An Evolutionary Game-Theoretic Trust Study of a Blockchain-Based Personal Health Data Sharing Framework

Raifa Akkaoui, Xiaojun Hei, Wenqing Cheng
School of Electronic Information and Communications
Huazhong University of Science and Technology
Wuhan, China, 430074
e-mail: {raifa_akkaoui, heixj, chengwq}@hust.edu.cn

***Abstract*—During the past few years, medical Internet-of-Things devices have experienced a massive growth and they are currently generating tremendous volumes of data every day, which are highly valuable as they can be of great importance to all stakeholders within the healthcare industry. In this context, many blockchain-based solutions have been proposed to mitigate the siloed burden in different healthcare systems which prevented achieving a patient-centric, transparent, and secure data sharing. However, when multiple independent entities try to share their data, trust is not necessarily guaranteed. The scope of this paper is to explore the impact of verification on the level of trust among the different entities of the health data-trading system by proposing an evolutionary game theoretic model. We also present the numerical analysis of the evolution of trust in terms of different game parameters adopted to evaluate their impact on eliminating malicious (i.e., untrustworthy) players from the system.**

Keywords-Blockchain, data sharing; evolutionary game theory; healthcare; internet of things; privacy; security; trust

I. INTRODUCTION

The medical Internet-of-Things (MIoT) has recently emerged as a new wave of IoT technologies with the main goal of supporting the e-healthcare industry by enabling a closer and efficient medical care and diagnosis to a larger population, precisely, for patients with chronic diseases requiring long-term and day-to-day monitoring [1]. MIoT has proven its great potentiality in improving the overall care and delivery of healthcare services, however, one of the major challenges faced by these systems is their lack of open and cooperative data sharing. Even though there exist a tremendous amount of medical sensor devices deployed everywhere, they often only communicate with a centralized cloud-based server and are bound to a single organization. Moreover, health service providers are susceptible to share, without consent, patients' personal health data (PHD) with other second care providers, big data analytics companies, or cloud service providers [2].

In point of fact, the security and privacy of patients' health data are two crucial aspects that need to be taken into account while managing these data [3]. In this context, several blockchain-based approaches have been designed to meet these requirements, blockchain as a new emerging technology, is seen as the appropriate solution for tackling the challenges of sharing health data [4], [5]. However, sharing PHD through a blockchain-based framework does not always guarantee the credibility of these data, precisely if participants are more incentivized to behave opportunistically, which motivates us to study trust within a blockchain-based PHD-sharing framework from an evolutionary game theoretic perspective.

In this paper, we first propose the design of our blockchain-based health data trading framework, we then use evolutionary game theory (EGT) to define a data-trading trust model. EGT has been used widely to study cooperative dilemma such as knowledge-sharing in supply chain and blockchain mining [6], [7]. However, there exists few research that has been on modeling trust [8], [9], not to mention that studying trust within a blockchain-based PHD-trading framework was seldom investigated. In our proposed trust model, players can be either data generators (i.e., patients) or data requestors (e.g., research institutions, pharmaceutical companies, insurance companies, etc.). Each generator or requestor has the choice to be either trustworthy or untrustworthy, leading to a game with four different strategy profiles: trustworthy patient (TP), untrustworthy patient (UP), trustworthy requestor (TR), and untrustworthy requestor (UR). The main contributions of this paper are summarized as the following:

1) We introduce the design of a secure blockchain-based PHD-trading system for patients and health institutions.

2) We propose a trust model consisting of four types of players and examine the development of trust in the so-called health sharing market from an EGT perspective.

The rest of this paper is organized as follows. The related work is discussed in Section II. In Section III, we introduce the components of the proposed blockchain-based PHD-trading framework. In Section IV, the proposed game model is formulated with a theoretical and numerical analysis on

978-1-7281-6776-3/20/$31.00 ©2020 IEEE

the evolution of trust. We then conclude this paper in Section V.

II. Related Work

The traditional centralized approach for managing health data relying on the cloud computing paradigm has been used for nearly a decade. For instance, Thilakanathan et al. [10] presented a cloud-based platform which enables the monitoring of patients by doctors through a secure sharing of health data. In addition, the work in [11] utilized the cloud computing paradigm for the collection, processing and storage of health data, the proposed platform is assumed to be fully trusted by all participants. However, this traditional centralized approach for managing data suffers from some limitations including its security vulnerabilities, such as hijacking and distributed denial of service attacks, as well as data breaches.

Meanwhile, blockchain has attracted the attention of many researchers, precisely to decentralize the process of data management in a health data sharing context. Fore instance, to deal with the heterogeneity of health data, Kaur et al. [4] combined blockchain and the cloud paradigm to ensure a secure process of sharing health data without any third parties. Furthermore, in [5] the authors proposed the design of a role-based access control smart contract to manage the access to the medical records in a decentralized, transparent, and auditable manner. Nevertheless, practical and trustworthy data trading models to build a healthcare data trading market for patients and researchers are seldom investigated.

III. Blockchain-based Personal Health Data-Trading System

With the volume of data generated from MIoT and body sensors explosively increasing, it is quasi-impossible to rely on cloud approaches for a secure storage and management of all these data. In this regard, our proposed PHD-trading system includes multiple local consortium blockchain platforms distributed geographically and near the source of data, Fig. 1 illustrates the system we propose which is composed of the entities explained in the following subsections.

A. Patients

Patients in our proposed framework are individuals who are willing to be part of the platform by contributing with their own PHD generated from MIoT devices or body sensors. For instance, if we take the scenario of a patient monitoring his health in a smart home, this one is expected to generate a huge amount of data (e.g., blood sugar level, temperature, heart rate, weight, activity, etc.) that can be leveraged in precision medicine to provide better health services. In order to motivate patients, these ones can get some rewards in the form of health tokens in case they accomplished any improvement in terms of their health.

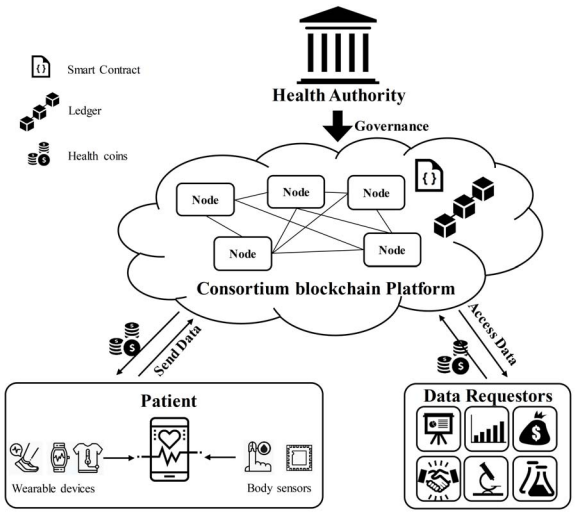


Figure 1. Blockchain-based health data trading system.

Thus, in the proposed PHD-trading system, patients play the role of data generators and they have the right to either share their data or not while taking into account the risk it might indulge (i.e., privacy concerns, untrustworthy requestors) and rewards.

B. Data Requestors

With the new emerging era of the big healthcare data, pooling the shared PHD has a tremendous potentiality for the improvement of patients' well-being, anticipate epidemics outbreaks, acquire new insights, prevent diseases, reduce the cost of health services, and ameliorate the conditions of life as a whole. For instance, if we take the scenario of a pharmaceutical company trying to improve its products, it can track the overall performance of a patient undergoing a certain treatment and see if there were any side effects and measure the effectiveness of the treatment based on analyzing the PHD generated by the patient using his MIoT devices. Requestors are also responsible for rewarding patients in order to encourage them to share more their data, by considering PHD as the patients' assets constituting a sustainable and dynamic health data market.

C. Sealers

In our blockchain-based trading system, sealers work as mining nodes to process the shared data, manage trading-related activities, access control policies, provide closer computing and artificial intelligence services. They are managed by health authorities and use the proof-of-authority consensus mechanism, which does not require any mining but instead is based on authorized peers, hence, supporting a high-speed communication between participants with no computational overhead.

IV. Evolutionary Trust Study of the Data-Trading System

The notion of trust is tremendously important as it is the fundamental base of our social and human interactions, ethics, culture and relationships, precisely when considering managerial and trading decision-making [12]. The widely known version of trust games revolves around the interaction of a trustor and a trustee. Fundamentally, the game represents a two-player game where the trustor (i.e., patient) would generate his data to share it with the requestor. Later, the trustee (i.e., data requestor) must analyze the data and reward the patient based on his progress.

TABLE I. Notations.

Symbol	Definition
$R_{p,r}$	Reward from being trustworthy for patient or requestor
$C_{p,r}$	Payoff from cheating for patient or requestor
$L_{p,r}$	Expected loss to patient or requestor
$P_{p,r}$	Penalty for untrustworthy patient or requestor
$f_{p,r}$	Frequency of verification for patient or requestor
$V_{p,r}$	Cost of verification for patient or requestor

A. Problem Formulation and Assumptions

In our proposed health data-trading blockchain-based framework, patients and requestors are gaming with each other most of the time. Precisely, patients are sharing their monitored health signs in order to get some rewards from the different data requestors part of the trading scheme, both patients and requestors can decide to be either trustworthy or untrustworthy. Obviously, trust within information sharing is a continuous process impacted by the environment, social norms, policies, and intercourses between patients and data requestors, making trust an evolutionary process. Hence, analyzing the factors influencing the spread of trust within this PHD-trading population can be achieved after the construction of the EGT model which is based on the assumptions defined below:

1) Players: In our proposed model, we consider the case of two agents gaming with each other, which are a patient and a data requestor. The players are self-interested, with symmetric information of each others' strategy choices and decide following a sequential order.

2) Space of strategies: Agents can pick from a strategy space of [T, U], where T refers to being trustworthy and U means the opposite.

3) Verification: In order to enforce trustworthiness we assume there is a way to verify the credibility of each agent, but this comes with a cost of verification $V_{p,r}$. Also, the players don't verify continuously at each round the behavior of the other party but they do so based on a frequency that we note as f_p and f_r. Since the proposed system is blockchain-based and the state updates are stored on the immutable data structure, this provides an avenue for implementing the verification mechanism.

4) Parameters: The rest of notations and parameters used in our model are detailed in Table I.

Based on the previous assumptions made and parameters defined above, we can deduce that there exist four strategy profiles that the players can choose: [T, T], [T, U], [U, T], [U, U] and the utility matrix of the game is detailed in Table.II.

TABLE II. Payoff matrix.

GS	TR	UR
TP	$R_p - f_p V_p$, $R_r - f_r V_r$	$-(1-f_p)L_P - f_p V_p$, $(1-f_p)C_r - f_p P_r - f_r V_r$
UP	$(1-f_r)C_p - f_r P_p - f_p V_p$, $-(1-f_r)L_r - f_r V_r$	$(1-f_r)C_p - f_r P_p - (1-f_p)L_p - f_p V_p$, $(1-f_p)C_r - f_p P_r - (1-f_r)L_r - f_r V_r$

Based on Table.II, by setting the rate of trustworthy requestors and trustworthy patients as $x(t) = x$ and $y(t) = y$ respectively, with $x, y \in [0, 1]$, we get the utility of a patient with a strategy (T) as:

$$U_P(T) = x[R_p - f_p V_p] + (1-x)[-(1-f_p)L_P - f_p V_p] \quad (1)$$

And the utility of a patient with a strategy (U) as:

$$\begin{aligned} U_P(U) &= x[(1-f_r)C_p - f_r P_p - f_p V_p] \\ &+ (1-x)[(1-f_r)C_p - f_r P_p - (1-f_p)L_p - f_p V_p] \end{aligned} \quad (2)$$

With (1) and (2), we can get the expected utility function of a patient as:

$$\begin{aligned} U_P = xyR_p + (1-y)[(1-f_r)C_p - f_r P_p] \\ - (1-x)(1-f_p)L_p - f_p V_p \end{aligned} \quad (3)$$

Similarly, the utility functions of a requestor with a trustworthy/untrustworthy strategies and the expected utility are also obtained.

B. Evolutionary Equilibrium Analysis

Following the Malthusian dynamic equation [13], the growth rate of a player's (i.e., patient or requestor) trustworthiness is directly proportional to the difference between the utility of a trustworthy strategy and the expected utility. Hence, from (1) and (3), the RDE of a patient (noted later as RDE_P) is expressed as:

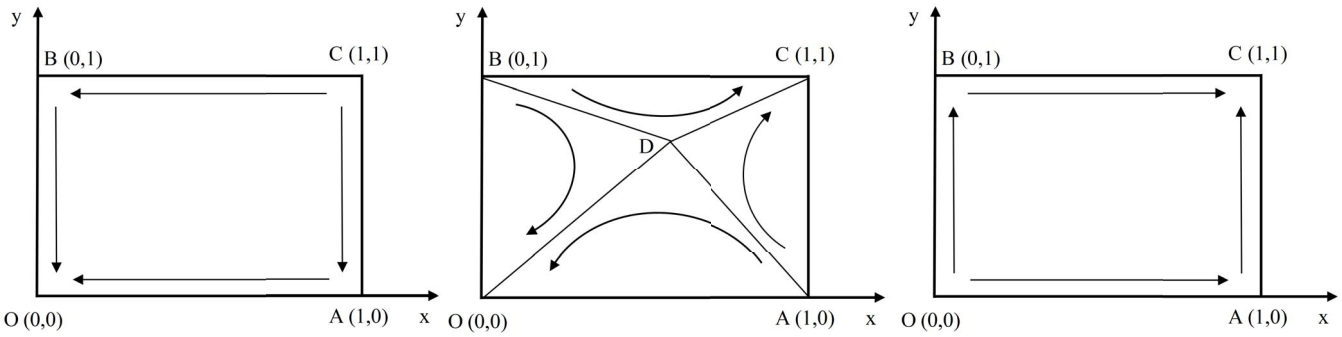
$$\frac{dy}{dt} = y(U_P(T) - U_P) = y(1-y)[xR_p - (1-f_r)C_p + f_r P_p] \quad (4)$$

Similarly, the RDE of a requestor (noted later as RDE_R) is obtained. Thus, the optimal strategy choices of the players are as follows:

$$x = 0, x = 1, y = y^* = \frac{(1-f_p)C_r - f_p P_r}{R_r} \quad (5)$$

$$y = 0, y = 1, x = x^* = \frac{(1-f_r)C_p - f_r P_p}{R_p} \quad (6)$$

Hence, the local equilibrium points that exist are (0, 0), (0, 1), (1, 0), (1, 1), and (x^*, y^*). In order to analyze whether



(a) Case I. (b) Case II. (c) Case III.

Figure 2. Evolution path diagrams

a point is stable the Jacobian matrix [14] can be utilized, which is defined as follows:

$$M_{jac} = \begin{pmatrix} \frac{\partial RDE_R(x)}{\partial x} & \frac{\partial RDE_R(x)}{\partial y} \\ \frac{\partial RDE_P(y)}{\partial x} & \frac{\partial RDE_P(y)}{\partial y} \end{pmatrix}$$

Based on the stability theorem, if the following conditions $Tr(M_{jac}) < 0$ as well as $Det(M_{jac}) > 0$ are met, the stability of the studied local equilibrium point can be concluded, with Tr being the trace of the matrix M_{jac} and Det the determinant.

For ease and without loss of generality, we assume that $R_p = R_r = R$ and so it goes for the rest of the parameters. Hence, from (5) and (6), if $R < (1-f)C - fP$, then $x^* > 1$ and $y^* > 1$. Which is inconsistent with our assumption. Hence, the only equilibrium points that exist are (0, 0), (0, 1), (1, 0), and (1, 1).

Case I: if $fP < (1-f)C$ meaning that the penalty from being untrustworthy is lower than the payoff from cheating, the stability of the system equilibrium points is analyzed in Table. III and the dynamic phase of evolution between patients and requestors is shown in Fig. 2a. The results show that regardless of the primary strategy profile choices made by the players, the point (0, 0) is an evolutionary stable strategy (ESS) meaning that the game will evolve to both parties choosing the non-cooperative strategy U.

TABLE III. Equilibrium points stability (Case I).

Equilibrium point	$Tr(M_{jac})$	$Det(M_{jac})$	Local stability
(0, 0)	-	+	ESS
(0, 1)	+	-	Unstable
(1, 0)	+	-	Unstable
(1, 1)	+	+	Unstable

If $R > (1-f)C - fP$, then $x^* < 1$ and $y^* < 1$. Which is consistent with our assumption. Hence, the equilibrium points that exist are (0, 0), (0, 1), (1, 0), (1, 1), and (x^*, y^*).

Case II: if $fP < (1-f)C$ meaning that the penalty from being untrustworthy is lower than the payoff from cheating, the stability of the system equilibrium points is analyzed in Table. IV, and the dynamic phase of evolution between patients and requestors is shown in Fig. 2b. The results show that when $x^* > 0$ and $y^* < ((1-f_p)C_r - f_pP_r)/R_r$, whatever initial strategic choices made, the evolution of the sharing game would lead to an untrustworthy population. However, when $x^* > ((1-f_r)C_p - f_rP_p)/R_p$ and $y^* < 1$ the game will evolve towards a trustworthy population.

TABLE IV. Equilibrium points stability (Case II).

Equilibrium point	$Tr(M_{jac})$	$Det(M_{jac})$	Local stability
(0, 0)	-	+	ESS
(0, 1)	+	+	Unstable
(1, 0)	+	+	Unstable
(1, 1)	-	+	ESS
(x^*, y^*)	0	-	Saddle point

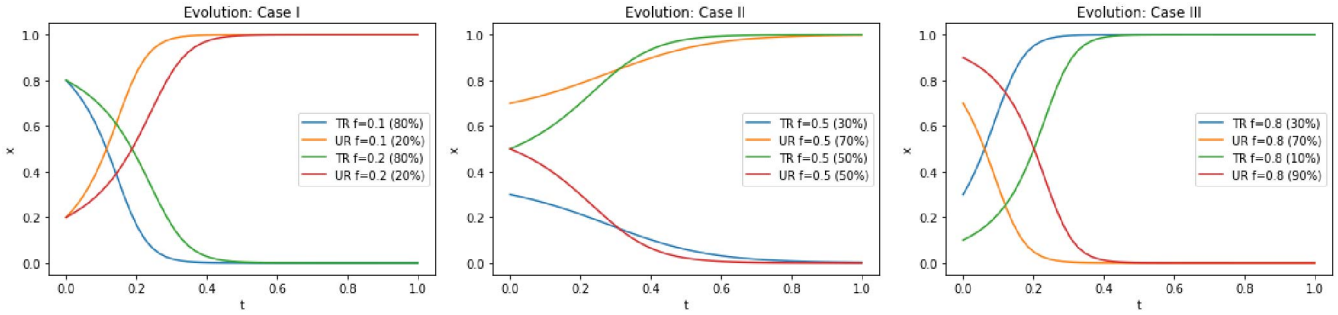
Case III: if $fP > (1-f)C$ meaning that the penalty from being untrustworthy is higher than the payoff from cheating, the stability of the system equilibrium points is analyzed in Table. V and the dynamic phase of evolution between patients and requestors is shown in Fig. 2c. The analysis shows that by setting the reward of being trustworthy higher than the payoff of being untrustworthy and by setting the penalty higher than the cheating payoff, the game will evolve towards a trustworthy population as the players are more incentivized to behave in a trusted manner.

TABLE V. Equilibrium points stability (Case III).

Equilibrium point	$Tr(M_{jac})$	$Det(M_{jac})$	Local stability
(0, 0)	+	+	Unstable
(0, 1)	+	-	Unstable
(1, 0)	+	-	Unstable
(1, 1)	-	+	ESS
(x^*, y^*)	0	-	Saddle point

C. Numerical Analysis

In order to validate the theoretical evolutionary path of both strategy choices (i.e., trustworthy or untrustworthy) and



(a) Evolution in the first case. (b) Evolution in the second case. (c) Evolution in the third case.

Figure 3. The impact of the frequency of verification and initial rate of trustworthiness on the evolution path.

visualize how certain parameters of the game influence the evolutionary stability, we utilized Python for the simulation of the evolution process by giving a fixed value to each parameter of the payoff matrix defined in Table. II as follows: $R = 20, C = 30, L = 10, P = 15, V = 5$. Even though we assigned the parameters in a random way, this has no effect on the results of our simulations. We then further discuss the impact of the frequency of verification as well as the initial distribution of trustworthy players in particular on the evolution of trust within the sharing population. For ease and without loss of generality we opted to study the symmetric case, hence, the evolution of $x(t)$ (i.e., rate of trustworthy requestors over time) is similar to $y(t)$ (i.e., rate of trustworthy patients).

In Fig. 3a we have set the initial distribution of requestors as 80% TR vs 20% UR and the frequency of verification under 0.22 which satisfies the fist case. Hence, even if the initial population contains more trustworthy players the game will evolve towards an untrustworthy population by the end which verifies the theoretical results. In Fig. 3b we fixed the value of the frequency of verification at 0.5 which satisfies the second case, and we evaluated the impact of the initial population on the evolution of trust. If we start with an initial distribution of requestors as 30% TR vs 70% UR the population will move towards an untrustworthy behavior. However, if we start with a $50\%/50\%$ population, trustworthy requestors will end up prevailing in the game. Finally, Fig. 3c represents the evolution under the third case, with a frequency of verification equal to 0.8 and even if we only start the game with a trustworthy population equal to 10% the game will evolve in favor of trust, which matches the theoretical results obtained.

V. Conclusion

In this paper, we presented the design of a blockchain-based framework to guarantee a secure and auditable sharing of health data generated from MIoT devices, which also provides an efficient trading market for patients and data requestors in order to promote better health care and data analysis. We then studied trust within this framework from an EGT angle, we defined theoretically the conditions under which a trustworthy population would prevail in the long run, and we validated the obtained results using simulations.

References

[1] S. B. Baker, W. Xiang, and I. Atkinson , "Internet of Things for smart healthcare: Technologies, challenges, and opportunities," *IEEE Access*, vol. 5, pp. 26521-26544, November 2017.

[2] Telegraph, NHS illegally handed Google firm 1.6m patient records. Available online: https://www.telegraph.co.uk/technology/2017/07/03/googles-deepmind-nhs-misused-patient-data-trial-watchdog-says/. Accessed on: May 7, 2020.

[3] W. Sun, Z. Cai, Y. Li, F. Liu, S. Fang, and G. Wang, "Security and privacy in the medical Internet of Things: A review," *Security and Communication Networks, Hindawi*, 2018.

[4] H. Kaur, M. A. Alam, R. Jameel, A. K. Mourya, and V. Chang, "A proposed solution and future direction for blockchain-based heterogeneous medicare data in cloud environment," *J. Med. Syst.,* vol. 42, p. 156, Aug. 2018.

[5] R. Akkaoui, X. Hei, C. Guo, and W. Cheng, "RBAC-HDE: On the design of a role-based access control with smart contract for healthcare data exchange," in *Proceedings of the* 6th *IEEE International Conference on Consumer Electronics, Taiwan,* 2019.

[6] C. Hao, Q. Du, Y. Huang, L. Shao, and Y. Yan, "Evolutionary game analysis on knowledge-sharing behavior in the construction supply chain," *Sustainability,* vol. 11, 2019.

[7] X. Liu, W. Wang, D. Niyato, N. Zhao, and P. Wang, "Evolutionary game for mining pool selection in blockchain networks," *IEEE Wireless Communications Letters,* vol. 7, no. 5, pp. 760-763, 2018.

[8] H. Abbass, G. Greenwood, and E. Petraki, "The N-player trust game and its replicator dynamics," *IEEE Transactions on Evolutionary Computation,* vol. 20, no. 3, pp. 470–474, 2016.

[9] M. Chica, R. Chiong, M. Kirley, and H. Ishibuchi, "A networked N-player trust game and its evolutionary dynamics," *IEEE Transactions on Evolutionary Computation,* vol. 22, no. 6, pp. 866–878, 2018.

[10] D. Thilakanathan, S. Chen, S. Nepal, R. Calvo, and L. Alem, "A platform for secure monitoring and sharing of generic health data in the cloud," *Future Generat. Comput. Syst.,* vol. 35, pp. 102-113, Jun. 2014.

[11] Y. Zhang, M. Qiu, C. W. Tsai, M. M. Hassan, and A. Alamri, "Health-CPS: Healthcare cyber-physical system assisted by cloud and big data," *IEEE Syst. J.,* vol. 11, no. 1, pp. 88-95, Mar. 2017.

[12] M. Alhamad, T. Dillon, and E. Chang, "A trust-evaluation metric for cloud applications," *International Journal of Machine Learning and Computing,* vol. 1, no. 4, 2011.

[13] J. Weibull, "Evolutionary game theory," *MIT press.,* 1995.

[14] D. Friedman, "Evolutionary games in economics," *Journal of The Econometric Society,* vol. 59, no. 3, p. 637-666, 1991.