普惠金融背景下用户隐私信息演化博弈及区块链方法应用研究

陈雪如，胡晓霁，宋炎*

* 陈雪如，浙江大学管理学院博士研究生，chenxueru@zju.edu.cn，Tel: 18867148721；胡晓霁，中国人民大学财政与金融学院博士研究生，huxiaojiy3@ruc.edu.cn；宋炎，华南理工大学硕士研究生，小米 AI Lab 图像视觉处理研究员，songyan3@xiaomi.com.

摘要：本文基于演化博弈理论，对提供普惠金融产品与服务的机构和普惠金融用户之间在隐私信息和数据安全方面的博弈关系进行了深入分析，探索了现实情况下两者之间的均衡策略关系，并此基础上进一步讨论了一种基于区块链技术的普惠金融用户隐私信息保护方法，从技术层面探索了如何避免用户隐私信息泄露事件和风险的发生。本文的研究结果显示，只有加强普惠金融服务商泄露用户信息的惩罚力度以及从政策、法律、市场等方面鼓励其主动为用户提供隐私保护服务，才有可能进一步激发个人及小微企业充分参与普惠金融的意愿，也才能最终促进普惠金融行业真正实现健康繁荣发展。在隐私保护的过程中，区块链技术可以作为重要的技术手段，为普惠金融服务商和用户之间在隐私信息和数据安全方面的矛盾提供新的解决方案。

关键词：隐私保护；普惠金融；演化博弈；区块链

1 引言

普惠金融（Inclusive finance）这一概念自 2005 年联合国提出以来，在全球范围内获得了广泛的关注，越来越多传统金融机构、互联网企业乃至科技企业开始关注这一传统金融市场中的长尾群体和弱势群体，推出了一系列金融产品和服务以可负担的成本为有金融服务需求的社会各阶层和群体提供适当、有效的金融服务。近年来，普惠金融也频繁出现在政府报告工作中，成为金融市场、行业企业和社会群体关注和热议的焦点。

在当前互联网信息科技快速发展的时代背景下，随着普惠金融服务可获得性不断提升，为广大个人用户和小微企业等群体提供便捷、个性化、深度化金融产品和服务的同时，基于其业务模式、技术属性和风险特征等特点，也面临了新的巨大的挑战，其中如何在信息使用上保持平衡，保护用户的信息安全和隐私，成为当下亟待解决的问题，也是未来制约中国数字普惠金融发展最大的制约和阻碍之一。随着大数据、云计算、人工智能等科技手段被越来越多运用到征信领域，国内外普惠金融服务机构协同征信机构、数据服务机构等逐步开始收集和利用用

户借贷信息之外的替代数据并对数据进行深度挖掘，从而创新金融产品和服务，以解决小微企业融资、普惠金融发展中的信息不对称问题。然而，由于金融监管的滞后和市场机制的不完善，普惠金融服务商在收集和使用用户信息的过程中存在着很多不科学、不规范甚至恶意售卖用户隐私信息的现象，带来了用户信息安全、隐私保护和信息主体权益保护等风险问题。

由于普惠金融服务发展过程中普惠金融服务机构和平台数据过度采集、滥用等现象日益突出，中国消费者协会于 2018 年 11 月 28 日通报了 100 款金融 APP 个人信息收集与隐私政策测评情况。测评显示，各类 App 普遍存在过度收集个人信息的问题，平台运行过程中的隐私条款内容不达标问题也十分突出，普惠金融服务商和用户之间的矛盾和博弈不断升级。一方面，普惠金融用户渴望享受更加高效、个性化、深度化、普惠化的金融产品和服务，但为了缓解在此过程中的信息不对称问题，其需要向普惠金融服务商提供更加详细的隐私信息；另一方面，普惠金融服务商缺乏保护用户隐私信息的动力和有效方式，监管的滞后和市场环境的纵容使得普惠金融服务商为了利益而滥用用户隐私信息，忽视用户的知情权并采取种种违规行为，使得用户因为隐私信息泄露而遭受电信诈骗、电话骚扰和暴力催收等恶性事件，甚至成为网络世界中的“透明人”。

实现数字普惠金融的健康发展，需要对数据安全和用户隐私保护加以足够的重视，提升普惠金融服务商数据治理、信息安全管理的能力并对其实行合理的监管，充分解决普惠金融服务商和用户在隐私信息之间的博弈难题，从而为更多的长尾用户和小微企业提供安全、高效、个性化的普惠金融产品和服务。当前，关于如何解决普惠金融服务商和用户之间的隐私信息安全与保护问题，还没有一个有效的解决方法，两者在金融服务与信息安全之间的博弈难题亟待更加深入的探讨和研究，以更好地实现在保证双方合理权益的同时保护用户信息安全、实现普惠金融的健康长久发展。

在此背景下，本文从博弈论的角度，基于演化博弈模型对普惠金融服务商和普惠金融用户在隐私信息保护中的具体情况进行研究和讨论，通过分析模型的稳定性探索普惠金融服务商和用户之间的博弈均衡策略；在模型求解的基础上，结合现实情况提出了利用区块链技术设计一个保护普惠金融用户隐私信息系统的具体应用方法和解决方案。

2 文献综述

2.1 金融用户隐私与信息安全问题研究

隐私权的概念于 19 世纪 90 年代被首次提出，自此，金融隐私保护这一问题不仅在学术研究上得到了充分关注，而且陆续走进了各国立法的实践（马运全, 2014)。国内对金融隐私和信息安全的关注大多从对个人信息或隐私的角度出发，并集中在法学层面。（谈李荣，2004）就以银行对金融隐私权的保护为切入点，以金融隐私权与信息披露的冲突与制衡为主线，对金融隐私与信息披露的主要法律问题进行比较系统的考察研究。（刘沛佩，2010）指出，从生态学理论的角度来看，金融消费者是金融生态圈中最脆弱的一环，其金融隐私面临被侵犯的风险，因此加强金融隐私权保护尤为必要。

同时，随着互联网的不断普及和发展，其所具有的无形性及虚拟性对金融隐私权的保护形成了较大的冲击（权洪森, 2018），互联网金融背景下的金融消费者隐私权保护问题也得到了更大关注。刘文茜（2015）提出网络载体在加速服务提供的同时也加速了隐私侵权的传播速度，扩大了隐私侵权的辐射范围，使得新时代背景下隐私遭受侵害的程度更加严重；

在普惠金融方面，胡文涛(2018)提出我国应制定和完善个人信息保护法律、重视推进普惠金融过程中金融隐私权保护的法律建设、致力于"走出去"的金融机构应广泛关注并遵循国外金融隐私权保护的法律规定。然而，深入探索普惠金融发展过程中的用户隐私保护和信息安全的研究很少，结合当下社会普惠金融发展过程中所遇到的现实问题和发展现状，这一领域的研究存在十分的迫切性和必要性。

2.2 演化博弈研究与应用

演化博弈理论(Evolutionary Game Theory)最早起源于 Fisher 和 Hamilton 等遗传生物学家对动物和植物的冲突与合作行为的博弈分析。与传统的非合作博弈相比，演化博弈理论假设博弈方是从最大的总体中随机抽取的，参与方按照社会方式反复进行博弈，在策略选择的总体分布上有种历时的演化过程，整个系统的是不断变化，最终达到一种稳定的均衡（乔根，2007)。

1973 年，Maynard & Price(1973)提出演化博弈模型的演化稳定策略(ESS)，

并指出，假设在选定某一特定策略的大群体中出现了一个选择不同于这一特定策略的突变小群体，如果突变小群体在博弈的获取的收益大于大群体中个体多获得的收益，那么突变小群体将实现入侵；反之，突变小群体将会在生物群体不断地演化过程中淘汰。如果一个群体能够抵御任何突变小群体的入侵那么则成这一群体达到了一种演化稳定状态，此时群体的策略选择就是演化稳定策略。

近年来，演化博弈理论被广泛运用到了社会科学与金融经济研究的多个方面。王永平，孟卫东（2004）运用演化博弈理论的方法，建立了一个供应链企业合作竞争机制演化博弈的数理模型，分析了供应链企业合作竞争机制演变的动态过程；郑君君等，2012）基于演化博弈理论与方法，研究了具有有限理性的不同类型风险投资家与外部投资者之间策略选择的互动机制，探讨了声誉的激励效应和监督机制的惩罚效应对不同风险投资家的有效性及其如何引导和制约风险投资家的策略选择；李煜华，武晓锋和胡瑶瑛（2013）在对战略性新兴产业集群创新主体关系和创新方式进行分析的基础上运用演化博弈理论，构建了集群内企业和科研院所创新博弈的复制者动态模型、分析了其在创新过程中的动态演化过程并提出了相应的协同创新策略；李军伟（2014）则基于用户行为收益框架理论将用户使用社交网络的感知收益和感知风险进行量化，构建了社交网络用户的收益函数并将演化博弈论运用在社交网络隐私研究中。

演化博弈理论在社会科学研究中显示出了极大的适用性，相比于传统博弈模型更加符合现实社会的一般特征，更有助于研究探索出实践活动中的真实结果。然而目前，尚没有研究运用演化博弈理论对普惠金融发展中的服务商与在用户隐私信息上的矛盾问题进行分析和研究。

2.3 区块链在隐私保护方面的研究

区块链技术是一种广泛应用于新兴数字加密货币的去中心化基础架构，具有去中心化、去信任化和区块数据基本不可篡改等特性，因此受到企业尤其是金融机构的追捧（沈鑫，裴庆祺和刘雪峰，2016），形成了一种全新的去中心化的信息存储、管理和使用方式，对于社会信任机制的重新构建形成了一定的创新冲击，对各行各业造成了潜在的深刻影响。

近年来，区块链技术在隐私保护方面的研究和实践得到了学者和业界的广泛关注。Zyskind & Nathan（2015）首次提出和设计了区块链技术在个人隐私信息

保护方面一般模型和系统，以确保以确保个人用户充分拥有和控制他们的个人隐私数据。Ji & Xu（2019）基于隐私保护问题在移动支付、电子投票、物联网、智能系统和数据共享方面存在的问题，对基于区块链的隐私保护技术在各个应用领域潜力进行了探究和分析。Jiang et al.（2019）针对现有的电子商务模式中所有权证明与隐私保护的两难问题，尝试设计了一种基于区块链的私有智能契约的保密业务协议，从而实现在允许交易对手在不披露身份、地址和电话号码等私人信息的情况下进行交易。国内学者（黄永刚，2016 ；田海博，何杰杰和付利青，2017）等也曾探究过区块链技术在医疗电子健康档案安全建设、隐私保护公平合同签署协议等方面的应用方案。

对于普惠金融的未来长久发展来说，用户隐私保护和信息安全十分重要，结合以上研究，我们认为区块链技术在普惠金融服务的用户隐私保护与信息保护方面可以发挥较大的作用，但目前没有文献针对区块链技术在这一场景的应用进行深度的研究。

3 基于演化博弈的普惠金融用户隐私博弈分析

与一般博弈理论相比，演化博弈理论（Evolutionary Game Theory）是一种复杂的动态重复博弈过程，是建立在群体参与人的有限理性基础之上，以不完全信息为前提的一种博弈方法。参与博弈的主体双方不一定能在一次博弈中找到最优策略，其行为规则和策略是在演化的过程通过不断地学习、模仿而实现修正和改进，从而通过比较不同策略所产生的收益而获得演化稳定策略。演化博弈过程一般可以分为选择和突变两个阶段。选择是指可以获得高收益的策略以后将会更多的被后来者选择，突变是指由于某种随机因素的作用博弈主体会尝试各种不同于群体的策略，突变通常被认为是演化过程的重要过程，它会改变博弈主体的策略选择，进而影响系统最终均衡状态。

3.1 普惠金融用户隐私演化博弈模型

在普惠金融活动中，用户作为一个独立的群体，其行为规则和策略往往随着时间的推进和对金融产品和服务以及背后的服务商的了解而不断学习、模仿、修正和改进的，不断受到外部环境的冲击和影响，从而选择是否参与普惠金融活动以及与服务商共享隐私数据和信息的程度。而普惠金融的提供方——服务商或者

平台也会根据用户群体策略的改变而相应改变自身的隐私保护策略，通过不断地演化实现自身收益的最大化。在这一过程中，博弈双方即普惠金融用户和普惠金融服务商都是有限理性的，具备模仿、学习的能力，可以在博弈过程中不断调整各自的策略，以获得最大的收益。

基于以上分析，我们做出以下假设：

（1）普惠金融用户通过接触普惠金融服务，在普惠金融服务商处获得的基础收益为B_1；

（2）普惠金融用户可以通过提供更详细的个人隐私信息而获得的个性化、深度化的金融服务，由此产生的增值收益为B_2；

（3）如果普惠金融用户向服务商提供个人隐私信息以寻求获得深度普惠金融服务，但普惠金融服务商未采取隐私信息保护措施而将用户个人隐私信息泄露给第三方或存在泄露风险，用户则会产生相应的损失L；

（4）普惠金融服务商在金融服务过程中由提供基本金融服务而获得的固定收益为S_1；

（5）普惠金融服务商在金融服务过程中获得用户个人隐私信息而通过提供个性化、深度化普惠金融服务而获得的额外收益为S_2；

（6）普惠金融服务商主动为用户提供个人隐私信息保护而付出的成本为 C；

（7）普惠金融服务商如果将用户个人隐私信息泄露给第三方，从第三方获得的额外收益为S_3；

（8）普惠金融服务商如果将用户个人隐私信息泄露给第三方，所产生的潜在的平台信誉损失和失去用户损失为R；

（9）以上所有参数均大于 0。

综合以上假设和分析，我们可以得到普惠金融服务商和用户的在隐私信息博弈过程中的收益矩阵如表 1 所示。

表 1 普惠金融服务商与用户隐私博弈收益矩阵

用户 \ 服务商	保护用户隐私信息	不保护用户隐私信息
提供隐私信息	$\mathrm{B}_1 + B_2$，$S_1 + S_2 - \mathrm{C}$	$\mathrm{B}_1 + B_2 - \mathrm{L}$，$S_1 + S_2 + S_3 - R$

不提供隐私信息	B_1，$S_1 - C$	B_1，S_1

假设普惠金融用户有 p 的概率向普惠金融服务商提供个人隐私信息，$(1-p)$的概率不提供个人隐私信息；普惠金融服务商有q的概率提供用户隐私信息保护，$(1-q)$的概率不提供用户隐私信息保护。

则对于提供个人隐私信息的普惠金融用户来说，其收益为：

$$\alpha_1 = q(B_1 + B_2) + (1-q)(B_1 + B_2 - L)$$

对于不提供个人隐私信息的普惠金融用户来说，其收益为：

$$\alpha_2 = qB_1 + (1-q)B_1$$

混合策略下普惠金融用户的期望收益为：

$$\bar{\alpha} = p\alpha_1 + (1-p)\alpha_2 = B_1 + pB_2 - p(1-q)L$$

根据演化博弈模型，当一种策略的收益比种群的平均收益高的时候，这种策略就会在种群中得以发展，表现为种群中采取这种策略的个体比例增长为正，从而形成复制者动态方程，用以描述某一策略被采用的频数/频率的动态微分方程。

因此，在这种情况下，普惠金融用户的动态复制方程为：

$$F_1(p) = \frac{d_{p(t)}}{dt} = p(\alpha_1 - \bar{\alpha}) = p(1-p)[B_2 - (1-q)L] \qquad (1)$$

另一方面，如果普惠金融服务商采取用户隐私信息保护措施，其收益为：

$$\beta_1 = p(S_1 + S_2 - C) + (1-p)(S_1 - C)$$

如果普惠金融服务商不为用户提供隐私信息保护措施，其收益为：

$$\beta_2 = p(S_1 + S_2 + S_3 - R) + (1-p)S_1$$

混合策略下普惠金融服务商的期望收益为：

$$\bar{\beta} = q\beta_1 + (1-q)\beta_2 = S_1 + pS_2 + (1-p)(S_3 - R) - qC$$

根据演化博弈理论，同理，普惠金融服务商的动态复制方程为：

$$F_2(q) = \frac{d_{q(t)}}{dt} = q(\beta_1 - \beta) = q(q-1)[p(S_3 - R) + C] \qquad (2)$$

3.2 普惠金融用户隐私演化博弈模型稳定性分析与仿真检验

根据演化博弈的性质，我们可以得知一个稳定的状态必须对局部的微小扰动有一定的抗干扰性或稳健性才能称之为演化稳定策略(ESS)，它是所有参与个体在经过反复博弈后选择某个最优的和稳定的策略。所谓最优，是指任何的参与个

体单方面改变自己的策略选择都是无利可图的、不能额外增加自身的收益；所谓稳定，是指任何参与主体由于偶然的错误偏离了均衡点，复制者动态的均衡点不会发生改变。演化稳定策略是考察系统落在均衡点吸引域范围之内的局部动态性质，不是考察落在均衡点吸引域范围之外的情况，可以描述系统的局部动态性质。

下面我们对普惠金融用户的隐私演化博弈模型的稳定性进行分析。根据微分方程的稳定性定理，对（1）（2）式分别求导得到，

$$F_1'(p) = (1-2p)[B_2 - (1-q)L] \qquad (3)$$

$$F_2'(q) = (2q-1)[p(S_3 - R) + C] \qquad (4)$$

我们知道当且仅当（1）式等于 0 且$F_1'(p) < 0$时，普惠金融用户的隐私演化模型策略将趋于稳定；同理，当普惠金融服务商的演化策略趋于稳定时，在（2）式中q应该满足$F_2(q) = 0$以及$F_2'(q) < 0$。

对普惠金融用户来说，由$F_1(p) = 0$可得$p = 0$或$p = 1$，但是由于$B_2 - (1-q)L$的符号不确定，因此需要对不同取值的参数进行分类讨论以分析确定最终稳定的演化策略。求解可得，

当$q < \frac{L-B_2}{L}$时，$F_1'(0) = [B_2 - (1-q)L] < 0$，$F_1'(1) = [B_2 - (1-q)L] > 0$，因此只有$p = 0$是普惠金融用户的演化稳定策略；

当$q > \frac{L-B_2}{L}$时，$F_1'(0) = [B_2 - (1-q)L] > 0$，$F_1'(1) = [B_2 - (1-q)L] < 0$，因此$p = 1$是普惠金融用户的演化稳定策略；

对普惠金融服务商来说，同样由$F_2(q) = 0$可得$q = 0$或$q = 1$，q^*需要满足$F_2'(q^*) = (2q^* - 1)[p(S_3 - R) + C] < 0$时才得得到服务商的演化稳定策略，由于$p^*(S_3 - R) + C$的符号不能确定，因此同样需要对不同参数的取值范围需要分别进行讨论。

如果$S_3 > R$，$F_2'(0) = -[p(S_3 - R) + C] < 0$，$F_2'(1) = [p(S_3 - R) + C] > 0$，因此则只有$q = 0$是演化稳定策略。

如果$S_3 < R$且$p < \frac{-C}{S_3 - R}$，$F_2'(0) = -[p(S_3 - R) + C] < 0$，$F_2'(1) = [p(S_3 - R) + C] > 0$，因此只有$q = 0$是演化稳定策略；

如果$S_3 < R$且$p > \frac{-C}{S_3 - R}$，$F_2'(0) = -[p(S_3 - R) + C] > 0$，$F_2'(1) = [p(S_3 - R) + C] < 0$，因此只有$q = 1$是演化稳定策略。

为了更直观的分析在不同初始情况下普惠金融服务商和用户群体的演化策略和最终稳定策略，我们根据模型稳定性分析的结果绘制如图 1，得到在参数$S_3 > R$和$S_3 < R$两种情况下，普惠金融服务商和用户的隐私演化博弈的最终稳定状态。

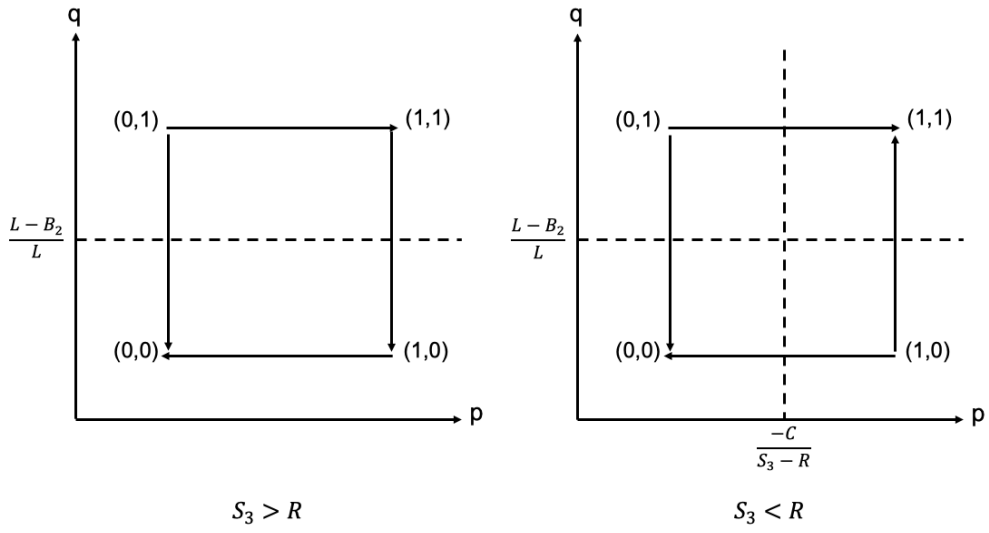


图 1 普惠金融服务商与用户隐私演化博弈动态相位图

通过分析稳定性结果我们发现，当$S_3 > R$时，也就是普惠金融服务商将用户个人隐私信息泄露给第三方获得的额外收益大于其所产生的潜在的平台信誉损失和失去用户损失时，该演化模型的群体稳定策略最终趋向于（0，0），也就是普惠金融用户不提供隐私信息，服务商不保护用户隐私信息。这意味普惠金融整个行业趋向于衰退，意味着用户对于普惠金融服务商信任的完全丧失（且不可逆）以及对于个性化、深度化普惠金融服务的放弃。

我们利用 python 演化博弈模型进行仿真，通过随机选定参数值和p, q参数的初始值，模拟现实环境下普惠金融服务商和用户的策略演化过程和均衡稳定状态。如图 2 展示的是在$S_3 > R$情况下，普惠金融服务商和用户的策略选择演化过程，群体稳定策略最终趋向了（0，0）。

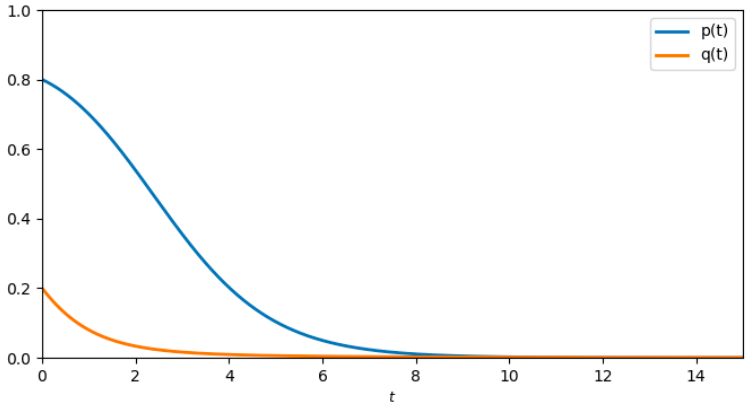
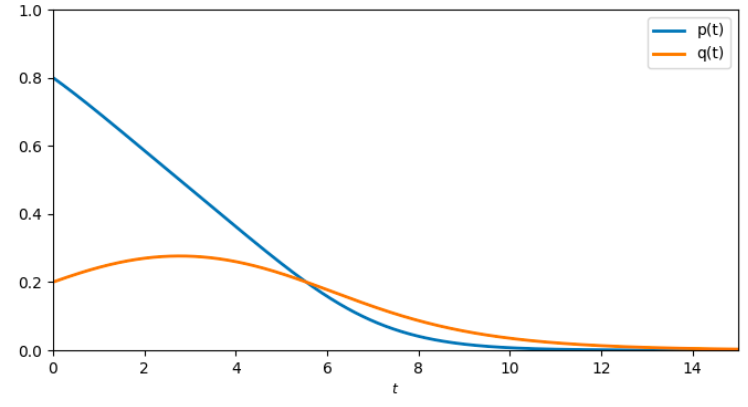


图 2 $S_3 > R$情况下普惠金融服务商与用户隐私演化博弈策略演化过程

当$S_3 < R$时，也就是也就是普惠金融服务商将用户个人隐私信息泄露给第三方获得的额外收益小于其所产生的潜在的平台信誉损失和失去用户损失时，服务商会因为泄露用户的隐私信息而受到更多的惩罚。此时，(0，0)和（1，1）都有可能成为普惠金融服务商和用户演化策略的均衡点，其关键在于用户和服务商之间的相互信任以及普惠金融服务商初始保护用户隐私信息意愿和动机的强烈与否。只有普惠金融服务商在初始时以一个较高的概率保护用户隐私信息时，用户才有意愿提供个人隐私信息，从而参与到普惠金融中来，从而使得行业整体获得积极的发展，最终实现用户群体有意愿提供隐私信息以享受更好的普惠金融服务、服务商群体从自身利益出发有意愿保护用户隐私信息的稳定健康局面。

图 3 是$S_3 < R$的情况下普惠金融服务商与用户隐私演化博弈策略演化过程仿真，上侧是服务商起始保护用户隐私信息概率低的情况，随着用户提供个人隐私信息概率的下降，整个系统最后也会演化到（0，0）的状态；下侧是服务商起始保护用户隐私信息概率高的情况，最终演化到（1，1）的稳定状态。



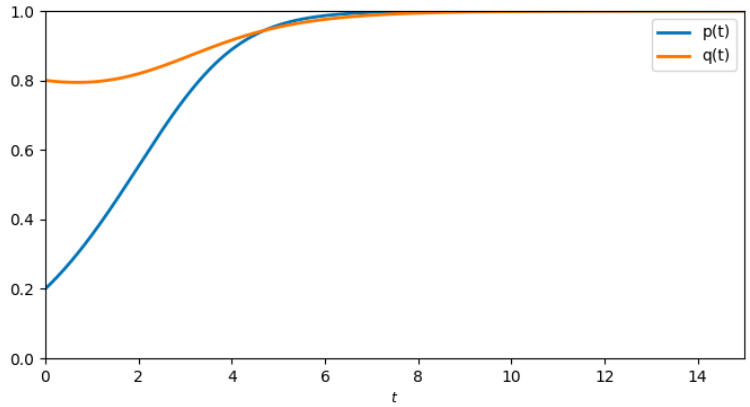


图 3 $S_3 < R$情况下普惠金融服务商与用户隐私演化博弈策略演化过程

4 基于区块链技术的普惠金融用户隐私保护方法

从普惠金融服务商和用户隐私演化博弈模型和稳定性分析结果中我们可以看到，促进普惠金融服务商保护用户隐私信息，促进行业整体健康发展，不仅需要加大对于服务商泄露用户隐私信息的惩罚力度，还要从政策、监管、市场等多个层面鼓励普惠金融服务商主动增加为用户提供隐私信息保护的意愿。这两个方面在目前这一普惠金融发展阶段中的实施都存在着较大的难度，因此我们可以考虑从技术角度解决这一问题，通过运用区块链技术，将用户的隐私信息实现链上管理和使用，从而从技术手段上杜绝服务商泄露用户隐私信息的现象发生。

在本框架中，我们将普惠金融用户设计为数据的拥有者，把普惠金融产品和服务设计为需要用户委派权限的客体。数据收集、分析的过程、方法和整体流程对于所有用户来说都是完全透明的。根据 Zyskind & Nathan（2015），利用区块链技术设计一个保护普惠金融用户隐私信息和信息安全的系统如下。

整个区块链系统涵盖了三大主要主体。第一个是普惠金融用户，也就是所有提供隐私信息以求获得个性化、深度化金融服务的个人或小微企业；第二个是普惠金融服务商，通过获取、分析、利用个人或小微企业信息而为其提供优质普惠金融服务的传统金融机构、互联网企业和新兴金融科技机构等；第三个是区块链网络中的节点（Node），指的是在区块链中提供分布式存储功能的授信实体。当用户加入系统后，程序会首先为用户创造一个 ID，然后由用户发送访问权限指令给区块链系统，用户也可以发送隐私数据到经过加密算法加密的区块链系统中，该数据最终形成一个指向该特定用户的指针，而非完整的用户隐私数据。当普惠

金融服务商的某项特定产品和服务需要访问用户的隐私信息时，首先需要向区块链系统发送一个指针数据，然后区块链系统在对数字签名进行验证之后判断请求来自于服务商还是用户。对于来自服务商的数据请求，系统会结合用户授权进行权限检查。用户在整个过程中可以随时向区块链系统发送指令修改或取消之前设定的对数据（包含之前数据）的访问权限。图 4 显示的就是这样一个基于区块链的普惠金融用户隐私信息保护系统的简要示意图。

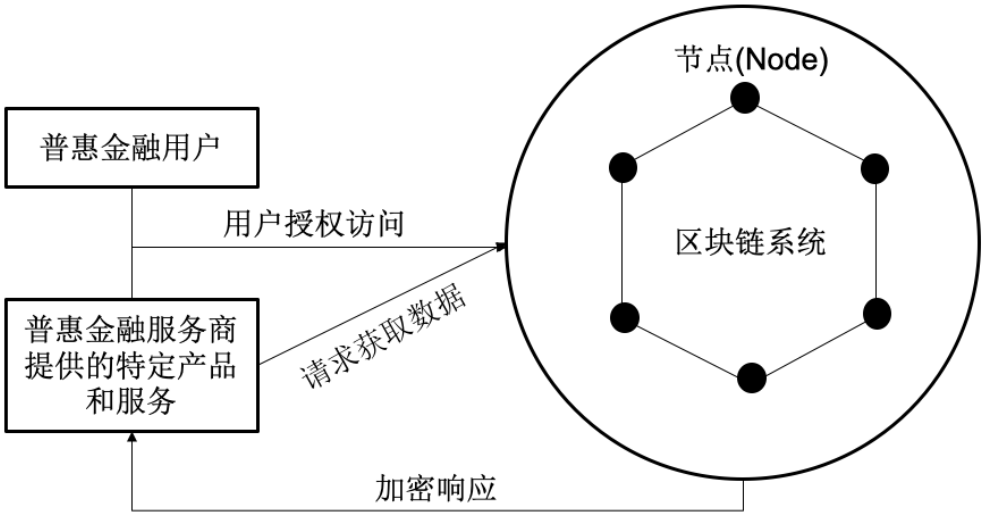


图 4 基于区块链的普惠金融用户隐私保护模型

下面我们对该基于区块链的普惠金融用户隐私保护系统的底层协议进行简要阐述。该协议采用标准加密构建方法，由三元组（$\mathcal{G}_{\text{enc}}$，$\mathcal{E}_{\text{enc}}$，$\mathcal{D}_{\text{enc}}$）定义的对称加密（encryption）方案，三元组中元素分别代表生成器，加密算法和解密算法。此外，数字签名方法（Digital Signature Scheme，DSS）的生成器、签名器和验证算法也可以用一个三元组（$\mathcal{G}_{\text{sig}}$，$\mathcal{S}_{\text{sig}}$，$\mathcal{V}_{\text{sig}}$）来表示，以及基于 SHA-256 的哈希加密函数$\mathcal{H}$。

该系统采用的是（伪）匿名的复合账户机制，普惠金融用户可以不限制地生成匿名账户，该账户可以实现多方共享，但是只有用户可以拥有完全的控制权。一个复合账户机制可以用如下形式表示：

$$Compound_{u,s} = (pk_{sig}^{u,s}, sk_{sig}^{u,s}, pk_{sig}^{s,u}, sk_{sig}^{s,u}, sk_{enc}^{u,s})$$

其中，pk表示私有秘钥，sk表示对称秘钥，u表示用户，s表示特定的普惠金融产品和服务，sig表示签名，enc表示加密。因此举例来说，$pk_{sig}^{u,s}$就表示用户在使用普惠金融产品和服务时经过签名的私有秘钥。下面的协议一至四分别利用伪代码的形式详细说明了该区块链系统生成用户复合账户信息、权限检查、获取控制以及存储和加载数据的具体流程和方法。

协议一：生成复合账户

执行 CompoundIdentity(u, s)

u 执行：

$(pk_{sig}^{u,s}, sk_{sig}^{u,s}) \leftarrow \mathcal{G}_{\text{sig}}()$
$sk_{enc}^{u,s} \leftarrow \mathcal{G}_{\text{enc}}()$

u 与 s 共享 $sk_{enc}^{u,s}$和$pk_{sig}^{u,s}$

s 执行：

$(pk_{sig}^{s,u}, sk_{sig}^{s,u}) \leftarrow \mathcal{G}_{\text{sig}}()$

s 与 u 共享$pk_{sig}^{s,u}$

return $sk_{enc}^{u,s}$，$pk_{sig}^{u,s}$和$pk_{sig}^{s,u}$

执行结束

协议二：区块链权限检查

执行 CheckPolicy(pk_{sig}^{k}, x_p)

s ← 0
$\alpha_{policy} = \mathcal{H}(pk_{sig}^{k})$

if L[α_{policy}] ≠ ∅, then

$pk_{sig}^{u,s}, pk_{sig}^{s,u}, POLICY_{u,s} \leftarrow$ Parse(L[α_{policy}])

if $pk_{s\square g}^{k} = pk_{sig}^{u,s}$ or ($pk_{sig}^{k} = pk_{sig}^{s,u}$ and $x_p \in POLICY_{u,s}$), then

s ← 1

end if

end if

return s

执行结束

协议三：获取控制

执行 HandleAccessTX(pk_{sig}^{k}, m)

s ← 0

$pk_{sig}^{u,s}, pk_{sig}^{s,u}, POLICY_{u,s} = Parse(\mathrm{m})$

if $pk_{sig}^{k} = pk_{sig}^{s,u}$, then

$\mathrm{L}[\mathcal{H}(pk_{sig}^{k})] = \mathrm{m}$

s ← 1

end if

return s

执行结束

协议四：存储与加载数据

执行 HandleDataTX(pk_{sig}^{k}, m)

$\mathrm{c}, x_p, rw = Parse(m)$

if CheckPolicy$(pk_{sig}^{k}, x_p) = True$, then

$p_{sig}^{u,s}, pk_{sig}^{s,u}, POLICY_{u,s} \leftarrow$ Parse(L[$\mathcal{H}(pk_{sig}^{u,s})$])

$\alpha_{x_p} = \mathcal{H}(pk_{sig}^{u,s} || x_p)$

if rw = 0, then

rw = 0 for write, 1 for read

$h_c = \mathcal{H}(\mathrm{c})$

$L[\alpha_{x_p}] \leftarrow L[\alpha_{x_p}] \cup h_c$

(DHT) $ds[h_c] \leftarrow c$

return h_c

else if $c \in L[\alpha_{x_p}]$, then

(DHT) return $ds[h_c]$

end if

end if

执行结束

在这样一个基于区块链技术设计的用户隐私保护系统中，普惠金融用户可以对自己的个人和企业隐私数据拥有完全的控制权，避免了普惠金融服务商和其他平台滥用数据，同时降低了黑客等外来网络攻击导致数据泄露的可能性。同时，用户可以随时修改隐私信息内容和访问的权限，针对各类普惠金融产品和服务实现实时化独立管理和使用，降低了信息安全风险，保障了普惠金融用户的合法权益。

5 总结

金融隐私与信息安全问题一直是行业和社会关注的焦点。在本文中，我们基于演化博弈模型对普惠金融中的产品与服务提供商和用户之间在隐私信息和数据安全之间的博弈关系进行了深入分析，探索了现实情况下两者之间的均衡策略关系。通过对模型进行稳定性分析和仿真分析我们发现，普惠金融行业的长久健康发展需要政府加大对服务商及平台泄露用户隐私信息的惩罚力度，从而通过增大服务商不保护用户隐私信息所承担的风险而促进隐私保护措施的实施。另一方面，政府应从政策、监管、市场等各个层面鼓励现有普惠金融服务商和行业新兴企业主动为用户提供隐私信息保护服务，从而才能够推动用户对行业整体信任程度的加强，从而进一步增加通过提供隐私信息而获取个性化、深度化服务的意愿，从而推动普惠金融更加繁荣有益发展。在此基础上，我们讨论了一种基于区块链技术的普惠金融用户隐私信息保护方法，进一步从技术层面探索如何避免用户隐私信息泄露事件和风险的发生。

总结来说，针对普惠金融发展过程中所存在用户隐私保护和信息安全问题，需要从三个层面加以改善和解决。首先，需要从国家立法层面来推动数据隐私权的保护，特别是金融信息的隐私权，在全社会加强金融信息安全教育工作，提升市场意识和能力；第二，监管部门要强化监管，加大对于数据安全的保护，改善金融监管与数字普惠金融的发展严重不匹配、不对应的问题，对于滥用乃至泄露用户隐私信息数据的行为要给予严厉的惩罚，对于拥有大量用户数据信息的平台和企业应实行特别监管；第三，应充分发挥区块链、大数据、云计算等新兴技术的作用，通过技术和底层手段降低用户隐私信息泄露的可能性，从而进一步保障普惠金融用户的合法权益，促进普惠金融行业长期健康繁荣发展，真正实现服务于小微，造福于人民。

参考文献

Ji H, Xu H. A Review of Applying Blockchain Technology for Privacy Protection[C]//International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing. Springer, Cham, 2019: 664-674.

Jiang Y, Wang C, Wang Y, et al. A Privacy-Preserving E-Commerce System Based on the Blockchain Technology[C]//2019 IEEE International Workshop on Blockchain Oriented Software Engineering (IWBOSE). IEEE, 2019: 50-55.

Maynard Smith, J. and Price, G. R. (1973). The logic of animal conflict. Nature, 246:15 - 18.

Zyskind G, Nathan O. Decentralizing privacy: Using blockchain to protect personal data[C]//2015 IEEE Security and Privacy Workshops. IEEE, 2015: 180-184.

胡文涛. 推进普惠金融应重视的问题:加强金融隐私权的保护[J]. 兰州学刊, 2018, No.299(08):166-174.

黄永刚. 基于区块链技术的电子健康档案安全建设[J]. 中华医学图书情报杂志, 2016(10): 38-40.

李军伟. 基于演化博弈的社交网络用户隐私行为研究[D]. 北京邮电大学, 2014.

李煜华, 武晓锋, 胡瑶瑛. 基于演化博弈的战略性新兴产业集群协同创新策略研究[J]. 科技进步与对策, 2013, 30(2):70-73.

刘沛佩.论金融生态观下金融隐私权的提出与保护——关于金融消费者权益保护的考察[J],金融与经济,2010 (10).

刘文茜. 互联网金融背景下消费者的隐私权保护[D]. 华东政法大学, 2015.

马运全. 个人金融信息管理:隐私保护与金融交易的权衡[D]. 山东大学, 2014.

乔根·W·威布尔 . 演化博弈论[M]. 上海：上海人民出版社，2007.

权洪森. 网络环境下金融隐私权保护制度研究[J]. 海南金融, 2018, No.354(05):55-63.

沈鑫，裴庆祺，刘雪峰．区块链技术综述[J]．网络与信息安全学报，2016，2(11)：11-20.

谈李荣．金融隐私权与信息披露的冲突与制衡[M]．2004.

王永平，孟卫东．供应链企业合作竞争机制的演化博弈分析[J]．管理工程学报，2004，18(2):96-98.

郑君君，韩笑，邹祖绪,等．IPO 市场中风险投资家策略的演化博弈分析[J]．管理科学学报，2012，15(2):72-82.