Blockchain-Based Approaches for User Reputation on E-Commerce

Subjects: Computer Science, Information Systems

Contributor: Maria José Angélico Gonçalves , Rui Humberto Pereira , Marta Alexandra Guerra Magalhães Coelho

User trust is a fundamental issue in e-commerce. To address this problem, recommendation systems have been widely used in different application domains including social media healthcare, e-commerce, and others. In the literature, on the one hand, blockchain-based reputation systems have been highlighted as possible solutions to effectively provide the necessary transparency, as well as effective identity management. On the other hand, new challenges are posed in terms of user privacy and performance, due to the specific characteristics of the blockchain. According to the literature, two major approaches have been proposed based on public and permissioned blockchains. Each approach applies adjusted models for calculating reputation scores.

reputation system | user reputation | blockchain | blockchain oracles | e-commerce | security

1. Introduction

Nowadays, e-commerce competes in many economic sectors, side by side with traditional commerce. Despite other issues, such as the need to feel and touch a product and shipping costs, lack of trust is one of the greatest barriers to massive adoption of e-commerce. Never before has this aspect been as relevant as it is today due to the acceleration of the digital transition, as a consequence of the global pandemic, in which we have witnessed an increase in the number of e-commerce transactions over the internet [1].

In the context of a commercial transaction, trust and reputation are distinct but related concepts. “Trust is the extent to which one party is willing to depend on something or somebody in a given situation with a feeling of relative security, even though negative consequences are possible” and “reputation is what is generally said or believed about a person’s or thing’s character or standing” [2].

The lack of trust is particularly relevant in B2C and C2C online business models, in which there is no prior relationship (i.e., trust) between the participants, as generally exists in the e-commerce B2B model or in traditional commerce, where a buyer can feel and touch a product. Recommendations and reputation scores have been used to address this problem by helping the user, usually, a buyer, become aware of the risk during a transaction. In general, all online marketplaces (e.g., Amazon and eBay) provide recommendation and reputation data about the user or the product, typically in the form of a score, in order to provide trust to buyers. Consequently, the trust which supports a buyer’s decision to buy a product/service is generally based on the reputation of the product or/and the seller.

2. E-Commerce

Digital transformation along with the widespread adoption of the internet and mobile technologies has resulted in the creation of global markets where buyers and sellers transact for goods and services using different physical and virtual network architectures for offering, creating, and delivering value [3]. E-commerce refers to the sale and purchase of goods and services over the internet, with the transfer of money and data to complete transactions [4]. E-commerce platforms, in addition to selling products, facilitate the discovery of product information, which allows price comparison and decision-making about a purchase and the seller [5].

A company's business model represents its core logic and strategic choices for creating and capturing value within a value network [6]. The e-commerce model includes commercial transactions between buyers and sellers; the main flows of products, services, information, and money; and the main benefits to participants.

There are several e-commerce business models, and more are being created every day [4]; however, despite the abundance of models, it is possible to identify the main models that have been developed for e-commerce. According to Aithal [7], all the major e-commerce business models fall under three key categories: B2B, business-to-business; B2C, business-to-consumer; and C2C, consumer-to-consumer. In B2B, the businesses transact with other businesses. In B2C, business transactions are carried out with individual consumers and include purchasing of retail goods, travel, and other types of online services and content. C2C provides a way for consumers to sell to each other, with the help of an online platform. According to Laudon [4], the most discussed type of e-commerce is B2C commerce.

However, a lack of trust is particularly relevant in B2C and C2C online business models, where there is no prior relationship between the participants, as is usually the case in the B2B e-commerce model or in traditional commerce, where the buyer may know the participants (buyer and seller). Over the past few years, recommendation models and reputation rating rankings have been used to address this problem, helping the user, usually a buyer or seller, to minimize transaction risk. In general, all online marketplaces provide recommendation and reputation data, typically in the form of a score, about the user or product, in order to gain the trust of users.

3. The Role of Trust

Herein, user reputation is the main focus, however, the concepts of trust and risk are important issues. Reputation and trust (or trustworthiness) are commonly confused [8] and used as synonyms, even though their meanings are distinctly different. Josang et al. [2] defined trust as "the extent to which one party is willing to depend on something or somebody in a given situation with a feeling of relative security, even though negative consequences are possible". Risk is often taken in the hope of some gain or benefit. Therefore, risk can be viewed as a situation where the outcome of a transaction is important to a party, yet the probability of failure is not zero [2]. By integrating the two definitions one can conclude the following: The amount of risk a party may be willing to tolerate is directly proportional to the amount of trust it has in the other party.

4. Reputation Systems and Reputation Models

The main purpose of user reputation systems is to establish trust between unknown parties. Based on a reputation model, a reputation system enables the collection, aggregation, and distribution of data about an entity that can, in

turn, be used to identify and predict the future actions of that entity. Using this data, e-commerce users can decide whom they will trust and to what degree. Reputation systems increase or decrease user ratings according to the information collected about the user. They can, therefore, give a positive score, leaving the user with a better ranking, or they can give a negative reputation to punish dishonest behavior. As a result, many online marketplace platforms have developed user reputation management systems that allow trading parties to submit a rating of the counterparty performed in a specific transaction, which is made available to all site visitors. A positive rating of a trading partner is likely to increase trust in the counterparty's performance.

According to Hoffman et al. [9], reputation models are composed of three fundamental dimensions: (1) formulation, (2) calculation, and (3) dissemination. In the formulation dimension, the mathematical basis and input types that feed the model are derived. In the calculation dimension, the algorithm of calculation produces a reputation score from the input data. The latter regards the mechanism that allows system participants to obtain the calculated reputation score.

Regarding the formulation dimension, the authors propose the following types: manual feedback, direct and indirect observations, and inferred data. Reputation systems quantitatively construct sellers' reputations by collecting feedback from buyers with whom the sellers have ever interacted, where feedback is usually presented by a rating that reflects the sellers' performances. The automatic sources are obtained automatically either via direct or indirect observations. In direct observations, automatic sources of information result from data directly observed by an identity, such as the success or failure of an interaction, or the direct observations of cheating. In the case of peer-to-peer (P2P) networks, the measurement of resource utilization is done by neighbors. Information that is obtained second hand or is inferred from first-hand information is classified as indirect. Liu et al. [10] proposed the (3R) model that incorporated observations, based on a buyer's repurchase/product return behavior information, into the calculation dimension in order to mitigate the negative impact of biased ratings.

Hendrikx et al. [11] proposed two families of reputation systems, explicit and implicit reputation systems. According to the authors, on the one hand, explicit systems have models that follow the same aforementioned principles and dimensions, in which a formulation and calculation have been explicitly defined. On the other hand, the implicit systems are not implemented in network services, but conceptually there is a model of reputation. As examples, the authors give social networks, such as Facebook or LinkedIn, and the Google search engine. In the first case, trust/reputation is inferred through relationships, i.e., friends of friends, while in the search engines, reputation is determined by the number of links that point to the page, and where the links originate. These are examples of automatic observations and inferred data that can enrich the model formulation in the explicit reputation models.

5. Common Vulnerabilities of Reputation Systems for E-Commerce

The rapid growth of e-commerce platforms and their extensive use and dependence on their reputation systems have led to various types of malicious behaviors and threats.

Dellarocas [12] identified two problems related to a major approach for deriving users' reputations based on feedback: (1) unfair ratings by buyers and (2) discriminatory seller behavior. In the first case, two types of fraud can occur: Ballot-

stuffing fraud, an attack where members positively rate themselves on fake (unfair) transactions in order to inflate their reputation and bad-mouthing fraud as a result of an attack where members misclassify others to deflate their reputation. These attacks are orchestrated in a collusion of a seller, or a group, and buyers. In discriminatory behavior, the seller strategically provides good service to a group of users and bad service to others, in order to gain benefits from that asymmetry of product/service quality. According to Panagopoulos [13], the most common threats against reputation systems include ballot-stuffing, bad-mouthing, and traitor attacks. The traitor attack is a type of attack where members exploit their reputation by tricking others until their reputation dissolves.

The author also mentions that the reputation systems use a much larger population sample than in the past and this fact may cause greater measurement bias from users who do not leave feedback on their transactions.

Following a suggestion by Brian Zill, Douceur [14] proposed the term *Sybil* attack in the context of P2P networks. In this type of attack to reputation systems, an entity forges multiple identities in the system, using it in collusion as a means to increase its influence. Whitewashing is another vulnerability in the identity management scope. In this type of behavior, an e-commerce user with a bad reputation can easily create a new identity and continue his activity without any consequence of his past transactions.

The architecture of the reputation system has also been subject to criticism due to vulnerabilities when centralized or distributed. According to Zulfiqar et al. [15], central authorities can potentially filter, tamper, add, or reject product reviews based on their preference. Schaub et al. [16] pointed out the same issues since, potentially, a centralized system can be abused by the central authority. Dhakal and Cui [17] presented the same arguments, stating that the current centralized systems are silos and non-transparent in the review process. In addition to the lack of transparency, these isolated centralized systems do not benefit from the reputation data of each other. Regarding the attacks based on the limitations of identity management, such as whitewashing and Sybil, Zeynalvand et al. [18] stated that it was hard to derive a robust model if users did not share information. However, in the case of decentralized systems, nodes could potentially manipulate the data users shared in the network, even if it was encrypted or signed. The researchers consider these issues to be a major problem, regarding the lack of transparency of reputation data, as well as a major difficulty to derive a robust reputation model.

6. Blockchain Technology

Over time, reputation systems have been widely implemented in e-commerce applications [19]. As already mentioned, reputation information can be stored in a decentralized or centralized manner. Decentralized storage of information, that is, shared from one node to the others in a distributed system, has advantages; however, it also has several challenges, such as those discussed in the previous section, which allow for ballot-stuffing and bad-mouthing frauds. These drawbacks render reputation systems useless since they cannot ensure the integrity of trust ratings, prevent data manipulation, and provide reliable mechanisms to support effective user identity management.

According to the recent literature, blockchain-based approaches to reputation systems may be capable of addressing these problems. Blockchain is the primary technology for Bitcoin and other digital currencies [20]. Stakeholders such as developers, entrepreneurs, and technologists claim blockchain technology has the potential to reconfigure the

contemporary economic, legal, political, and cultural landscape. A smart contract removes the need to build trust between individuals and organizations through intermediaries such as lawyers, and social activities such as meetings, where actors get to know one another. Smart contracts build the transactional relationship of a contract into a technical code that is executed automatically.

As noted by Sherman [21], blockchains are a way of changing the way online reputation systems are managed. By integrating a proof-of-individuality framework into the verification system, a blockchain model protects against attacks and prevents scenarios such as spoofing, creating multiple identities, and manipulating scores. This technology has driven researchers to make new advances in continuing to perform processing efficiently. However, we should note that some issues cannot be directly addressed by the blockchain paradigm, such as false and unfair ratings, discriminatory behaviors, and the "bias towards positive ratings" [2] explained as positive ratings as an exchange of courtesies or given in the hope of getting a positive rating in return, and negative ratings that are avoided because of fear of retaliation from another party. These problems are already known in the literature as the blockchain oracle problem [22][23][24][25].

As more and more people rely on online services and communities, user reputation systems will continue to play an increasingly important role in facilitating their interactions. It is already clear that online services can play a profound role in business. Therefore, implementing robust user reputation systems is crucial.

References

1. Settey, T.; Gnap, J.; Beňová, D.; Pavličko, M.; Blažeková, O. The Growth of E-Commerce Due to COVID-19 and the Need for Urban Logistics Centers Using Electric Vehicles: Bratislava Case Study. Sustainability 2021, 13, 5357.
2. Jøsang, A.; Ismail, R.; Boyd, C. A survey of trust and reputation systems for online service provision. Decis. Support Syst. 2007, 43, 618–644.
3. Goyal, S.; Sergi, B.S.; Esposito, M. Literature review of emerging trends and future directions of e-commerce in global business landscape. World Rev. Entrep. Manag. Sustain. Dev. 2019, 15, 226–255.
4. Laudon, K.C.; Traver, C.G. E-Commerce: Business, Technology, Society, 2nd ed.; Pearson: Upper Saddle River, NJ, USA, 2019.
5. Ghandour, A. Ecommerce website value model for SMEs. Int. J. Electron. Commer. Stud. 2015, 6, 203–222.
6. Shafer, S.M.; Smith, H.J.; Linder, J.C. The power of business models. Bus. Horiz. 2005, 48, 199–207.
7. Aithal, P.S. A Review on Various E-Business and M-Business Models & Research Opportunities. Int. J. Manag. IT Eng. 2016, 6, 275–298.

8. Mui, L.; Mohtashemi, M.; Halberstadt, A. Notions of reputation in multi-agents systems: A review. In AAMAS'02, Proceedings of the First International Joint Conference on Autonomous Agents and Multiagent Systems: Part 1, Bologna, Italy, 15–19 July 2002; Association for Computing Machinery: New York, NY, USA, 2009; pp. 280–287.
9. Hoffman, K.; Zage, D.; Nita-Rotaru, C. A survey of attack and defense techniques for reputation systems. ACM Comput. Surv. 2009, 42, 1–31.
10. Liu, Y.; Zhou, X.; Yu, H. 3R model: A post-purchase context-aware reputation model to mitigate unfair ratings in e-commerce. Knowl. Based Syst. 2021, 231, 107441.
11. Hendrikx, F.; Bubendorfer, K.; Chard, R. Reputation systems: A survey and taxonomy. J. Parallel Distrib. Comput. 2015, 75, 184–197.
12. Dellarocas, C. Mechanisms for coping with unfair ratings and discriminatory behavior in online reputation reporting systems. In ICIS'00, Proceedings of the Twenty-First International Conference on Information Systems, Atlanta, GA, USA, 10-13 December 2000; Association for Information Systems: Brisbane, Australia; pp. 520–525.
13. Panagopoulos, A.; Koutrouli, E.; Tsalgatidou, A. Modeling and evaluating a robust feedback-based reputation system for e-commerce platforms. ACM Trans. Web 2017, 11, 1–55.
14. Douceur, J.R. The Sybil Attack. In Lecture Notes in Computer Science, Proceedings of the International Workshop on Peer-to-Peer Systems, Cambridge, MA, USA, 7–8 March 2002; Druschel, P., Kaashoek, F., Rowstron, A., Eds.; Springer: Berlin/Heidelberg, Germany, 2002; Volume 2429.
15. Zulfiqar, M.; Tariq, F.; Janjua, M.U.; Mian, A.N.; Qayyum, A.; Qadir, J.; Sher, F.; Hassan, M. EthReview: An Ethereum-based Product Review System for Mitigating Rating Frauds. Comput. Secure. 2021, 100, 102094.
16. Schaub, A.; Bazin, R.; Hasan, O.; Brunie, L. A Trustless Privacy-Preserving Reputation System. In ICT Systems Security and Privacy Protection, Proceedings of the International Conference, Ghent, Belgium, 30 May–1 June 2016; Springer: Berlin/Heidelberg, Germany; pp. 398–411.
17. Dhakal, A.; Cui, X. DTrust: A Decentralized Reputation System for E-commerce Marketplaces. 2019. Available online: https://www.researchgate.net/publication/332672141_DTrust_A_Decentralized_Reputation_System_for_E-commerce_Marketplaces (accessed on 10 May 2021).
18. Zeynalvand, L.; Luo, T.; Andrejczuk, E.; Niyato, D.; Teo, S.G.; Zhang, J. A Blockchain-Enabled Quantitative Approach to Trust and Reputation Management with Sparse Evidence. In AAMAS'21, Proceedings of the 20th International Conference on Autonomous Agents and MultiAgent Systems, 3–7 May 2021; International Foundation for Autonomous Agents and Multiagent Systems: Richland, SC, USA, 2021.
19. Christidis, K.; Devetsikiotis, M. Blockchains and smart contracts for the internet of things. IEEE Access 2016, 4, 2292–2303.

20. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Available online: www.bitcoin.org (accessed on 22 May 2021).
21. Sherman, L. A Decentralized Reputation System: How Blockchain Can Restore Trust In Online Markets. 2018. Available online: https://www.forbes.com/sites/shermanlee/2018/08/13/a-decentralized-reputation-system-how-blockchain-can-restore-trust-in-online-markets/#70b74337481 (accessed on 28 May 2021).
22. Damjan, M. The interface between blockchain and the real world. Region Prat. 2018, 2018, 379–406.
23. Egberts, A. The Oracle Problem-An Analysis of how Blockchain Oracles Undermine the Advantages of Decentralized Ledger Systems. SSRN Electron. J. 2017.
24. Frankenreiter, J. The Limits of Smart Contracts. J. Inst. Theor. Econ. 2019, 175, 149–162.
25. Caldarelli, G. Understanding the Blockchain Oracle Problem: A Call for Action. Information 2020, 11, 509.