

数字货币交易匿名性与监管的博弈分析

张娴, 朱建明, 隋智源, 明盛智

(中央财经大学信息学院, 北京 100081)

摘要: 通过利用区块链等技术, 数字货币作为一种新型货币资产推动了数字经济的发展。数字货币交易平台在数字货币用户对私有数字货币使用中占有重要角色。现有的数字货币交易平台可能存在泄露用户个人隐私的风险, 为不法分子提供参与“空投”事件、勒索、骗局等各种异常交易行为的条件; 数字货币交易平台对用户强匿名性保护也会增加监管部门对于数字货币交易情况的监管难度。因此数字货币交易平台选择对用户的匿名性保护的强弱不仅需要考虑用户的个人隐私安全, 而且要考虑如何符合监管部门对其监管工作的要求。基于对数字货币交易平台和监管部门之间关系的分析, 建立演化博弈模型, 对数字货币交易平台与监管博弈模型进行定义和构建, 根据数字货币交易平台与监管部门收益矩阵求解复制动态方程并得出均衡解。通过构建雅可比矩阵对演化系统在不同参数取值下的均衡点进行稳定性分析, 并分析在不同情况下, 数字货币交易平台与监管部门的演化稳定选择及策略。结合 Matlab 实验环境, 对数字货币交易平台的强弱匿名性保护策略和监管部门的强弱监管策略进行仿真实验, 验证博弈模型的准确性。结合实验结果, 提出对数字货币交易平台的监管建议, 为我国将来开展数字货币交易平台的监管工作提供理论依据。

关键词: 演化博弈; 数字货币交易平台; 隐私保护; 匿名性; 监管

中图分类号: TP393

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2022068

Analysis on anonymity and regulation of digital currency transactions based on game theory

ZHANG Xian, ZHU Jianming, SUI Zhiyuan, MING Shengzhi

School of Information, Central University of Finance and Economics, Beijing 100081, China

Abstract: By using technologies such as blockchain, digital currency, as a new type of monetary asset, has been promoting the development of digital economy. Digital currency trading platform plays an important role in the use of private digital currency by digital currency users. Existing digital currency trading platforms may expose users' privacy and provide illegal elements with the conditions to participate in various abnormal trading behaviors such as "air dropping" events, extortion, fraud, etc. The strong anonymity protection of users by digital currency trading

收稿日期: 2022-03-24; 修回日期: 2022-04-29

通信作者: 张娴, zxian_cufe@163.com

基金项目: 中央财经大学新兴交叉学科建设项目

Foundation Item: Emerging Interdisciplinary Project of CUFU

引用格式: 张娴, 朱建明, 隋智源, 等. 数字货币交易匿名性与监管的博弈分析[J]. 网络与信息安全学报, 2022, 8(5): 150-157.

Citation Format: ZHANG X, ZHU J M, SUI Z Y, et al. Analysis on anonymity and regulation of digital currency transactions based on game theory[J]. Chinese Journal of Network and Information Security, 2022, 8(5): 150-157.

platforms also make it more difficult for regulatory authorities to supervise digital currency transactions. Therefore, the strength of the anonymity protection of users by digital currency trading platforms need to consider not only the privacy protection of users, but also meet the regulatory requirements. For this reason, based on the analysis of the relationship between the digital currency trading platforms and the supervisory departments, an evolutionary game model was established, the digital currency trading platform and the supervisory game model were defined and constructed, and the replication dynamic equation was solved and the balanced solution was obtained according to the income matrix between the digital currency trading platform and the supervisory department. By building a Jacobian matrix, the stability of the evolutionary system under different parameters was analyzed. Besides, the evolutionary stable selection and strategy of the digital currency trading platform and the regulatory authority under different conditions were also analyzed. With Matlab, different strategies of anonymity protection of the digital currency trading platform and different strategies of supervision strategy of the regulatory department were simulated to verify the accuracy of the game model. Based on the results of the simulations, some suggestions on the supervision of digital currency trading platforms are put forward, which provides a theoretical basis for the future supervision of digital currency trading platforms in China.

Keywords: evolutionary game, digital currency trading platform, privacy protection, anonymity, regulatory

0 引言

数字货币具有高效、方便等优点，引起了各国的关注。按照数字货币发行方对于货币的信用程度，现有的数字货币可以被分为法定数字货币与私有数字货币^[1]。本文主要探讨私人数字货币的监管问题。

数字货币交易平台在用户对私有数字货币使用中占有重要角色。各国对于数字货币交易平台的监管力度和法律措施不尽相同，其中美国、英国及一些欧盟国家对于数字货币交易平台的法律监管措施较为完善。美国统一法律委员会制定了统一的法律规定，重点明确了美国联邦及各州监管部门对于数字货币交易平台一系列具体的监管措施，以此规范监管部门监管工作的实施；英国政府则采取“沙盒监管”模式对数字货币交易行为进行监管，来实现数字货币交易与监管的平衡；由于数字货币在欧洲的市场规模较大，欧盟也对数字货币交易平台提出了相应的监管措施，以监管洗钱、逃税等行为^[2]。除此之外，国际货币基金等国际组织纷纷发布有关数字货币交易的监管文件，来降低数字货币交易过程中可能产生的风险。相较于国外，国内对于数字货币交易平台监管问题的研究程度相对薄弱。2017年9月4日，发布了《关于防范代币发行融资风险的公告》发布，金融管理部门等依法关闭了交易网站平台及

移动 App，虚拟币交易平台宣布停止人民币交易业务。虽然目前我国没有数字货币交易平台，但研究数字货币交易平台与监管之间的問題对我国将来开展数字货币的交易与监管仍具有重要意义。

一些平台在发展初期会通过强保护用户匿名性来保证用户个人隐私^[3]，以此吸引用户，同时降低成本。但是，对于监管部门来说，数字货币交易平台对用户的匿名性保护越强，交易可追踪性就越弱，监管难度就越大，即所需要耗费的人力物力越多。交易平台对于用户匿名性保护的强弱和监管部门对于交易监管的力度可以被抽象为两个参与方的博弈行为。

演化博弈作为一种成熟的博弈模型，可以被运用到多种场景的博弈问题中^[4]。数字货币交易平台若选择对用户匿名性强保护，就可以吸引更多的用户，但监管部门就不易对平台的数字货币交易进行监管，难以监测和追踪一些非法的数字货币异常交易行为，使部分用户资产造成损失，影响社会稳定性和公平性；数字货币交易平台若选择对用户匿名性弱保护，用户就可能面临个人隐私泄露的风险，对平台发展不利，但监管部门对其监管难度降低，所需要耗费的人力物力减少，更有利于数字货币交易市场整体长期稳定发展。针对数字货币交易过程中可能出现的风险和问题，本文基于数字货币交易平台和监管部门关系

的分析,建立演化博弈模型,对系统均衡点进行稳定性分析,通过仿真实验验证博弈模型的准确性,并对数字货币交易平台的监管问题提出建议。

1 数字货币交易平台与监管演化博弈模型

在一般情况下,数字货币交易平台和监管部门在进行选择时,都会选择对自身收益大的策略。数字货币交易平台对用户强匿名性保护可以在打着“方便用户交易”和“保护用户个人隐私”的口号吸引用户注资的同时降低自己的成本;而对用户弱匿名性保护需要用户在进行交易前向平台提交并通过平台认证其身份信息,平台会保留用户相关交易记录,并可以在监管部门执行监管工作时提供相关用户身份和交易信息进行查询和追踪。监管部门对于平台的不同监管程度会影响平台的选择,对于监管部门来说,数字货币交易平台的不同选择会影响监管部门对于监管力度的选择^[5]。如果数字货币交易平台为了降低成本选择强保护匿名策略,那么监管部门的监管难度就会加大,监管成本就会增加,需要选择强监管策略来保证交易平台合法运行;当平台较少考虑保护用户隐私选择弱保护匿名性策略时,监管部门能够更方便、及时地追踪到洗钱、勒索等一些非法的异常交易行为,但用户面临个人隐私泄露等风险的概率就会增加,也难以防范一些数字货币平台利用用户信息非法盈利。

下面通过建立用户匿名性保护与监管的演化博弈模型,对参与双方数字货币交易平台和监管部门的博弈进行探讨,首先对博弈问题相关概念进行定义,之后得出博弈模型。

1.1 博弈模型定义

定义 1 定义匿名性保护与监管演化博弈模型 (APSEGN, anonymity protect-supervise evolutionary game model) 是一个 4 元组, $APSEGM = (A, C, P, F)$ 。

定义 2 $A = (A_u, A_s)$, A 为此博弈模型的主体集合,其中 A_u 为数字货币交易平台主体, A_s 为监管部门主体。

定义 3 $C = (C_u, C_s)$, C 为此博弈模型的主体的策略集合,其中 C_u 为数字货币交易平台主体的策略集合, C_s 为监管部门主体的策略集合。

定义 4 $P = (p, q)$, P 为此博弈模型的混合策略概率集合,其中 p 为匿名性策略的概率参数, q 为监管部门选取监管策略的概率参数。

定义 5 $F = (m, n)$, F 为此博弈模型的收益函数集合,代表参与博弈的各参与方在此博弈中的收益, m 为数字货币交易平台收益, n 为监管部门收益。

定义 6 通过分析数字货币交易平台对用户的匿名性保护和监管部门监管的博弈过程,假设数字货币交易平台主体可选择的策略集 $C_u = \{\text{强匿名性保护策略 } U1, \text{弱匿名性保护策略 } U2\}$;监管部门主体可选择的策略集 $C_s = \{\text{强监管策略 } S1, \text{弱监管策略 } S2\}$ 。

定义 7 参与主体的收益参数定义: D 表示数字货币交易平台通过用户进行的数字货币交易所能获得的固定收益; R 表示数字货币交易平台选择强匿名性保护策略 $U1$ 时,监管部门选择强监管策略 $S1$ 时获得的监管收益; T 表示数字货币交易平台选择弱保护策略 $U2$ 时,监管部门选择 $S1$ 时获得的监管收益; J 表示数字货币交易平台选择强匿名性保护策略 $U1$ 时,监管部门选择弱监管策略 $S2$ 时获得的监管收益; K 表示数字货币交易平台选择弱匿名性保护策略 $U2$ 时,监管部门选择 $S2$ 时获得的监管收益。

定义 8 参与主体的成本参数定义: $v1$ 表示数字货币交易平台在选择强匿名性保护策略 $U1$ 时所需要承担的成本,特指平台需要承担的平台内出现非法交易后被政府处罚的风险成本, $v2$ 表示数字货币交易平台在选择弱匿名性保护策略 $U2$ 时所需要承担的成本,包括用户身份识别和交易信息进行查询和追踪等技术成本,假设 $v1 < v2$; $w1$ 表示监管部门选择 $S1$ 时所需要的监管成本, $w2$ 表示监管部门选择 $S2$ 时所需要的监管成本,且 $w1 > w2$ 。

1.2 博弈模型构建

根据上述的模型定义可以得出博弈模型收益矩阵与其改进矩阵,进而得出不同个体在选择不同策略时的收益函数,确定复制动态方程,并求出均衡点。在演化博弈模型中,复制动态方程的基本形式为 $\frac{dx(t)}{dt} = [f(s_i, x) - f(x, x)]x_i$, 其中, s_i 表示演化群体内博弈的策略集, x_i 表示在某一

刻 t 下博弈群体中有多少比例的个体选择了策略 s_i , $f(s_i, x)$ 表示当博弈个体选择 s_i 时, 个体的期望收益, $f(x, x)$ 表示整个群体的平均期望收益。

数字货币交易平台与监管部门收益矩阵如表 1 所示。

表 1 数字货币交易平台与监管部门收益矩阵
Table 1 Revenue matrix of digital currency trading institutions and regulatory authorities

主体策略	强监管策略 S_1	弱监管策略 S_2
强匿名性保护策略 U_1	$D-v_1-R, R-w_1$	$D-v_1-J, J-w_2$
弱匿名性保护策略 U_2	$D-v_2-T, T-w_1$	$D-v_2-K, K-w_2$

将上述收益矩阵公式进行整理以方便做下一步分析。令 $X = D - v_1 - J$, $g_1 = R - J > 0$; $Y = D - v_2 - K$, $g_2 = T - K > 0$; $Z = T - w_1$, $h_1 = T - R > 0$; $O = K - w_2$, $h_2 = K - J > 0$ 。

由上述简化公式可以得到

$$\begin{aligned} g_1 - g_2 &= R - J - T + K = \\ K - J - T + R &= h_2 - h_1 \end{aligned} \quad (1)$$

令 $g_1 - g_2 = R - J - T + K = h_2 - h_1 = \mu$, 数字货币交易平台与监管部门收益改进矩阵如表 2 所示。

表 2 数字货币交易平台与监管部门收益改进矩阵
Table 2 Revenue improvement matrix of digital currency trading institutions and regulatory authorities

主体策略	强监管策略 S_1	弱监管策略 S_2
强匿名性保护策略 U_1	$X-g_1, Z-h_1$	$X, O-m_2$
弱匿名性保护策略 U_2	$Y-g_2, Z$	Y, O

根据数字货币交易平台与监管部门收益改进矩阵可以得出数字货币交易平台和监管部门两方参与者在选择不同策略时的收益函数 L_1 、 L_2 和 L_3 、 L_4 以及平均收益函数 E_u 和 E_s 。

L_1 为数字货币交易平台选择强匿名性策略时的收益函数, L_2 为数字货币交易平台选择弱匿名性策略时的收益函数, E_u 为数字货币交易平台的平均收益函数。

$$L_1 = q(X - g_1) + (1 - q)X = X - qg_1 \quad (2)$$

$$L_2 = q(Y - g_2) + (1 - q)Y = Y - qg_2 \quad (3)$$

$$E_u = pL_1 + (1 - p)L_2 \quad (4)$$

L_3 为监管部门选择强监管策略时的收益函

数, L_4 为监管部门选择弱监管策略时的收益函数, E_s 为监管部门的平均收益函数。

$$L_3 = p(Z - h_1) + (1 - p)Z = Z - ph_1 \quad (5)$$

$$L_4 = p(O - m_2) + (1 - p)O = O - pm_2 \quad (6)$$

$$E_s = qL_3 + (1 - q)L_4 \quad (7)$$

数字货币交易平台的强匿名性保护策略和监管部门的强监管策略的复制动态方程^[6]为

$$F_1(p, q) = U(p) = \frac{dp(t)}{dt} = \quad (8)$$

$$p(L_1 - E_u) = p(1 - p)(X - Y - \mu q)$$

$$F_2(p, q) = S(q) = \frac{dq(t)}{dt} = \quad (9)$$

$$q(L_3 - E_s) = q(1 - q)(Z - O + \mu p)$$

联立式(8)、式(9), 并令式(8)、式(9)分别等于 0。

$$\begin{cases} F_1(p, q) = p(1 - p)(X - Y - \mu q) = 0 \\ F_2(p, q) = q(1 - q)(Z - O + \mu p) = 0 \end{cases} \quad (10)$$

可求出此复制动态方程组的均衡解为

$$\left\{ \begin{aligned} e_1 &= (0, 0) \\ e_2 &= (0, 1) \\ e_3 &= (1, 0) \\ e_4 &= (1, 1) \\ e_5 &= \left(\frac{O - Z}{\mu}, \frac{X - Y}{\mu} \right) \end{aligned} \right. \quad (11)$$

经过分析可知, e_1, e_2, e_3, e_4 为鞍点, e_5 为中心点。同时, 在上述假设中, $g_1 - g_2 = h_2 - h_1 = \mu$, 即收益指标 $O - Z$ 、 $X - Y$ 在此演化博弈中对数字货币交易平台与监管部门博弈的稳定有较大的影响。

2 演化均衡稳定性分析

Friedman 提出由微分方程描述的群体动态演化系统中均衡点的稳定性可以用复制动态方程构建雅克比矩阵分析判断, 即通过构建雅可比矩阵对上述分析得出的 5 个均衡点进行稳定性分析^[7]。

根据复制动态方程组(10)构建雅克比矩阵为

$$J = \begin{pmatrix} \frac{\partial F_1(p, q)}{\partial p} & \frac{\partial F_1(p, q)}{\partial q} \\ \frac{\partial F_2(p, q)}{\partial p} & \frac{\partial F_2(p, q)}{\partial q} \end{pmatrix} \quad (12)$$

$$\begin{bmatrix} (1-2p)[X-Y-\mu q] & -p(1-p)\mu \\ q(1-q)\mu & (1-2q)[Z-O+\mu p] \end{bmatrix}$$

计算矩阵(12)的行列式(13)和迹(14)。

$$\det J = (1-2p)(1-2q)[X-Y-\mu q] \cdot [Z-O+\mu p] + pq(1-p)(1-q)\mu^2 \quad (13)$$

$$\text{tr} J = (1-2p)[X-Y-\mu q] + (1-2q)[Z-O+\mu p] \quad (14)$$

将所有得出的均衡解代入式(13)、式(14)，分别计算其对应的 J 的行列式符号和 J 的迹符号，如表 3 所示。

表 3 不同均衡点对应的 $\det J$ 和 $\text{tr} J$
Table 3 $\det J$ and $\text{tr} J$ corresponding to different equilibrium points

均衡点	$\det J$	$\text{tr} J$
$e_1=(0, 0)$	$(X-Y)(Z-O)$	$X-Y+Z-O$
$e_2=(0, 1)$	$(O-Z)(X-Y-\mu)$	$O-Z+X-Y-\mu$
$e_3=(1, 0)$	$(Y-X)(Z-O+\mu)$	$Y-X+Z-O+\mu$
$e_4=(1, 1)$	$(X-Y-\mu)(Z-O+\mu)$	$X-Y-Z+O$
$e_5=\frac{O-Z}{\mu}, \frac{X-Y}{\mu}$	$(1-p)(1-q)(O-Z)(Y-X)$	0

通过表 3 可以看出，此博弈矩阵中 $O-Z$ 和 $X-Y$ 取值会影响其对应雅克比矩阵的 J 的行列式符号和 J 的迹符号的正负，均衡点的类型判断如表 4 所示。

表 4 均衡点类别判断
Table 4 Classification judgment of equilibrium points

均衡点	J 的行列式符号	J 的迹符号	局部稳定性
e_1	-	不确定	鞍点
e_2	+	+	不稳定点
e_3	+	-	稳定点
e_4	+	0	中心点
e_5	0	+	不稳定点

由于 μ 取值的不确定性，分别对 μ 是否等于 0 的情况进行分类分析。

当 μ 等于 0 时， $g_1=g_2$ ， $h_1=h_2$ ，复制动态方程组(10)包括 4 个均衡解，分别为 e_1 、 e_2 、 e_3 和 e_4 。把 4 个均衡解代入其对应的 $\det J$ 和 $\text{tr} J$ ，并通过判断均衡点类别，得出数字货币交易平台与监管部门系统在 4 种情况（ $X>Y, Z>O$ ； $X>Y, Z<O$ ； $X<Y, Z>O$ ； $X<Y, Z<O$ ）时，对应的均衡稳定点为 $e(1,1)$ ， $e(1,0)$ ， $e(0,1)$ ， $e(0,0)$ 。

当 μ 不等于 0 时，复制动态方程组(10)包括 5 个均衡解 e_1 ， e_2 ， e_3 ， e_4 以及 $e_5=(\frac{O-Z}{\mu}, \frac{X-Y}{\mu})$ 。根据演化博弈稳定策略，下面分别针对 e_5 不同的取值，对得出的结果进行分析。

对于 $F_1(p, q)$ ，若 $q = \frac{X-Y}{\mu}$ ，不论数字货币

交易平台的匿名性保护策略 p 为任何值，均存在 $\frac{dp(t)}{dt} = 0$ ，说明不论数字货币交易平台的匿名性

保护策略 p 为任何值，方程都一直是在稳定状态；

若 $q \neq \frac{X-Y}{\mu}$ ， $\frac{dp(t)}{dt} = 0$ 且 $\frac{d^2 p(t)}{dt^2} < 0$ 时， p 是演化稳定选择，其稳定状态有两种情况，分别为 $p=0$ 和 $p=1$ 。由此可知，若 $q < \frac{X-Y}{\mu}$ ， $p=0$ 是

数字货币交易平台参与者的演化稳定选择，则数字货币交易平台要考虑选择匿名性弱保护；若 $q > \frac{X-Y}{\mu}$ ， $p=1$ 是数字货币交易平台参与者的演

化稳定选择，则此时数字货币交易平台要考虑选择匿名性强保护。

同理，对于 $F_2(p, q)$ ，若 $p = \frac{O-Z}{\mu}$ ，不论监

管部门的监管策略 q 为任何值，均存在 $\frac{dq(t)}{dt} = 0$ ，

说明不论数字货币交易平台的匿名性保护策略 p 为任何值，方程都一直是处于稳定状态；若 $p < \frac{O-Z}{\mu}$ ，则监管部门要考虑选择弱监管策略；

若 $p > \frac{O-Z}{\mu}$ ，则监管部门要考虑选择强监管策略。

3 实验分析与建议

本文使用 Matlab R2016a 作为实验环境对博

弈模型进行实验验证。实验设 $\mu=10$ ，选取不同数值的 $X-Y$ 、 $O-Z$ 验证博弈模型，对数字货币交易平台的强弱匿名性保护策略和监管部门的强弱监管策略进行仿真。图1为数字货币交易平台复制动态方程变化曲线。

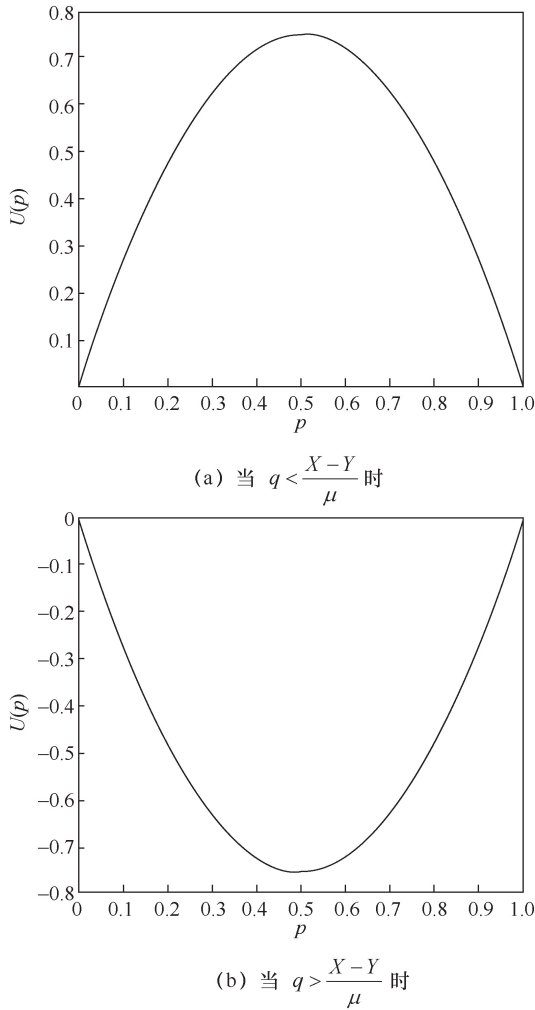


图1 数字货币交易平台复制动态方程变化
Figure 1 Digital currency trading institutions replicate dynamic equation changes

在图1(a)中，为了满足条件 $q < \frac{X-Y}{\mu}$ ，选取 $Y-X=8$ ， $q=0.5$ ，可以看出在 $0 < p < 1$ 时， $U(p) > 0$ ，且当 p 的值为0和1时系统状态稳定。在图1(b)中，为了满足条件 $q > \frac{X-Y}{\mu}$ ，选取 $Y-X=2$ ， $q=0.5$ ，可以看出 $0 < p < 1$ 时， $U(p) < 0$ ，同样，当 p 的值为0和1时，系统状态稳定。由此表明 $X-Y$ 的取值对数字货币交

易平台用户匿名性保护策略的选择有较大影响，同时，与数字货币交易平台选取对用户匿名性的强保护策略 U_1 时监管部门的收益 J 、 K 相关。

图2为监管部门复制动态方程变化曲线。

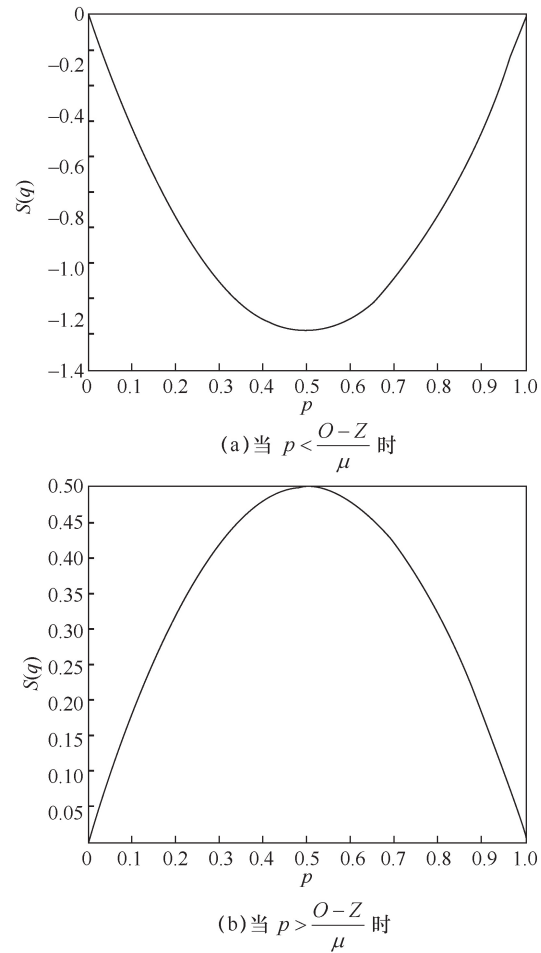


图2 监管部门复制动态方程变化
Figure 2 Regulators replicate dynamic equation changes

在图2(a)中，为了满足条件 $p < \frac{O-Z}{\mu}$ ，选取 $O-Z=10$ ， $p=0.5$ ，可以看出在 $0 < q < 1$ 时， $S(q) < 0$ ，且当 q 的值为0和1时系统状态稳定。在图2(b)中，为了满足条件 $p > \frac{O-Z}{\mu}$ ，选取 $O-Z=3$ ， $p=0.5$ ，可以看出 $0 < q < 1$ 时， $S(q) > 0$ ，同样，当 q 的值为0和1时，系统状态稳定。由此表明 $O-Z$ 的取值对监管部门监管力度策略的选择有较大影响，同时，与数字货币交易平台选取弱监管策略 U_2 时监管部门的收益

K 、 T 相关。

上述结果验证了匿名性保护与监管演化博弈模型的正确性,可以在现实环境中为我国将来开展数字货币交易与监管部门执行监管工作提供以下建议。

1) 完善对数字货币交易平台的监管制度。在涉及数字货币交易平台对用户的匿名性保护时,应该遵循在保证用户个人隐私的基础上实现部分匿名性,方便监管工作的执行,同时严格规范数字货币交易平台对用户个人隐私数据的内容和使用方式,避免平台利用用户数据非法获利。

2) 降低监管部门对数字货币交易平台的监管成本。由于数字货币相关法律法规和政策制度在不断改变和完善中,监管工作对于数字货币交易平台尤为重要。监管部门的监管工作需要耗费人力物力等成本,成本过高会导致部门在执行监管任务时着重考虑成本与收益的关系,从而降低监管积极性^[8],影响监管工作带来的社会效益。

3) 建立对数字货币交易平台的激励政策和处罚措施。对于能够在保护用户信息不被泄露的基础上配合监管部门完成监管工作的数字货币交易平台,政府应适当给予资金或政策支持等激励行为;对于自身操作不当导致用户个人隐私泄露以及发生恶意用户利用平台进行非法交易行为情况的平台,政府应当采取相应的处罚措施。激励政策和处罚措施的完善不仅能够帮助数字货币交易平台正向发展,也能帮助监管部门提高监管效率,缓解监管压力。

4 结束语

数字货币交易平台在数字货币的发展过程中扮演着重要角色。针对用户通过平台进行数字货币交易的过程中出现的个人隐私泄露风险、恶意用户通过平台进行非法交易行为,以及监管部门对用户匿名性保护强的平台监管困难等问题,本文利用演化博弈基本理论,对参与博弈的双方关系进行分析并建立了一个演化博弈模型,之后通过雅可比矩阵的局部稳定性分析法对系统均衡点进行稳定性分析,使用 Matlab 软件实验验证博弈

模型的准确性并对数字货币交易平台的监管问题提出建议。

在本文研究的博弈模型中,直接设定了强弱策略下所付出成本的多少,对两方博弈的收益影响考虑较少,在后续的研究中会进一步完善博弈模型,使其更加符合真实场景中数字货币交易平台运行和监管的过程。

参考文献:

- [1] 付烁,徐海霞,李佩丽,等.数字货币的匿名性研究[J].计算机学报,2018,42(5):1045-1062.
FU S, XU H X, LI P L, et al. A survey on anonymity of digital currency[J]. Chinese Journal of Computers, 2018, 42(5): 1045-1062.
- [2] 曾宪力.私人数字货币的法律属性及监管研究[D].上海:华东政法大学,2021.
ZENG X L. Research on legal attribute and supervision of private digital currency[D]. Shanghai: East China University of Political Science and Law, 2021.
- [3] 沈蒙,桑安琪,祝烈煌,等.基于动机分析的区块链数字货币异常交易行为识别方法[J].计算机学报,2021,44(1):193-208.
SHEN M, SANG A Q, ZHU L H, et al. Abnormal transaction behavior recognition based on motivation analysis in blockchain digital currency[J]. Chinese Journal of Computers, 2021, 44(1): 193-208.
- [4] 胡俏,齐佳音.基于SD演化博弈模型的数字货币扩散演化仿真研究[J].系统工程理论与实践,2021,41(5):1211-1228.
HU Q, QI J Y. Cryptocurrency diffusion evolution simulation based on SD evolution game model[J]. Systems Engineering-Theory & Practice, 2021, 41(5): 1211-1228.
- [5] 郭阳楠,蒋文保,叶帅.可监管的区块链匿名交易系统模型[J].计算机应用,2022,42(9):2757-2764.
GUO Y N, JIANG W B, YE S. Supervisable blockchain anonymous transaction system model [J]. Journal of Computer Applications, 2022, 42(9): 2757-2764.
- [6] 张前程,王明成.农村金融监管的演化博弈模型分析[J].安徽工业大学学报(社会科学版),2010,27(5):3-5.
ZHANG Q C, WANG M C. Evolutionary game analysis of rural financial supervision[J]. Journal of Anhui University of Technology (Social Sciences), 2010, 27(5):3-5.
- [7] 刘荣,王凤兰,王非.基于演化博弈模型的网络攻防策略[J].科学技术与工程,2020,20(21):8671-8675.
LIU R, WANG F L, WANG F. Network attack and defense strategy based on evolutionary game model[J]. Science Technology and Engineering, 2020, 20(21): 8671-8675.
- [8] 丁佳.第三方支付机构洗钱风险的评估与监管问题研究[D].南京:南京师范大学,2019.
DING J. Third-party payment institution money laundering risk assessment and regulatory issues research[D]. Nanjing: Nanjing Normal University, 2019.

[作者简介]



张娴（1998- ），女，河南开封人，中央财经大学硕士生，主要研究方向为区块链安全、隐私保护、数字货币。



隋智源（1984- ），男，山东诸城人，中央财经大学讲师，主要研究方向为应用密码学、信息安全、隐私保护。



朱建明（1965- ），男，山西太原人，中央财经大学教授、博士生导师，主要研究方向为信息安全、区块链技术、隐私保护。



明盛智（1999- ），男，广西桂林人，中央财经大学硕士生，主要研究方向为区块链技术、隐私保护、隐私计算。