和PAX诞生,使稳定代币这一特殊的加密货币项目走向大众视野.截止到2019年7月,稳定代币市场价值49亿美元,虽然整体市值在整个加密货币行业比例较小,但是稳定代币对加密货币行业的发展有举足轻重的作用.

随着稳定代币在加密货币兑换业务中的有效应用,稳定代币的潜在价值得到更多关注.稳定代币具备的减少交易中介、提高交换效率的特征不仅可以运用在加密货币行业,同样可以运用在传统金融领域.这种潜力使得稳定代币的应用范围从价值千亿美元的加密货币市场推广到价值数十万亿美元的跨国金融贸易行业.摩根大通公司首先推出了针对公司内部全球业务的稳定代币项目摩根币(JPM Coin),利用基于区块链的稳定代币技术,能够优化摩根大通在全球范围内的金融交易,减少中介消耗.阿里巴巴公司在香港推出的跨境支付业务,虽然没有直接使用稳定代币的概念,但是也采用了稳定代币相同的交易模式.Facebook公司推出的Libra项目则是希望依托Facebook公司在全世界范围内20亿用户规模,建设遍布全球的金融服务,提供跨越国界的、高效便捷的资金交换.

作为一种具有重大影响力的区块链应用,稳定代币将给区块链技术落地实践、区块链金融监管等领域带来重大机遇和挑战.因此,非常有必要调研稳定代币的研究进展,分析稳定代币存在的缺陷,展望稳定代币的技术发展趋势.

1 稳定代币的特征

"稳定代币"是区块链行业产生的一个新词.其中"币"代表这是一种基于区块链技术的加密货币,这限定了其主要的技术特征."稳定"体现了其不同于其他加密货币的特征,即通过锚定现实世界的资产保持相对稳定的价值.通过结合加密货币与现实资产的优势,稳定代币与现有的法币、电子货币、加密货币有明显区别.

1.1 稳定代币的加密货币特性

加密货币是一个历史悠久的名词,早在1988年就出现了Ecash、B-money等一系列基于密码技术的电子货币(也称为数字货币,密码货币).但是,由于当时的技术条件难以解决双花问题、伪造支付问题,这些加密货币都只在少量密码极客圈子内部流通.2008年,中本聪首次提出了一种能够解决双花问题的密码货币机制"比特币",并很快开发、运行了首个比特币客户端,开启了比特币系统的运行.截止到2019年7月,比特币系统作为一种没有实体机构运维的去中心化系统,仅仅依靠全球范围的自愿者,稳定运行了10年之久.目前(2019年7月28日)比特币系统已经产生58万个区块,约150亿条交易数据,创造的比特币市值超过1 700亿美元[4-5].随着比特币系统的成功,逐步出现了以太币、门罗币、EOS等不同类型、不同特征的加密货币.加密货币的技术架构、功能性能、应用范围都得到极大的扩展.但是,从本质上看,加密货币系统遵循了以下主要原则:

1)高冗余存储:指所有已经发生的交易记录将在大量节点中冗余存储.例如,比特币系统在全球范围内的活跃节点维持在9 585个节点左右(2019年7月数据,https://bitnodes.earn.com/),即比特币系统运行10年的所有交易记录在全球范围内大约有10 000个完整备份.这种高度冗余机制使得加密货币的交易记录具有"不可篡改"的特性(任意篡改都将被正常节点发现),使得所有维护账本的节点能够在不需要信任单一节点的条件下,对交易数据产生较高的公信力.

2)分布式执行:指交易的验证和记录操作由分布式节点各自独立完成.在传统的金融结算系统中,交易的执行过程是由具有特殊权限的中心节点完成的,其他节点不能参与执行过程.在基于区块链的加密货币系统中,交易的验证和记录过程由经过共识机制挑选的记账节点(也被称为"矿工节点")负责执行,理论上任意节点都有被挑选到的机会.通过选取非固定的节点执行区块链交易的验证和记录过程,能够提高系统稳定性,减少部分节点失效或恶意操作的风险.

3)多数决策:指当区块链系统中出现分歧时,采用少数服从多数的原则对分歧进行仲裁.在分布式场景中,由于受到网络延迟、节点偏好等多方面的影响,不同节点之间在数据同步、策略选择等过程容易产生分歧.加密货币所依赖的区块链系统通常采用多数决策的机制解决此类分歧.例如,比特币系统中,当存储交易记录的数据结构"链"出现分叉时,比特币网络中的节点将按照"最长链"原则(即选择比特币网络中包含区块最多的链作为主链)选择其中一个分叉作为同步数据源.最终,被大多数节点选择的分叉将成为合法的数据源.通过采用多数决策原

则,加密货币系统能够在无人监管的条件下实现稳定的运行,并取得较高的公信力.

加密货币所具备的上述特征使其能够构造一种不依赖可信机构的可信交易系统,与传统的法币、电子货币有明显区别.相比法币,加密货币不需要国家机构提供信任背书,不需要传统银行体系提供复杂的管理流程,甚至不需要传统的 IT 运维机构提供设备维护、安全防护等基本服务.仅仅依靠全球志愿者提供的分布式节点,比特币系统成功抵抗了各种网络攻击事件和频繁的市场波动,已经稳定运行了 10 年.相比传统的电子货币(例如 Q 币),加密货币不需要依赖公司提供的信任体系,不会受到单个公司的操控,而是能够建立一种跨越公司、跨越国界的可信交易市场.

稳定代币作为一种特殊的加密货币,自动继承了加密货币"高冗余存储"、"分布式执行"和"多数决策"的核心特征.例如,USDT 稳定代币的交易数据直接内嵌在比特币交易的 OP_RETURN 参数中,和普通的比特币交易一样被所有节点冗余存储.GUSD 稳定代币利用以太坊的智能合约技术实现,每一笔交易的执行过程都被所有节点共同执行.Libra 稳定代币虽然是采用独立的许可链技术实现,但是依然按照多数决策的原则实现.虽然 Libra 稳定代币项目是由 Facebook 公司发起,但是对于 Libra 稳定代币的管理工作是由 Libra 协会负责,协会的每个参与方能够从技术底层对 Libra 稳定代币进行状态监测和管理.

由于稳定代币具备了加密货币的特征,这使得稳定代币具备了跨国界运行、低成本运行的特点.首先,稳定代币的交易过程不经过传统的交易体系,目前针对法币的管理体系无法发挥作用,任何人都可以通过自行创建区块链账号参与稳定代币的全球交易,这使得稳定代币具备了跨国界运行的潜力.其次,稳定代币建立在去中心的区块链系统之上,能够减少中间环节,实现快速、高效、可信的价值转移.相比传统复杂的金融体系(例如 swift),稳定代币的运行成本更低,效率更高.

1.2 稳定代币的价值稳定特性

稳定代币具备价值稳定的特性是指通过锚定法币货币体系(或者其他现实世界资产,例如黄金),使稳定代币与特定法币的汇率保持稳定.稳定代币的这种特性与加密货币和法币都不相同.

在现实货币金融环境中,法币的价值建立在各国的经济基础之上,依赖黄金储备、外汇储备等实体资产作为其价值支撑,由各国政府提供信任背书.各国的法币也需要保持相对稳定的汇率,但是现代中央银行追求的货币稳定目标,大多旨在维持货币跨期购买力的稳定,与国际收支、外汇储备、利率有密切关系,而不是仅仅保持数值的稳定[6].

在加密货币环境中,加密货币的价值不依赖任何实体资产,而是建立在加密货币系统的整体价值之上,依靠分布式算法和开源代码提供信任背书.以比特币为例,比特币的生产过程是为了奖励为系统提供安全保证的矿工,矿工收获的比特币的价值越高,矿工提高"挖矿"性能的动机就越强,比特币系统的性能和安全性就越强.另一方面,比特币的系统的性能和安全性越强,使用比特币系统的用户就越多,比特币系统的价值就越高,这将促进比特币价值的提升.理论上,随着比特币系统的性能和安全性接近理论峰值,比特币的价值将跟随比特币系统的整体价值,趋于稳定状态.但是,实际上由于比特币等密码货币系统面临严重的市场操控风险[7]、网络攻击风险[8-9]和政策调控风险[10-11],比特币目前的价值更多的是依赖参与者的信心,跟随投资环境剧烈波动.

不同于法币和普通的加密货币,稳定代币的价值既不依赖政府提供信任背书,也不依赖虚拟的系统价值,而是通过人为设定的机制,与特定的法币资产保持固定的兑换比例.为了实现稳定代币的价值稳定性,必须满足 3 个具体要求:

1)健康的买入和退出渠道.作为一种虚拟的加密货币,稳定代币的运维机构本身必须提供兜底的代币买入和退出机制,这是保持币值稳定的基础措施.此外,由于稳定代币项目通常涉及全球大量用户,很难由运维机构提供全部兑换业务,在实际运行中通常是由全球各地的加密货币交易所(例如币安、bitrelix)承担面向终端用户的代币交易.在这些交易所中,稳定代币的兑换比例将根据稳定代币的市场信誉、退出难度进行动态调整.稳定代币的运维机构必须与主流交易所建立价格稳定机制,确保终端用户在代币买入和退出时能够享受相对稳定的兑换比例.

2)高效可靠的交易过程.稳定代币的核心作用是充当价值交换的媒介.为了满足这种需求,稳定代币系统的性能和可靠性必须满足实际业务的需求.目前稳定代币主要是运用在加密货币行业中,市场规模和交易频率相对较低,现有稳定代币采用的技

术架构还能够满足业务需求.但是,随着稳定代币技术走向现实金融业务,交易过程的效率和可靠性将成为稳定代币系统必须重点研究的问题.

3)满足监管机构的监管需求.由于稳定代币直接和法币体系挂钩,这使得稳定代币更容易对金融秩序造成影响.相对于普通的加密货币,监管机构将对稳定代币提出更高的监管需求.如何满足监管机构的监管需求,将成为稳定代币系统能否稳定运行的关键问题.

1.3 稳定代币与其他货币的对比

表1对法币、Q币、比特币、稳定代币的特征进行了对比分析.其中,法币对应各国发行的法定货币(例如美元、人民币),Q币(腾讯公司运行的电子积分系统)代表了利用中心化技术构建的电子货币,比特币代表了典型的加密货币,稳定代币是指基于区块链技术并具备价值稳定属性的特殊加密货币.

从运维机构和信任机制的角度看,法币主要是由政府机构运行,依靠政府持有的实体资产作为价值担保,政府提供法偿保证.以Q币为代表的电子代币通常是由公司运营,主要在公司业务范围内充当价值媒介,此类代币系统通常只提供单向买入功能,不提供反向兑换服务.类似的产品还包括游戏公司的游戏币,以及各种类型的电子积分.比特币系统运行在由全世界范围内的志愿者提供的分布式服务器节点之上,依靠可信的分布式算法和开源的代码提供信任机制,不存在一个实体的机构负责系统的日常维护.比特币的算法升级和代码更新依赖于整个比特币开源社区的集体贡献.目前比特币核心代码部署在GitHub上,任何人都可以推送新的代码方案.虽然代码在整合到主版本时依赖少数几个核心开发人员和维护者的操作,但是本质上算法和代码更新的决定权依然是由社区决定,不会受到个别机构或者个人的控制[12].

从技术层面,法币和类似Q币的电子货币都采用了中心化的数据存储机制和交易执行机制,建立了一套高度依赖中心机构的交易体系.在体系内部,这种机制能够提供足够的公信力和超高的性能.但是,当交易超过体系范围时,就必须依赖额外的机制保证交易的可靠性.比特币、稳定代币等加密货币采用了去中心化的数据存储机制和交易执行机制,建立了一套不依赖中心机构的交易体系.在这种机制下,加密货币的信任范围可以根据参与者的增加动态提升.

从价值层面,法币的价值(汇率)是由中央银行根据国家的国际收支、外汇储备、利率等情况动态调控,体现了国家的经济状况.Q币等电子货币的价值则是由公司根据自身业务特点自行设定的,公司具有绝对的解释权.例如,2019年7月,腾讯公司的Q币就进行了全面的涨价.比特币等加密货币的价格则是根据市场自发调控.由于不存在实体机构负责日常维护,此类加密货币的价格主要来源于全球主要数字货币交易所实时变化的价格数据.当市场买入需求提升时,兑换比例将提升,当市场抛售需求提升时,兑换比例将下降.这种完全受控于市场需求的价格变化机制使得比特币等加密货币的价格长期处于剧烈变化的状态,而且很容易受到市场操控、负面消息的影响.

2 稳定代币系统架构

2.1 系统架构

作为一种特殊的加密货币,稳定代币不仅需要依赖区块链技术构建系统运行所必须的底层基础设施,而且需要复杂的运营机制来保证价值稳定的特性.此外,还需要一套价值稳定机制来协调底层区块链基础设施和上层的运行机制.如图1所示,稳定代币系统架构主要包含3个方面:

1)区块链基础设施:指用于构建稳定代币系统核心功能的技术模块.此模块是稳定代币系统能够正常运转的基础保证,将实现交易功能、管理功能和数据记录功能.此模块的设计与系统的性能、安全性、可扩展性密切相关,是稳定代币技术革新的主要区域.

表1 稳定代币与其他货币的对比

Table 1 Comparison between stable coins and other currencies

种类	运维机构	信任机制	数据存储机制	交易执行机制	价格变化机制
法币	政府	实体资产+政府信誉	集中存储	中心化执行	政府调控
Q币	公司	公司信誉	集中存储	中心化执行	公司调控
比特币	无	算法+开源代码	冗余存储	去中心执行	市场调控
稳定代币	公司	算法+开源代码+公司信誉	冗余存储	去中心执行	算法维持

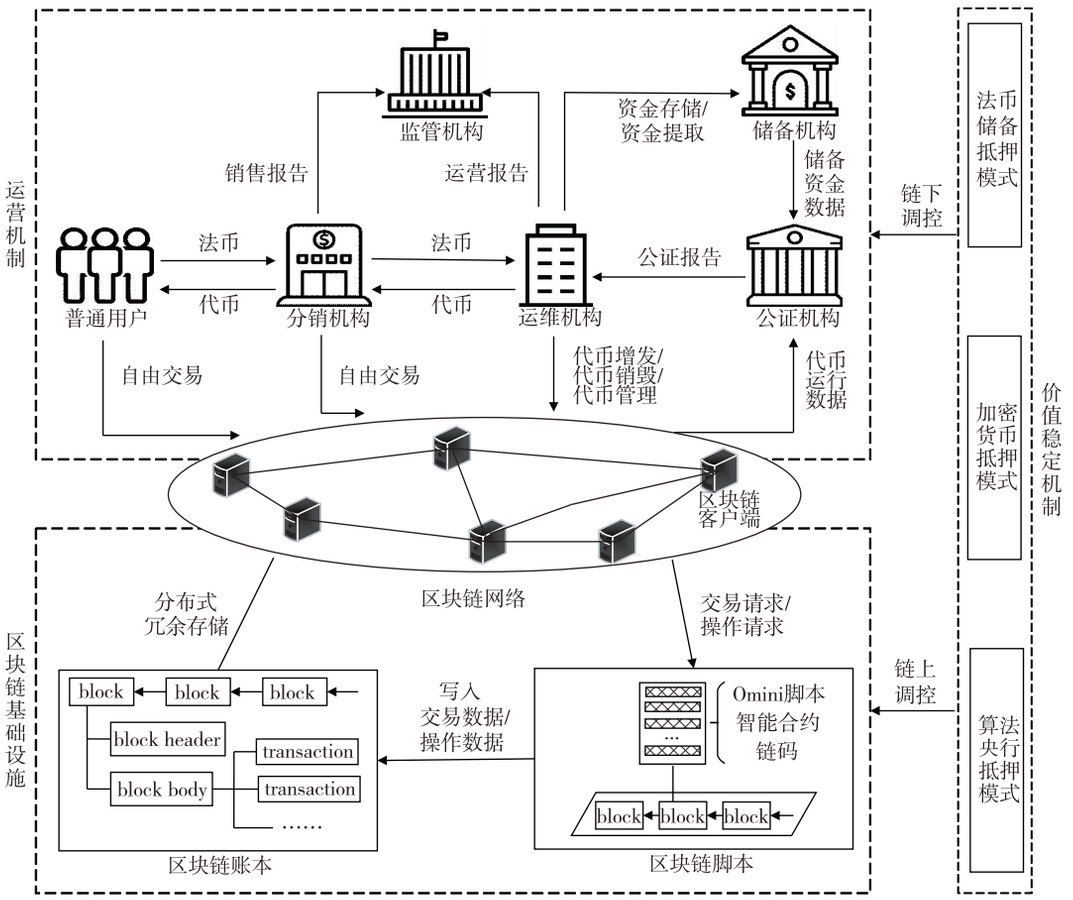

图 1　稳定代币系统架构

Fig. 1　System architecture for stable coins

2)运营机制:指用于维持稳定代币系统健康运行的管理模块.此模块是稳定代币系统能够正常提供服务的关键,将涉及稳定代币运维管理、代币分销、资金存储、审计公证、监督监管等工作.此模块的设计与系统的合规性、易用性、资金安全性密切相关.

3)价值稳定机制:指用于调节稳定代币价值的策略模块.此模块通过对区块链基础设施模块和运营机制模块进行调控,保证稳定代币价值趋于稳定.此模块的设计是稳定代币分类的主要依据.

这 3 个方面从不同角度描述了稳定代币系统运行的整体架构,三者之间既有各自负责的功能,也有密切联系.其中,“区块链网络”是连接区块链基础设施和运营机制的桥梁.一方面,区块链网络代表了稳定代币系统的技术模式,即利用区块链的组网机制、信息传输机制和数据共享机制,构建一个去中心化的数据交互系统.另一方面,区块链网络体现了运营机制中不同实体的参与模式,即每个实体通过运行一个区块链客户端程序成为稳定代币系统的一个节点,进而参与稳定代币交易、管理、数据查询等业务.价值稳定机制通过链上调控和链下调控手段,对区块链基础设施和运营机制进行管理,调节稳定代币的价值.

2.2　区块链基础设施

区块链是一种分布式技术架构,通常被分为数据层、网络层、共识层、激励层、合约层和应用层[13-14].其中,网络层涉及组网模式、通信机制等网络层的协议;数据层描述区块链的块链结构;共识层介绍不同区块链节点之间如何进行公平可信的数据交互;激励层介绍激励区块链节点参与维护区块链网络的机制;合约层描述区块链系统支持的脚本技术;应用层介绍区块链技术为应用提供的接口及技术方案.

本文为了介绍稳定代币系统的架构,从稳定代币系统实现模式的角度对区块链基础设施进行分类:

1)区块链网络:负责实现稳定代币系统基础的

组网、通信、交互功能.涵盖传统区块链架构的网路层、共识层、激励层.

2)区块链账本:负责存储稳定代币系统的交易记录和操作记录.主要涉及区块链架构的数据层.此处重点介绍稳定代币系统的数据如何存储在区块链账本中.

3)区块链脚本:负责实现稳定代币系统的交易功能和管理功能.主要涉及区块链架构的合约层.此处重点介绍稳定代币系统的核心代码如何存储、如何执行.

2.2.1 区块链网络

稳定代币本质上是一个基于区块链技术的应用.不同于传统的基于中心化架构的应用系统,稳定代币系统运行在去中心化的区块链网络之上.区块链网络中的每一个节点(指运行了区块链客户端程序的服务器)都参与稳定代币的交易过程,并存储稳定代币的交易记录.因此,稳定代币系统的特性与其采用的区块链网络的特性密切相关.考虑到稳定代币系统的实际特点,本文从组网模式和共识机制两个方面介绍区块链网络的特性.

组网模式描述了区块链网络中节点的选取机制,这与区块链网络的去中心化程度、系统公信力密切相关.根据区块链网络组网模式的区别,区块链技术体系被分为公链和许可链.其中,公链对参与节点没有身份限制,任何用户都可以通过运行区块链客户端程序自由加入或退出区块链网络.这种特性使得公链的去中心化程度较高,更容易获得公信力.但是这种特性也使得很难控制区块链网络的规模、性能和复杂程度,导致区块链系统整体的交易性能较低,延迟较高.典型的公链包括比特币、以太坊[15].许可链对参与者节点有身份限制,只允许经过身份认证的用户参与区块链网络的运行.这种特性使得许可链能够控制区块链网络的规模和单个节点的性能,使区块链系统能够拥有较高的交易性能和隐私保护能力.但是许可链的去中心化程度较低,系统的可靠性建立在少数区块链节点的可靠性之上,公信力较低.典型的许可链技术包括超级账本技术[16].

共识机制描述了区块链网络中不同节点进行数据交互的协商机制,这与区块链网络的交易性能、交易可靠性密切相关[17-18].根据共识机制的使用场景,共识机制可以分为针对公链的共识机制和针对许可链的共识机制.公链场景中,节点数量较多,网络环境复杂,很难在有效时间内使所有节点达成一致性状态.因此,针对公链的共识机制通常采用弱一致性的设计,即允许网络中的部分节点出现不一致的情况,使大部分节点快速达成一致性状态,然后再利用最长链机制逐渐使不一致状态消失.典型的算法包括 POW[19]、POS[20]等.许可链场景中,节点数量少、性能高,能够高效的实现数据一致性,所以针对许可链的共识机制通常采用了强一致性的设计,一旦数据写入区块,就不会被篡改.典型的算法包括 PBFT[21-22].

公链和许可链技术有各自的优势,在不同的场景中能够发挥不同的价值.因此,目前稳定代币系统的区块链网络在公链和许可链两种技术路线上都有探索.表2介绍了当前典型稳定代币采用的区块链网络的类型.

表2 典型稳定代币采用的区块链技术

Table 2 Blockchain technologies in stable coins

稳定代币	区块链网络	共识技术	交易性能/(笔/s)	扩展性/个
USDT	比特币公链	POW	10	10 000
PAX	以太坊公链	POW	15	8 000
DAI	以太坊公链	POW	15	8 000
Libra	自营许可链	HotStuff	1 000	100

USDT 是利用比特币系统的 OMNI 协议建立的稳定代币,目前在稳定代币市场中占据主流地位.PAX 是首批获得政府(纽约金融服务局 NYSDF)批准的稳定代币.DAI 是一种与黄金锚定的稳定代币.USDT、PAX、DAI 由于采用了公链技术,其交易性能严重受限于公链的性能瓶颈,每秒只能处理十几笔交易.这导致此类稳定代币很难支撑高频小额的交易.另一方面,由于公链普遍建立在大规模的分布式节点之上,此类稳定代币系统的公信力很高,很容易借助公链将影响力扩展到全球范围.

Libra 是由 Facebook 公司计划开发的依托许可链技术的稳定代币.Libra 项目的创始成员目前包括 Uber, PayPal, Visa 和硅谷投资巨头 Andreessen Horowitz,最终将拥有100名地域多元化的创始成员.通过支付1 000万美元的初始最低投资,这些创始公司将获得加入 Libra 网络的许可,负责运营区块链网络节点.Libra 网络采用了 HotStuff 共识机制,这是一种基于 BFT 机制的改进协议,能够取得更好的交易性能和安全性,Libra 网络的交易性能预计能达到每秒1 000笔交易[23].

稳定代币项目对区块链网络的选择取决于实际

需求.USDT、GUSD 虽然交易性能较低,但这些稳定代币由于建立在典型公链系统之上,与这些公链系统的交互更加方便.因此,此类稳定代币更适合作为连接加密货币和现实世界的桥梁,充当加密货币市场的价值中介物.Libra 稳定代币的设计用途是解决现实世界金融需求,因此对性能的要求是第一位的.此外,Libra 稳定代币将面临更强的金融监管,监管需求也使得此类稳定代币必须采用许可链的模式加强对节点的监管能力.

2.2.2 区块链账本

稳定代币系统建立在区块链网络之上,没有单独运维数据库服务器,所有的交易数据和操作数据都是以区块链交易的形式存储在每一个区块链节点中.区块链交易是不同区块链节点进行交互的基本数据格式,也是区块链系统中数据存储的基本数据单元.一段时间的多个区块链交易将被打包成一个区块(区块链中基本的数据存储结构),并按照时间顺序串联起来,构成基于时间排序的区块链条.这种区块链条被称为区块链账本,在功能上类似于中心化架构系统中的"数据库".区别在于:首先,区块链账本通常只支持存储、查询,不支持修改和删除;其次,区块链账本是由所有节点冗余存储.

稳定代币系统的数据主要分为两类:交易数据和操作数据.交易数据是指稳定代币系统的用户之间进行稳定代币的交易记录;操作数据是指系统管理员或特定用户对稳定代币系统的操作记录.本质上,稳定代币系统是区块链上的应用,交易数据和操作数据其实都是用户调用稳定代币系统的 API 实现的.因此,从区块链数据层的角度,稳定代币系统的交易数据和操作数据都是一种特殊的区块链交易,存储方式都是一致的.

根据稳定代币系统采用区块链网络的区别,可以将稳定代币分为基于公链的附属稳定代币和基于许可链的独立稳定代币.

1)基于公链的附属稳定代币:指稳定代币系统建立在已有公链之上,没有单独运维区块链网络.这种稳定代币和其他区块链应用共享公链的存储空间和通信带宽,在性能和扩展性上受到公链的限制.

2)基于许可链的独立稳定代币:指稳定代币系统建立在单独运维的区块链网络之上.这种稳定代币独享区块链网络的存储空间和通信带宽,在性能和扩展性上有更高的潜力.但是,由于许可链在去中心化程度上的劣势,这种稳定代币的公信力较低,需要借助实体机构提供信任保证.

针对基于公链的附属稳定代币,稳定代币的交易记录和操作记录主要以数据参数的形式存储在区块链交易中.典型的公链系统通常有原生的代币机制,例如比特币系统中的比特币,以太坊系统中的以太币.在这些公链系统中,区块链交易的本质就是不同区块链地址(区块链系统中的账号)之间进行代币转移的过程.区块链交易中必须包括发送方地址、接收方地址、交易金额 3 个参数.此外,为了扩展区块

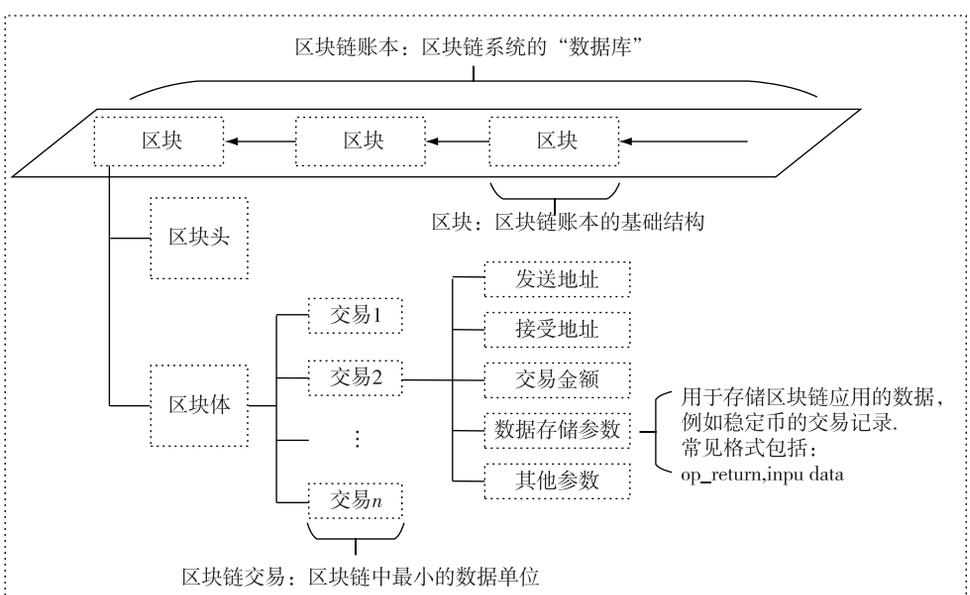

图 2 区块链账本结构

Fig. 2 Data structure in blockchain ledger

链交易的功能,通常还涉及了专门用于存储数据的参数,例如比特币交易中的 OP_RETURN 参数,以太坊交易中的 Input 参数.图 2 介绍了区块链账本的数据结构.稳定代币系统的数据就存储在区块链账本的“数据存储参数”中.

图 3 展示了稳定代币 GUSD(建立在以太坊网络中的稳定代币应用)的真实交易数据,其中 From、To、Value 参数描述的是以太坊交易的发送方地址、接收方地址和以太币的交易金额.稳定代币的交易数据存储在 Input Data 参数中,根据代码中的注释可以看出,Input 参数中编码了稳定代币交易的接收方和交易金额.

2.2.3 区块链脚本

稳定代币系统本质上是一个基于区块链技术的加密货币应用,除了基础的交易功能之外,稳定代币系统还需要实现代币增发、代币销毁、代币冻结等管理功能.不同于传统的中心化架构应用,稳定代币的核心功能不是通过部署在中心化节点的代码实现,而是通过运行在所有区块链节点上的区块链脚本实现.

区块链脚本是区块链系统为了实现多样化应用需求而设计的编程语言.脚本的数据存储在区块链账本中,脚本的运行过程由所有节点共同参与.在第 1 代区块链技术中,典型区块链比特币系统就已经支持脚本技术(OMNI 协议[24]),此阶段的脚本技术仅支持顺序执行和少量的 API,主要用于延时交易等简单功能.第 2 代区块链技术体系中,区块链脚本已经成为核心创新技术,典型代表以太坊系统提出了支持图灵完备的脚本技术,被称为“智能合约”[25].相对于区块链 1.0 比特币系统的脚本,智能合约功能更加强大,不仅支持循环等复杂操作,还可以调用外部 API.这使得区块链脚本能够实现更加复杂的功能,解决复杂的实际问题.正是由于智能合约技术的巨大潜力,区块链技术不再局限于金融业务,而是将应用范围向能源、电信、版权保护等众多行业扩展.在正在演进的第 3 代区块链技术体系中,区块链脚本技术仍然是创新的热点,如何让区块链脚本技术更高效、更安全成为解决区块链技术落地的关键问题.Facebook 的 Libra 项目中采用的新型区块链架构就专门设计了新的脚本语言 MOVE,在灵活性、安全性和可验证性方面有较大提升[23].

相对传统的编程语言,区块链脚本在公信力方面有特殊优势.首先,区块链脚本的代码存储在区块链账本中,基于区块链账本不可篡改的特点,区块链脚本也具有安全可靠的特点,避免了因黑客攻击导致的代码篡改问题.其次,基于区块链账本公开透明的特点,区块链脚本的代码可以被公众验证,这使得区块链应用的算法和安全性受到公众监管,比黑盒程序更容易获得用户信任.最后,区块链脚本的执行过程是由全体节点参与,执行结果由全体节点存储和维护,这使得区块链脚本的执行过程是安全可信的.综上所述,区块链脚本能够降低传统程序面临的代码篡改、代码后门、代码恶意操作等风险,实现高公信力的分布式应用.

2.3 价值稳定机制

加密货币的价值一直处于剧烈波动的状态.自从比特币诞生以来,加密货币的种类、市值都出现爆


Transaction Hash:
0xeed45d3ae09823f747ecf055f8f29b9de6f713ec926bbfd61c32a37510cba447
From:
0x272c1feaee0ca813fcff39a71fdcb8c8aefedf56
To:
0x056fd409e1d7a124bd7017459dfea2f387b6d5cd
Value:
0
Input Data:
{
0xa9059cbb //稳定代币合约 API 的散列值，此处的散列对应的 API 是“transfer”
000000000000000000000006bcacf0effc02a617467775afc3673534d67d877 //稳定代币交易接收方地址
000000000000000000000000000000000000000000000000000000000000493e0//稳定代币交易金额的 16 进制
}

图 3 稳定代币 GUSD 的交易数据

Fig. 3 Trading data of stable coins GUSD

炸式增长.截止到2019年7月,全球加密货币市场的市值超过2 638亿美元,其中比特币的市值超过1 701亿美元.从市值看,加密货币市场已经是相当庞大.但是,从价值稳定性的角度看,加密货币市场非常不成熟,加密货币的价格随着市场剧烈变动,甚至频频出现一夜之间价值归零的极端现象.从本质上分析,加密货币价值剧烈变动的原因来自于其底层依赖的区块链技术.区块链技术的核心特点是去中心化信任体系,即不依赖中心节点的信任,而是依赖分布式节点自治、开源代码、加密技术来实现去中心化的信任.在这种信任机制体系中,没有任何机构为系统网络的运维负责,没有任何个体为代码的安全性负责,参与者只能依靠对架构、算法的信任来对比特币建立信任.因此,比特币等加密货币的价格实际上是建立在用户群体的信任之上.这就导致加密货币的价格将随着用户群体观念的变化而剧烈波动.

作为一种特殊的加密货币,稳定代币系统同样建立在去中心的区块链网络之上,在技术架构层面缺乏中心化的信任体系.为了保持价格稳定,稳定代币系统在区块链架构之外,必须设计独立的价值稳定机制.目前常见的机制主要分为3类[26]:

1)基于法币抵押的稳定代币.利用同等价值的法币储备为稳定代币的价值背书.根据法币储备数量来发行或者销毁稳定代币,确保在市场上运行的每一个稳定代币都对应储备机构中的一个法币.代表产品有USDT[27]、TUSD[28]、PAX[29]、GUSD[30]和Digix[31].

2)基于数字资产抵押的稳定代币.利用超额的数字资产储备为稳定代币价值背书.根据数字资产的价值变化,动态调整储备比例,确保在任意时刻储备的数字资产的价值超过发行的稳定代币的价值.代表产品有Bitshares[32]、MakerDAO[33]、Haven[34]和DUO Network[35].

3)无抵押的稳定代币.利用供需平衡模型为稳定代币价值背书.此模式中稳定代币没有任何价值抵押物,而是根据市场形势动态发行或者销毁稳定代币,通过调控代币的供应数量,来维持代币的价值稳定.代表产品有Basis[36]、Carbon[37]、Terra[38]和Reserve[39].

这3种模型中,法币抵押模型对价格稳定性的保证最强,面临的主要风险包括:法币本身的价值波动,法币储备的安全性.这两项风险都可以利用现有的金融管控手段解决.数字资产抵押模式的关键在于抵押物的调控策略能否有效应对抵押物的价值波动.当抵押物的价值小幅波动时,调控策略可以通过追加抵押物、清仓抵押物的方式保持价值稳定.但是,一旦抵押物价值波动幅度超过调控能力,价值平衡机制就面临失败风险.当前以加密货币为代表的数字资产面临政府监管、黑客攻击等多重风险,本身就处于价值剧烈波动的状态,所以数字资产抵押模式很难有效保证价值稳定性.无抵押模式利用纯粹的调控算法解决价值稳定问题,其价值完全取决于市场和用户对其模式的信心,本质上与传统加密资产的价值模式是一样的,将面临相同的价值波动风险.针对这种模式,姚前等[6]认为如果稳定代币价格突然大幅低于宣示价格,市场参与者信心可能被打破,价格调控有可能陷入所谓“死亡螺旋”的周期循环.

图4从市值和单价2个角度展示了8种稳定代币运行情况.其中红色实线条代表采用法币抵押模式的稳定代币,包括USDT、TUSD、PAX.绿色点线条代表采用数字资产抵押模式的稳定代币,包括BTIUDS(Bitshares)、DAI(MakerDAO)、XHV(Havven).紫色短线条代表采用无抵押模式的稳定代币,包括:CARBON(Carbon)、RSR(Reserve).图中的市值数据和单价数据来自coinmarket网站,抽取了从2018年1月到2019年7月的数据.

图4a展示了市值变化情况.USDT作为最早出现的稳定代币,占据了稳定代币市场80%以上的市值.TUSD和PAX两种采用法币抵押模式的稳定代币的市值也处于快速增长的状态.采用数字资产抵押模式的3种稳定代币中,只有DAI稳定代币的市值超过了0.5亿美元.采用无抵押模式的2种稳定代币的市值都非常小.

图4b展示了稳定代币单价的变化情况.此案例中8种稳定代币的单价都是锚定美元的.作为稳定代币,在设计层面他们的单价应该稳定在1美元.但是在运行中,由于受到市场信心、购买渠道等因素的干扰,各种稳定代币在交易所的价值是波动的.一种优秀的稳定代币的单价应该保持尽量小的波动.从图中可以看出,3种采用法币抵押模式的稳定代币(红色实线条)的波动是最小的.采用数字资产抵押模式的稳定代币(绿色点线条)在1美元附近剧烈波动.采用无抵押模式的稳定代币(紫色短线条)的价值则始终远低于1美元.

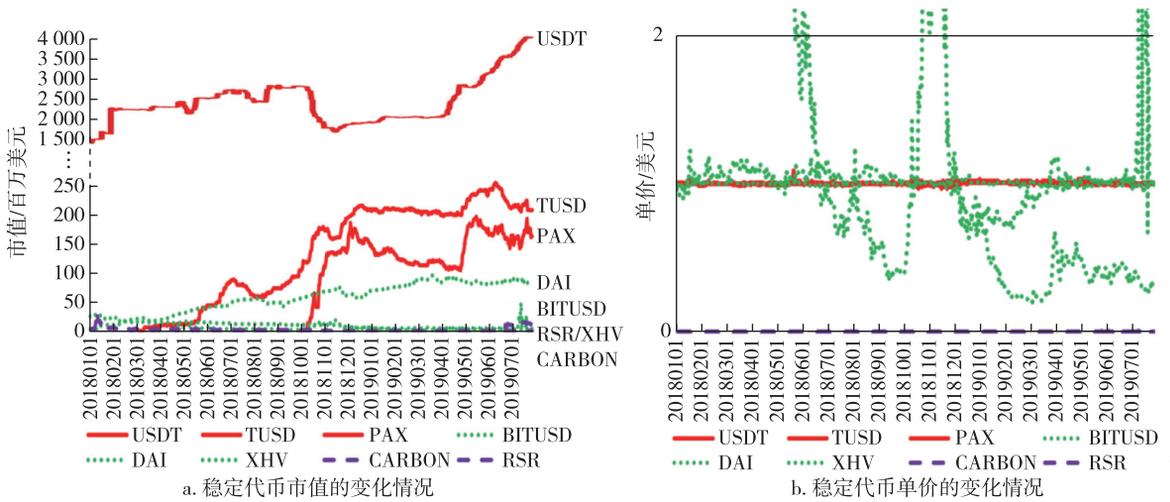

图 4　采用 3 种不同价值稳定机制的稳定代币运行情况

Fig. 4　Variation of (a) market capitalizations, and (b) prices of stable coins using three different value stability mechanisms

从市值和单价 2 个角度结合分析,可以看出目前采用法币抵押模式的稳定代币技术最为成熟,被市场接受程度最高,在稳定代币行业占据统治地位.采用数字资产抵押模式的稳定代币在价值稳定性方面仍存在显著缺陷,市场认可度处于缓慢提升的状态.采用无抵押模式的稳定代币完全无法实现价值稳定的特性,在稳定代币行业处于边缘状态.

2.4　运营机制

如 2.3 节所示,基于法币的价值稳定模型较为实用,而且只有这种模式需要较多的外部实体机构为稳定代币系统提供额外的信任能力.因此,本小节重点介绍法币抵押模式稳定币的运营机制.表 3 介绍了 4 种典型稳定代币的运营机制.

为了保证稳定代币系统能够健康运转,需要一套完善的运营机制.运营机制的主要目标包括:

1)确保系统核心功能的正常运行.指用户能够正常的购买、出售、自由交易稳定代币.

2)确保价格稳定性.指稳定代币的价格稳定机制能够有效运行,防止稳定代币的价值剧烈波动.

为了确保系统核心功能的正常运行,需要运维机构、分销机构和用户的参与.运维机构负责稳定代币的发行、销毁等管理操作.稳定代币的发行过程是利用稳定代币系统的程序接口实现.不同于比特币等加密货币,稳定代币的发行不需要额外的“挖矿”操作,只要运维机构拥有合法的权限,就可以发行任意数量的代币.但是,为了保证价格的稳定性,运维机构在发行代币时通常会遵循价格稳定机制,例如,在区块链上每发行一个稳定代币,就要向指定的存储机构存储 1 美元.同理,销毁和其他管理操作也将按照设定进行.分销机构是指承担稳定代币销售任务的数字货币交易所.在实际运行中,由于受到地域、语言、监管政策的影响,运维机构很难面向全球用户提供服务.因此,运维机构需要和数字货币交易所合作,扩展稳定代币的服务范围.一种稳定代币的分销机构越多,证明其运行状态越健康.用户可以从分销机构的网站中购买和出售稳定代币,也可以利用支持稳定代币的区块链客户端实现用户之间的交易.

为了确保价格的稳定性,需要运维机构、储备机构、公证机构和监管机构的参与.针对法币抵押模式的稳定代币,价值稳定的关键是保证储备的法币能够足额偿付市场中存在的稳定代币.为了达到这一

表 3　4 种稳定代币的运维机制

Table 3　Maintenance mechanisms of four stable coins

稳定代币	锚定资产	运维机构	储备机构	公证机构	监管机构
USDT	美元	Tether 公司	Nobel 银行[41]	FSS 律师事务所[40]	无
GUSD	美元	Gemini 公司	道富银行[42]	BPM 会计师事务所[43]	纽约金融服务厅
PAX	美元	Paxos 公司	FDIC 投保的美国银行[44]	Withum 会计师事务所[45]	纽约金融服务厅
Libra	一篮子法定货币	Libra 协会	顶级银行机构	监管小组	各国的监管机构

目标,运维机构在发行代币时,将向储备机构存储等值的法币,当用户卖出稳定代币时,运维机构将从储备机构提取法币支付给用户,同时将稳定代币销毁.通过将稳定代币的发行/销毁与法币储备的增减挂钩,就能够从理论上保证价值的稳定性.为了保证上述模式的可靠运行,稳定代币系统中的储备机构和公证机构通常会选择世界知名的金融机构和律师事务所承担储备和公证业务.例如,表 3 中的 Nobel 银行[41]、道富银行[42]是世界知名的银行,FSS 律师事务所[40]、BPM 会计师事务所[43]、Withum 会计师事务所[45]是世界知名的律师事务所.储备机构将按照各国的金融法规对法币资产进行可靠管理,保证资产存储过程的安全性.公证机构将基于稳定代币系统的运维规则,从稳定代币系统获取代币运行数据(例如,代币发行量,交易统计数据等),从储备机构获得资产储备的数据,然后定期出具公证报告,证明稳定币系统是按照运维规则运行.监管机构负责定期检测稳定代币系统的链上运行情况和链下运维情况,及时发现违规问题.储备机构、公证机构和监管机构的引入,本质上是利用实体机构的信誉为稳定代币系统提供信誉保证,帮助普通用户监督运维机构的操作.

3 稳定代币面临的问题及发展方向

稳定代币的出现使区块链技术有机会解决实际的金融问题,将对金融行业带来巨大影响.但是,受限于当前区块链技术、监管机制的限制,稳定代币系统还面临众多缺陷.

3.1 监管和隐私保护的矛盾

稳定代币系统在实际应用过程中间面临监管需求和隐私保护需求的矛盾.

一方面,支持监管是金融行业各项业务得以正常进行的基础条件.特别是在稳定代币涉及的跨境支付、资金转移领域,目前已经有多种监管需求.例如 KYC 政策(了解你的客户),反洗钱政策等.由于稳定代币采用的区块链技术与传统的金融 IT 架构不一致,已经给现有的监管机制带来了巨大的挑战.目前采用的监管机制主要是要求数字货币交易所等区块链服务商对用户信息进行备案.这种方法对恶意用户的防控能力较弱,恶意用户可以通过其他国家的交易所及假身份绕过监管.目前已经有一些针对加密货币系统的监管方案[46-47],但是这些方案实施的前提是监管者必须有权查看区块链网络上的详细交易数据.

另一方面,区块链技术采用的账本公开的机制,虽然能够提升系统公信力,但是带来了显著的隐私泄露隐患.例如,比特币系统建议用户采用频繁更换区块链地址(区块链系统中的账号)的方式增强匿名性,但是现有的研究表明比特币地址的匿名性是一种"假匿名"[48-49],攻击者可以通过网络溯源[50-51]、交易数据分析[52-53]等多种方式推测比特币地址背后的用户身份信息.因此,目前出现了众多聚焦隐私保护的区块链系统,例如门罗币(Monero)[54]、零币(Zcash)[55-56].通过采用环签名、零知识证明等密码学技术,这些系统能够在满足分布式共识机制的条件下,隐藏区块链交易的发送地址、接收地址和交易金额.但是,这种高度隐藏的技术将进一步增加监管难度.目前门罗币已经代替比特币,成为犯罪活动首选的支付方式.

对稳定代币系统来说,支持监管和保护用户隐私都是其必须解决的问题.如何平衡监管需求和隐私保护需求,为合法的监管机构提供数据处理的权限,同时增加攻击者分析数据的难度,是未来稳定代币研究的一个方向.

3.2 高性能和高公信力的矛盾

USDT、PAX 等稳定代币系统建立在比特币、以太坊等非许可链网络之上,任何人都可以自由加入网络,参与数据的维护和交易的验证工作.这种机制充分实现了去中心化的思想,具有较高的公信力.但是,这种机制也导致系统的性能很难提高,难以满足现实金融业务的性能需求.当前公链系统虽然推出了众多提高性能的机制,包括增大区块容量,降低出块时间.但是这些方案对区块链系统交易性能提升的幅度有限,而且有可能增加中心化的风险[57].

Facebook 的 Libra 稳定代币系统建立在许可链网络之上,通过采用高可信、高性能的服务器组建小规模的分布式网络,许可链的响应速度和交易性能得到显著提高.但是,这种机制弱化了去中心化的思想,不能完全实现区块链技术去中心化信任的潜力.而且,当前的许可链系统的性能虽然远超过公链系统,但是相对于传统金融系统的性能仍有较大差距.例如,Libra 稳定代币系统底层的许可链网络预计能达到每秒 1 000 笔交易,而 visa、MasterCard 等传统金融系统的交易性能通常能够达到万笔交易每秒.因此,许可链系统很难通过继续降低去中心化程度的方式来提高性能指标.

未来随着稳定代币系统应用到业务量更加复杂的行业,这种矛盾将更为突出.例如,Facebook 的 Libra 项目计划向遍及全球的 20 亿用户提供金融服务,这种金融场景不仅需要巨大的性能支撑,也需要一套能够满足全世界范围不同用户的信任需求.Libra 项目采用了渐进式的发展方式,目前采用了基于 BFT 协议的改进版共识协议,首先实现大约 100 个节点的许可链网络,然后随着技术的革新,在逐渐过渡到非许可链网络.目前,在非许可链共识机制上,已经出现了一些兼具高性能和去中心化的技术,包括 DAG[58]、AGLAND[59].随着共识机制的不断发展.稳定代币系统有望逐渐在性能和公信力方面达到平衡状态.

4 结论

稳定代币通过将去中心区块链技术的优势与中心化信任体系的优势相结合,使区块链技术能够在现实金融业务中发挥其减少中介、降低沟通成本的能力.这不仅将对现有的金融业务产生重要影响,也将对区块链技术在其他领域的应用有促进和启发作用.本文首先详细介绍了稳定代币的特征,分析稳定代币与法币、加密货币之间的关系.然后从区块链基础设施、价值稳定机制、运营机制 3 个角度详细介绍了稳定代币系统的架构和运行机制.最后分析了稳定代币面临的问题和可能的解决方案.

参考文献

References

[1] Nakamoto S. Bitcoin: a peer-to-peer electronic cash system[EB/OL].[2019-07-28].http://www.bitcoin.org/bitoin.pdf

[2] 百度百科.泰达币[EB/OL].[2019-07-28].https://baike.baidu.com/item/%E6%B3%B0%E8%BE%BE%E5%B8%81/22415301
BAIKE.USDT[EB/OL].[2019-07-28].https://baike.baidu.com/item/%E6%B3%B0%E8%BE%BE%E5%B8%81/22415301

[3] Wikicryptocoins.Tether[EB/OL].[2019-07-28].https://www.wikicryptocoins.com/currency/Tether

[4] BTC.COM.比特币区块[EB/OL].[2019-07-28].https://btc.com/
BTC.COM.Bitcoin block[EB/OL].[2019-07-28].https://btc.com/

[5] CoinMarketCap.Top 100 cryptocurrencies by market capitalization [EB/OL].[2019-07-28].https://coinmarketcap.com/

[6] 姚前,孙浩.数字稳定代币的试验与启示[J].中国金融,2018(19):49-50
YAO Qian, SUN Hao. Experiment and enlightenment of stable coins[J].China Finance,2018(19):49-50

[7] 邓伟.比特币价格泡沫:证据、原因与启示[J].上海财经大学学报,2017,19(2):50-62
DENG Wei. Price bubbles in bitcoin: evidence, causes and implications[J].Journal of Shanghai University of Finance and Economics,2017,19(2):50-62

[8] Heilman E,Kendler A,Zohar A,et al.Eclipse attacks on Bitcoin's peer-to-peer network[C]//Proceedings of the 24th USENIX Conference on Security Symposium,2015:129-144

[9] Fedorov A K,Kiktenko E O,Lvovsky A I.Quantum computers put blockchain security at risk[J].Nature,2018,563(7732):465-467

[10] 尹振涛.ICO 监管的国际经验[J].中国金融,2017(20):87-89
YIN Zhentao.International experience in ICO regulation[J].China Finance,2017(20):87-89

[11] 任哲.ICO 国际监管与趋势[J].中国金融,2018(5):81-83
REN Zhe.The international regulation and trend of ICO[J].China Finance,2018(5):81-83

[12] 洒脱喜.谁在控制比特币 Core 软件? 开发者揭露秘辛[EB/OL].[2019-07-28].https://www.8btc.com/article/330348
8BTC.Who controls bitcoin Core software? Developers reveal secrets[EB/OL].[2019-07-28].https://www.8btc.com/article/330348

[13] 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
YUAN Yong,WANG Feiyue.Blockchain:the state of the art and future trends[J].Acta Automatica Sinica,2016,42(4):481-494

[14] Bonneau J,Miller A,Clark J,et al.SoK:research perspectives and challenges for bitcoin and cryptocurrencies[C]//IEEE Symposium on Security and Privacy,2015,DOI:10.13140/RG.2.1.4179.5605

[15] Alisie M,Hoskinson C,Di Iorio A,et al.Ethereum:a next-generation smart contract and decentralized application platform[EB/OL].[2019-07-28].https://genius.com/Ethereum-ethereum-whitepaper-annotated

[16] Androulaki E,Barger A,Bortnikov V,et al.Hyperledger fabric:a distributed operating system for permissioned blockchains[EB/OL].[2019-07-28].https://arxiv.org/pdf/1801.10228.pdf

[17] 袁勇,倪晓春,曾帅,等.区块链共识算法的发展现状与展望[J].自动化学报,2018,44(11):2011-2022
YUAN Yong,NI Xiaochun,ZENG Shuai,et al.Blockchain consensus algorithms: the state of the art and future trends[J].Acta Automatica Sinica,2018,44(11):2011-2022

[18] Xiao Y,Zhang N,Lou W,et al.A survey of distributed consensus protocols for blockchain networks[J].arXiv e-print,arXiv:1904.04098

[19] Andrychowicz M,Dziembowski S.PoW-based distributed cryptography with No trusted setup[M]//Lecture Notes in Computer Science.Berlin,Heidelberg:Springer Berlin Heidelberg,2015:379-399

[20] Proof of stake [EB/OL]. [2018-04-11]. https://en.bitcoin.it/wiki/Proof of Stake
[21] Sousa J, Bessani A, Vukolic M. A byzantine fault-tolerant ordering service for the hyperledger fabric blockchain platform[J]. arXiv e-print, arXiv:1709.06921
[22] Sukhwani H, Martinez J M, Chang X L, et al. Performance modeling of PBFT consensus process for permissioned blockchain network (hyperledger fabric)[C]// IEEE 36th Symposium on Reliable Distributed Systems (SRDS), 2017, DOI:10.1109/SRDS.2017.36
[23] Libra. Libra 白皮书[EB/OL]. [2019-07-28]. https://Libra.org/zh-CN/white-paper/\#the-Libra-currency-and-reserve
Libra. Libra white paper[EB/OL]. [2019-07-28]. https://Libra.org/zh-CN/white-paper/\#the-Libra-currency-and-reserve
[24] Github. OMNI layer[EB/OL]. [2019-07-28]. https://github.com/OMNILayer/OMNIcore
[25] Atzei N, Bartoletti M, Cimoli T. A survey of attacks on ethereum smart contracts (SoK)[M]// Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2017:164-186
[26] 袁煜明,朱翊邦.合规基础设施系列(上):稳定代币[EB/OL]. [2019-07-28]. https://www.jianshu.com/p/3277d9cd58cb
YUAN Yuming, ZHU Yibang. Compliance infrastructure series (part 1): stable coins[EB/OL]. [2019-07-28]. https://www.jianshu.com/p/3277d9cd58cb
[27] Tether USDT [EB/OL]. [2019-07-28]. https://tether.to/
[28] Trust Token. TUSD [EB/OL]. [2019-07-28]. https://www.trusttoken.com/
[29] Paxos. PAX [EB/OL]. [2019-07-28]. https://www.paxos.com/PAX/
[30] Gemini. GUSD[EB/OL]. [2019-07-28]. https://gemini.com/dollar/
[31] Digix. Digix [EB/OL]. [2019-07-28]. https://digix.global/dgd/
[32] BitShares. bitUSD[EB/OL]. [2019-07-28]. https://bitshares.org/
[33] MakerDAO. DAI[EB/OL]. [2019-07-28]. https://makerdao.com/zh-CN/
[34] Haven. XHV[EB/OL]. [2019-07-28]. https://www.havenprotocol.com/
[35] DUO Network. DUO Network Token(DUO)[EB/OL]. [2019-07-28]. https://duo.network/
[36] Basis. Basis [EB/OL]. [2019-07-28]. https://www.basis.io/
[37] Carbon. Carboncoin (CARBON)[EB/OL]. [2019-07-28]. https://carboncoin.cc/
[38] Terra. Terra (LUNA)[EB/OL]. [2019-07-28]. https://terracoin.io/
[39] Reserve. Reserve Rights (RSR)[EB/OL]. [2019-07-28]. https://reserve.org/
[40] Freeh Sporkin & Sullivan, LLP[EB/OL]. [2019-07-28]. https://www.freehsporkinsullivan.com/
[41] Noble Bank[EB/OL]. [2019-07-28]. https://www.noblebank.pl/
[42] StateStreet[EB/OL]. [2019-07-28]. http://www.statestreet.com/home.html
[43] BPM LLP [EB/OL]. [2019-07-28]. https://www.bpmcpa.com/
[44] FDIC. Federal Deposit Insurance Corporation[EB/OL]. [2019-07-28]. https://www.fdic.gov/
[45] Withum [EB/OL]. [2019-07-28]. https://www.withum.com/
[46] 高峰,祝烈煌,刘胜,等.区块链数字货币监管技术研究:以区块链稳定币为例[C]//金融科技青年论文选集(2018),北京,2018
GAO Feng, ZHU Liehuang, LIU Sheng, et al. A study on blockchain digital currency regulatory technology: a case study of stable coins[C]// Intelligence Finance (2018), Beijing, 2018
[47] 李文红,蒋则沈.分布式账户、区块链和数字货币的发展与监管研究[J].金融监管研究,2018(6):1-12
LI Wenhong, JIANG Zeshen. A study of the development and supervision of distributed ledger technology, blockchain and digital currencies [J]. Financial Regulation Research, 2018(6):1-12
[48] 祝烈煌,高峰,沈蒙,等.区块链隐私保护研究综述[J].计算机研究与发展,2017,54(10):2170-2186
ZHU Liehuang, GAO Feng, SHEN Meng, et al. Survey on privacy preserving techniques for blockchain technology [J]. Journal of Computer Research and Development, 2017, 54(10):2170-2186
[49] Reid F, Harrigan M. An analysis of anonymity in the bitcoin system[M]// Altshuler Y, Elovici Y, Cremers A B, et al. Security and Privacy in Social Networks. New York: Springer, 2012:197-223
[50] 高峰,毛洪亮,吴震,等.轻量级比特币交易溯源机制[J].计算机学报,2018,41(5):989-1004
GAO Feng, MAO Hongliang, WU Zhen, et al. Lightweight transaction tracing technology for bitcoin [J]. Chinese Journal of Computers, 2018, 41(5):989-1004
[51] Biryukov A, Khovratovich D, Pustogarov I. Deanonymisation of clients in bitcoin P2P network[C]// Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, 2014, DOI: 10.1145/2660267.2660379
[52] Meiklejohn S, Pomarole M, Jordan G, et al. A fistful of bitcoins: characterizing payments among men with no names[C]// Proceedings of the 2013 Conference on Internet Measurement Conference, 2013, DOI: 10.1145/2504730.2504747
[53] Monaco J V. Identifying bitcoin users by transaction behavior[C]// SPIE SPIE Defense, Security and Sensing, 2015, DOI:10.1117/12.2177039
[54] Monero. A note on chain reactions in traceability in cryptoNote 2.0[EB/OL]. [2019-07-28]. https://web.getmonero.org/resources/research-lab/pubs/MRL-0001.pdf
[55] Miers I, Garman C, Green M, et al. Zerocoin: anonymous distributed E-cash from bitcoin[C]// IEEE Symposium on Security and Privacy, 2013, DOI: 10.1109/SP.2013.34
[56] Sasson E B, Chiesa A, Garman C, et al. Zerocash: decentralized anonymous payments from bitcoin[C]// IEEE

Symposium on Security and Privacy, 2014, DOI: 10.1109/SP.2014.36
[57] 喻辉,张宗洋,刘建伟.比特币区块链扩容技术研究[J].计算机研究与发展,2017,54(10):2390-2403
YU Hui, ZHANG Zongyang, LIU Jianwei. Research on scaling technology of bitcoin blockchain[J]. Journal of Computer Research and Development, 2017, 54(10): 2390-2403
[58] Li C, Li P, Zhou D, et al. Scaling nakamoto consensus to thousands of transactions per second[J]. arXiv e-print, arXiv:1805.03870
[59] Gilad Y, Hemo R, Micali S, et al. Algorand: scaling byzantine agreements for cryptocurrencies[EB/OL].[2018-04-10].http://eprint.iacr.org/2017/454

Research progress on stable coins

GAO Feng[1] ZHU Liehuang[1] DING Kai[1] GONG Guopeng[2] DAI Qingzhu[3]
1 School of Computer Science & Technology, Beijing Institute of Technology, Beijing 100081
2 Linyi Guanqi Information Technology Co., Ltd, Linyi 276000
3 Hangzhou Chainv Technology Co., Ltd, Hangzhou 310012

Abstract As a special cryptocurrency based on value-stable attributes, stable coins not only act as a bridge to link blockchain crypto assets and real-world assets, but also have the potential to be an effective tool for reducing the cost of intermediary services in the real financial industry and improving the efficiency of capital transmission. Since the announcement of stable token programs by internationally renowned companies such as JP Morgan and Facebook, the stable coins have become a research hotspot for financial regulators, business circles and scientific institutions. By comparing the legal currency, cryptocurrency and stable coins, this paper introduces the characteristics of stable tokens in detail, and then introduces the system architecture and operation mechanism of stable tokens from three aspects of blockchain infrastructure, value stability and operation mechanism. Finally, we analyze the defects and possible solutions of the stable token system combined with its technical characteristics.

Key words blockchain; cryptocurrency; stable coins; consensus mechanism; privacy preserving