中国科学: 信息科学 2018 年 第 48 卷 第 9 期: 1275–1282
SCIENTIA SINICA Informationis
《中国科学》杂志社
SCIENCE CHINA PRESS
观点与争鸣

法定数字货币在互联网投资借贷的应用研究

姚前

中国人民银行数字货币研究所 *, 北京 100088
E-mail: yaoqian@pbc.gov.cn
* 作者系中国人民银行数字货币研究所所长, 本文仅代表个人学术观点, 不代表所在机构意见.

收稿日期: 2018–03–06; 接受日期: 2018–03–28; 网络出版日期: 2018–09–07

摘要 当前互联网投资借贷平台存在资金挪用风险, 缺乏有效手段保障资金安全和交易一致性. 传统方式着重于加强对平台主体的评估和管控, 以此间接保障交易和合同执行的安全, 而本文提出了一种全新的基于法定数字货币的解决思路: 基于法定数字货币钱包应用服务体系创造可信的运行环境, 通过联合签名机制管控资金用途, 解决资金安全问题, 并利用钱包应用中的智能合约保障交易一致性, 实现交易过程的公开透明、安全可控. 目前陷入困境的互联网金融平台可借此转型, 作为法定数字货币增值服务商, 在数字货币生态体系中更透明、更规范地助力数字普惠金融创新.

关键词 法定数字货币, 央行数字货币, 互联网投资借贷平台, 智能合约, 联合签名

1 引言

一般而言, 当谈到法定数字货币 (亦称央行数字货币) 的重要意义时, 我们更多的是从印钞造币技术 (数字技术) 的进步及央行可以更好履职的角度展开论述. 比如发行法定数字货币可以降低传统纸币发行、流通的高昂成本, 提升经济交易活动的便利性和透明度, 减少洗钱、逃漏税等违法犯罪行为, 提升央行对货币供给和货币流通的控制力, 更好地支持经济和社会发展, 助力普惠金融的全面实现 [1].

实际上, 相比传统货币 —— 无论是纸币还是电子货币, 法定数字货币对于持币者的好处亦可大书特书. 传统纸币有发行机构的信息, 但不会有持有人登记的概念, 更不会保存流转过程中全生命周期的信息. 这样一种根本性的差异使得法定数字货币的持币者对自己资金的自主可控有了一个质的飞跃.

本文拟以法定数字货币在互联网投资借贷中的应用为案例, 具体剖析数字货币持有者如何在借贷链中实现自有资金的穿透式监控, 以提高交易透明度, 更好地保护投资者自身权益. 目前陷入困境的互联网金融平台亦可借此转型, 作为数字货币钱包应用服务商, 在数字货币生态体系中, 更透明、更规范化地发挥数字普惠金融创新作用.

引用格式: 姚前. 法定数字货币在互联网投资借贷的应用研究. 中国科学: 信息科学, 2018, 48: 1275–1282, doi: 10.1360/N112018-00045
Yao Q. Study on the application of digital fiat currency in peer-to-peer investment and lending (in Chinese). Sci Sin Inform, 2018, 48: 1275–1282, doi: 10.1360/N112018-00045

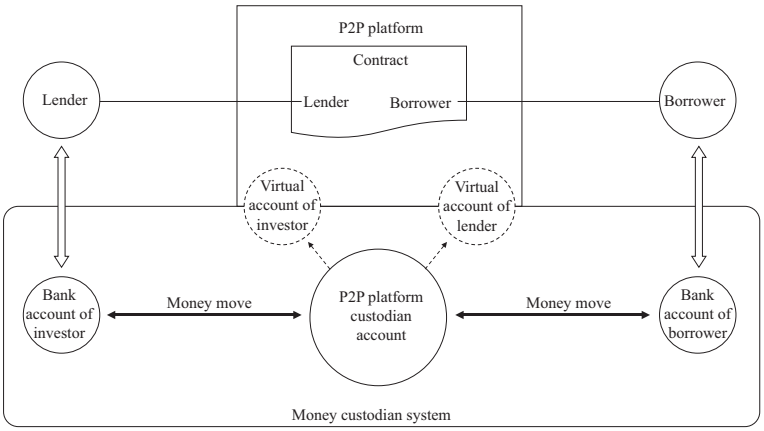

图 1　互联网投资借贷平台交易示意图

Figure 1　Diagram of transactions on Internet-based investment and lending platform

2　互联网投资借贷平台存在的问题

(1) 平台及参与方概述

本文提及的互联网投资借贷平台 (以下简称 “平台”) 是指通过互联网平台, 为个体之间合法的直接金融交易提供信息服务的中介公司, 包括 P2P 网络借贷, 网络众筹等. 如图 1 所示, 平台交易双方为出资人和筹资人. 出资人和筹资人通过平台信息撮合达成交易意向, 并签订网络合同, 约定交易双方的权利义务.

以网络借贷为例, 平台作为信息中介, 为交易双方提供信息搜集、信息公布、资信评估、信息交互、借贷撮合等服务 [2]. 互联网借贷平台相比于传统借贷机构, 所有交易和操作信息更加公开透明 [3]. 筹资人作为借款人发布借款标的信息募集资金, 此时可以有多个出资人投标. 在投标期间, 因为可能出现募集失败的情况, 出资人资金会先划拨到平台设立的存管账户. 直到募集结束, 如果募集成功, 扣除平台手续费后的资金, 从存管账户划拨到筹资人账户. 如果募集失败, 资金原路返回出资人账户.

(2) 平台存管账户模式存在的问题

从资金划拨角度, 互联网投资借贷平台目前比较常见的模式是平台客户分散账户的模式 [4, 5]. 现有资金存管系统通过存管账户进行统收统付. 整个平台会建立一个大的存管账户, 同时出资人和筹资人在存管账户下挂靠虚拟账户, 记录在存管账户的资金余额. 出资人和筹资人银行账户之间的资金划拨通过存管账户完成.

存管账户沉淀了大量在途资金, 虽然银行对存管账户进行监管, 但仍然无法杜绝平台虚假挪用的风险. 同时, 存管账户是以平台主体名义开立, 与平台信息中介角色不符, 并可能因平台主体自身原因造成资金风险.

(3) 资金用途和交易一致性缺乏保障

当前互联网投资借贷环境下, 缺乏有效手段保障资金用途和交易一致性. 首先是资金用途方面, 问题比较突出. 虽然有合同约定, 但筹资人从平台拿到资金后, 实际上拥有自主使用权, 很难防止挪用, 由此造成出资人风险. 同时, 由于是通过网络达成的交易, 出资人无法接触到筹资人, 亟需能够自主追踪和监控资金流向的工具. 一旦发现挪用能及时阻止, 避免发生损失.

其次现有模式存在平台主体自身的操作风险和安全风险, 主要体现为交易信息一致和合同执行一

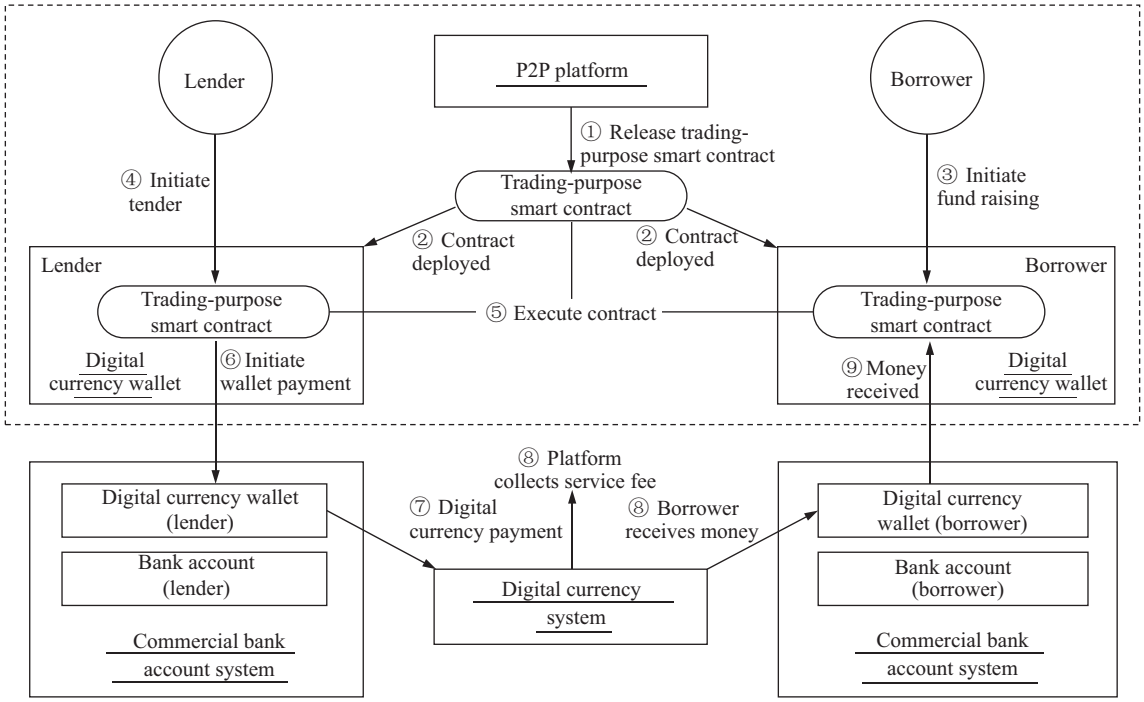

图 2 数字货币整体方案应用示例

Figure 2 Example of general plan for digital currency application

致问题. 互联网投资借贷平台作为第三方, 所有信息都来自平台单方面提供, 出资人、筹资人、监管机构及其他参与方难以相互核对交易信息. 另一方面, 出资人和筹资人通过平台签订网络合同, 整个交易和合同的执行过程都是由平台主导控制, 缺乏监督和保障. 因而存在平台可能造假的操作漏洞和平台自身的安全隐患.

3 互联网投资借贷平台数字货币整体方案设想

如何解决现有平台的诸多问题, 传统方式着重于加强对平台主体的评估和管控, 间接保障交易和合同执行的安全. 而数字货币提供了一种新的解决思路, 通过技术手段剥离平台对业务过程的控制力, 由可信的系统来完成交易和合同执行, 从根本上隔离了平台风险. 整体技术方案分为两层: 基于数字货币钱包应用提供技术可信的运行环境, 保障交易过程公开透明、安全可控; 基于数字货币在技术上保障资金流转安全、便捷、自主可控.

(1) 数字货币和钱包整体方案设想

如图 2 所示, 数字货币体系分为两层, 上层为数字货币应用服务体系, 基础是数字货币钱包应用(以下简称 “钱包应用”). 下层是数字货币系统, 由数字货币发行机构提供. 商业银行在现有账户体系引入数字货币钱包 [6], 连接上下两层, 实现数字货币从发行到场景应用的连通. 商业银行提供数字货币钱包访问的接口, 钱包应用可调用该接口实现数字货币操作. 钱包应用支撑场景的应用服务, 并可利用智能合约提供技术可信的运行环境. Szabo [7] 在 1996 年提出了 “智能合约” (smart contract) 的概念, 指出智能合约通过软硬件系统实现强制执行的特征, 当前兴起的分布式账本技术为智能合约的实现提供了一种技术参考.

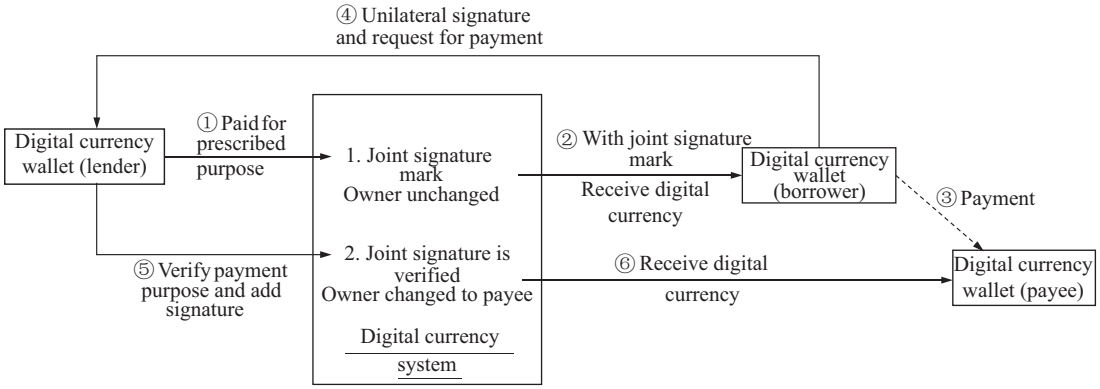

图 3　数字货币联合签名机制管控资金用途

Figure 3　Joint signature mechanism of digital currency to control the use of funds

平台发布交易智能合约, 出资人和筹资人通过钱包应用部署该合约, 就可以参与交易. 筹资人通过钱包应用调用智能合约发起筹资, 并提供带签名的个人信息. 平台对智能合约中筹资人信息出具资信认证签名. 出资人根据平台认证的智能合约信息进行投标, 同时提供带签名的个人信息. 智能合约自动完成双方交易撮合, 并自动发起出资人数字货币钱包的支付交易. 出资人钱包应用商业银行数字货币钱包, 通过数字货币系统完成数字货币直接转移, 最终筹资人收到数字货币, 同时平台收到以数字货币支付的手续费. 智能合约按事先约定自动控制整个募集和后续还款过程, 后续流程在此不再详述. 整个过程参与各方在智能合约层均保持完全一致.

(2) 通过数字货币联合签名解决资金安全问题

数字货币在形式上就是一串经过加密的字符串, 该字符串包含所有者标识. 出资人将数字货币字符串直接转移给筹资人, 可以通过联合签名机制来有效监控资金用途. 所谓联合签名, 就是数字货币的支付必须要多方同时签名认可才能完成, 因此筹资人在收到数字货币后, 也没有完全自主使用权, 从而有效防范了挪用风险. 同时在联合签名下, 出资人作为发起方, 将数字货币转移给筹资人, 可以不变更所有者, 虽然筹资人收到数字货币, 但其所有者仍然是出资人, 必须经双方签名才能使用. 在使用权和所有权均得到有效控制的情况下, 可以解决现有的资金安全问题.

具体流程如图 3 所示, 出资人通过数字货币钱包发起定向用途支付, 要求采用两方联合签名验证. 数字货币系统在待转移的数字货币上设置两方联合签名标识, 同时不变更所有者. 筹资人收到带标识的数字货币, 在需要向外付款时, 将带标识的数字货币加上筹资人签名后发送给出资人, 请求付款并提供付款信息, 包括付款用途、收款人信息等. 出资人审核确认付款信息符合用途后, 在单签名的数字货币上加上出资人签名后, 形成两方联合签名发送给数字货币系统. 数字货币系统验证两方联合签名通过后, 直接将所有者变更为收款人, 并发送给收款人 [8~12].

通过联合签名机制, 出资人将数字货币转移给筹资人后, 对该货币后续用途能够完全掌控. 出资人投标成功就可以转移数字货币, 无需存管账户, 也没有沉淀资金风险. 同时, 投资人虽然无法接触筹资人, 但能够在资金使用上进行直接控制, 有效防止了虚假交易和资金挪用风险.

(3) 利用钱包应用中的智能合约保障交易一致性

在数字货币体系下, 出资人、筹资人、平台以及其他角色, 通过钱包应用连接起来, 如图 4 所示. 原有平台内部交易系统, 被可信的智能合约运行环境替代, 成为一个可以多方参与的公开透明的平台.

钱包应用作为应用访问接入层, 为参与各方提供个性化的应用服务功能, 同时进行统一的权限控

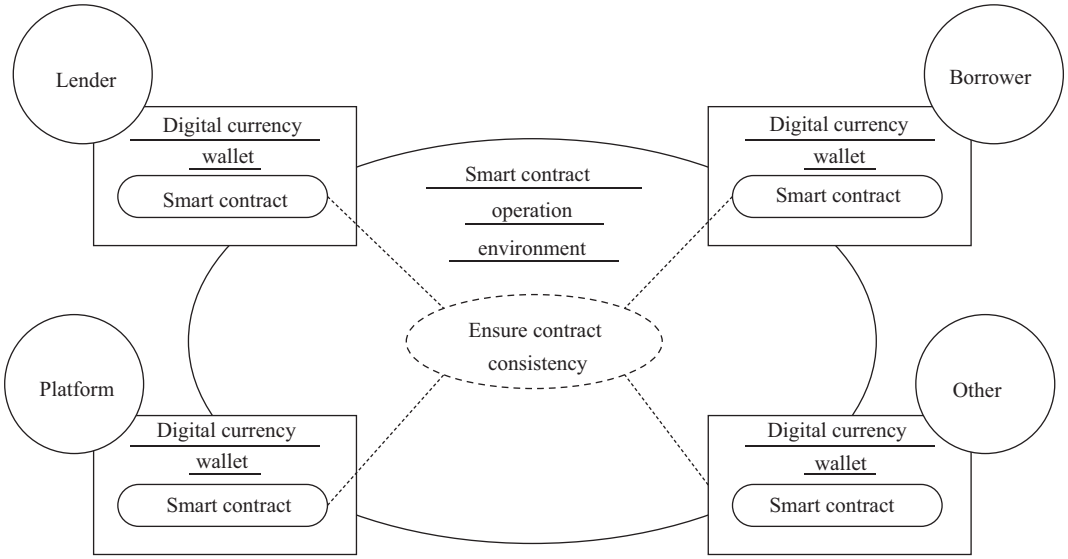

图 4 利用钱包应用的智能合约保障交易一致性

Figure 4 Smart contracts of wallet applications to ensure consistency of transactions

制. 智能合约运行环境为钱包应用提供了统一的可信的技术基础, 保障交易内容和过程对参与各方的一致性. 平台无法修改智能合约运行环境, 无法破坏合约一致性, 从而修复了原有平台操作风险漏洞. 智能合约运行环境可以采用中心化系统也可以采用分布式系统.

钱包应用体系既保留了应用的多样性, 也维护了运行的一致性和安全性. 针对互联网投资借贷这种开放的交易场景, 在为创新服务提供应用支撑的基础上, 也为其他参与方 (例如: 第三方评估机构等) 加入提供了便利. 通过技术可信保证交易合约的信息一致, 降低多方信息同步成本, 提高交易的透明性, 杜绝造假可能. 同时也为方便监管提供了新的技术手段.

(4) 技术实现构想

传统的互联网投资借贷业务, 平台作为需要可信的第三方, 存在着信用风险和操作风险. 基于数字货币的技术方案需要平台做出重大的功能转型, 从交易第三方转型成为信息服务与合约执行服务方. 从技术方案选择上, 可以采用中心化的体系架构, 亦可采用分布式的架构, 都是因为出资人和筹资人的直接对接缺乏信任基础, 需要从技术上保障整个业务是在可信的环境中完成.

(i) 基于中心化服务的解决方案. 解决方案基本类似于传统的互联网投资借贷系统, 弱化了平台作为可信第三方的角色, 如图 5 业务方案设想中所述, 利用数字货币所携带的流通全生命周期的全息记录, 引入应用端数字货币钱包概念, 对整个业务流程作出改进.

(ii) 基于分布式账本技术的解决方案. 解决方案包括银行端数字货币钱包、应用端数字货币钱包、互联网投资借贷应用程序、智能合约开发与执行环境, 以及底层分布式账本服务. 为了更好地满足金融行业隐私保护、交易吞吐量、运营规模等要求, 可采用分层和隔离模式下的分布式账本技术 [13]. 如图 6 所示, 整体架构简单来说有两层结构, 数字货币钱包应用层 (其中包括钱包应用与智能合约逻辑)、分布式账本层. 业务参与角色有钱包应用服务商 (平台)、出资人、筹资人、银行机构, 也可根据需要增加非直接参与者如监管机构等, 本方案中不做赘述.

该系统既可部署在云上, 亦可沿用各方已有的信息系统投资而采用 API 的方式对接. 平台方从传统的交易第三方转变为数字货币钱包运营商, 主要职责是信息发布与撮合、智能合约的发布、数字货

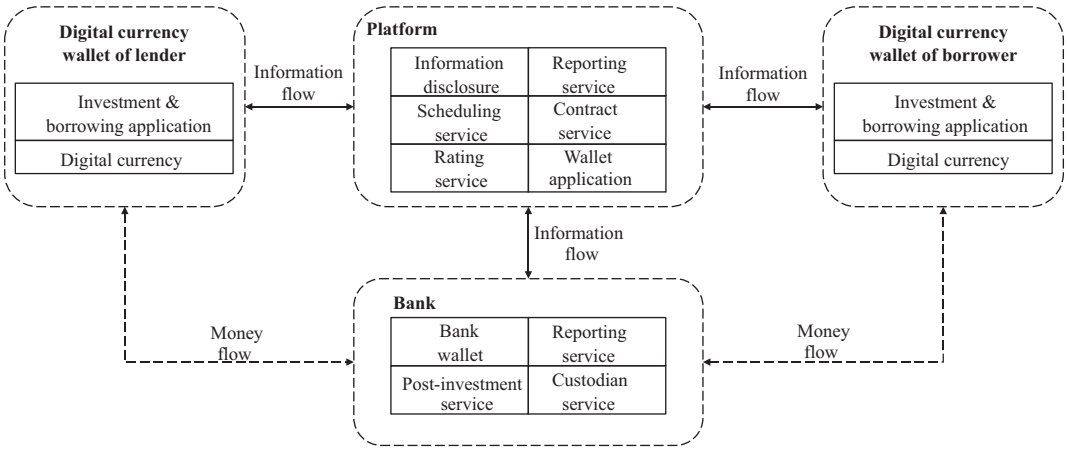

图 5　基于中心化系统的解决方案

Figure 5　Solution based on centralized system

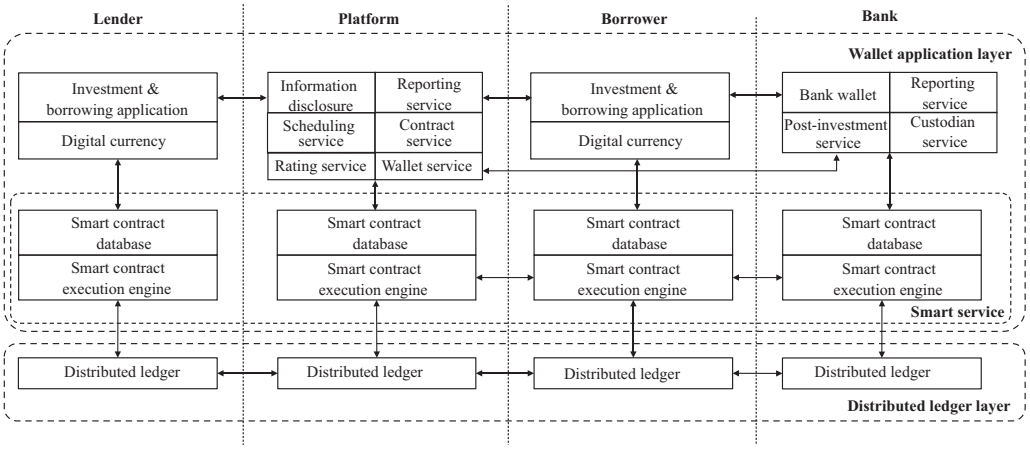

图 6　基于分布式账本技术实现的解决方案

Figure 6　Solution based on distributed ledger technology

币的存管, 以及与银行数字货币钱包/账户的对接. 银行方的职责就是数字货币的出入账服务, 亦可提供跟踪资金用途等增值服务.

由市场参与者共建全局统一的分布式账本, 能够创建一个可信的环境, 改变原有高度依赖中介的传统交易模式, 改进原有流程, 为登记、确权和交易等操作提供良好的技术保障. 资金权益和交易信息安全可靠、不可篡改、不可抵赖, 整个交易过程公开透明且可追踪. 基于智能合约技术, 还能够为市场参与者提供更加智能化的交易服务. 此外全局统一账本也给了监管机构一份完整的业务视图, 可以改变事后监督为事前预防和事中预警.

4　基于分布式账本技术实现的解决方案

在数字货币钱包应用体系下, 平台从交易控制方还原为本来的中介服务方, 基于钱包应用和智能合约运行环境, 参与交易过程, 为出资人和筹资人提供信息中介服务. 平台提供服务的内容没有变化,

但服务的形式发生了变化. 平台可以开发个性化的钱包应用, 为交易各方提供服务. 同时平台开发的交易产品载体变为智能合约, 平台可以着力于制定和发布各种智能合约, 以满足多样化交易需求. 在这种情况下, 开发交易产品的过程大幅简化, 甚至可以为客户提供定制化交易智能合约.

在钱包应用的下一层, 数字货币体系通过数字货币钱包连通商业银行账户体系, 为平台提供了统一、便捷的点对点 (P2P) 直接资金结算能力. 可以实现交易双方资金的直接转移, 简化平台现有的支付过程, 消除了存管账户的问题. 同时, 数字货币通过类似联合签名等方式, 能够为交易提供资金监控和追踪能力, 极大增强了交易保障功能. 平台可以充分基于数字货币的诸多优势特性, 为签约后的交易执行提供增值服务, 例如定制化的资金交割模式等.

数字货币和钱包可运行在现有金融设施之上, 为数字普惠金融提供了更强有力的支撑. 传统互联网金融平台可以借此机会寻求转型, 作为数字货币钱包应用服务商, 将传统平台内部的交易改造为通过钱包应用的智能合约交易. 有了钱包应用和数字货币, 传统交易和支付过程大幅简化. 基础设施的统一性、技术保障的交易可信和一致性, 将大大降低平台在系统和业务方面的投入和维护工作. 平台可以集中资源, 充分挖掘钱包应用创新和数字货币支付创新的潜力, 强化对客户的服务优势, 开发更具竞争力的产品和服务, 在数字货币生态体系中, 更透明、更规范化地助力数字普惠金融创新.

5 结语

数字经济的浪潮必然基于数字加密技术. 因为在数字化的世界里, 加密 (资金加密、交易加密、投资加密等) 才是对投资者最基本的保护. 如果说监管者追求的穿透式监管偏于宏观层面, 那么微观上让投资者管好自己的钱更合乎自负其责的理念 —— 当然得在投资者有这个能力的基础之上. 理想的数字货币系统就是想为投资者打造这样一个让持币者可以放心使用自有数字现金的基础平台.

本文以法定数字货币在互联网投资借贷中的应用为案例, 系统展示数字货币持有者如何在借贷链中实现自有资金的自主可控. 理想的数字货币具备不可重复花费性、不可伪造性、匿名性、系统无关性、可分性、可传递性、可追踪性、可编程性、公平性等特性, 其中蕴含的全新品质, 必将使法定数字货币得以开启并支撑全新的更为广阔的商业应用模式.

参考文献

1 The People's Bank of China. The People's Bank of China Digital Currency Symposium was held in Beijing. 2016. http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/3008070/index.html [中国人民银行. 中国人民银行数字货币研讨会在京召开. 2016. http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/3008070/index.html]

2 Puhui Finance Department. Interim Measures for the Administration of the Business Activities of Online Lending Information Intermediary Institutions. CBRC Order [2016] No. 1. 2016. http://www.cbrc.gov.cn/govView_37D312933F1A4CECBC18F9A96293F450.html [普惠金融部. 网络借贷信息中介机构业务活动管理暂行办法. 银监会令 [2016]1 号. 2016. http://www.cbrc.gov.cn/govView_37D312933F1A4CECBC18F9A96293F450.html]

3 Jackson K. A detailed look into peer to peer lending. Honors Economics Senior Thesis. Berkeley: University of California, Berkeley, 2016

4 Naïdji C. Regulation of European peer-to-peer lending Fintechs Regulatory framework to improve SME's access to capital. Dissertation for Master Degree. Brussels: Faculty Of Economics And Business Campus Brussels, 2017

5 Bottiglia R, Pichler F. Crowdfunding for SMEs: A European Perspective. London: Palgrave Macmillan UK, 2016. 93–210

6 Yao Q. Digital currency and bank account. Tsinghua Financ Rev, 2017, 7: 63–67 [姚前. 数字货币和银行账户. 清华金融评论, 2017, 7: 63–67]

7 Szabo N. Smart contracts: building blocks for digital markets. 2016. https://kameir.com/smart-contracts/

8 Institute of Digital Money, The People's Bank of China. A transaction method, system and apparatus for investment financing based on digital money. China, 201710496964.3 [P]. 2017-11-7 [中国人民银行数字货币研究所. 一种基于

数字货币的投资筹资的交易方法、系统和装置. 中国, 201710496964.3 [P]. 2017a-11-7]
9 Institute of Digital Money, The People's Bank of China. Digital money circulation method and device. China, 201710495071.7 [P]. 2017b-11-7 [中国人民银行数字货币研究所. 数字货币的流通方法和装置. 中国, 201710495071.7 [P]. 2017b-11-7]
10 Institute of Digital Money, The People's Bank of China. A method and system for binding App wallet and bank digital money wallet. China, 201710493140.0 [P]. 2017c-11-7 [中国人民银行数字货币研究所. 数字货币的应用钱包与银行钱包进行绑定的方法和系统. 中国, 201710493140.0 [P]. 2017c-11-7]
11 Institute of Digital Money, The People's Bank of China. A method and system for realizing digital money wallet payment through bank account. China, 201710494152.5 [P]. 2017d-11-17 [中国人民银行数字货币研究所. 一种通过银行账户实现数字货币钱包支付的方法和系统. 中国, 201710494152.5 [P]. 2017d-11-17]
12 Institute of Digital Money, The People's Bank of China. A method and system for payment of digital money wallet. China, 201710493211.7 [P]. 2017e-11-7 [中国人民银行数字货币研究所. 一种数字货币钱包支付的方法和系统. 中国, 201710493211.7 [P]. 2017e-11-7]
13 Digital Asset. The Digital Asset Platform Non-technical White Paper. 2016. http://hub.digitalasset.com/digital-asset-platform-non-technical-whitepaper

Study on the application of digital fiat currency in peer-to-peer investment and lending

Qian YAO

Institute of Digital Money of the People's Bank of China, Beijing 100088*, China*
E-mail: yaoqian@pbc.gov.cn
* This article does not represent the opinions of the author's organization.

Abstract Currently, peer-to-peer lending platforms are faced with the risk of funds misappropriation and lack effective means to ensure funds security and transaction consistency. The traditional method focuses on the assessment and control of the platform to indirectly guarantee the security of transactions and execution of contracts. This paper proposes a new solution based on digital fiat currency (DFC), which creates a trusted operating environment via a DFC wallet application service system and uses joint signatures to monitor the flow of funds to ensure security. Moreover, the proposed solution implements smart contracts in DFC wallets to achieve transaction consistency in order to ensure that the transaction process is open, transparent, safe, and controllable. In this way, troubled Internet finance platforms can transform themselves into DFC value-added service providers, playing a more transparent and regulated role in promoting inclusive finance in the digital currency ecosystem.

Keywords digital fiat currency, central bank digital currency, peer-to-peer lending platform, smart contract, joint signature

Qian YAO was born in 1970. He is vice director-general of the Technology Department of the People's Bank of China (PBC), head of the Institute of Digital Money of PBC, and the current secretary-general of the China Financial Standardization Technical Committee. Holding a Ph.D. degree in engineering, he is a professorate senior engineer. Before joining the PBC in 2010, Dr. YAO worked in the Information Statistics Department and the IT Service Center of the China Securities Regulatory Commission and the China Securities Depository and Clearing Corporation. During his time in PBC, Dr. Yao served as vice director-general of the Credit Reference Center and member of the Academic Committee of the Center for Postdoctoral Studies of the Financial Research Institute and the Credit Reference Center of PBC.