A Game-Based Secure Trading of Big Data and IoT Services: Blockchain as a Two-Sided Market

Ahmed Saleh Bataineh[1], Jamal Bentahar[1], Omar Abdel Wahab[2(✉)], Rabeb Mizouni[3], and Gaith Rjoub[1]

[1] CIISE Department, Concordia University, Montreal, Canada
{ah_batai,bentahar,g_rjoub}@encs.concordia.ca
[2] Université du Québec en Outaouais, Gatineau, QC, Canada
omar.abdulwahab@uqo.ca
[3] Khalifa University of Science and Technology, Abu Dhabi, UAE
rabeb.mizouni@ku.ac.ae

Abstract. The blockchain technology has recently proved to be an efficient solution for guaranteeing the security of data transactions in data trading scenarios. The benefits of the blockchain in this domain have been shown to span over several crucial security and privacy aspects such as verifying the identities of data providers, detecting and preventing malicious data consumers, and regulating the trust relationships between the data trading parties. However, the cost and economic aspects of using this solution such as the pricing of mining process have not been addressed yet. In fact, using the blockchain entails high operational costs and puts both the data providers and miners in a continuous dilemma between delivering high-quality security services and adding supplementary costs. In addition, the mining leader requires an efficient mechanism to select the tasks from the mining pool and determine the needed computational resources for each particular task in order to maximize its payoff. Motivated by these two points, we propose in this paper a novel game theoretical model based on the two-sided market approach that exhibits a mix of cooperative and competitive strategies between the (blockchain) miners and data providers. The game helps both the data providers and miners determine the monetary reward and computational resources respectively. Simulations conducted on a real-world dataset show promising potential of the proposed solution in terms of achieving total surpluses for all involved parties, i.e., data providers, data consumers and miners.

Keywords: Game-based trading · Big data · IoT · Blockchain · Two-sided market

1 Introduction

Blockchain technology has lately emerged as a revolutionary paradigm for addressing the challenges of finding trustworthy third-parties and guaranteeing

E. Kafeza et al. (Eds.): ICSOC 2020, LNCS 12571, pp. 85–100, 2020.
https://doi.org/10.1007/978-3-030-65310-1_7

the privacy and security of data trading transactaions in critical domains such as Internet of Things (IoT), data analytics, mobile crowd-sensing, and machine learning. Interestingly, recent statistics estimate that the data contained in the blockchain ledger is expected to worth up to 20% of the global big data market and to generate up to 100 billion in annual income to the data market that already hit $203 billion dollar of revenue at the end of 2019 [6,9]. In the context of data trading using blockchain, three players are to be considered: miners, data providers and data consumers. Miners are responsible for supervising and regulating the execution of what is known as *smart contracts*. A Smart contract is a self-executing computer program that states and organizes the agreed terms of a certain data transaction such as the desired quality of service clauses and secure payment mechanism between the data providers and data consumers. Processing smart contacts by miners entails high (mining) operational costs and processing time, which might negatively affect the execution time of real-time and delay-critical applications such as IoT and data analytics. In the literature, there is lack of attention on the business model that would enable data trading over blockchain where the main stream research in the general context of data focuses on developing mechanisms of data resource management such as [14–16]. Several challenging issues are yet to be addressed, in particular, assigning optimal amount of computational units to the mining tasks, sustaining optimal payoffs to involved players and serving data requests on time. In this work, our objective is to provide a novel contribution to the data trading over blockchain through proposing a game-theoretic-based business model that helps regulate the secure data trading of IoT and big data analytics services. In particular, we aim to address the following two substantial research challenges: 1) how should the blockchain node distribute the computational resources of the mining process among the data providers in such a way to maximize its payoff; and 2) how should the data providers decide on the optimal monetary reward that needs to be given to the miners versus their service in such a way to guarantee optimal execution time of their transactions while avoiding over-payments.

1.1 Motivating Example

We provide in Fig. 1 a motivating example to better clarify the research gap in the literature and highlight the need of our solution. As explained in the figure, data consumers request to run real-time data analytics on an edge IoT server. Following the blockchain technology, the request is deployed as a smart contract which includes clauses that regulate the relationships between the data consumers and the edge IoT server in terms of data quality, data size and processing speed. The execution of the smart contract is supervised and executed by the blockchain node, which manages the mining process and the mining computational units. Smart contracts vary in their terms, and hence they differ in their executions in terms of execution time and required resources. For instance, in Fig. 1, the hospital server is exposed to more privacy threatens as it stores patients data, which requires more computational units from the blockchain node to authenticate only trusted consumers. This creates the need for a distributing

mechanism that determines the optimal amount of resources for each smart contract. However, the absence of such a mechanism might assign more resources to less profitable contracts.

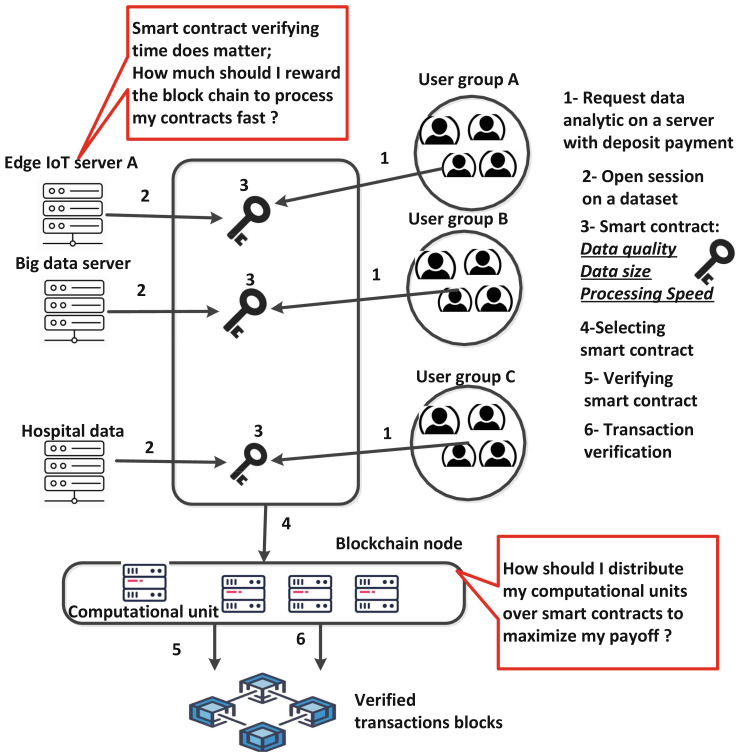


Fig. 1. Motivating scenario: run real time data analytics procedures on Edge IoT server using the blockchain technology.

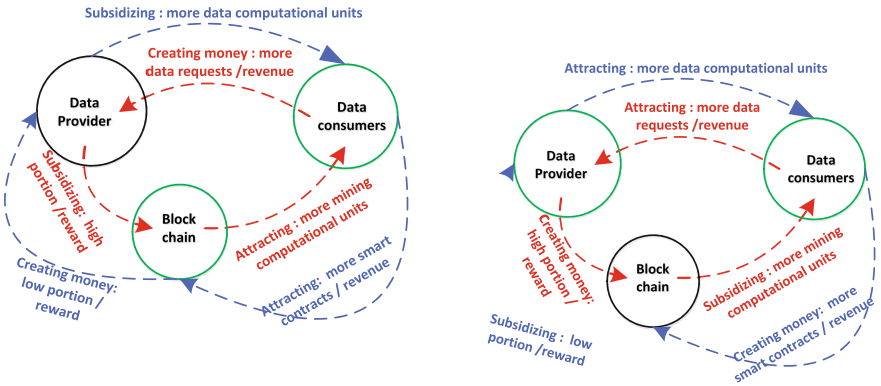
1.2 Related Work and Problem Statement

The state-of-the-art proposals focus on deploying verification approaches into the blockchain technology in order to tackle the privacy and security issues such as preserving the anonymity of the data providers, and preventing impersonation attacks and colluding miners. For instance, the approaches proposed in [18,22] leverage the blockchain technology to address the problem of user location impersonation and re-identification attacks respectively in a crowd-sensing context. The approaches proposed in [8,11] aim to increase the engagement of the crowd system participants through capitalizing on the anonymous and reliable interaction features provided by the blockchain technology.

The proposals [10,13,19,20] propose game theoretical foundations in the context of mobile blockchain supported by edge computing services. The interactions between miners and edge computing nodes are modeled using Stackelberg games and auctions to derive an optimal price for the proof-of-work for offloading allocation tasks. The main limitation of such games is that they result in putting the miners into an aggressive competition situation between each other from one side, and with the edge computing services from the other side. This leads to less efficient outcomes in terms of total surpluses for all these parties. In [21], the authors propose to deploy blockchain for big data sharing in a collaborative edge environment. Similar works have also been proposed in [12,23]. The aforementioned proposals, and the state-of-the-art in general suffer from several problems. In fact, they 1) do not explain how the mining resources should be distributed over the existing smart contracts and miners; 2) do not provide any mechanism to derive the optimal payment that should be given by data providers to miners); and/or 3) propose pricing schemes for the mining process based on pure competitive games, which entails an aggressive competition among the involved parties and results in lower payoffs for them.

1.3 Contribution

To address the aforementioned issues, we extend the work in [3,4] by proposing a novel double two-sided game that models the interactions among the involved parties (i.e., blockchain node, data providers and data consumers) using the two-sided market theory [17]. In the proposed game, as shown in Fig. 2, both the data providers and blockchain node act as a two-sided platform that gets on board two market sides. Specifically, the blockchain node intermediates the interactions between the data providers and data consumers, while the data providers intermediate the interactions between the blockchain node and data consumers. As shown in the figure, the data providers either 1) subsidize the blockchain node by a higher portion of revenue to motivate it to supply more mining computational units, which results in attracting more data consumers and increasing the revenue; or 2) subsidize the data consumers by more data computational units, which increases the consumers' demand and hence contributes in attracting the blockchain node. Similar strategies are set up to the blockchain node as shown in Fig. 2b. The proposed game combines both strategies as two separate games. The solution of the games helps derive the equilibrium in terms of shared revenue among the blockchain node and data providers and amount of mining resources that each smart contract should be assigned with.



Data provider as two-sided market Blockchain as two-sided market

Fig. 2. Proposed model: a double two-sided market game

2 Proposed Model for Secure Trading of Data

2.1 Model Description: A Double Two-Sided Game Formulation

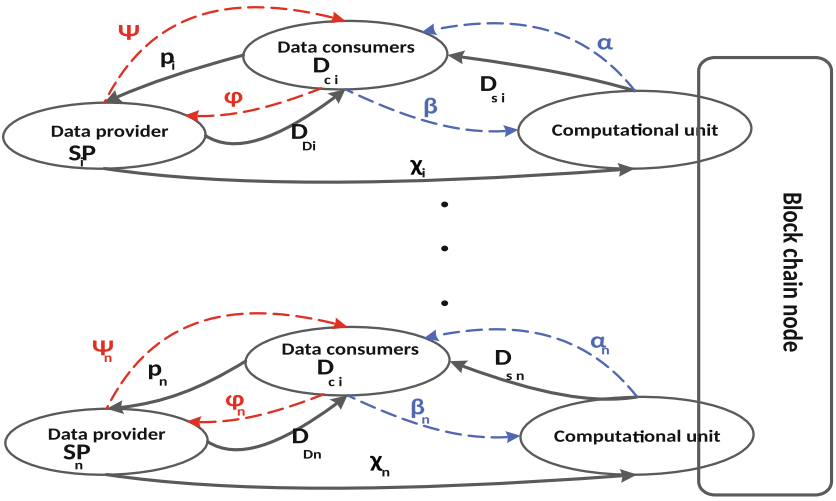


Fig. 3. Double two-sided game

The proposed secure data trading model, depicted in Fig. 3, consists of three entities: Data Service Consumers (SC), Big Data Service Providers (SP) and Blockchain node (BC) that consists of a network of miners. In our solution, a certain big data service provider SP_i receives a monetary value of P_i per a data service consumer's access to its services. The service provider SP_i provides both

the data and computing resources that are required to execute the data analytics duties of the data consumers. The interactions between data providers and data consumers include negotiating the data type, quality of provided services, payments, and all the associated terms of delivered data services. The blockchain node BC is in charge of executing the transactions of smart contracts in order to append a correct block into the blockchain. Executing smart contracts will also ensure the sustainability of consumers' access security, verification of the identities of the data providers and consumers, protection of the privacy of data providers and enforcement of quality control of data services. In our model, the blockchain node seeks to distribute and allocate its computing resources for the mining process among service providers in such a way to maximize its own payoff.

The Consumers' demand on data service i provided by a service provider SP_i is denoted by D_{c_i} and the computing resources allocated by service i to run the data analytics duties of its consumers is donated by D_{D_i}. D_{D_i} is measured in terms of the throughput per second of executing the data requests. The relationship between consumers' demand D_{c_i} and supplying service i is modeled using the two-sided market theory [17] as cross-group externalities ϕ and ψ. Here, ψ represents the increase in the number of data consumers obtained when some new computing and storage resources are added to D_{D_i}. ϕ represents the amount of profit that the data service provider earns when one more new consumer is added to D_{c_i}. Similarly, the computing resources allocated by the blockchain node to regulate the smart contracts of service i is denoted by D_{s_i}. The relationship between consumers' demand and the supply of the blockchain node is likewise modeled using the two-sided market theory as cross-group externalities α and β. Here, α represents the increasing of data consumers obtained when some new computing and storage resources are added to D_{s_i} and β represents the amount of benefits that the blockchain node earns when one more new consumers are added to D_{c_i}. The parameters α, β, ϕ, and ψ are dependant on the service i. However, the variable i is omitted from the notations of these parameters to simplify the equations when the service i is understood from the context. Thus, instead of using α_i for instance, α will be used. The same simplification is applied for the other parameters that appear as exponents in our equations.

The interaction between SP and BC is modeled as a two-stage game, where BC acts as the game leader and SP are the followers. In the first stage of the game, each service provider SP_i providing service i observes the amount of money returns χ_i requested by BC in order to adjust the supply volume of computing resources and the price to be charged to service consumers SC_i consuming the service i. In quest of the price specified by SP_i, BC determines the optimal amount of computing resources D_{s_i} that should be supplied to handle the smart contracts between SP_i and SC_i. The model forms a closed loop of dependencies that involves subsidizing techniques from the two-sided market theory. Thus, SP_i may chose to subsidize BC by an extra amount of payment that exceeds the contribution of BC. The objective is to keep an optimal level of D_{s_i} that maximizes the return revenues $P_i * D_{c_i}$. Alternatively, BC may subsidize SP_i with a low portion of the resulting

revenue to keep an optimal level of P_i. The different parameters and symbols used in our proposed solution are summarized in Table 1.

2.2 Players Demands and Utility Functions

The consumer's demand and supply are modeled using the Cobb-Douglas function, which have the ability to represent the elasticity of the computing and storage resources supply (D_{s_i}, D_{D_i}) and its variations depending on the user's demand. These demand functions are defined as per Eqs. (1), (2), and (3). By substituting Eqs. (2) and (3) into Eq. (1), we can express the consumer's demand as a function of χ_i and P_i as described in Eq. (4).

$$D_{c_i} = k_1 P_i^{-\gamma} D_{s_i}^{\alpha} D_{D_i}^{\psi} \tag{1}$$

$$D_{s_i} = k_2 (\chi_i P_i D_{c_i})^{\beta} \tag{2}$$

$$D_{D_i} = k_3 (P_i D_{c_i})^{\phi} \tag{3}$$

Table 1. Model parameters

Model parameters	Descriptions
SP_i	Service provider providing service i
BC	A blockchain node
SC_i	Consumers of service i
D_{c_i}	SC_i's demand
D_{D_i}	IT-infrastructure supply to handle requests of SC_i
D_{s_i}	IT-infrastructure supply to handle smart contracts between SP_i and SC_i
P_i	Service i's price
χ_i	Portion of revenue required by BC from SP_i
α	The Network effects (externality) on D_{c_i} by D_{s_i}
β	The Network effects (externality) on D_{s_i} by D_{c_i}
ψ	The Network effects (externality) on D_{c_i} by D_{D_i}
ϕ	The Network effects (externality) on D_{s_i} by D_{c_i}
γ	D_{c_i}'s elasticity with respect to P_i
k_1, k_2, and k_3	Constant multipliers
f_c	Associated costs per smart contract
f_s	Associated costs per service request by a consumer
π_i	SP_i's payoff
π	Blockchain node's payoff
a_1	$= -\gamma + \alpha\beta + \phi\psi$
a_2	$= \alpha\beta$
a_3	$= 1/(1 - \alpha\beta - \psi\phi)$

$$D_{c_i} = (k_1 k_2^{\alpha} k_3^{\psi} P_i^{a_1} \chi_i^{a_2})^{a_3} \tag{4}$$

Each big data service provider SP_i is subject to a fixed cost f_s per each consumer access. SP_i aims to maximize its payoff as described in Eq. (5).

$$\pi_i = ((P_i)(1 - \chi_i) - f_s) D_{c_i} \tag{5}$$

The blockchain node BC is subject to a fixed cost f_c per each smart contract between SP_i and a data consumer. As a rational agent, the blockchain node seeks to maximize its payoff as given in Eq. (6).

$$\pi = (P_i \chi_i - f_c) D_{c_i} \tag{6}$$

2.3 Game Equilibrium

The equilibrium of the above-described game is solved using a backward induction methodology. Specifically, the followers' (data service providers) sub-game is solved first to obtain their optimal response P_i^* to the service consumers. The leader's (blockchain node) sub-game is then computed to obtain the optimal χ_i^*. The game equilibrium is stated in Theorem 1.

Theorem 1. *Under the assumption validated in [4] stating that the cross-group externalities are not too week and not too strong,* $(0.1 < \alpha\beta < 0.8)$ *and* $(0.1 < \phi\psi < 0.8)$*, The equilibrium of our double two-sided game is given by the best responses of the different players as follows:*

1. *The best response of the data service provider SP_i is given by:*

$$P_i^* = \frac{a_1 a_3 f_s}{(a_1 a_3 - 1)(\chi_i^* - 1)} \tag{7}$$

$$\textit{if:} \quad 1 < (1/a_1 a_3)$$

2. *The best response of the Blockchain node with respect to a service i is given by:*

$$\chi_i^* = \frac{a_2 a_3 f_c}{(a_2 a_3 + 1) P_i^*} \tag{8}$$

Proof. From Eq. (5) of the data service provider's payoff, using log for both sides of the equation, we obtain:

$$\log \pi_i = \log(P_i(1 - \chi_i) - f_s) + \log D_{c_i} \tag{9}$$

Then, the optimal price P_i^* is defined by $\partial \pi_i / \partial P_i = 0$ as follows:

$$\frac{1}{\pi_i} \times \frac{\partial \pi_i}{\partial P_i} = \frac{1 - \chi_i}{P_i(1 - \chi_i) - f_s} + \frac{1}{D_{c_i}} \times \frac{\partial D_{c_i}}{\partial P_i} = 0 \tag{10}$$

By deriving Eq. (4) with respect to P_i, then:

$$\frac{\partial D_{c_i}}{\partial P_i} = a_1 a_3 D_{c_i} P_i^{-1} \tag{11}$$

By substituting Eq. (11) into Eq. (10), we get:

$$P_i = \frac{a_1 a_3 f_s}{(a_1 a_3 - 1)(\chi_i - 1)} \tag{12}$$

Since $P_i > 0$, $fs > 0$, $((\chi_i - 1) < 1)$ then $(a_1 a_3/(a_1 a_3 - 1) < 0)$, so the condition. By considering the acceptable range for γ analysed in [5], $0.2 < \gamma < 0.3$ then $\partial \pi_i / \partial P_i > 0$ when $P_i < (a_1 a_3 f_s)/((a_1 a_3 - 1)(\chi_i - 1))$ and $\partial \pi_i / \partial P_i < 0$ when $P_i > (a_1 a_3 f_s)/((a_1 a_3 - 1)(\chi_i - 1))$. Consequently, P_i is the best response.

For the second result of the theorem, we consider and take the log for both sides of the equation of the blockchain node's payoff (Eq. (6)) and obtain:

$$\log \pi = \log(P_i \chi_i - f_c) + \log D_{c_i} \tag{13}$$

Then, the optimal χ_i^* is defined by $\partial \pi / \partial \chi_i = 0$ as follows:

$$\frac{1}{\pi} \times \frac{\partial \pi}{\partial \chi_i} = \frac{P_i}{P_i \chi_i - f_c} + \frac{1}{D_{c_i}} \times \frac{\partial D_{c_i}}{\partial \chi_i} = 0 \tag{14}$$

By deriving Eq. (4) with respect to χ_i, we get:

$$\frac{\partial D_{c_i}}{\partial \chi_i} = a_2 a_3 D_{c_i} \chi_i^{-1} \tag{15}$$

By substituting Eq. (15) into Eq. (14), then:

$$\chi_i = \frac{a_2 a_3 f_c}{(a_2 a_3 + 1) P_i} \tag{16}$$

$\partial \pi / \partial \chi_i > 0$ when $\chi_i < (a_2 a_3 f_c)((a_2 a_3 + 1) P_i)$ and $\partial \pi / \partial \chi_i < 0$ when $\chi_i > (a_2 a_3 f_c)((a_2 a_3 + 1) P_i)$. Consequently, χ_i is the best response, so the theorem.

3 Simulation and Empirical Analysis

3.1 Simulation Setup

Our simulation analysis is grounded on statistical observations from big data and IoT services from the AWS marketplace [2], BMR [1]—the annual statistical report that publishes the revenues, payoffs and market growth of the the AWS marketplace—and a real-world dataset from Google [7]. The price, P_i, of the data service is chosen from the interval $[0.2, 3.2]$ USD/hour, following the price distribution of 150 data and IoT services from the AWS marketplace. According to [1], Amazon Web services (AWS) received 30 billion USD in revenue with a net income of approx. 12 billion. The gap between the gross and net revenues is caused by the marginal operating costs which made up approx. 60% of revenue. The operating costs represents in our model the costs associated with the smart contracts f_c and service requests initiated by data consumers f_s. The Google dataset [7] records statistics on the execution of big data requests executed on

Google-powered virtual machines, which are similar to the instances of Amazon cloud infrastructure (EC2). According to these statistics, each virtual machine takes on average 1.42 to 10 s to complete a data processing request (with a mean of 5.71 s and standard deviation of 4.29 s). The instances and their average computational power are respectively represented in our model by D_{s_i} and the externality factor α. Adding a compute instance has a direct impact on the increase of the consumers' demand between 0.1 to 0.7 data request per second. By following the mathematically proved result in [4] that the cross-group externalities should not be neither too weak nor too strong, the cross-group externalities should be bounded by $0.1 < \alpha\beta < 0.8$. Hence, the externality factor β would range from $0.1/\alpha$ to $0.8/\alpha$. We follow those estimations and set up the cross-group externalities ϕ and ψ in the same range of α and β. The price elasticity γ is set to 0.15, which is similar to the sensitivity of mobile/telecommunication services price estimated in the literature [5]. The simulation takes the aforementioned parameters as inputs, and then calculates the optimal shared revenue χ_i from each service i according to Eq. (8) in Theorem 1. Moreover, the simulation inputs meet the theoretical condition $(1 < 1/a_1a_3)$ in Theorem 1. Thus, by substituting the real ranges of the simulation parameters, the mathematical term representing the strength of total externalities (a_3) is greater than zero (i.e $\alpha\beta + \phi\psi < 1$). Hence, we demonstrate our three dimensional results in three sets of criteria: 1) week externalities $(0.1 < \alpha\beta < 0.4,\ 0.1 < \phi\psi < 0.4)$; 2) strong externalities of $\alpha\beta$ - weak externalities of $\phi\psi$ $(0.4 < \alpha\beta < 0.7,\ 0.1 < \phi\psi < 0.2)$; and 3) strong externalities of $\phi\psi$ - weak externalities of $\alpha\beta$ $(0.1 < \alpha\beta < 0.2,\ 0.4 < \phi\psi < 0.7)$.

3.2 Shared Revenues and Computational Costs over Externalities

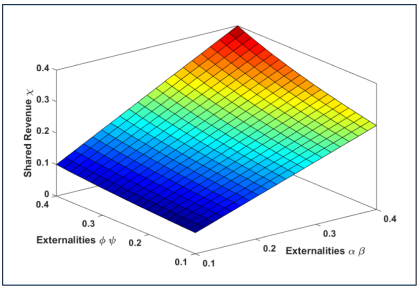


Fig. 4. Shared revenue over week externalities

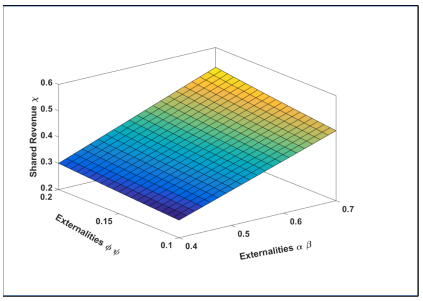


Fig. 5. Shared revenue over strong externalities $\alpha\beta$

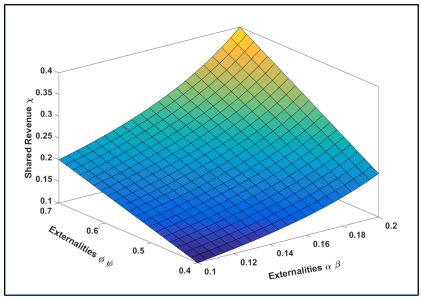


Fig. 6. Shared revenue over strong externalities $\phi\psi$

In this section, we study the impact of the cross group externalitie metrics $(\alpha\beta)$ and $(\phi\psi)$ on the shared revenue χ_i among data providers and blockchain node. In Fig. 4, we study the percentage of shared revenue received by the blockchain node for a weak level of externalities between, on one side the data providers and blockchain node, and on the other side the data consumers. In Figs. 5 and 6, we study the shared revenue for a stronger level of externalities $\alpha\beta$ and $\phi\psi$ respectively. As shown in these figures, the blockchain node receives a higher percentage of revenue as the externality factors $\alpha\beta$ and $\phi\psi$ become stronger. Another important observation is that the average of shared revenues increases at a higher pace over the blockchain node externalities with data consumers $(\alpha\beta)$ than that over data provider and data consumers $(\phi\psi)$. This behavior is clearly observed in Fig. 5 which shows that the shared revenue reaches 60% over strong externalities of $\alpha\beta$ versus a maximum of 40% over strong externalities of $\phi\psi$ as shown in Fig. 6. This behavior is interpreted as follows. The demand of data consumers is positively impacted when its externalities with the blockchain node $(\alpha\beta)$ become stronger. Consequently, the data providers entice the blockchain node by a higher portion χ_i of revenues to supply more computational units with the aim of increasing the consumers' demand and hence the total revenue. Nonetheless, the blockchain node faces higher operating costs by increasing its supply of mining computational units. Consequently, it would ask for a higher portion of revenue. Moreover, the consumers' demand is positively impacted as its externalities with data provider become stronger. Thus, the data providers would face higher operating costs when they add more computational units in an attempt to increase the consumers' demand. This forces the blockchain node to subsidize data providers with a lower portion χ_i of revenue to sustain a higher level D_{c_i} of consumers' demand. In general, increasing the consumers' demand adds more computational cost on the blockchain node, which leads to increasing the portion of blockchain node as the externalities among the data provider and data consumers become stronger. This explains the slower increase pace of shared revenues over the externalities $\phi\psi$ compared to the externalities $\alpha\beta$.

3.3 Data Consumers' Demand and Computational Unit Supply

In this section, we study the impact of cross-group externalities among all the involved parties (i.e., data providers, blockchain node, and data consumers) on the data consumers' demand. As shown on Figs. 7, 8 and 9, the consumers' demand is higher under a weak level of externalities than the strong level. Those observed results are interpreted as follows. A higher externality level among the market players incurs a higher cost for the two-sided market platform to get the market players on board. Specifically, under a strong level of externalities among the blockchain node and data consumers $\alpha\beta$, data providers either (1) subsidize the blockchain node with a higher portion of revenue to attract more data consumers (as discussed in Sect. 3.2); or (2) subsidize the data consumers by supplying higher amounts of data computational units, which in turns, leads to incentivizing the blockchain node. However, data providers cannot ultimately subsidize data consumers due to their mutual cross-group externalities ($\phi\psi$). To study this phenomenon, we show in Figs. 10 and 11 the amount of data computational units supplied by data providers as well as the number of data consumers attracted over the externalities $\phi\psi$ respectively. As shown in Fig. 10, the amount of supplied computational units increases under weak externalities ($\phi\psi \in [0.1 - 0.4]$) and gradually decreases as the cross-group externalities become stronger (i.e., $\phi\psi \in [0.4 - 0.8]$). However, as shown in Fig. 11, the number of attracted data consumers exponentially decreases over the whole range of externalities. This implies that the subsidizing technique becomes costly as the externalities become stronger. For instance, data providers attract 2×10^5 data consumers by providing 20 data computational units at an externality level of 0.2, while they attract a number of data consumers that is 0.1×10^5 less by providing the same amount of data computational units but with a higher externality level of 0.5. In both cases (i.e., subsidizing data consumers and data providers), the data providers would undergo higher costs. Similarly, under a strong level of externalities between data providers and data consumers, the blockchain node subsidizes either the data providers (by asking lower portion of revenues) or the data consumers (by supplying a higher amount of computational units), which entails higher costs for both cases. Similarly, the blockchain node cannot ultimately subsidize the data consumers due to their mutual cross-group externalities represented by $\alpha\beta$. Similar observations are depicted in Fig. 12 in terms of mining computational units over $\alpha\beta$.

3.4 Data Providers and Blockchain Payoffs

In this section, we investigate the impact of externalities on the payoff of the data providers and blockchain node. Figure 13 shows the payoff of data providers under weak externalities, while Figs. 14 and 15 depict providers' payoff under strong externalities $\alpha\beta$ and $\phi\psi$ respectively. As illustrated in these figures, the data providers' payoff gradually decreases as the externalities increase. The reason behind this increasing is that the overall demand of consumers decreases while computational costs and asked shared revenue increase over externalities

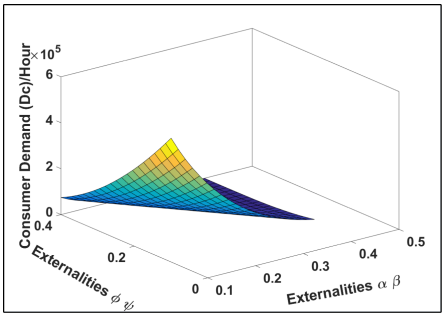


Fig. 7. Consumers' demand over week externalities

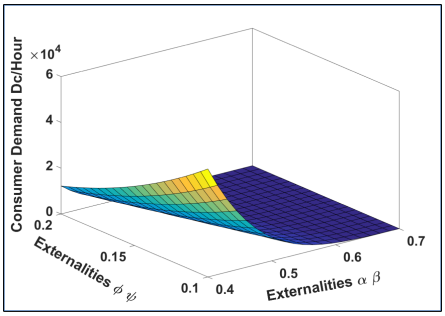


Fig. 8. Consumers' demand over strong externalities $\alpha\beta$

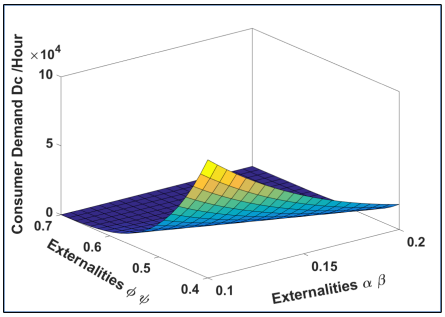


Fig. 9. Consumers' demand over strong externalities $\phi\psi$

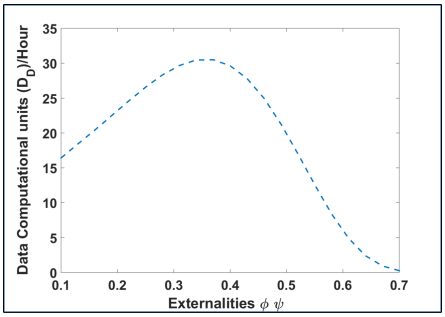


Fig. 10. Data computational units over $\phi\psi$

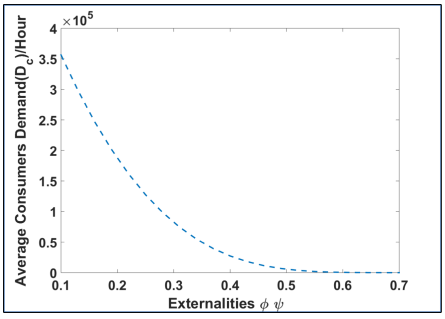


Fig. 11. Number of attracted consumers over $\phi\psi$

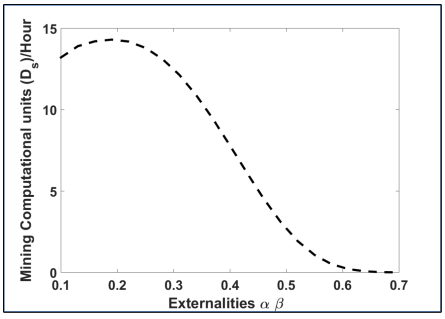


Fig. 12. Mining computational units over $\alpha\beta$

as discussed in Sects. 3.2 and 3.3. Similarly, the payoff of the blockchain node decreases under externalities as shown Figs. 16, 17 and 18.

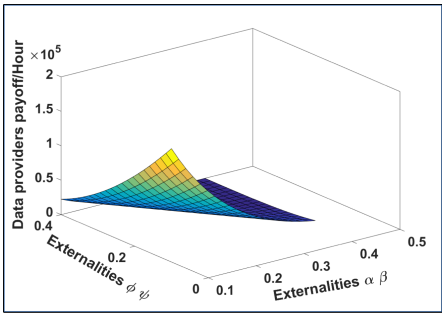


Fig. 13. Data providers payoff over weak externalities

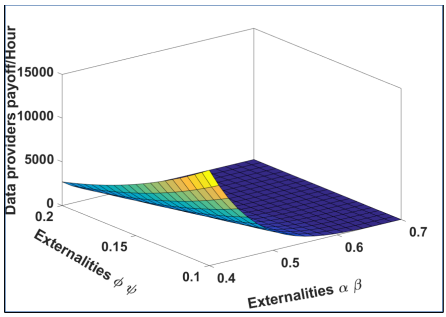


Fig. 14. Data providers payoff over strong externalities $\alpha\beta$

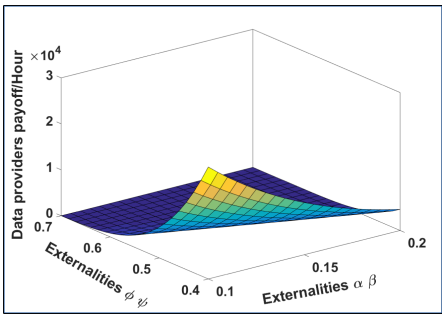


Fig. 15. Data providers payoff over strong externalities $\phi\psi$

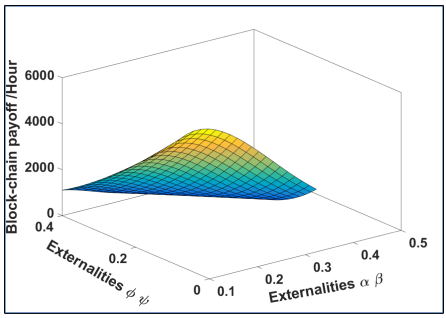


Fig. 16. Blockchain payoff over weak externalities

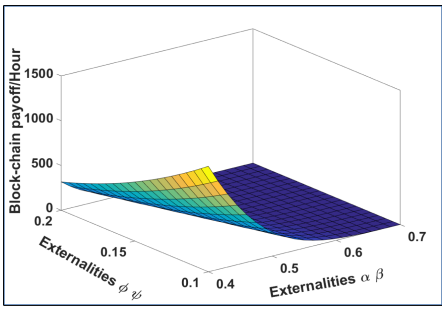


Fig. 17. Blockchain payoff over strong externalities $\alpha\beta$

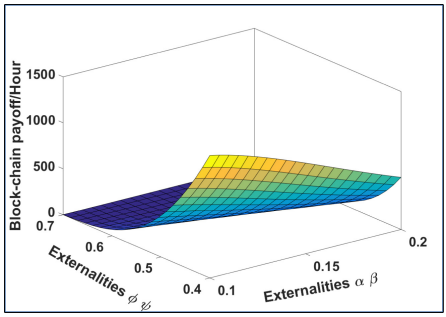


Fig. 18. Blockchain payoff over strong externalities $\phi\psi$

4 Conclusion

In this work, we proposed a new game-based business model for data trading over blockchain. The problem is formulated as a double two-sided game that

solved the problem of maximizing the players' payoff by optimally distributing the mining computational powers over smart contracts. Technically, the game considered the smart contract characteristics as well as the impact of the mining computational units on the data service and consumers' demand. The theoretical and simulation results proved the efficiency of the proposed game.

References

1. DMR Amazon statistical report 2018. https://expandedramblings.com/index.php/downloads/dmr-amazon-web-services-report/. Accessed 31 Jan 2019
2. Amazon: IoT and big data services in Amazon market places. https://aws.amazon.com/marketplace/search?page=1&category=96c2cd16-fe69-4b1899cc-e016c61e820c. Accessed 19 Nov 2019
3. Bataineh, A.S., Mizouni, R., Barachi, M.E., Bentahar, J.: Monetizing personal data: a two-sided market approach. Procedia Comput. Sci. **83**, 472–479 (2016)
4. Bataineh, A.S., Mizouni, R., Bentahar, J., Barachi, M.E.: Toward monetizing personal data: a two-sided market analysis. Future Gener. Comput. Syst. **111**, 435–459 (2020)
5. Danaher, P.J.: Optimal pricing of new subscription services: analysis of a market experiment. Mark. Sci. **21**(2), 119–138 (2002)
6. Fedak, V.: Blockchain and big data: the match made in heavens (2018). https://towardsdatascience.com/blockchain-and-big-data-the-match-made-in-heavens-337887a0ce73. Accessed 02 Jan 2019
7. Google: Google cluster data. https://github.com/google/cluster-data. Accessed 19 July 2019
8. Hu, J., Yang, K., Wang, K., Zhang, K.: A blockchain-based reward mechanism for mobile crowdsensing. IEEE Trans. Comput. Soc. Syst. **7**(1), 178–191 (2020)
9. Jiao, Y., Wang, P., Feng, S., Niyato, D.: Profit maximization mechanism and data management for data analytics services. IEEE Internet of Things J. **5**(3), 2001–2014 (2018)
10. Jiao, Y., Wang, P., Niyato, D., Xiong, Z.: Social welfare maximization auction in edge computing resource allocation for mobile blockchain. In: 2018 IEEE International Conference on Communications (ICC), pp. 1–6 (2018). https://doi.org/10.1109/ICC.2018.8422632
11. Kadadha, M., Otrok, H., Mizouni, R., Singh, S., Ouali, A.: Sensechain: a blockchain-based crowdsensing framework for multiple requesters and multiple workers. Future Gener. Comput. Syst. **105**, 650–664 (2020)
12. Liu, Z., et al.: A survey on blockchain: a game theoretical perspective. IEEE Access **7**, 47615–47643 (2019). https://doi.org/10.1109/ACCESS.2019.2909924
13. Luong, N.C., Xiong, Z., Wang, P., Niyato, D.: Optimal auction for edge computing resource management in mobile blockchain networks: a deep learning approach. In: 2018 IEEE International Conference on Communications (ICC), pp. 1–6 (2018)
14. Rjoub, G., Bentahar, J., Abdel Wahab, O., Saleh Bataineh, A.: Deep and reinforcement learning for automated task scheduling in large-scale cloud computing systems. Concurr. Comput. Pract. Exper. (2020)
15. Rjoub, G., Bentahar, J., Wahab, O.A.: Bigtrustscheduling: trust-aware big data task scheduling approach in cloud computing environments. Future Gener. Comput. Syst. **110**, 1079–1097 (2020)

16. Rjoub, G., Bentahar, J., Wahab, O.A., Bataineh, A.: Deep smart scheduling: a deep learning approach for automated big data scheduling over the cloud. In: 7th International Conference on Future Internet of Things and Cloud (FiCloud), pp. 189–196 (2019)
17. Rochet, J., Tirole, J.: Platform competition in two-sided markets. J. Eur. Econ. Assoc. **1**(4), 990–1029 (2003)
18. Wang, J., Li, M., He, Y., Li, H., Xiao, K., Wang, C.: A blockchain based privacy-preserving incentive mechanism in crowdsensing applications. IEEE Access **6**, 17545–17556 (2018)
19. Xiong, Z., Feng, S., Wang, W., Niyato, D., Wang, P., Han, Z.: Cloud/fog computing resource management and pricing for blockchain networks. IEEE Internet of Things J. **6**(3), 4585–4600 (2019). https://doi.org/10.1109/JIOT.2018.2871706
20. Xiong, Z., Feng, S., Niyato, D., Wang, P., Han, Z.: Optimal pricing-based edge computing resource management in mobile blockchain. In: 2018 IEEE International Conference on Communications (ICC), pp. 1–6. IEEE (2018)
21. Xu, C., et al.: Making big data open in edges: a resource-efficient blockchain-based approach. IEEE Trans. Parallel Distrib. Syst. **30**(4), 870–882 (2019). https://doi.org/10.1109/TPDS.2018.2871449
22. Yang, M., Zhu, T., Liang, K., Zhou, W., Deng, R.H.: A blockchain-based location privacy-preserving crowdsensing system. Future Gener. Comput. Syst. **94**, 408–418 (2019)
23. Yang, R., Yu, F.R., Si, P., Yang, Z., Zhang, Y.: Integrated blockchain and edge computing systems: a survey, some research issues and challenges. IEEE Commun. Surv. Tutor. **21**(2), 1508–1532 (2019). https://doi.org/10.1109/COMST.2019.2894727