Research on the Used Car System Based on Blockchain and Cryptographic Technology

[1]CHI HUANG, [1]CHENGLIAN LIU, [2]SONIA C-I CHEN
[1]Department of Science and Engineering, Shiyuan College of Nanning Normal University, Nanning 530226, CHINA
[2]School of Economics, Qingdao University, Qingdao 266061, CHINA

Abstract: Different countries have different issues with related to topic of used car in all of world, and used car issues involve very wide range of fields, such as environmental protection, market economy, sales services, information systems, regulations and policies, components, materials, and logistics so on. In this study the authors would like to propose a scheme of used car transaction information system from perspective of mathematical modelling. We introduce the concept of a third party appraiser as an arbitrator between buyers and sellers in this solution. In order to avoid collusion between third parties and sellers, the blockchain and cryptography technology be used to prevent collusion and ensure fair and just transactions.

Keywords: Third Party, Anonymous, Diffie-Hellman Protocol, Used Car Trading System

Received: April 21, 2021. Revised: June 23, 2022. Accepted: July 25, 2022. Published: September 14, 2022.

1. Introduction

To overview relevant references from domestic and foreign. The literatures on second-hand cars can be roughly divided into several categories. We classify information systems and platforms into one category [1]–[6], policies and regulations into one category [7]–[11], sales and marketing into one category [12]–[20], technologies and artificial intelligence into one category [4], [21]–[28], and services with strategies into one category [29]–[31]. Research by Mbaye et al. [30] shows that discrimination based on information rather than taste is common in the French's used car market. Grodzinsky et al. [31] proposed an interesting topic "Developing artificial agents worthy of trust–Would you buy a used car from this artificial agent?". Both buyers and sellers will seek favorable prices for themselves, this question is probably one of the most difficult they have to face; Marshall [29] points to the crux of the problem. Gabbott [8] studies the second-hand car market in the UK, noting that the consumer problem is very serious, and also mentions the application of the compulsory licensing system for second-hand car dealers introduced in Scotland. In any second-hand market, there is a buyer/seller information asymmetry, because the seller may know the history of the product better than the buyer. Nicks [7] presented an article "Speak no evil-Known defects in the FTC's used car rule", described the FTC's (Federal Trade Commission) issued to a trade regulation on used car sales that required dealers to disclose to potential buyers known defect in 1981. Later, the FTC removed this important consumer protection by reissued rule version in 1985. Wang et al. [9] discuss the second-hand car transaction model in China's quality certification market, and there are two ways to make the market successful: (1) eliminate the incompleteness of information; (2) increase the cost of counterfeiting. Certification bodies are required to make actual quality commitments, and to a certain extent assume relevant responsibilities, in order to improve the effectiveness of quality certification, to further ensure the authority, fairness and objectivity of certification. In addition to Gabbott's mention of information asymmetry, Ahn [3] proposed an article "Implementation for used trading management system based blockchain (Case-used car)"; he uses smart contracts to ensure the reliability of Ethereum without third-party intervention. Furthermore, the system alleviates information asymmetry between buyers and sellers, and reduces with prevents brokerage fees in the distribution process without a third party. Yoo and Ahn [6] mentioned that in the second-hand car trading market, all kinds of second-hand car trading damages are caused by the information asymmetry between the buyer and the seller. Zhang and Ma [5] describe an SVR (support vector machine regression) algorithm

that can accurately estimate the price of used cars, and the method can also be extended to other second hand products. Sun et al. [4] presented an optimized BP (back propagation) neural network algorithm to analyze the price data of various vehicles, and then build the second hand car price assessment model for an online used car platform to get the best price for the car. Ogawa [1] and Kumar et al. [2] also contributed their research results on used car trading platforms. In this paper the authors would like to propose a scheme using mathematical model and cryptology skill to used car information system. Due to limited conditions, this study lists parts of good contributions, but is a little different then what is discussed in this article, please see Table 1.

TABLE 1
ENGLISH RELATED LITERATURES

System/Platform	Policy/Rule	Marketing	Technology/AI	Service/Strategy
Ogawa [1]	Nicks [7]	Huang & Liu [12]	Sun et al. [4]	Marshall [29]
Kumar et al. [2]	Gabbott [8]	Shibuya [13]	Aksezer [21]	Mbaye et al. [30]
Ahn [3]	Wang et al. [9]	Shibuya [14]	Ozturan [22]	Grodzinsky et al. [31]
Sun et al. [4]	FTC [10]	Shibuya [15]	Yu et al. [23]	
Zhang & Ma [5]	Figlin [11]	Shibuya [16]	Sawicki & Scherer [24]	
Yoo & Ahn [6]		Wang & Wang [17]	Sathiya et al. [25]	
		Haan & de Boer [18]	Papagapiou et al. [26]	
		Kooreman & Hann [19]	Guda & Tsurikov [27]	
		Rivas-Sánchez et al. [20]	Pehlken et al. [28]	

2. Literatures Review

The COVID-19 epidemic has affected in the past two years, the global economy slowed down, and China is no exception. However, the large volume of China's market (such as a large population and relatively large supply and demand) is accompanied by discussions on the used car market. According to our survey, the Chinese literature of used cars can also be roughly divided into five categories: platform [32]–[34], block chain [35], education [36]–[39], occupation (certificated) [40], [41], and others [42], [43]. The information system-related content is classified in the platform, based on blockchain or virtual currency of used car topic is classified in blockchain. In China's education system, there is a type of vocational education; i.e. in the curriculum design of automobile engineering or mechanical engineering, one course name is "used car identification and evaluation", this is classified in education. In recent years, China has also attached importance to the development of professional license (or certificated) system. There are many emerging categories, including used car brokers, third-party appraisers and so on. This category of occupation refers to these. On September 24, 2021, the People's Bank of China issued a notice on further preventing and dealing with the risk of speculation in virtual currency transactions. The notice pointed out that virtual currency does not have the same legal status as legal currency. Bitcoin, Ethereum, Tether and other virtual currencies have the main characteristics of being issued by non-monetary authorities, using encryption technology and distributed accounts or similar technologies, and existing in digital form. They are not legal compensation and should not and cannot be used as currency in the market [44], [45]. Even so, it does not affect the application of blockchain and cryptology to the used car transaction system. Wu and Liu [46] described an anonymous delivery system using blind signature scheme. Later, Wu et al. [47] also presented a conception which used anonymity purchasing to mobile payment. Zhang et al. [48] connected RSA [49] with ElGamal [50] two algorithms in their idea on mobile purchasing without bank card. Lv et al. [51] applied to library complaint information system. Based on mathematical reasoning and model inference, we get inspiration there. Some Chinese related literatures lists in Table 2.

TABLE 2
CHINESE RELATED LITERATURES

Platform	Blockchain	Education	Occupation	Others
Lu & Yu [32]	Zhu [35]	Wang & Wang [36]	Gao [40]	Cheng & Song [42]
Liu et al. [33]		Yin & Peng [37]	Qiao [41]	Zhang [43]
Li [34]		Yin & Lin [38]		
		Liu et al. [39]		

3. Our Scheme and Methodology

The well-known algorithms ElGamal [50] and Diffie-Hellman [52] schemes have similar properties in public key cryptosystems, our study adopts the spirit of these two algorithms to propose a framework and concept of used car trading system. The role of the seller, the buyer and the third party are independent of each others. Eliminate collusion between any two sides (such as collusion between the buyer and the seller, or collusion between the seller and the third party), and strengthen the role and ability of the third party appraiser under this framework. There are totally eight phases in this framework, and we conceptually introduce the main six phases here. Namely, inquiring, forwarding, checking, paying, confirming, and delivering phases. We would describe as following sections.

Step 1. The buyer consults the second-hand car dealer for car purchase information.
Step 2. Used car dealers provide information to third-party appraisers.
Step 3. The third party provides professional information to the buyer.
Step 4. The buyer shall make a decision and pay according to the suggestions of the third-party

appraiser, and entrust the third party to buy the second-hand car.

Step 5. The third-party appraiser exercises the agency right to buy a car from a third party.

Step 6. The used car dealer shall deliver the car to the buyer according to the agreement.

More detailed information flow, please see Figure 1.

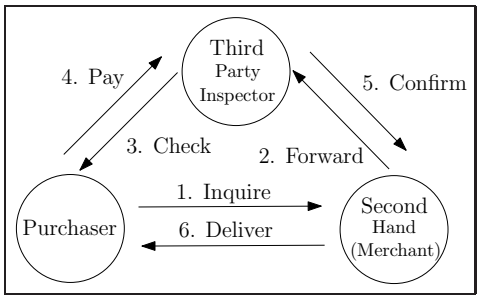

Fig. 1. The Diagram of Our Scheme.

We usually assume p is a large prime which its over 1024 bits length, and g is a primitive root of $\mathbb{Z}_p^*$, others symbols and meanings are shown as follows.

Notation and Significant:

p: prime number.
g: primitive root of $\mathbb{Z}_p^*$.
x_i: secret key in ElGamal-like algorithm.
y_i: public in ElGamal-like algorithm.
$h()$: one-way hash function.
M_i: digitized message.
Purchaser: express buyer or consumer.
Third party: express the third party inspector (or appraiser).
Second hand: express the second hand car (or used car) dealer or merchant or seller.

3.1. System Initializing Phase

The purchaser randomly selects a secret key x_a where $\gcd(x_a, p-1) = 1$, and finds the public key

$$y_a \equiv g^{x_a} \pmod{p}. \tag{1}$$

The merchant also randomly selects a secret key x_b and finds its public key

$$y_b \equiv g^{x_b} \pmod{p}. \tag{2}$$

The third party randomly selects a secret key x_c, and finds its public key

$$y_c \equiv g^{x_c} \pmod{p}. \tag{3}$$

They did not publish their secret key but published their own public key, see Figure 2.

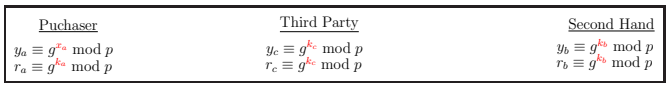

Fig. 2. Initializing Phase.

3.2. Inquiring Phase

Purchaser computes S_a where

$$S_a \equiv y_a \cdot r_c \pmod{p}, \tag{4}$$

and

$$m_i \equiv h(M_i) \pmod{p}, \tag{5}$$

before he sends S_a and m_i to second hand car dealer or merchant, see Equation (4) to (5) and Figure 3.

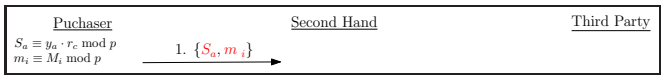

Fig. 3. Inquiring Phase.

3.3. Forwarding Phase

When merchant receives S_a and m_i by purchaser, he uses his secret key x_b to generate T_1 before forward to third party, see Equation (6) and Figure 4.

$$T_1 \equiv S_a^{x_b} \cdot m_i \cdot r_c^{-x_b} \pmod{p}. \tag{6}$$

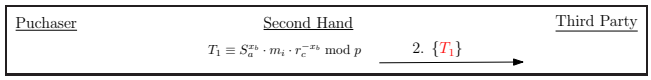

Fig. 4. Forwarding Phase.

3.4. Checking Phase

Third party inspector uses his secret key x_c to sign the parameter T_1 before transmit T_2 to purchaser, see Equation (7) and Figure 5.

$$T_2 \equiv (T_1)^{x_c} \cdot m_i^{-x_c} \pmod{p}. \tag{7}$$

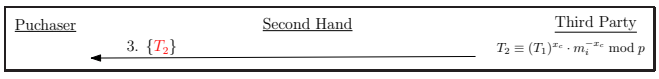

Fig. 5. Check Phase.

3.5. Paying Phase

Purchaser receives parameter T_2 by third party inspector; purchaser pays for inspector after the information of inspection has confirmed. Purchaser generates T_3 and then returns to inspector, see Equation (8) and Figure 6.

$$T_3 \equiv (T_2) \cdot (r_b)^{k_a} \pmod{p}. \tag{8}$$

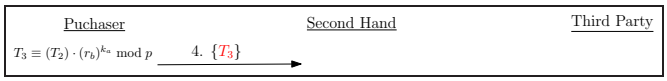

Fig. 6. Paying Phase.

3.6. Confirming Phase

Purchaser authorized inspector to buy the second hand car, namely inspector delegates purchaser to buy the car. Inspector calculates T_4 and transmits to merchant, see Equation (9) and Figure 7.

$$T_4 \equiv (T_3)^{k_c} \cdot (T_2)^{-k_c} \pmod{p}. \tag{9}$$

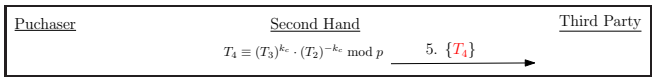

Fig. 7. Confirming Phase.

3.7. Delivering Phase

Merchant passed inspector's confirmation, he then delivers T_5 to purchaser before uses semi key k_b^{-1} to sign T_4, see Equation (10) and Figure 8.

$$T_5 \equiv (T_4)^{k_b^{-1}} \pmod{p}. \tag{10}$$

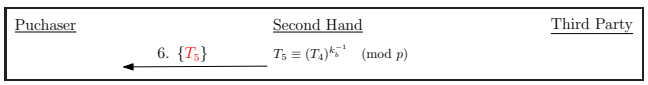

Fig. 8. Confirming Phase.

3.8. Purchaser Verifying Phase

If the merchant does not collude with a third party, the merchant can fetch $r_a^{k_c}$ after recovered T_4 by inspector, the proof see Equation (11) and (12).

$$T_5 \stackrel{?}{\equiv} r_c^{k_a} \pmod{p}. \tag{11}$$

Proof.

$$\begin{aligned} T_5 &\stackrel{?}{\equiv} (T_4)^{k_b^{-1}} \pmod{p} \\ &\equiv [(r_b^{k_a})^{k_c}]^{k_b^{-1}} \pmod{p} \\ &\equiv r_a^{k_c} \pmod{p} \\ &\equiv r_c^{k_a} \pmod{p}. \end{aligned} \tag{12}$$

□

By Equation (12), the proof is finished.

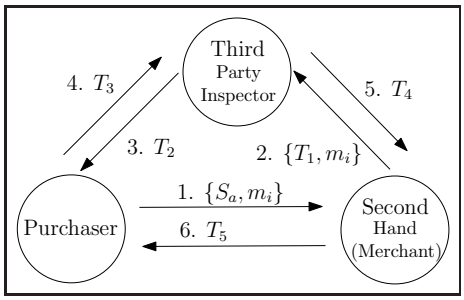

Fig. 9. A Concept of Used Car Scheme Based on Cryptographic Protocol.

4. Security Analysis

In this section, we discuss two types of security: theoretical security and practical security. And then describes three definitions, three lemmas, and three scenarios of attack model.

Definition 1. *Discrete Logarithm Problem (DLP)*
As known parameters $\{p,\ g,\ y_i\}$ *where the formula* $y_i \equiv g^{x_i} \pmod{p}$*, it is very hard to find the private key* x_i *while prime approaching infinite. Based on this assumption of computation and condition, it is called solving the discrete logarithm problem (Solving Discrete Logarithm Problem) [53]. The current public key cryptosystem based on discrete logarithm has value parameters that are greater than* 1024 *bit length or* 2048 *bit length.*

Definition 2. *Computation Diffie-Hellman Problem (CDHP)*
The Computation Diffie-Hellman Problem [54]is derived on the Diffie-Hellman key exchange principle (Diffie Hellman Key Exchange) [55]. The main ideas are described as follows: Given $\{g,\ g^x,\ g^y\}$ *to find* g^{xy}*. Here,* g *is known parameter, the* x *and* y *are unknown parameters.*

Definition 3. *Decisional Diffie-Hellman Problem (DDHP)*
The Decisional Diffie-Hellman Problem [56] is a variant of the Diffie-Hellman computation problem.

Given $\{g,\ g^x,\ g^y,\ g^z\}$*, to find the* $\mathbb{Z}_p$ *is satisfied* $z = xy$*. Given* $\{g,\ g^x,\ g^y\}$*, to find* g^{xy}*. Here the parameter* g *is known, and the parameters* $\{x,\ y,\ z\}$ *are all unknown.*

4.1. Theoretical Security

We suppose adversary is holding unlimited computing resources and time, he then can offenses any target information system what he wants. If the system is secure against this attack, this is to say theoretical security, also called unconditional security.

Lemma 1. *If purchaser is honest, the Equations (4), (5), (8) and (12) would be correct.*

Proof. As known from Equation (4) since $S_a \equiv y_a \cdot r_c \pmod p$. The merchant can verify Equation (13) since

$$y_a \cdot r_c \stackrel{?}{\equiv} S_a \pmod p. \tag{13}$$

If purchaser cheated, it does not hold to the Equation (13). This stage is for the merchant to verify the purchaser. Another verification method, the merchant produced T_1, he can check

$$T_1 \stackrel{?}{\equiv} y_a^{x_b} \cdot m_i \pmod p. \tag{14}$$

If it does not hold, it means the purchaser is a liar. □

Lemma 2. *If merchant is honest, the Equations (5), (6) and (10) would be correct.*

Proof. In forwarding phase, the merchant uses his secret key x_b to produce T_1; then in checking phase, the third party also uses his secret key x_c honestly, the T_2 is the starting point of the agreement signed by the three sides such as purchaser, merchant and the third party inspector. In T_3 phase, the purchaser has signed mark "$r_b^{-k_a}$" where it express both sides i.e. purchaser and merchant. In T_4 phase, the third party inspector uses his semi-key k_c and $-k_c$ for his agency right. Turn around to T_5 phase, it became $(r_a)^{k_c}$. It showed the merchant honestly; otherwise, it is a contradiction. □

Lemma 3. *If third party inspector honest, the Equations (7), (9) and (11) would be correct.*

Proof. The third party inspector uses his key x_c, k_c to sign in T_2 and T_4 phases, If third party inspector cheated all, then the Equations (15), (16) and (17) do not hold.

$$T_2 \equiv y_a^{x_b x_c} \pmod p, \tag{15}$$

since

$$T_4 \equiv r_b^{k_a k_c} \pmod p, \tag{16}$$

and

$$T_5 \equiv r_a^{k_c} \pmod p. \tag{17}$$

Obviously, those are contradicts to Lemma 1 and Lemma 2. Thus, the third party inspector is honest to all. □

4.2. Practical Security

The practical security is also called conditional security. If a system depends on the computational cost to defense any cryptanalysis, we say computational security or conditional security.

Scenario 1: Outside attack

If attacker tries to find the private key x_a by y_a, modulus p and an element primitive generator g of $\mathbb{Z}_p^*$. The attacker would challenge the DLP which describes through Definition 1.

Scenario 2: Insider attack

We suppose the attacker came from merchant side, namely one of employee instead of his manager to use a fake secret key x_b' by pass forwarding phase.

$$T_1' \equiv (S_a)^{x_b'} \cdot m_i \cdot (r_c)^{-x_b'} \pmod p. \tag{18}$$

And then cheated third party inspector to calculate

$$T_2' \equiv (T_1')^{x_c} \cdot m_i^{-x_c} \equiv (y_a)^{x_b' \cdot x_c} \pmod p. \tag{19}$$

Consequently, purchaser replies T_3' to third party inspector as following:

$$T_3' \equiv T_2' \cdot r_b^{k_a} \equiv (y_a)^{x_b' \cdot x_c} \cdot r_b^{k_a} \pmod p. \tag{20}$$

Third party received T_3' and calculated T_4', prompt

$$T_4' \equiv (T_3')^{k_c} \cdot (T_2')^{-k_c} \pmod p. \tag{21}$$

Although the insider deceived third party inspector and successfully passed T_1' to T_4' phases. However, the insider can not pass T_5' since he did not own the original semi-key k_b, therefore he would fail and stop on delivering phase since he faked semi-key $k_b'^{-1}$ to find

$$T_5 \not\equiv T_5' \equiv (T_4')^{k_b'^{-1}} \pmod p. \tag{22}$$

Thus, the insider can not cheat purchaser successfully on the final stage. The concept of description is shown in Figure 10.

Scenario 3: Message leakage issue

As known from Equation (5), the original message had digitized and hashed, if insider wants to recover M_i, it is very hard since insider challenges one-way hash functions [57] such as two properties: re-image resistance and collision resistance.

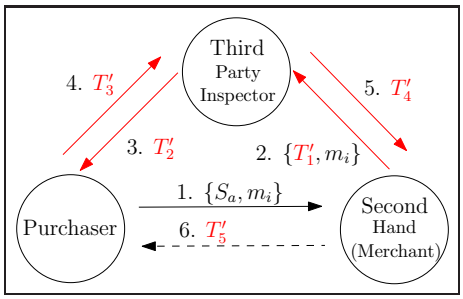

Fig. 10. Simulating insider attack model.

5. Conclusion

In this paper the authors propose a used car trading system based on blockchain and cryptography technology. Our scheme is different from other literatures in the following points: (1) The method we proposed is very specific, not just a concept. According to this algorithm, we can realize the code and transform it into an information system. (2) We use blockchain and cryptography technology to protect consumers' individual privacy. (3) This is an anonymity scheme. (4) We give three definitions, three lemmas, three simulated attack scenarios, and twenty-two mathematical formulas, which perfectly provide strong theoretical support for our scheme; especially in the provably secure. There is another key point, we prevent third-party inspector colluded with seller to cheat buyer; or third-party inspector colluded with buyer to cheat seller. These are not mentioned in other literatures, It is the highlight and contribution of this paper.

Acknowledgments

The authors would like to thank the reviewers for their comments that help improve the manuscript. This work is partially supported by the project number X2021110650493 from College Students Innovation and Entrepreneurship Training Program of China by Qingdao University.

References

[1] S. Ogawa, *An Informal Used-Car Trading System Between Hong Kong and East African Countries Using ICT*. Cham: Springer International Publishing, 2021, pp. 131–152. [Online]. Available: https://doi.org/10.1007/978-3-030-55579-5_6

[2] M. S. Nikhil Kumar, G. C. Akshatha, M. D. Bangre, M. Dhanush, and C. Abhishek, "Decentralized used cars bidding application using Ethereum," in *2021 IEEE International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS)*, 2021, pp. 1–7.

[3] B. Ahn, "Implementaion for used trading management system based blockchain (Case: Used car)," in *Frontier Computing*, J.-W. Chang, N. Yen, and J. C. Hung, Eds. Singapore: Springer Singapore, 2021, pp. 405–412.

[4] N. Sun, H. Bai, Y. Geng, and H. Shi, "Price evaluation model in second-hand car system based on bp neural network theory," in *2017 18th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)*, 2017, pp. 431–436.

[5] W. Zhang and L. Ma, "Research and application of second-hand commodity price evaluation methods on B2C platform: take the used car platform as an example," *Annals of Operations Research*, pp. 1–13, October 2021, 10.1007/s10479-021-04332-5.

[6] S. G. Yoo and B. Ahn, "A study for efficiency improvement of used car trading based on a public blockchain," *The Journal of Supercomputing*, vol. 77, no. 9, pp. 10 621–10 635, September 2021.

[7] S. J. Nicks, "Speak no evil: Known defects in the FTC's used car rule," *Journal of Consumer Policy*, vol. 10, no. 1, pp. 69–87, March 1987.

[8] M. Gabbott, "The licensing of second hand car dealers in Scotland," *Journal of Consumer Policy*, vol. 13, no. 1, pp. 53–64, March 1990.

[9] X. Wang, X. Liu, X. Zhang, and Q. Su, "The two-person double-price second-hand vehicle trade model of quality certification market in China," in *2007 International Conference on Service Systems and Service Management*, 2007, pp. 1–7.

[10] Federal Trade Commission: Consumer Information, "Buying a used car from a dealer," https://www.consumer.ftc.gov/articles/buying-used-car-dealer.

[11] Victor Figlin, "Local dealership offers a new way to de-risk used car buying in Indiana," Website, https://www.pressrelease.cc/2021/08/04/local-dealership-offers-a-new-way-to-de-risk-used-car-buying-in-indiana-2/.

[12] G. Huang and H. Liu, "Estimating expectations-based reference-price effects in the used-car retail market," *Quantitative Marketing and Economics*, vol. 19, no. 3, pp. 457–503, December 2021.

[13] Y. Shibuya, *The Excess Demand for Used Cars*. Singapore: Springer Singapore, 2020, pp. 59–74. [Online]. Available: https://doi.org/10.1007/978-981-15-0825-7_4

[14] ——, *Facebook Page Topics and the Excess Demand for Used Cars*. Singapore: Springer Singapore, 2020, pp. 91–100. [Online]. Available: https://doi.org/10.1007/978-981-15-0825-7_6

[15] ——, *Topics on Twitter and the Excess Demand for Used Cars*. Singapore: Springer Singapore, 2020, pp. 101–112. [Online]. Available: https://doi.org/10.1007/978-981-15-0825-7_7

[16] ——, *Public Sentiment and the Excess Demand for Used Cars*. Singapore: Springer Singapore, 2020, pp. 113–124. [Online]. Available: https://doi.org/10.1007/978-981-15-0825-7_8

[17] W. Wang and H. Wang, "The research on E-business marketing pattern of second-hand car," in *2010 International Conference on Electrical and Control Engineering*, 2010, pp. 3105–3107.

[18] M. A. Haan and H.-W. de Boer, "Has the internet eliminated regional price differences? evidence from the used car market," *De Economist*, vol. 158, no. 4, pp. 373–386, November 2010.

[19] P. Kooreman and M. A. Haan, "Price anomalies in the used car market," *De Economist*, vol. 154, no. 1, pp. 41–62, March 2006.

[20] M. Rivas-Sánchez, M. P. Guerrero-Lebrero, E. Guerrero, G. Bárcena-Gonzalez, J. Martel, and P. L. Galindo, *Product Matching to Determine the Energy Efficiency of Used Cars Available at Internet Marketplaces*. Cham: Springer International Publishing, 2018, pp. 203–215. [Online]. Available: https://doi.org/10.1007/978-3-319-62359-7_10

[21] C. S. Aksezer, "Failure analysis and warranty modeling of used cars," *Engineering Failure Analysis*, vol. 18, no. 6, pp. 1520–1526, 2011. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1350630711001336

[22] C. Özturan, "Used car salesman problem: A differential auction-barter market," *Annals of Mathematics and Artificial Intelligence*, vol. 44, no. 3, pp. 255–267, July 2005.
[23] Y. Yu, C. Yao, Y. Zhang, and R. Jiang, "Second-hand car trading framework based on blockchain in cloud service environment," in *2021 2nd Asia Conference on Computers and Communications (ACCC)*, 2021, pp. 115–121.
[24] B. Sawicki and M. Scherer, "Learnings from the swiss second-hand car market for e-mobility," in *2020 17th International Conference on the European Energy Market (EEM)*, 2020, pp. 1–6.
[25] V. Sathiya, M. Chinnadurai, S. Ramabalan, and A. Appolloni, "Mobile robots and evolutionary optimization algorithms for green supply chain management in a used-car resale company," *Environment, Development and Sustainability*, vol. 23, no. 6, pp. 9110–9138, June 2021.
[26] A. Papagapiou, J. Mingers, and E. Thanassoulis, "Would you buy a used car with DEA?" *OR Insight*, vol. 10, no. 1, pp. 13–19, January 1997.
[27] A. N. Guda and A. N. Tsurikov, "The artificial neural network application for service-oriented evaluation of the used cars," in *Advances in Automation*, A. A. Radionov and A. S. Karandaev, Eds. Cham: Springer International Publishing, 2020, pp. 965–975.
[28] A. Pehlken, B. Koch, and M. Kalverkamp, "Assessment of reusability of used car part components with support of decision tool RAUPE," in *Cascade Use in Technologies 2018*, A. Pehlken, M. Kalverkamp, and R. Wittstock, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2019, pp. 75–82.
[29] J. Marshall, "Some reflections on second-hand cars:: With hints on their purchase," *The Lancet*, vol. 205, no. 5292, pp. 249–250, 1925, originally published as Volume 1, Issue 5292. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0140673600560322
[30] S. Mbaye, M. Bunel, Y. L'Horty, P. Petit, and L. du Parquet, "Discriminations in the market for "Lemons": A multicriteria correspondence test in france," *Economics of Transportation*, vol. 24, p. 100192, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2212012220301283
[31] F. S. Grodzinsky, K. W. Miller, and M. J. Wolf, "Developing artificial agents worthy of trust: "would you buy a used car from this artificial agent?"," *Ethics and Information Technology*, vol. 13, no. 1, pp. 17–27, March 2011.
[32] X. hai Lu and J. kun Yu, "Research on second-hand car trading system based on blockchain," *Software Guide*, vol. 20, no. 9, pp. 185–190, 2021.
[33] L. Liu, H. Shu, and Y. Zhang, "Operation mechanism of the whole used car industry chain intelligent entrepreneurship and innovation platform," *Industrial Technology and Vocational Education*, vol. 19, no. 2, pp. 114–117, 2021.
[34] Y. Li, "Pay attention to seven problems of online used car trading platform," *China Quality Wan Lixing Magzine*, no. 8, pp. 82–83, 0221.
[35] G. Zhu, F. Zhao, H. Hao, and Z. Liu, "Blockchain technology and its application in automotive field," *Automotive Engineering*, vol. 43, no. 9, pp. 1278–1284, 2021.
[36] S. Wang and Y. Wang, "Research of the reform of second-hand car appraisal and evaluation curriculum," *Heilongjiang Science*, vol. 12, no. 15, pp. 80–81, 2021.
[37] X. Yin and B. Peng, "Curriculum design of used car technology appraisal based on working process," *Internal Combustion Engine and Parts*, no. 15, pp. 250–251, 2021.
[38] X. Yin and S. Lin, "Exploration on the construction of professional curriculum system of used car appraisal and evaluation in vocational schools," *Auto Time*, no. 15, pp. 28–29, 2021.
[39] X. Liu, H. Zou, D. Yue, W. Niu, B. Zhao, and T. Fu, "Research on the teaching reform of the course certificate integration of second-hand car appraisal and evaluation under the background of "1+x" certificate system," *Automobile Applied Technology*, no. 12, pp. 152–154, 2021.
[40] Z. Gao, "Tesla introduces a third-party appraiser to provide old car replacement services," *For Repair and Maintenance*, no. 4, p. 16, 2021.
[41] C. Qiao, "18 new occupations such as beverage dispenser and used car broker 'become regular'," *Modern Youth*, no. 6, pp. 44–46, 2021.
[42] X. Cheng and Q. Song, "On second hand car and its appraisal and evaluation method," *Auto Time*, no. 6, pp. 183–184, 2021.
[43] R. Zhang, "The second-hand appraisal and evaluation based the case analysis," *Auto Time*, no. 6, pp. 185–186, 2021.
[44] "The relevant person in charge of the people's bank of china on notice on preventing and dealing with the risk of speculation in virtual currency transactions," *Financial Accounting*, no. 10, pp. 5–6, September 2021.
[45] Ma, Ling, "Maintain a high-pressure crackdown on virtual currency trading speculation," Financial News, September 2021.
[46] J. Wu and C. Liu, "A study of anonymous delivery based on blind signature scheme," *Procedia Computer Science*, vol. 52, pp. 1065–1070, 2015.
[47] J. Wu, C. Liu, and D. Gardner, "A study of anonymous purchasing based on mobile payment system," *Procedia Computer Science*, vol. 83, pp. 685–689, 2016.
[48] C. Zhang, Y.-Z. Luo, C. Liu, and B. Zhao, "A dynamic passcode system for mobile purchasing without bank card," in *2018 9th International Symposium on Parallel Architectures, Algorithms and Programming (PAAP)*, 2018, pp. 111–113.
[49] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.
[50] T. ElGamal, "A public-key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469–472, 1985.
[51] Y. Lv, C. Liu, and T. Huang, "Research on the university library anonymous customer complaint system based on blockchain technology," *Design Engineering*, no. 2, pp. 681–689, 2021.
[52] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Technology*, vol. IT-22, no. 6, pp. 644–654, 1976.
[53] Wikipedia, "Discrete logarithm," https://en.wikipedia.org/wiki/Discrete_logarithm.
[54] ——, "Computational Diffie-Hellman assumption," https://en.wikipedia.org/wiki/Computational_Diffie-Hellman_assumption.
[55] ——, "Diffie-Hellman key exchange," https://en.wikipedia.org/wiki/Diffie_Hellman_key_exchange.
[56] ——, "Decisional Diffie-Hellman assumption," https://en.wikipedia.org/wiki/Decisional_Diffie-Hellman_assumption.
[57] ——, "Cryptographic hash function," https://en.wikipedia.org/wiki/Cryptographic_hash_function.