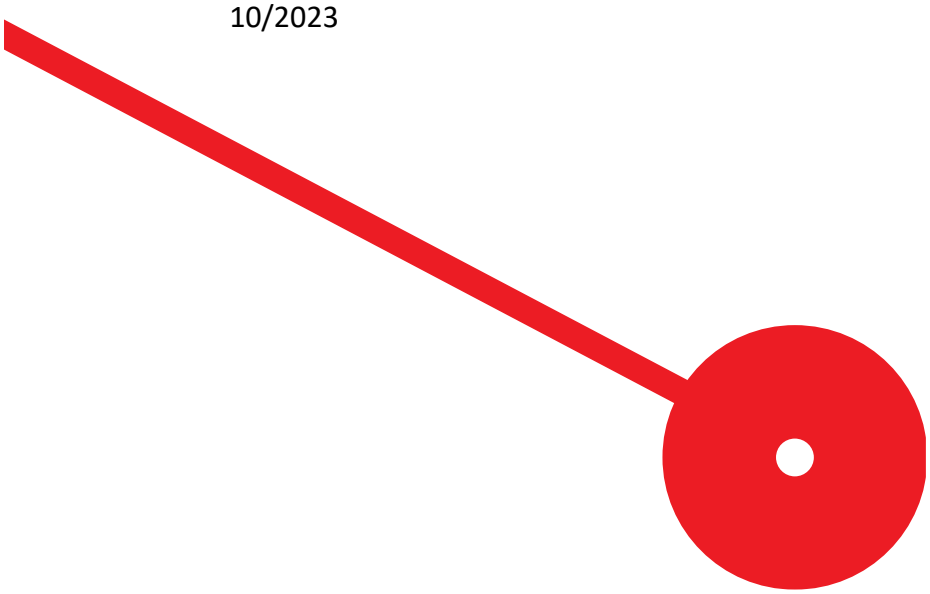
INSTITUTO
SUPERIOR
DE CONTABILIDADE
E ADMINISTRAÇÃO
DO PORTO
POLITÉCNICO
DO PORTO

M MASTER'S
Electronic Business

Blockchain-based Reputation Models for E-commerce – A systematic literature review

Marta Alexandra Guerra Magalhães Coelho

10/2023



Nome. Blockchain-based Reputation Models for E-commerce – A systematic literature review 10/2023

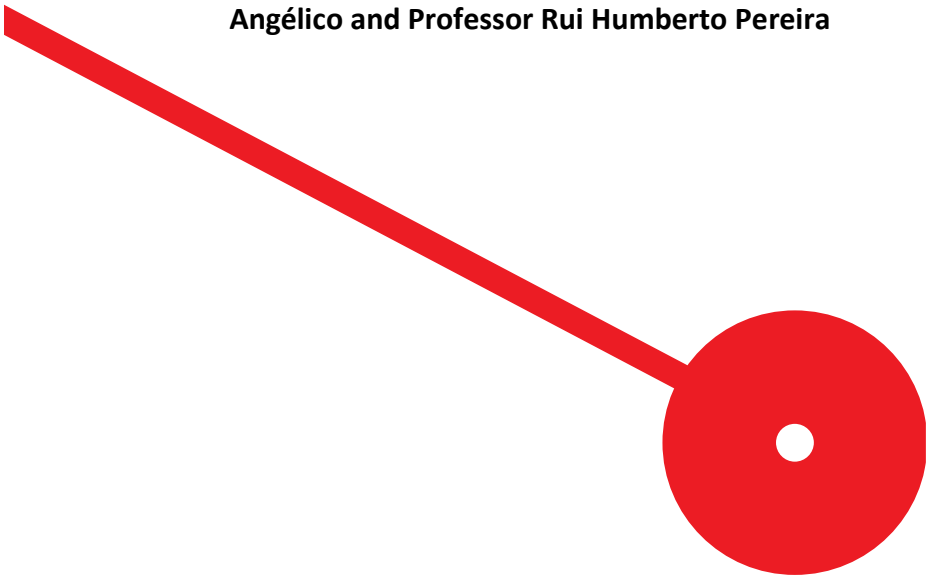
INSTITUTO
SUPERIOR
DE CONTABILIDADE
E ADMINISTRAÇÃO
DO PORTO
POLITÉCNICO
DO PORTO

M MASTER'S
Electronic Business

Blockchain-based Reputation Models for E-commerce – A systematic literature review

Marta Alexandra Guerra Magalhães Coelho

Master's Dissertation presented to Instituto Superior de Contabilidade e Administração do Porto to obtain the degree of Master in e-Business, under the guidance of Professor Maria José Angélico and Professor Rui Humberto Pereira



Nome. Blockchain-based Reputation Models for E-commerce – A systematic literature review 10/2023

Acknowledgements

I want to thank, first and foremost, my family and my close friends.

I want to thank my teachers for all the help and, specifically, my adviser professors for guiding me and for the patience they demonstrated towards me.

Last but certainly not least, thank you, my colleagues, for making this journey so much fun.

Abstract:

The Digital Age is the present, and nobody can deny that. With it has come a digital transformation in various sectors of activity, and e-commerce is no exception. Over the last few decades, there has been a massive increase in its utilization rates, as it has several advantages over traditional commerce. At the same time, the rise in the number of crimes on the Internet and, consequently, the understanding of the risks involved in online shopping has led consumers to become more cautious, looking for information about the seller and taking it into account when making a purchase decision.

The need to get to know the merchant better before making a purchase decision has encouraged the creation of reputation systems, whose services play an essential role in today's e-commerce context. Reputation systems act as mechanisms to reduce information asymmetry between consumers and sellers and establish rankings that attest to fulfilling standards and policies considered necessary for shops operating in the digital market.

The critical problems in current reputation systems are the frauds and attacks that such systems currently have to deal with, which results in a lack of trust between users.

These security and fraud issues are critical because users' trust is commonly based on reputation models, and many of these current systems are not immune to them, thus compromising e-commerce growth. The need for a better and safer model emerges with the development of e-commerce. Through reading the articles and pursuing the answers to the primary questions, blockchain is data register technology to be analysed in order to gain a better acknowledgment of the potential of such technology. More research work and investigation must be done to fully understand how to create a more assertive reputation model.

Thus, this study systematizes the knowledge generated by reputation models in E-commerce studies in Scopus, WoS databases, and Google Scholar, using PRISMA methodology.

A systematic approach was adopted in conducting a literature review. The need for a systematic literature review came from the knowledge that there are reputation systems that mitigate some of the problems. In addition to identifying some indicators used in reputation models, we also conclude that these models could help provide some insurance

to buyers and sellers, with a commitment to being a problem solver, being able to mitigate known problems such as Collusion, Sybil attacks, laundering attacks, and preventing online fraud ranging from ballot stuffing and bad-mouthing. Nevertheless, the results of the present work demonstrate that even though these reputation models still cannot solve all of the problems, attacking one fraud opens the door to an attack. The architecture of the models was identified, with the realization that a few lacks that need to be fulfilled.

Key words: Ecommerce; Reputation Model; Security; Blockchain

INDEX

Chapter I - Introduction 10

Chapter II – Theoretical Background 14

2.1 E-Commerce 15

2.2 Security and trust 15

2.3 Reputation Systems and Reputation models 16

2.4 Blockchain architecture 18

Chapter I I I – Methodology 21

3.1 Definition of research questions 25

3.2 Conducting the search 26

3.2.1 Identification 26

3.2.2 - Screening and selection of relevant articles 27

IV – Discussion and Results Presentation 32

4.1 Papers Discussion 33

4.2 Literature review summary 50

Chapter V – Blockchain based Reputation Model guidelines 52

5.1 Attacks and frauds 53

5.2 Reputation models 54

5.3 Why blockchain 56

5.4 Public vs. Private Blockchain 58

5.5 The appropriate blockchain for reputation models on e-commerce 60

5.6 Reputation model Guidelines 61

Chapter VI – Conclusion 64

Bibliographic References 68

Webgraphy References 77

Appendages 79

FIGURE INDEX

Figure 1 - PRISMA flowchart https://www.prisma-statement.org/ 24
Figure 2 - Steps followed in the systematic review..... 28

TABLE INDEX

Table 1 - Selected Articles..... 28
Table 2 - Which is the Best Blockchain? 60

Abbreviations

ARNE – Average Received Normalized Evaluation

BFT – Byzantine Fault Tolerance

CA – Certificate Authority

CBC – Consortium Blockchain

CRS – Centralized Reputation Systems

DApps - Decentralized Applications

DHT – Distributed Hash Tables

DPoS – Delegated Proof-of-Stake

DTR – Direct Trust

EVM – Ethereum Virtual Machine

IPFS – Interplanetary File System

IR – Individual Rational

ITR – Indirect Trust

NE – Normalized Evaluation

P2P – Peer-to-Peer

PBFT – Practical Byzantine Fault Tolerance

PEC – Personal Evaluation Criteria

PoR – Proof of Reputation

PoS – Proof-of-Stake

PoW – Proof-of-Work

PRISMA - Preferred Reporting Items for Systematic Reviews and Meta-Analyses

TDW – Time Difference Weight

TMS – Trust Management Systems

TPS – Transaction per second

TRM – Trust and Reputation Management

The buying and selling of products and services online is referred to as electronic commerce or e-commerce. It is revolutionizing how people conduct business, and its growth over the years has been remarkable. E-commerce has enabled businesses to reach a wider audience and has provided customers with the convenience of shopping from the comfort of their homes.

The growth of e-commerce can be traced back to the 1990s, with the development of the Internet. However, it was in the 2000s that e-commerce gained widespread popularity. The introduction of secure payment gateways, faster internet speeds, richness of contents, and the proliferation of mobile devices have all contributed to the growth of e-commerce.

According to statista.com[1], a website that shares information and statistics, global e-commerce sales amounted to $4.11 trillion in 2023 and are projected to reach $6.35 trillion by 2027. This growth can be attributed to several factors, including the increasing popularity of mobile commerce, the rise of social media marketing, and the shift towards online shopping due to the COVID-19 pandemic. (Gu et al., 2021)

E-commerce has also transformed various industries, including retail, travel, and entertainment. Retail giants like Amazon and Alibaba have disrupted traditional brick-and-mortar stores, while online streaming platforms like Netflix have revolutionized the entertainment industry.

Despite its technological evolution, growth, and popularity, several challenges and problems still need to be solved. One of these significant challenges is the lack of trust. Buyers and sellers need to trust each other to conduct business online. In general, reputation management is addressed with reputation systems, which track user activity, giving his reputation score to help other users trust him.

In e-commerce, trust is what a buyer is looking for for when going through the reviews and feedback of others. It is especially important to maintain reliable feedback from other users. Unfortunately, as is known, we can expect certain frauds, such as bad-mouthing, where members misclassify others to deflate their reputation, and attacks as collusion (Gonçalves et al., 2022), that is when the seller strategically provides a good service to a group of users and bad services to others, to get benefits of that asymmetry

[1] https://www.statista.com/outlook/dmo/ecommerce/worldwide

of product/service quality (Gonçalves et al., 2022), and Sybil attacks, where an entity forges multiple identities in the system, using it in collusion as a mean to increase his influence (Gonçalves et al., 2022) to lower the rating of a seller and/or product. M. Soleimani, (2022). This example demonstrates how confidence is essential to computer-mediated processes and transactions. However, because computerized communication technologies are progressively distancing us from established modes of engagement, it can be challenging to judge the reliability of distant entities. People can evaluate a considerably greater range of cues related to reliability through physical interaction and conventional means of communication than is now possible through computer-mediated communication. A typical brick-and-mortar street presence requires financial effort, which gives some comfort that those undertaking it are serious participants. This starkly contrasts the relative ease and low expense of creating a professional-looking online presence, which reveals little about the confidence of the organization supporting it. It can be challenging to tell which Internet service providers are trustable and which are of low quality because it is tough to gather information concerning unidentified transaction partners. As a result, both the academia and the e-commerce sector are paying close attention to trust in open computer networks. (Jøsang et al., 2007)

Reputation systems support to build trust between buyers and sellers. They allow users to rate and review products and sellers based on their personal experience, thereby creating a reputation score that can be used to evaluate the trustworthiness of a seller or a buyer. Reputation systems are crucial for e-commerce platforms as they help weed out bad actors and ensure that transactions are conducted safely and trustworthy.

Based on the user's prior encounters with other people, a reputation system gathers, accumulates, and disseminates feedback about the behaviour or reputation of the user. Digital reputations present a promising mechanism to build trust between strangers on the Internet and facilitate transactions, much like real-world markets where personal or corporate reputations play a vital role in pricing commodities and launching transactions. (Swamynathan et al., 2010)

With that said, the purpose of this literature review is to study the problems that e-commerce platforms suffer most with, such as frauds, that are a consequence of the fragility they have to some types of attacks, mainly due to the centralized architecture of the current reputation systems. A systematic literature review took place to understand the problem better. The existing reputation systems and models to address those problems

are discussed in the present work. After a prior study of the literature, we found that blockchain-based systems potentially can mitigate many of the known fragilities; thus, motivating us to focus our literature review on blockchain-based reputation systems.

Blockchain has been brought up in several articles, so scientific research has that keyword in mind and searched reputation models based on blockchain. Z. Zhou et al. (2020) stated that the results of their study about a blockchain-based decentralized reputation system showed reliability and usability.

So, in this dissertation, chapter II presents the main concepts of the area of investigation, the identification of security problems, reputation models, and the blockchain technology that is used as a solution to minimize the problems, even doe, as stated before, it needs more investigation and research. The methodologic approach followed this in Chapter III, where the main research questions were identified, how the search was conducted, and how the selection of the articles was managed.

Chapter IV discusses these articles in the state of the art. The discussion focuses on the current reputation models or systems and how they work daily.

Chapter V will specify the variables, e.g., guidelines, necessary for a blockchain reputation system. This chapter will clarify the benefits of such a reputation system in more detail.

The dissertation will end with the conclusions from the systematic literature review and some pointers to a future direction this work can take in chapter VI.

To clarify and for a better understanding of the purpose of this dissertation, the main concepts and strategies adopted to solve the problems e-commerce faces are presented. In addition, a glossary will be presented as an appendage II.

2.1 E-Commerce

E-commerce is the direct sale of goods or services to a customer via the internet through a vendor's website. The gateway accepts payments via credit card, debit card, or electronic fund transfer using a wireless shopping cart or shopping basket.

In commercial transactions, electronic communications and digital information processes are used to establish, alter, and redefine value-generating relationships between organizations and people. (Bhumika et al., 2022)

Lauden & Traver (2020 – pp. 45), said that e-commerce is Using applications or browsers running on the Internet, the web, or mobile devices to conduct business transactions.More formally, it is digitalized commerce between individuals and organizations and between organizations.

2.2 Security and trust

By enhancing the security, privacy, and ownership of the data, decentralized data storage will assist in removing the most common types of data failures and outages. (Ali et al., 2018)

Trust and reputation are two separate yet linked ideas. Jsang et al. (2007) make a distinction between "Decision trust" and "Reliability trust." The author uses the definition put forth in (Gambetta, 1988) in the first notion. However, the authors believe that the idea of trust is more nuanced, describing it as follows: Decision trust: "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" (Jøsang et al., 2007, p. 620). According to the Concise Oxford Dictionary, the same writers' definition of repute is as follows: "Reputation is generally said or believed about a person's or thing's character or standing" (Jøsang et al., 2007, p. 620). Therefore, the decision to proceed with an e-commerce transaction is based on two subjective concepts—trust and reputation—while tolerating a certain amount of risk.

This finding enables us to pinpoint the initial drawback of reputation systems. Additionally, it is critical to have a method to ensure that a user can only have one identity and cannot open multiple accounts.

Sybil attacks are typically used in conjunction with Collusion assaults, where the seller strategically provides an excellent service to a group of users and inadequate services to others to get benefits of that asymmetry of product/service quality. (Druschel et al., 2002)

Whether in sybil attacks, collusion attacks, or traitor attacks, members exploit their reputation by tricking others until their reputation dissolves. The centralization of the information is one of the reasons this happens, and one user must have the information on every marketplace to guarantee an outstanding reputation, bringing us back to the need for a software/platform that can store a massive amount of information and be decentralized.

An e-commerce user with a bad reputation can easily create a new identity and continue his activity without any consequences of past transactions. This is a common way to bend the rules and continue the activity, and this knowledge needs to be more secure when online shopping; this is called whitewashing. Gonçalves et al,. (2022).

A ballot-stuffing attack is where members positively rate themselves on fake and unfair transactions to inflate their reputation. (Panagopoulos et al., 2017)

It is essential to guarantee that the transaction information is accurate and that it cannot be adulterer, and one should not be able to rate themselves or try to influence a third party in a positive way.

When members misclassify others to deflate their reputation, it is bad-mouthing. (Panagopoulos et al., 2017)

Even though the reputation models address many of the problems, some issues remain to be solved. In our literature review, we will be able to understand that better.

2.3 Reputation Systems and Reputation models

E-commerce platforms and marketplaces allow the discovery and transaction of product information, which allows price comparison and decision-making about the

purchase. J. Theor (2021). These transactions require a guarantee of some security. Here, the reputation models, which are the basis of reputation systems, are entered.

As a result, many online marketplace platforms have developed user reputation management systems that allow trading parties to submit a rating of the counterparty's performance in a single transaction, which will be visible to all site users. However, a mediator, usually the platform manager, can moderate the reviews.

A positive rating for my trading partner will likely boost my faith in the counterparty's performance. (Jøsang et al., 2007).

The primary purpose of a reputation system is to prevent frauds to which a user is vulnerable. Attacks are malicious activities that attempt to collect, disrupt, deny, degrade, or destroy information system resources or the information itself. In the case of e-commerce, the attacks intend to degrade or increase a seller's/product's reputation. Saeed, (2023).

As mentioned , attacks, with the intent of fraud, have one intent: to decrease the reputation of a seller or product (being the seller is the part focused on this dissertation, but it must be said that the buyer can also be at the receiving end of attacks and frauds, making them untrusty for the seller).

Understanding the most common attacks is crucial. One of the most common and mentioned in most articles is Sybil Attack, when an entity forges multiple identities in the system, using it in collusion to increase its influence.

The primary goal of user reputation systems is to build confidence between unknown people. A reputation system based on a reputation model enables the gathering, analysing, and distributing of data about an entity, which may then be used to identify and forecast that entity's future activities.

Reputation systems are divided into implicit and explicit systems. Systems without a clearly defined reputation system are implicit, even though their members use reputation data to aid decision-making. Examples of these reputation-based strategies may be seen in social networks (such as Facebook and LinkedIn), where we can infer a certain level of reliability from the data obtained through friends of friends. Another illustration is the Google search engine, where the order of the search results corresponds

to a rating of pages depending on each page's reputation. The quantity and nature of links pointing to a page are indicators of its repute (Hendrikx et al., 2015).

Reputation helps to build trust in e-commerce in several ways. Atif, Y. (2002) Firstly, it provides buyers and sellers with a measure of the other party's trustworthiness before engaging in a transaction. This can reduce the risk of fraud and increase the likelihood of successful transactions.

Secondly, reputation can act as a deterrent to fraudulent activities. Sellers with a good reputation are less likely to engage in fraudulent activities as this can damage their reputation and lead to negative feedback.

Finally, reputation can help to build long-term relationships between buyers and sellers. Buyers are more likely to return to sellers with a good reputation, and sellers are more likely to sell to buyers with a good reputation. This can lead to repeat business and increased customer loyalty. (Soleimani, 2021)

Contrarily, explicit reputation systems have established a paradigm that makes estimating a reputation using a score possible. The current paper focuses on these later.

The three aspects of the reputation estimation model are (1) data sources and types, (2) the algorithm based on calculations, and (3) the format of the output for the reputation score and its dissemination. Formulation, Calculation, and Dissemination are the names the writers give to these three dimensions (Hoffman et al., 2009).

The model's efficacy and the kinds of threats it is resistant to play a role in how accurate the reputation score is. The model's architecture, a central or distributed system, is another feature.

The highlighted elements are systematized and explored in other publications on the second level of the taxonomy given by Hendrikx et al. (2015) (Hoffman et al., 2009).

2.4 Blockchain architecture

There is common sense in what blockchain is, and most authors agree that it is a digital ledger of transactions that uses cryptography to secure and validate transactions. It is decentralized, meaning it is not controlled by a single entity and is maintained and updated by a network of computers worldwide. The most well-known example and

successful blockchain technology is Bitcoin, a decentralized digital currency that uses a blockchain to record transactions. S. Nakamoto., (2019).

One of the key features of blockchain technology is its immutability, meaning that once a block of transactions is added to the chain, it cannot be altered or deleted. This provides high transparency and security for the data stored on the blockchain.

This might be the main reason blockchain is considered one reliable software to keep the data information necessary for a transaction and potentialize a seller's trustworthiness.

Blockchain technology is still fragmented, with different blockchain networks operating in silos. Currently, there needs to be an easy way for these networks to communicate with one another, which limits their usefulness in some applications.

Blockchain has significant limitations, such as high energy consumption, particularly in the case of proof-of-work (PoW) consensus mechanisms. This has led to concerns about the environmental impact of blockchain, and efforts are underway to develop more energy-efficient consensus mechanisms.

Blockchain is a peer-to-peer distributed ledger in which cryptographic hash links and secures entries known as blocks. Blockchains are ideal for record management tasks, including financial transactions, identity management, provenance, and authentication, since they are decentralized, secure, immutable, and highly fault-tolerant by design. Blockchain can be used as a permission or permissionless blockchain, such as the Hyperledger Project by The Linux Foundation. The system actors in a permissionless or public blockchain are unknown. The blockchain network allows anyone to join or leave at any time, which could pose security vulnerabilities to the system. (Ali et al., 2018)

However, only a known and identifiable group of players are explicitly admitted to the blockchain network in a permissioned or private blockchain. As a result, there are fewer bad actors in the network. As a result, the network's security is increased to meet the needs of enterprise applications by allowing only authenticated and authorized actors to participate. (Ali et al., 2018)

Particularly for non-financial use cases (other than cryptocurrencies), where users are authenticated and authorized to participate in the network, the permissioned blockchain garners much attention. Health, government services, supply chain

management, the Internet of Things, peer-to-peer cloud storage, and many more interesting non-financial industries are among those that take advantage of permissioned blockchains' capabilities. A fascinating use of blockchain is P2P cloud storage, which offers a decentralized data storage facility without utilizing a client-server architecture or any trusted third parties (e.g., STORJ1, Sia2, Filecoin3).

Any investigation process must be sustained in a search of previous works, to have a clear understanding of the evolution of the matter in question.

Cardoso, Alarcão, and Celorico (2010) states that every investigator must analyse in detail the previous investigators, and only after they have a clear understanding of the issue, they can start their own adventure.

For Webster and Watson (2002), literature review authors may come from research processes that result in substantial progress positioning the author to convey findings to their peers and outline ways forward to achieve better outcomes and from scholars who have completed a literature review prior to the start of the project and have developed some theoretical conceptualization derived from this assessment.

With that being said, a systematic review of the scientific literature on blockchain technology in user reputation systems was made, so the author of this dissertation, and scientific community could gain a better acknowledgment of the issue in study and to understand the technological evolution in this area.

Systematic reviews are a form of meta-analysis designed to collect, investigate, and summarise what is known and what is not known about a "specific practice-related question." Systematic reviews are used across a broad range of disciplines and qualitative studies have established a place for themselves within the methodology, as evidenced by initiatives such as the Cochrane qualitative methods group and textbooks such as Systematic Reviews in the Social Sciences and An Introduction to Systematic Reviews.

Guidance on the synthesis of qualitative and mixed-method implementation evidence is developed and published by the Cochrane Qualitative and Implementation Methods Group. When creating a strict protocol and carrying out the synthesis, selecting suitable approaches, methods, and tools is crucial. To respond to queries with a comparable structure, Cochrane authors who perform qualitative evidence syntheses have thus far employed a restricted number of straightforward techniques. Cochrane has made investments in methodological work to create new tools and support the creation of model reviews to highlight the benefits of more creative approaches that can handle a wider range of issues. We offer revised recommendations on the choice of tools to evaluate methodological limits in qualitative investigations and procedures to collect and synthesize qualitative information in this paper, the latest in a series (Noyes et al., 2018).

The purpose of these guidelines is to assist review authors in carrying out a qualitative synthesis of evidence, which is subsequently integrated with the results of one or more Cochrane reviews of the effectiveness of similar interventions.

Examination of intervention effects can be performed simultaneously with qualitative evidence synthesis or separately (Noyes et al., 2018).

In this study, in addition to following the primary objectives of the systematic review as defined by J. Frizzo-Barker, et al. out of PRISMA, we also support the paper through the theoretical perspective of disruptive innovations and diffusion of innovations to analyse our findings presented in chapter 4. Systematic reviews have several positive features for the social sciences. A systematic review is an effective exploratory methodology.

This methodology was used in recent papers developed to give awareness of reputation models, reputation systems and reputation security, articles such as: Reputation Systems: A framework for attacks and frauds classification, (Pereira et al., 2023) and User Reputation on E-Commerce: Blockchain-Based Approaches, (Gonçalves et al., 2022).

After deeper research about methodological approaches to a literature review, PRISMA came as the best approach for the area in study, also being a methodology very use in the technological area. PRISMA stands for Preferred Reporting Items for Systematic Reviews and Meta-Analyses.

In Figure 1, we present the flowchart that contains the phases of PRISMA:

1. **Identification**: The first thing to do is to identify the relevant studies from different sources. You may find the relevant studies from Google Schola, IEEE Explore, ISI Web of Knowledge, Scopus, Elsevier, and Springer, that contain the most relevant research articles. In this phase, mention the number of records a) Identified from databases, registers, websites, organizations, and other sources respectively b) Removed before screening (duplicate records removed, ineligible records discarded by automation tools, records removed for other reasons)

2. **Screening:** In this phase, mention the number of records a) Screened and excluded b) Retrieved and not-retrieved c) Assessed for eligibility and

records excluded for various reasons (mention the reasons and respective number of records excluded for each reason)

3. **Included:** Lastly, mention the total number of records included in your final systematic review here.

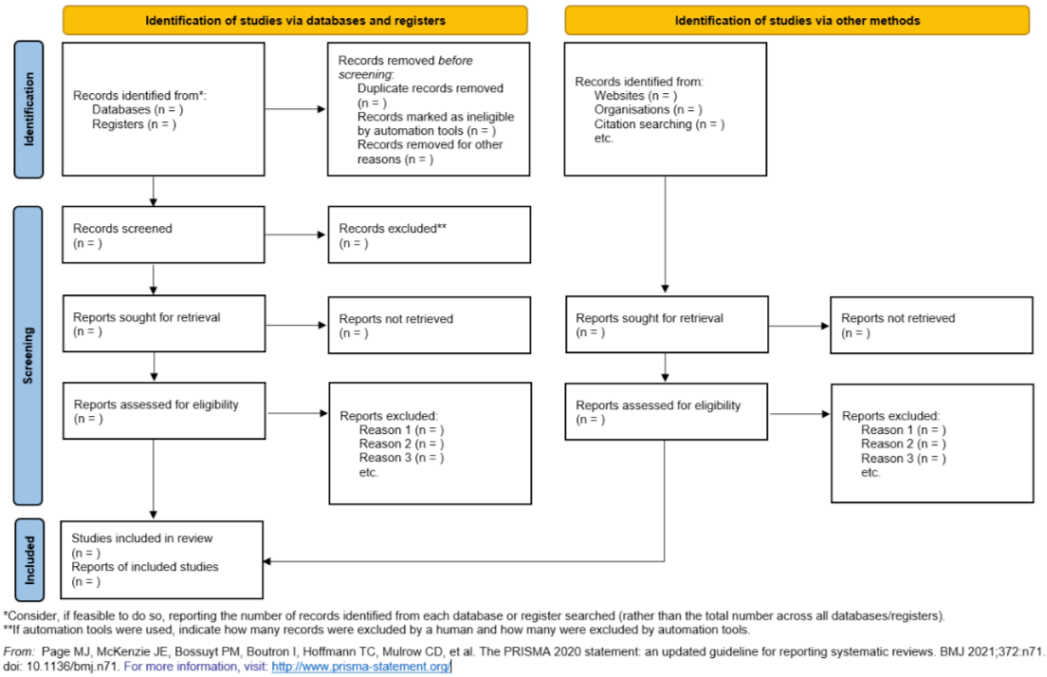


Figure 1 - PRISMA flowchart https://www.prisma-statement.org/

PRISMA has a 27 checklist items in total, that must be included in a systematic review, here it will be presented the summarized checklist (N. Tahsin, 2022):

1. **Title:** According to the PRISMA checklist, your Systematic Literature review document should contain an appropriate title that identify the report as a systematic review.

2. **Abstract:** Your document should contain a proper abstract.
3. **Introduction:** In the introduction section, you should describe the *rationale* for the review in the context of existing knowledge and provide an explicit statement of the *objective*(s) or question(s) the review addresses.
4. **Methods:** This section should contain the Eligibility criteria, Information sources, Search strategy, Selection process, Data collection process, Data items, Study risk of bias assessment, Effect measures, Synthesis methods,

Process of reporting bias assessment and certainty assessment. Detail about each of the items can be accessed from here.

5. **Results:** This section should contain Study selection process, Study characteristics, Risk of bias in studies, Results of individual studies, Results of syntheses, Reporting biases and Certainty of evidence.
6. **Discussion:** Present the general interpretation of the results, limitations of the evidence included in the review, limitations of the review processes used, implications of the results for practice, policy, and future research in this section.
7. **Other information:** Registration and protocol, support, competing interests, Availability of data, code and other materials should be put here.

There are some steps to conducting a systematic review. In the first step of the methodology, several research questions are defined to be answered based on the literature review. In the second step, a protocol was defined to support the evaluation of the scientific studies that were relevant to the study. The last step involved the process of answering the research questions initially raised (in the first step).

In this study, besides conducting the literature review following its primary objectives according to Moher (2009) we also substantiate the results obtained with a literature review, presenting theoretical perspectives and innovations from leading authors in the field. First, the research question is defined; this is followed by a research protocol for evaluating the selected scientific articles. The last step involves answering the research questions (in the first step), based on the scientific articles identified as relevant (in the second step). Figure 1 summarizes the steps followed by the adopted methodology. Figure. 2 presents the steps followed by the adopted methodology. The researched was conducted by 3 investigators, 2 PhD's and a master's student.

3.1 Definition of research questions

The first step, see Figure 2, of the adopted methodology is related to the definition of the research questions of this study. The main research question intends to raise the state of the art concerning our study characteristics (traced in the Introduction): "Which are the blockchain-based reputation systems to determine the user reputation in e-commerce?." The main question brought up new concerns, while reading some articles, we realised that

a deeper approach was necessary, and so we need more answers to have a deeper understanding. The analyses of the articles referred to frauds, lack of transparency, limitation of the current reputation systems, and the mitigation method provided.

So, a sub-division of the main question was necessary:

1. What are the most common attacks and frauds on e-commerce platforms?
2. What are the main techniques and methods used to increase trust in online transactions?
3. What are the main guidelines for developing a blockchain-based reputation model?

After the definition of the research questions, the second step was related to the selection of the empirical data to be analysed, as presented at the Figures 2.

3.2 Conducting the search

In step two, data collection, we developed our search protocol, which outlines the methods used to carry out a systematic review. This process is designed to reduce researcher bias since a systematic review is often a collaborative effort, Figure 2.

This step was decomposed into three phases (following the PRISMA statement approach (see Figure.1, PRISMA flowchart).

3.2.1 Identification

We started our research work in search of scientific literature on Blockchain-Based Reputation Systems. The search was conducted in the two main databases where the articles with the highest impact and quality in the scientific area in question are located, Web of Science (WoS) and SCOPUS. The use of these databases makes the article more robust, as it covers more articles of greater academic importance. Additionally, we conducted grey literature searches (google scholar and scholars' web pages) to complement and update the results. The search was conducted during the month of May 2021, and was complemented in 2023, with more research.

Using the WoS and SCOPUS databases, we searched for papers that included TOPIC: (trust AND electronic commerce AND blockchain) OR TOPIC: (online identity AND commerce AND blockchain) OR TOPIC: (online trust AND blockchain) in their title, abstract, or keywords. This search resulted in 101 articles selected from WoS and

501 from Scopus. The lists were exported to excel for further analysis and the following fields were chosen: Authors, Title, Year, Link, Abstract, and Keywords. Additionally, in google scholar, we performed a manual search with the same terms. Then, we selected the articles from the first 3 pages of the results (20 papers), using the same method, we extracted the fields referred to above and filled in an excel sheet. Figure 2.

This data base where selected because they have the most extensive international scientifical articles (Gouvêa et al., 2022).

3.2.2 - Screening and selection of relevant articles

Next, we evaluated the articles based on the inclusion criteria to determine their relevance to our study. An article had to include the search terms as the core technology under analysis. This was typically evidenced by its emphasis in the title, abstract, and keywords. We selected only academic peer-reviewed journal papers and conference proceedings and excluded others, namely: a) papers without full availability, b) papers not available in English, c) duplicate articles and d) papers that not discussed reputation system, or its models, from a technical, engineering, or computing science perspectives. The identification and inclusion process of our systematic review is presented in Figure 2. Our initial search was carried out in May 2021 yielded 622 articles. Once we eliminated duplicates, entries without full-text availability papers not available in English and not e-commerce-reputation centred papers, we were left with a population of 581 papers. Next, our research team, including two professors, and a master's student, reviewed this collection of articles for relevancy. In the first round of our inclusion process, we assessed the articles for their relevance based on title, abstract and keywords. This process led to the selection of 41 articles. Any articles we did not agree upon, were also excluded from the population. In the next round of revisions, we assessed the articles based on the full paper. We eliminated 16 papers that are only concerned with the architecture, or the prototype of the blockchain-based user reputation model is not presented. Thus, we identified 25 relevant articles in our final population for analysis.

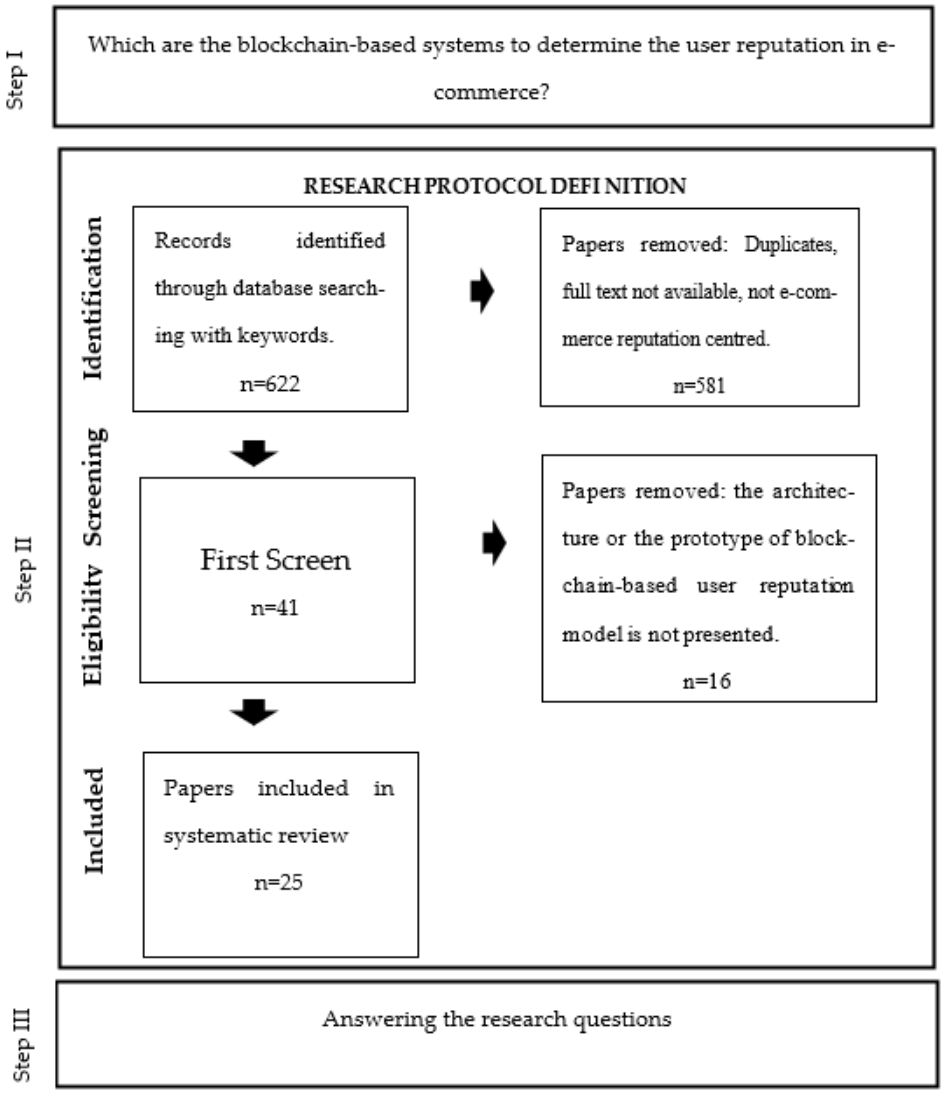


Figure 2 - Steps followed in the systematic review

The resulted list of papers that will be targeted for a deep study to produce a state-of-the-art are listed on table 1.

Table 1 - Selected Articles

ARTICLE NAME	MODEL NAME	REFERENCE
Rep on the block : A next generation reputation system based on the blockchain	Rep on the block	Dennis, R., & Owen, G. (2015). Rep on the block: A next generation reputation system based on the blockchain. In 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST). IEEE. https://doi.org/10.1109/icitst.2015.7412073

3R model: A post-purchase context-aware reputation model to mitigate unfair ratings in e-commerce	3R	Liu, Y., Zhou, X., & Yu, H. (2021). 3R model: A post-purchase context-aware reputation model to mitigate unfair ratings in e-commerce. Knowledge-Based Systems, 231, 107441. https://doi.org/10.1016/j.knosys.2021.107441
Anonymous and Verifiable Reputation System for E-commerce Platforms based on Blockchain	RepChain	Li, M., Zhu, L., Zhang, Z., Lal, C., Conti, M., & Alazab, M. (2021). Anonymous and Verifiable Reputation System for E-commerce Platforms based on Blockchain. IEEE Transactions on Network and Service Management, 1. https://doi.org/10.1109/tnsm.2021.3098439
DTrust: A Decentralized Reputation System for E commerce Marketplaces	Dtrust	Dhakal, A., & Cui, X., (2019). DTrust: A Decentralized Reputation model for E-commerce Marketplaces.
A Model for Deriving Trust and Reputation on Blockchain-Based e-Payment System	Reptor	Ahn, J., Park, M., & Paek, J. (2018). Reptor: A Model for Deriving Trust and Reputation on Blockchain-based Electronic Payment System. In 2018 International Conference on Information and Communication Technology Convergence (ICTC). IEEE. https://doi.org/10.1109/ictc.2018.8539641
Using Blockchain Technology To Improve Trust In eCommerce Reviews		Ramachandiran, R., (2018). Using Blockchain Technology to Improve Trust In eCommerce Reviews. 10.13140/RG.2.2.29324.00646.
Rep on the Roll: A Peer to Peer Reputation System Based on a Rolling Blockchain	Rep on the block	Dennis, R., & Owen, G. (2015). Rep on the block: A next generation reputation system based on the blockchain. In 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST). IEEE. https://doi.org/10.1109/icitst.2015.7412073
TrustChain: Trust Management in Blockchain and IoT supported Supply Chains	Trustchain	Malik, S., Dedeoglu, V., Kanhere, S. S., & Jurdak, R. (2019). TrustChain: Trust Management in Blockchain and IoT Supported Supply Chains. In 2019 IEEE International Conference on Blockchain (Blockchain). IEEE. https://doi.org/10.1109/blockchain.2019.00032
A Trustless Privacy-Preserving Reputation System		Schaub, A., Bazin, R., Hasan, O., & Brunie, L. (2016). A Trustless Privacy-Preserving Reputation System. In ICT Systems Security and Privacy Protection (pp. 398–411). Springer International Publishing. https://doi.org/10.1007/978-3-319-33630-5_27
A Reputation Based Hybrid Consensus for E-Commerce Blockchain		Sun, Y., Zhang, R., Xue, R., Su, Q., & Li, P. (2020). A Reputation Based Hybrid Consensus for E-Commerce Blockchain. In Web Services – ICWS 2020 (pp. 1–16). Springer International Publishing. https://doi.org/10.1007/978-3-030-59618-7_1
Decentralized Reputation System on a Permissioned		Kugblenu, C., & Vuorimaa, P. (2020). Decentralized Reputation System on a Permissioned Blockchain for E-Commerce Reviews. In Advances in Intelligent Systems and Computing (pp. 177–182).

Blockchain for E-Commerce Reviews		Springer International Publishing. https://doi.org/10.1007/978-3-030-43020-7_24
Anonymous Reputation System for IIoT-Enabled Retail Marketing Atop PoS Blockchain		Liu, D., Alahmadi, A., Ni, J., Lin, X., & Shen, X. (2019). Anonymous Reputation System for IIoT-Enabled Retail Marketing Atop PoS Blockchain. IEEE Transactions on Industrial Informatics, 15(6), 3527–3537. https://doi.org/10.1109/tii.2019.2898900
A Novel Framework for Decentralized C2C E-commerce using Smart Contract		Joshi, P., & Kumar, A. (2020). A Novel Framework for Decentralized C2C E-commerce using Smart Contract. In 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT). IEEE. https://doi.org/10.1109/icccnt49239.2020.9225377
The impact of blockchain on e-commerce: A framework for salient research topics		Treiblmaier, H., & Sillaber, C. (2021). The impact of blockchain on e-commerce: A framework for salient research topics. Electronic Commerce Research and Applications, 48, 101054. https://doi.org/10.1016/j.elerap.2021.101054
Blockchain-based decentralized reputation system in E-commerce environment		Zhou, Z., Wang, M., Yang, C.-N., Fu, Z., Sun, X., & Wu, Q. M. J. (2021). Blockchain-based decentralized reputation system in E-commerce environment. Future Generation Computer Systems, 124, 155–167. https://doi.org/10.1016/j.future.2021.05.035
RTChain: A Reputation System with Transaction and Consensus Incentives for E-commerce Blockchain	RTChain	Zhou, Z., Wang, M., Yang, C.-N., Fu, Z., Sun, X., & Wu, Q. M. J. (2020). RTChain: A Reputation System with Transaction and Consensus Incentives for E-commerce Blockchain
A Blockchain-Enabled Quantitative Approach to Trust and Reputation Management with Sparse Evidence		Zeynalvand, L., Luo, T., Andrejczuk, E., Niyato, D., Teo, S. G., & Zhang, J. (2021, May). A Blockchain-Enabled Quantitative Approach to Trust and Reputation Management with Sparse Evidence. In Proceedings of the 20th International Conference on Autonomous Agents and MultiAgent Systems (pp. 1707-1708).
EthReview: An Ethereum-based Product Review System for Mitigating Rating Frauds		Zulfiqar, M., Tariq, F., Janjua, M. U., Mian, A. N., Qayyum, A., Qadir, J., Sher, F., & Hassan, M. (2021). EthReview: An Ethereum-based Product Review System for Mitigating Rating Frauds. Computers & Security, 100, 102094. https://doi.org/10.1016/j.cose.2020.102094
Solving the Buyer and Seller's Dilemma: A Dual-Deposit Escrow Smart Contract for Provably Cheat-Proof Delivery and Payment		Asgaonkar, A., & Krishnamachari, B. (2019). Solving the Buyer and Seller's Dilemma: A Dual-Deposit Escrow Smart Contract for Provably Cheat-Proof Delivery and Payment for a Digital Good without a Trusted Mediator. In 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). IEEE. https://doi.org/10.1109/bloc.2019.8751482

for a Digital Good without a Trusted Mediator		
Blockchain in the operations and supply chain management: Benefits, challenges and future research opportunities		Wamba, S. F., & Queiroz, M. M. (2020). Blockchain in the operations and supply chain management: Benefits, challenges and future research opportunities. International Journal of Information Management, 52, 102064. https://doi.org/10.1016/j.ijinfomgt.2019.102064
DEFS—Data Exchange with Free Sample Protocol	DEFS	Genés-Durán, R., Hernández-Serrano, J., Esparza, O., Bellés-Muñoz, M., & Muñoz-Tapia, J. L. (2021). DEFS—Data Exchange with Free Sample Protocol. Electronics, 10(12), 1455. https://doi.org/10.3390/electronics10121455
An Architecture for Blockchain-Based Cloud Banking		Do, T. (2021). An Architecture for Blockchain-Based Cloud Banking. In Lecture Notes in Networks and Systems (pp. 805–824). Springer International Publishing. https://doi.org/10.1007/978-3-030-80126-7_57
A Secure Personal-Data Trading System Based on Blockchain, Trust, and Reputation		Camilo, G. F., Rebello, G. A. F., de Souza, L. A. C., & Duarte, O. C. M. B. (2020). A Secure Personal-Data Trading System Based on Blockchain, Trust, and Reputation. In 2020 IEEE International Conference on Blockchain (Blockchain). IEEE. https://doi.org/10.1109/blockchain50366.2020.00055
Blockchain as a confidence machine: The problem of trust & challenges of governance		De Filippi, P., Mannan, M., & Reijers, W. (2020). Blockchain as a confidence machine: The problem of trust & challenges of governance. Technology in Society, 62, 101284. https://doi.org/10.1016/j.techsoc.2020.101284
Blockchain for Businesses: A Systematic Literature Review		Grover, P., Kar, A. K., & Vigneswara Ilavarasan, P. (2018a). Blockchain for Businesses: A Systematic Literature Review. In Lecture Notes in Computer Science (pp. 325–336). Springer International Publishing. https://doi.org/10.1007/978-3-030-02131-3_29

On the last step of the methodology, presented on chapter IV a discussion of the articles will be presented, as well as the answer to the research questions, Figure 2.

The systematic literature review will follow the subsequent guidelines: the results of the analyses and a discussion. Following the literature review, a conceptualization of a reputation model will be provided.

The selected articles are mentioned in Table 1; however, in order to give a clear view of the reputation articles and due to their complexity and extension, the main characteristics are present in this chapter. Nonetheless, the architecture of these articles is explained in full detail in Appendage 1. The same appendage has a complete list of the initial articles selected per database.

The selected articles approach the main problems in online transactions and are very contextualized and self-explanatory. We intend to present the results of the proposed reputation models and the difficulties they faced while developing such models.

The fundamental problem with current product review systems, according to M. Zulfiqar et al. (2021), is their centralized underlying design. According to the authors, reputation systems based on reviews on e-commerce platforms are vulnerable to the aforementioned rating frauds (bad-mouthing and ballot-stuffing). Furthermore, these e-commerce platforms are controlled by a single authority, making them vulnerable to tampering with reviews by the centralized authority to enhance product sales. The authors also claim that fraudulent and manipulated reviews lead to a poor online purchasing experience and a lack of trust in e-commerce platforms.

4.1 Papers Discussion

4.1.1EthReview

Zulfiqar et al., 2021, suggest an Ethereum blockchain-based peer-to-peer product review system to solve these flaws. The authors say that their method, dubbed EthReview, is resistant to rating fraud, which is common in existing traditional product review systems, and effectively mitigates the limitations of centralized product review systems. The authors claim their approach protects against the following attacks/fraud: Sybil, ballot stuffing, bad-mouthing, and collaboration. Furthermore, it does away with the necessity for a central authority or a trusted third party to validate the integrity of the uploaded reviews.

The authors' solution includes a blockchain-based platform that supports a P2P consortium network of randomized endorser nodes for review validation and verification and a two-token system. These two tokens are the Product Review Authorization Token (PRAT), used for review authorization, and the Product Review Discount Token (PRDT), intended to reward honest reviewers by providing them product discounts and boosting their position to endorser nodes.

There are two sorts of users in EthReview: sellers and buyers, to which four roles can be assigned: sellers, buyers, reviewers, and endorsers. Endorsers are a subset of reviewers who are given this role based on honest behaviour. Reviewers are a subset of customers who post reviews regarding purchased products. The role is assigned automatically via Ethereum smart contracts. Endorsers must validate the credibility of the uploaded reviews by endorsing them (i.e., voting up or down on the review).

New users, sellers, or purchasers must give a credit card number to register on the platform. This is required since the EthReview system charges a Gas cost in terms of Wei for each operation: when a seller uploads a new product, when a buyer reviews, and so on. This charge is applied to the seller's account. The user's identity is linked to his Ethereum address and is used in EthReview to track all the activities of a single user.

This strategy, according to the authors, addresses both aforementioned issues. Concerning the lack of effective identity management, the authors claim that their solution resists Whitewashing and Sybil assaults by restricting accounting creation to the unique credit card number and user ID (connected to Ethereum address).

The proposed model addresses the second mentioned concern, a need for more transparency in data management due to its blockchain-based nature. The authors say that collusion attacks, such as those with central authorities, are avoided by blockchain's tamper-proof features, which do not allow changing or hiding bad ratings after they are posted. This trait and the P2P multi-node endorser model inhibit the insertion of bogus reviews, and the two proposed tokens make the model resistant to ballot stuffing and bad-mouthing fraud. Furthermore, false reviews can be quite costly because the financial model could be more economically sustainable owing to the financial effort required for product purchases.

Karode et al. (2020) propose a global-scale online travel review system based on blockchain in the tourist sector. This concept focuses on product reviews, namely tourist

items, and allows the same version of user reviews to be displayed smoothly on any tourism platform connected to a blockchain. As a result, consumers may be confident that the platform providers do not influence the review score.

The authors say their plan benefits consumers and businesses more than centralized options, pointing out flaws in those systems first because the review is regulated by the platform providers, who have complete control over their platforms. Because each centralized platform has its database and may employ various processes, a product's score may differ from one platform to the next. Aside from distinct practices, a platform may retain an appealing view of a specific business partner. According to the authors, blockchain technology increases the system's openness by allowing information to be shared publicly throughout connected platforms, shown publicly, and cannot be modified. As a result, the proposed system does not require a central authority.

The authors' contribution is a set of guidelines for developing an Ethereum-based platform. A smart contract is the central component of the proposed system. According to the authors, this method enforces a rule that all participants must observe. The rules in the smart contract code are visible to all participants, who can then select whether or not to join the system. Furthermore, the authors' approach incorporates a community-driven model in which all conceivable user rules and procedures are defined to increase the quality of the reviews and, as a result, the accuracy of the reputation scores. When most users agree, the provided reviews might be labeled as "fake" or "low-quality."

In its original state, an Ethereum blockchain user is a customer. A user becomes a seller after recording the first product (e.g., hotel room, meal, tour guide, accommodation, and other travel products) in the smart contract.

Because the blockchain platform incurs a cost with each transaction, such as the recording of a new product, the recording/update of a user profile, a product review, or any other type of operation, the authors propose using the Interplanetary File System (IPFS) to reduce the amount of data and the number of operations in the blockchain, thereby lowering the system's operating costs. This is significant since authors can amend and delete their reviews, with all operations logged and available in a traceable history. Furthermore, fraudulent reviews are judged by the user community, increasing the number of transactions even further.

In terms of performance, the system was evaluated on the Ethereum Ropsten test network because, at the time, this network used Proof-of-work (POW) as the blockchain network's consensus mechanism. As a result, the outcome is closest to the core network. The authors propose to measure transaction cost and response time in this performance test. The most extended response times were roughly 20 to 30 seconds, and the expenses for adding a product were 0.0575 USD. The authors explain that this cost is affected by the price of Ether at the time of the operation, as well as the technical difficulty of new technologies, such as blockchain, with which most consumers are unfamiliar. Furthermore, the authors claim that the system guarantees high-level data safety because theoretical attacks on the blockchain, such as the 51% Attack, are nearly impossible.

4.1.2 BEQA

The BEQA proposal by L. Zeynalvand et al. (2021) addresses issues in user reputation systems. According to the authors, the current systems have two flaws: (1) Users now have many more places to share information, making it challenging to detect identity-based attacks like whitewashing and Sybil; (2) The cost of attacks has decreased significantly due to the proliferation of bots in e-commerce applications, which tends to invalidate the traditional assumption that most users are honest.

The proposed system employs an economic model based on blockchain transaction fees to deter identity-based assaults. Each piece of input has a cost and a weight attached to it. The costs increased over time using an exponential growth function with an undetermined rate of rise. The total amount spent on transaction fees is used as a whitewashing deposit by BEQA.

To provide feedback on an entity, a user with a public key must first sign the input with its private key (each user has a randomly generated key pair). According to the authors, this method makes BEQA resistant to repudiation attacks. BEQA checks the user signatures of fetched feedback when they are fetched.

According to the authors, this prevents identity-based attacks in which an attacker associates malicious feedback with a legitimate user's identity.

The authors evaluated their model, and the results enable them to state that, in general, a higher publicity expenditure leads to a higher Sybil attack cost. According to

the authors, this is a desired property that discourages Sybil's attacks and encourages higher publicity expenditure as a deposit against whitewashing.

According to Dhakal et al. (2019), the fundamental problem with present reputation systems is their centralized character because reputation is not shared with other systems (platforms in silos) and can be manipulated by the central authority. Other challenges are also presented by the authors: Many fraudulent feedback are typically purchased by vendors to boost their reputation score (ballot stuffing). There needs to be more user incentive to offer continual reviews to platforms and a lack of credible reviews (some vendors tend to eliminate competitors' items by hiring reviewers to put negative reviews on competitors' products - bad-mouthing).

4.1.3 DTrust

Dhakal, A., & Cui, X., (2019) propose DTrust, a system based on the Ethereum blockchain and IPFS, to address these issues. DTrust allows e-commerce platforms to store and retrieve reputation data. As a result, user reputation data and scores are shared across numerous e-commerce platforms. The reputation data is saved in IPFS, while the data indexes are stored in the blockchain. Expenses (Gas) savings are realized by storing reputation data in IPFS and content indexes in the Ethereum blockchain. The DTrust system is built on a set of smart contracts that run on the blockchain.

The DTrust provides tools for managing user and product reputation. Both items, users, and products have their profiles to which all reviews are posted. Regarding identity management, users' accounts on the e-commerce site are linked to their Ethereum public addresses. As a result, a global picture of the user's reputation is possible.

In order to motivate reviewers to write quality reviews, the authors also offer a financial incentive. If a user finds another review valuable, he can upvote it. Thus, quality reviews will be appreciated by other users, and in exchange, the reviewer will be awarded Reputation Tokens (also known as DTrust Tokens) that can be used for various purposes, such as purchasing goods on specific platforms or exchanging them for fiat currencies. Vendors can also use these tokens to market their products on various e-commerce platforms.

The authors say the system may now exchange reputation data across decentralized e-commerce sites. However, they do not specify how implying that each

portal must communicate directly with the smart contracts. The writers also do not specify whether any condition is imposed on a user before rating another user or product, such as a product purchase.

Dennis R. et al. (2015) claim to have developed the first blockchain-based generalized reputation system that can be deployed to different networks. The authors highlight the centralized management strategy as an issue, owing to the central authority's manipulation of reputation data and changes in their algorithms. The authors note that systems based on a centralized server, even in the event of several web services, need to be revised for P2P networks, in which decentralized control is the primary premise and no entity has control. Another issue addressed in this study is identity management, which does not assure the linkage of an identity to a single user, preventing that user from obtaining more than one identity. The authors believe this is the key to stopping users from abusing the system by creating several identities and transacting between them. The authors also pose the open topic of how to quantify reputation and whether the reputation classification left by a user is accurate and based on an actual transaction.

To address these issues, the authors propose a universal blockchain-based reputation system that addresses three major hurdles that earlier generations of reputation systems failed to address. Furthermore, the suggested method can prevent typical assaults on current-generation reputation systems. The authors' approach is focused on P2P networks, but it can also be applied in an e-commerce scenario, according to the authors.

Due to the load and inflation in the Bitcoin blockchain, the authors propose the creation of a new blockchain with the sole purpose of storing reputation data from completed transactions, also based on miners who mine new blocks containing transaction data and the respective reputation data (0 or 1).

In the case of P2P networks, the authors advise removing the human choice from the transaction to address one of the aforementioned issues, reputation measurement. To stop a user from having many identities, the authors recommend linking a user to an IP address, claiming that the expenses of an IPv4 address constitute a financial barrier, making a successful attack expensive. This option is limited because sharing a single IP address among numerous users in a private network is usual practice when they are behind a gateway. Furthermore, a user may change his IP address, necessitating concurrent access control. The authors supplement their strategy by proposing high entry fees to the

network. However, they need to specify who manages and how or whether there is any authority. According to the authors, preventing many identities from a single machine and the high costs of network entry are critical in averting a Sybil attack. To adapt this approach to e-commerce, the authors advise replacing the IP address with the public key of the item's sender (we assume the seller), but they do not specify how a user's public and private keys are issued.

This concept also incorporates a proof-of-stake economic model in which, while beginning a transaction, people with a poor or no reputation stake a tiny quantity of currency (Bitcoins) to verify their honesty. If their behaviour is dishonest, the money is transferred to a pool, which the network utilizes as an incentive for miners who find blocks. They are staked back if they act honestly during the deal.

The authors also recommend that the reputation score be calculated on the client side using user-defined criteria, eliminating potential attacks such as collusion by allowing the user to choose the best criteria.

Regarding constraints, the authors highlight the blockchain's ability to manage a high volume of transactions, storage space requirements, and successful global adoption. To address the performance issue, the authors propose raising the size of the blocks, which would enhance the rate of processing new transactions while decreasing the time necessary for each block to be mined. However, neither approach addresses the issue of storage space or bandwidth. As a remedy, the authors propose that nodes no longer need to download the complete blockchain; only miners would need to download and maintain the entire blockchain. To calculate a user's reputation, the node must now contact a pool of miners who have requested the data for that specific user.

Furthermore, Dennis and Owenson (2016) propose a change to the mechanism of formation of the "genesis block" that would occur daily. Active users should be initialized in these particular blocks to avoid data erasure. According to the authors, their solution, a rolling Blockchain, ensures that the size of the blockchain does not grow endlessly. The authors detail their solution, suggesting it is sufficiently resilient to rogue miners already in the network.

This concept is mainly focused on P2P networks. Even though it is well founded, it also fits in the e-commerce situation and may be generalized, as well as other previously discussed aspects.

Li et al. (2021) identify the primary issues with current reputation systems that use a centralized approach. First, a single point of failure/attack is created by keeping reputation data in a centralized server. Furthermore, such a model is vulnerable to being faked by the wrong platform without the users' knowledge. The second issue is isolation when reputation data is kept from other platforms. The third issue raised by the authors arises from the previous two in that it is impossible to forecast a user's behaviour based on his reputation to minimize financial risks or other damage.

Li et al. (2021) offer a blockchain-based, transparent, tamper-resistant, and cross-platform reputation system to address these issues. According to the authors, including blockchain in the reputation system might result in a public and tamper-resistant record of ratings and reputations and access to supplier reputation data from various platforms. This blockchain can aggregate the data reputation of multiple platforms that agree to work and co-establish in a consortium blockchain, thereby breaking down the data barrier between platforms and building a harmonious online retail ecosystem.

However, due to the blockchain's public access paradigm, personal data privacy issues (in the form of a lack of rating privacy) and potential assaults must be handled in such an approach. Furthermore, the authors discuss the enormous technological problems of developing a blockchain-based reputation platform that allows diverse platforms to collaborate while maintaining privacy and unlikability and resisting security threats in an untrusted and distributed network.

4.1.4 RepChain

RepChain is a reputation system for e-commerce proposed by Li et al. (2021). The authors claim their approach addresses the aforementioned issues by providing reputation access and rating privacy across different networks in a decentralized context. The authors claim to have created a concrete strategy to provide security and privacy protection. They also claim to have formally demonstrated the proposed scheme's privacy and security. The authors created a prototype based on the Ethereum test network to test the viability of their idea and evaluate the suggested scheme's performance.

The above-mentioned technical issues, privacy, and security for a consortium blockchain in which various e-commerce platforms (such as eBay and Amazon) might join were addressed in RepChain using cryptography and a paradigm based on a state machine (with five phases/states). A Certificate Authority (CA), an e-commerce business

association co-founded by all platforms, is in charge of accepting new platforms into the consortium. This CA is in charge of producing system settings and cryptographic keys for users and the platform and handling user registration requests. According to the authors, the central authority does not affect the system's decentralized character because it remains offline after system startup and entity registration.

Despite their reference to user registration requests to the CA, the authors only refer to the case of multiple rating attacks and anomalous rating attacks without discussing identity management vulnerabilities, which may result in Sybil and Whitewashing assaults.

In terms of efficiency, the authors propose lightweight computational costs in mining and verifying rating transactions, as well as keeping the total length of a rating transaction as short as possible, claiming that the experimental results show that RepChain's computational costs and communication overhead are moderate when compared to existing proposals. However, more is needed regarding high-volume transaction processing and storage capacity, given that some platforms, such as eBay, may conduct over one billion daily transactions, as the authors noted.

4.1.5 Reptor

Ahn et al. (2018) offer Reptor, a blockchain-based approach for determining trust and reputation. This concept employs electronic payment and rating data related to business transactions, which are kept in a blockchain. Ahn et al. (2018) demonstrate and analyse the concept using a prototype built on the Nodehome platform[2].

Ahn and colleagues According to Ahn et al. (2018), their approach is practical for generating reputation and trust from raw evaluations in blockchain-based online payment system transactions. The model considers several concepts and notions related to human behaviour and psychological factors in its mathematical-based approach, such as (1) time difference weight (TDW), (2) personal evaluation criteria (PEC), (3) more belief in a person with a higher reputation, (4) friend-of-a-friend, and (5) losing confidence is much easier than maintaining it. To acquire a normalized evaluation given by a user, a Normalized Evaluation (NE) value is computed. Based on the grading criterion PEC, the normalizing function is a sigmoid function. Average Received Normalized Evaluation

[2] https://nodehome.io

(ARNE) is another metric that is an average of all NE that user B has received from others, averaged using a time-adaptive parameter for transactions conducted by user B.

Using these metrics, the proposed model derives the Direct Trust (DTR), which is a direct trust from user A to B, and the Indirect Trust (ITR), which is based on inferring trust from others who have done transactions with both A and B, even though A and B have never transacted.

As previously stated, the proposed paradigm was tested in a Nodehome prototype. This network provides a blockchain-based electronic payment, which includes information about commercial transactions and rating data. Users can use the system to buy things, make payments, and transfer money, and they can also rate each other depending on their satisfaction with a transaction in which they are participants. An intriguing component of this system is that rating data is viewed as a transaction in its virtual "ratings" currency. Using data from the blockchain, the system computes reputation based on the model. To solve the blockchain paradigm's performance difficulties, the authors offer a cache that significantly reduces the latency of queries to the blockchain. The authors explain their local caching technique and propose a periodic renewal.

The authors used two datasets to evaluate the built prototype and model: a simulation dataset and another obtained from extensive, accurate data from the actual Bitcoin transaction history and synthetic rating data produced from the actual Bitcoin transaction history. The authors claim that their evaluation results from both datasets demonstrate the effectiveness and resilience of the proposed model.

4.1.6 Reputation systems prototypes

Schaub et al. (2016) propose a reputation system based on blockchain that is suited for e-commerce applications. The authors assert that their solution is thrustless, decentralized, and anonymizing. Furthermore, the authors claim that such a system can generate little overhead for transaction processing while being robust and allowing customers to provide ratings and textual evaluations.

To achieve their goals of trustlessness (primarily, not relying on TTPs or CAs), e-commerce suitability, decentralization, anonymity preservation, and robustness (to common attacks such as bad-mouthing, ballot-stuffing, Sybil attacks, and whitewashing),

the authors' proposal includes a protocol supported by two basic building blocks: the blockchain and blind signatures, as well as public keys and blinded tokens. This protocol defines the whole lifetime of a commercial transaction, beginning with the buyer obtaining the reputation of a seller in order to decide on his purchase and ending with the block being broadcast in the network. Concerning the blockchain consensus mechanism utilized in the protocol, the authors offered Proof-of-Stake without addressing this choice.

The buyer's anonymity is a formal goal in this piece. Despite the fact that the buyer must provide his identity and, eventually, his shipping address, the authors propose a waiting time between the end of the transaction and the rating in order to complicate the correlation between the buyer and his review, as well as the use of blinded tokens that grant the right to review the transaction.

The authors propose a cost imposed on the service provider (seller) when a transaction is reviewed, thus aiding in preventing ballot-stuffing attempts. By requiring a token connected with a transaction, the potential of bad-mouthing attacks is considerably reduced. Concerning whitewashing assaults, the authors offer a blockchain operation in order to apply a fee, which jeopardizes the economic sustainability of such an attack. Sybil attacks are dealt with in the same way, with charges and a necessary token with origin in a transaction. As an open issue, a solution to the problem of information leaking regarding the time at which reviews are filed is required.

In terms of performance, the proposed model links each seller's rating to the previous one (through a pointer to the block). Thus, in order to ask the blockchain about the reputation of a given seller, one must first go back in time till they identify the first transaction (in a block) of that seller and then follow the linked blocks.

The economic model in this proposal also contains a reward, so every time a new block is formed, an award is given to the user who formed it. It should be noted that in this suggested system, coin ownership is required in order to acquire a reputation.

The authors address their proposal for a model based on a protocol, an economic model, cryptography, and blockchain in this article without exhibiting any prototype or real experiment.

D. F. Camilo et al. (2020) recognized existing concerns with centralized data-storage systems as the loss of control over personal data, the payment of excessive costs,

the signature of agreements that frequently undermine privacy, and the risk of data leaks. Furthermore, criminal individuals frequently damage cloud-based services via internal attacks and denial of service (DoS) attacks. Due to its properties of distributed and auditable data storage, as well as the fault-tolerance property of the consensus protocol, which requires that the attacker control the majority of organizations to effectively affect the consensus protocol, the authors claim that blockchain technology is a more efficient way to ensure security and privacy while preserving the owner's control over the data.

The authors suggest a blockchain-based safe data marketplace system, saying that it is a secure, adaptable, and effective system for distributed, automatic, and transparent data trade.

According to the authors' plan, three major types of transactions are recorded in the blockchain, with a fourth for feedback proposals. These three main transactions enable advertising, purchasing, and responding. To advertise a seller's product (data), a buyer's purchase, and, finally, a response with the key that allows the buyer to decrypt the received data (stored in an external storage system). Smart contracts manage these transactions, which include payments. Following a successful commercial transaction, the buyer might provide rating feedback to the seller within the boundaries of the transaction.

The suggestion of the authors intends to prevent five sorts of attacks: (1) bad-mouthing assault, (2) on-off attack, (3) Sybil attack, (4) newbie attack, and (5) conflicting-behaviour attack. The authors address these types of attacks using the suggested model and the blockchain paradigm's features.

The model contains an adaptive aging function that prioritizes recent interactions over previous ones in order to account for any changes in a seller's behaviour. As a result, the second sort of attack, the on-off attack, is avoided. In contrast to prior systems that use a fixed forgetting factor, the authors claim that the forgetting factor of the aging function adapts based on the likelihood that the seller will act honestly.

The authors propose using a permissioned blockchain and implementing limits on sellers on a per-organization basis to prevent assaults based on identity management fragilities, sybil, and newbie (whitewashing).

If a seller believes that rating feedback is unfair, he or she may display a discontent flag. According to the authors, bad-mouth assaults can be mitigated by using a smart contract that analyses customer rating behaviour and seller flags. It needs to be clarified, however, how that flag is recorded in the system.

Concerning the fifth type of assault, the conflicting-behaviour attack, the authors argue that all feedback are publicly verifiable as blockchain transactions, but they do not examine how effective this countermeasure is. It may arise as a result of the suggested model that derives user reputation.

Signatures in transactions, asymmetric encryption, and redundant communication pathways between blockchain network participants round out the authors' approach to security.

Based on Hyperledger Fabric v2.0, the author created a prototype. The authors emulated a blockchain network with five ordering nodes, the Raft consensus method, smart contracts written in Go, and each block enabling 100 transactions by running the nodes in a Docker environment. There were two types of experiments: (1) evaluating the influence of the adaptive forgetting factor in comparison to a static forgetting factor when an on-off attack happens, and (2) evaluating the evolution of a new-comer seller's reputation by entering a system where other sellers already have a high reputation. Both tests, according to the authors, confirmed the efficiency of the reputation model.

According to Kugblenu et al. (2020), due to the centralized nature of today's major online retailers such as Amazon, Alibaba, and Walmart, consumer reviews and ratings are locked to the retailer's platform. Furthermore, retailers choose which reviews are promoted as top-rated on a product page without a defined metric, influencing customer purchasing decisions.

The authors suggest a permissioned blockchain-based decentralized reputation system that allows shops to construct reputations for products and, by extension, sellers, or producers. This technology ensures that product ratings and reviews are gathered in a transparent manner across several store platforms. Customer privacy is further ensured because product reviews are linked to a validated order and product, which does not reveal the customer's identity. According to the authors, this idea enhances system transparency without jeopardizing security, performance, or data privacy.

Because the suggested system is based on a permissioned blockchain, there are three sorts of participants in this proposal: (1) customer, (2) retailer, and (3) agency membership service. This latter organization is in charge of issuing, managing, and auditing retailer credentials. The writers trust this agency because it is a third party with no reason to be malicious. This strategy, according to the authors, mitigates attacks based on identity management vulnerabilities such as sybil.

The authors defend utilizing a permissioned blockchain for a consortium network because it allows them to use alternative consensus algorithms besides PoW, and a permissioned blockchain is more efficient and scalable than a public blockchain using a POW consensus algorithm.

The authors created a proof-of-concept using Hyperledger Fabric. To enable product rating, a token is generated that is linked to the product, store, and order. Multiple reviews with the same token invalidate the previous transaction, and a smart contract is put up to limit the amount of times a customer may give a product a review. Smart contracts are used to aggregate and accumulate product ratings.

The authors outline various restrictions, the most important of which is acceptance by online sellers. How can they be encouraged to participate in the permissioned blockchain and integrate it into their processes? Another significant drawback identified by the authors in relation to the proposed system is retailers who act deliberately and carry out undefended attacks such as collusion attacks.

In the framework of the Industrial Internet-of-Things (IIoT) ecosystems, Liu et al. (2019) propose a reputation system for consumer-retailer channels. In such circumstances, retailers can build reputations based on customer input. Because only aggregated review numbers for shops are made public, the proposed system attempts to safeguard consumers from being followed or retaliated against. Furthermore, the authors claim that a blockchain-based design improves the openness and stability of the reputation system by allowing public access to the system's reputation data and mitigating potential attacks.

There are three categories of entities in the proposed system: (1) customers, 2) retailers, and (3) identity management entities. The latter is a government organization in charge of issuing and managing consumer and retailer identities and credentials. The writers believe this entity may be completely trusted.

According to the authors, there needs to be more attention to efficiency and scalability difficulties in some publications for blockchain-based reputation systems. Simultaneously, the implementation issues of a blockchain-based reputation system should be thoroughly examined in the system's architecture in order to achieve interoperability with existing blockchain platforms.

The authors also propose an off-chain rating token production phase to reduce on-chain storage and processing cost. This token ensures two of the system's six properties: the anonymity of the user who submits the rating and the unforgeability of the rating, as it requires a valid token to submit it. Because of the token, a restricted unlikability characteristic is also conceivable. The general public needs to find out if two valid evaluations for separate retailers are from the same person. If a customer leaves multiple reviews for the same retailer, the reviews are linked. The fourth condition, bound confidentiality, ensures that only aggregated reputation data is made public, while individual consumer review statistics are kept secret. Only the identity management entity has access to the buyer's identity. The sixth property, blockchain security, ensures the fifth property, transparency, as well as robustness and immutability. The creators chose the Proof-of-Stake (PoS) consensus algorithm for the blockchain because of its efficiency and security.

The authors create a proof-of-concept blockchain network based on Ethereum Parity. The experimental results, according to the authors, indicate the efficiency and viability of their proposal. The authors believe that only their solution achieves the aforementioned qualities when compared to other centralized, decentralized, and blockchain-based architectures.

According to Zhou et al. (2021), there are three major concerns in centralized reputation systems maintained by a single entity: (1) Malicious employees or outside attackers can easily manipulate these data, compromising the system's reliability. (2) There are many bogus comments and ratings on popular retailing platforms (e.g., Amazon) as a result of common attacks such as unfair rating attacks and collusion attacks. (3) There is no monetary incentive mechanism in place to encourage consumers to comply.

To address these three concerns, the authors suggest a decentralized reputation system for online purchasing that makes use of blockchain, IPFS, and smart contract

technology. According to the authors, due to the decentralized and distributed nature of blockchain and IPFS technologies, it is extremely difficult to change the data saved in IPFS and the address published on the blockchain. According to the authors, the suggested model for reputation evaluation is resistant to popular attacks such as unfair rating attacks and collusion attacks. Finally, the authors suggest a smart contract that distributes monetary rewards in the form of bitcoin from vendors to purchasers who have contributed comments and reviews. According to the authors, this monetary incentive mechanism creates a virtuous circle of motivated customers who give ratings and comments, as well as others who are well-educated about the things they purchase. The product vendor bears all operational costs.

The system allows buyers and sellers to rate each other, calculating reputation as well as comments made by purchasers regarding the products. To increase score accuracy and reduce potential fraud, the authors offer a reputation evaluation scheme that takes three weighting elements into account: (1) transaction time, (2) transaction amount, and (3) past reputation ratings of users.

The idea was evaluated by the authors utilizing an Ethereum blockchain testing environment. The authors claim that the fees paid by goods sellers are very cheap and acceptable (e.g., Evaluation and reward 0.14 USD, 1 ether = 1576.01 USD).

Resistance to alteration and common attacks were also assessed. The authors assert that their idea is immune to these two concerns. Finally, the performance of the reputation evaluation scheme was examined. The authors claim that the proposed approach has good reliability and that the monetary incentives are successful based on a simulation.

According to R. Ramachandiran (2018), because of the centralized architecture of reputation systems employed in online marketplaces, the business could provide incentives to the ratter or reviewer to provide fake or biased evaluations in order to improve sales and popularity. As a result, the legitimacy of these internet ratings is jeopardized. Furthermore, the reputation systems, such as reviews and ratings, are restricted to the marketplace's own platform, preventing users/vendors from exploiting the reputation elsewhere. To overcome this issue, the author advocates the use of blockchain to place trust in technology rather than the goodwill of a party.

The proposal's discussion is divided into two parts: (1) the generation of the review blockchain and (2) access to the review blockchain. In the first section, new businesses and customers must register on the blockchain by submitting legitimate ID documents, such as the business registration document and tax ID in the case of a business, and the mobile phone and credit card number in the case of a customer. Despite the fact that these facts are maintained in a public blockchain, the contents are not visible to third parties.

After concluding the commercial transaction, the buyer provides the Evaluation, which is then graded by an external service, such as IBM Watson, for relevance, profanity level, timeliness of review, and so on. If it is approved, it is added to the blockchain; otherwise, it is held in a partially concealed rejected review blockchain to aid in the improvement of the quality check algorithms.

The author suggests system operating expenses, with two degrees of access to blockchain data: normal vendors and premium suppliers. Vendors access, source, and display reviews via an API interface.

In this suggestion, some product categories, such as electronics, may have a shorter validity / expiry term for a review than categories in healthcare. Furthermore, it prevents a limited number of first reviews from influencing initial trust - Set the minimum number of reviews to something statistically or psychologically important.

According to the literature, contemporary reputation systems, whether centralized or decentralized, have significant limitations: they are managed by one entity, which does not provide all guarantees of transparency; they are isolated systems that do not share the reputation data, so a user or product may have distinct reputation scores in each platform; identity management is ineffective, allowing sybil and whitewashing attacks; and because the reputation data is not shared by the e-commerce platforms, combating the common types of fraud - ballot stuffing and bad-mouthing - is more difficult.

Because of its decentralized and tamper-proof qualities, the blockchain paradigm provides the conditions for mitigating the aforementioned drawbacks in current approaches for reputation systems. One fundamental issue is a lack of trust among the groups in charge of the e-commerce platforms. The blockchain may be the means to record this desired trust, in which all parties can exchange their data in a decentralized,

tamper-proofed, and transparent manner, which is the major challenge to the blockchain network's global acceptance.

There are two keyways presented in the literature: public blockchain networks and permissioned networks under consortium. The first strategy is based on economic viability, which means that it is not economically viable to be a dishonest user while honest users are rewarded. By accepting the regulations, the platform is accepted into a consortium. Typically, there is a central organization that manages both the consortium and the user identities.

4.2 Literature review summary

In short, the reputation model formulation in blockchain-based systems could be more effective when determining reputation scores, limiting typical types of fraud, ballot stuffing, and bad-mouthing. One could increase the model's performance by using economic models that add costs to operations and financial incentives such as rewards or financial penalties to dishonest users. Furthermore, in addition to the manual feedback provided by users and the economic viability-based method, various input approaches can be found in the literature. These proposals are based on both direct and indirect data, such as human behaviour and psychological aspects, inferred observations, and aging mechanisms.

As far as we are aware, these are the most current and relevant works on the subject of blockchain-based reputation systems in various stages of development: proposal, model, or prototype.

Despite the benefits of these blockchain-based solutions, numerous challenges remain. The blockchain paradigm is a public ledger in which all participants have read access to the data contained in the blocks. This necessitates extra cryptographic measures, often based on tokens, bling signatures, and asymmetric encryption, to safeguard user anonymity, prohibit retaliation against users who review a product or vendor, and make users unlikable to their feedback. This topic has received a lot of attention in the literature.

All history in a blockchain network is recorded from the "genesis block" to the last transaction in the last block. Despite its transparency, this strategy is extremely difficult to implement in terms of performance. We discovered four approaches in the reviewed literature: use of external storage systems, such as IPFS, to reduce the amount

of data in the blockchain while also lowering operational costs, cache mechanisms, and changes to the blockchain to reduce its size. Generate a daily genesis block and link the blocks of the same seller.

Despite its financial expenditures in miner nodes, the blockchain was initially developed using a POW consensus method, which is a secure algorithm. Other consensus algorithms, such as the PoS on the public Ethereum blockchain, have been suggested and deployed to address this issue. The blockchain is only compromised when the attacker obtains 51% of the network's control, regardless of the consensus algorithm.

There seems to be a mutual consensus regarding the key points to develop a more efficient reputation model.

The information of the users must be decentralized and protected at the same time. Other important data is feedback, the reliability of such feedback, how that feedback is shared, and whether it must be shared between platforms.

Based on the literature review, we came to some conclusions about the same variables that seem to be important when talking about a reputation model. The architecture of the current, relevant reputation models is on Appendages I and served as a base for the presented variables.

E-commerce platforms are popular targets for various types of cyber-attacks due to the valuable data and financial information they handle.

To prevent these types of attacks, e-commerce platforms should implement strong security measures such as multi-factor authentication, encryption, and access controls. Regular security assessments and updates to software and systems can also help to identify and address potential vulnerabilities. It's also important to educate customers about how to spot and avoid phishing attacks and other scams.

5.1 Attacks and frauds

Reputation models are used in e-commerce to help assess the trustworthiness of sellers and buyers. These models can help identify potentially fraudulent activity and protect against various types of attacks, including fake reviews: Sellers may use fake reviews to artificially boost their reputation and attract more buyers. Gonçalves et al. (2022). Reputation models can help identify suspicious patterns in reviews and flag them for further investigation. Patterns such as:

Account takeover attacks: Attackers may attempt to gain access to a legitimate user's account to make fraudulent purchases or steal sensitive information. Reputation models can help detect unusual activity or changes in behaviour that may indicate an account takeover.

Chargeback fraud: Buyers may attempt to initiate chargebacks, claiming that they did not receive the product or that it was not as described, to receive a refund. Reputation models can help identify patterns of fraudulent chargeback activity and take steps to prevent it.

Counterfeit products: Sellers may attempt to sell counterfeit or fake products, damaging their reputation and potentially causing harm to consumers. Reputation models can help identify sellers with a history of selling counterfeit products and take action to prevent them from doing so.

Spam and phishing attacks: Attackers may attempt to use phishing emails or other methods to steal sensitive information or gain access to user accounts. Reputation models can help identify suspicious activity and prevent users from falling victim to these types of attacks.

Overall, reputation models can play an important role in protecting e-commerce platforms and their users from various types of attacks and fraudulent activity. By analysing user behaviour and identifying patterns of suspicious activity, reputation models can help maintain a safe and secure e-commerce environment.

5.2 Reputation models

As mentioned before, the reputation model is a way to measure the trustworthiness or credibility of individuals or entities in a network or system. There are different types of reputation models, including binary, linear, and level-based models. Hoffman et al.(2009)

The binary reputation model assigns either a positive or negative reputation score to each user, depending on their past behaviour. The advantage of this model is its simplicity and ease of implementation. It is also suitable for scenarios where the trustworthiness of a user is a binary decision, such as granting access to a resource or validating a transaction.

The linear reputation model assigns a numerical score to each user based on their past behaviour. The advantage of this model is its ability to provide more fine-grained information about a user's trustworthiness. It can also be used to incentivize good behaviour, as users can increase their reputation score by performing desirable actions.

The level-based reputation model assigns users to different levels based on their reputation score. The advantage of this model is its ability to differentiate between users with similar reputation scores. Users can progress through different levels by achieving certain reputation thresholds, which can incentivize them to improve their behaviour.

While reputation models can be helpful in many contexts, they are not foolproof and can be vulnerable to security breaches.

If a reputation model is breached, it could lead to several security concerns. For example, an attacker could potentially manipulate the reputation scores of individuals or entities, causing them to be falsely perceived as trustworthy or untrustworthy.

To prevent security breaches of reputation models, it is important to implement strong security measures such as access controls, encryption, and monitoring for unusual activity. Additionally, regular audits and vulnerability assessments can help to identify and address potential security weaknesses. It is also important to have a response plan in place in the event of a breach, which includes steps to contain and mitigate the damage and to communicate with affected parties.

To create a reputation model, you would typically need the following to input certain information: data, that same data that we want to be sure is secure.

That information includes the user information, and there's a need to know who the user is and have a way to identify them uniquely. This could be a username, email address, or some sort of identifier that the user uses to log in or interact with the platform.

The user's activity and actions need to be tracked. This includes activities like the products they purchase, the content they create or share, the comments they leave, and the interactions they have with other users.

The user's feedback is important, and the user's feedback about other users' actions is important, including ratings, reviews, comments, or other forms of feedback that indicate how other users perceiver other behaviours.

One needs to establish rules and criteria for how the user's reputation is going to be evaluated, whether it is going to be by the number of positive or negative feedback ratings, the recency of the feedback, or the type of actions that are being evaluated.

Scoring a reputation on e-commerce typically involves calculating a reputation score for each user based on their actions and feedback from others.

We need to determine the criteria that you will use to evaluate a user's reputation. This could include things like the number of positive or negative reviews, the recency of the reviews, the number of products sold, the percentage of successful transactions, and the timeliness of shipping.

Gather data on the user's actions and feedback from others. This data could include product reviews, seller ratings, order histories, and shipping information. Assign weights to the different criteria based on their relative importance. For example, you may decide that the number of positive reviews is more important than the recency of the reviews. Use the criteria and weights to calculate a reputation score for each user. This

could be done using a mathematical formula that considers the user's actions and feedback from others. Display the reputation score on the user's profile and/or product listings. This will allow other users to make informed decisions about whether to purchase from the user or not. Continuously monitor the user's actions and feedback from others and update the reputation score, as necessary. This will ensure that the reputation score remains accurate and reflects the user's current reputation on the platform. Gonçalves et al., (2022)

It's important to note that scoring a reputation on e-commerce can be a complex process and may require the use of advanced algorithms and machine learning techniques. It's also important to balance the need for accurate reputation scores with the need to protect user privacy and prevent bias. Gonçalves et al., (2022)

The model shall be based on blockchain, so one must understand how it works and which path is more beneficial.

5.3 Why blockchain[3]

In the context of blockchain, reputation models can help increase the security and trustworthiness of the network. Assigning reputation scores to users makes it easier to identify bad actors and prevent malicious behaviour. Reputation models can also be used to incentivize good behaviour and reward users for contributing to the network.

A reputation model for e-commerce based on blockchain technology can be a decentralized system that allows users to have more control over their reputation and transactions.

By implementing a reputation model based on blockchain technology, e-commerce platforms can provide users with a secure and transparent way to conduct transactions and build trust within their communities.

Why decentralized? When we have a decentralized model, we do not have any central authority controlling it; the system is run by a network of computers, which ensures the transparency and fairness of the transaction.

We find it important that each user has his or her own reputation score that reflects his or her past transactions and behaviour on the platform. This score can be calculated

[3] https://www.blockchain-council.org/blockchain/types-of-blockchains-explained-public-vs-private-vs-consortium/

using various factors such as feedback from other users, dispute resolution, and history of successful transactions.

Being feedback is one of the ways to score reputation, and it's important that users leave such feedback and reviews about their experiences with other users on the platform. These reviews should be recorded on the blockchain, with the purpose of making them immutable and tamper-proof.

One way to make users leave their feedback is by giving incentives. For example, users who give their feedback can get discounts, priority access to new products, or any other benefit.

The reputation model should have a transparent and democratic governance structure, allowing users to have a say in how the system is run. This can be achieved using decentralized autonomous organizations (DAOs) that allow users to vote on proposals and make decisions collectively.

The reputation model can be implemented using smart contracts that are executed automatically based on predefined conditions. For example, if a seller fails to deliver a product on time, the smart contract can automatically release a refund to the buyer.

Even though Blockchain technology has numerous advantages, such as decentralized control, transparency, immutability, and security, there are also some limitations to this technology that are important to consider.

Blockchain technology is still limited in terms of scalability, with some networks being unable to handle more than a few transactions per second. This is a significant challenge for large-scale adoption of blockchain, particularly in high-transaction volume industries such as finance.

While blockchain technology is generally considered to be secure, it is not completely immune to attacks. For example, 51% of attacks, where an attacker gains control of most of the network's computing power, can compromise the integrity of the blockchain.

Blockchain technology is designed to be immutable, meaning that once data is written to the blockchain, it cannot be deleted or altered. This creates challenges for storing sensitive or personal data on the blockchain, as there is no way to remove it once it has been added.

Overall, while blockchain technology has many benefits, it is not bulletproof, and there are still some limitations that must be addressed before it can achieve its full potential.

5.4 Public vs. Private Blockchain[4]

Public Blockchain and Private Blockchain are two different types of blockchain networks with unique features and use cases.

One of the pros of public blockchains is that they are decentralized networks that are not controlled by any central authority or individual. This makes sure that the network remains transparent and trustworthy.

Public blockchains use advanced cryptographic algorithms to secure the network and ensure that data cannot be tampered with.

Once data is stored on the public Blockchain, it cannot be altered or deleted. This guarantees that the data remains transparent and immutable.

Public blockchains have large user bases and network effects that enable them to be more resilient and secure.

Some cons that we find are that public blockchains can suffer from scalability issues, making them slower and more expensive to use.

Public blockchains are open to anyone, which means that all data stored on the network is visible to everyone. This can be a concern for businesses or individuals who need to keep their data private.

Public blockchains can be difficult to govern, as there is no central authority responsible for maintaining the network.

Public Blockchain is more used in cryptocurrencies, such as Bitcoin and Ethereum, that are used as decentralized digital currencies.

Public blockchains can be used to create and execute smart contracts that are transparent, secure, and immutable. It can be used to track and trace goods throughout the supply chain, ensuring transparency and authenticity.

[4] https://www.blockchain-council.org/blockchain/types-of-blockchains-explained-public-vs-private-vs-consortium/

Regarding the costs of public blockchains, they charge transaction fees to users to incentivize miners to validate transactions. The fees can vary based on network congestion and can be higher during periods of high demand.

Public blockchains require significant amounts of computational power, which can lead to high energy consumption and associated costs. It requires ongoing maintenance and updates to ensure security and performance, which can lead to ongoing costs. Building decentralized applications (DApps) on public blockchains can require specialized expertise and development costs.

The other side of the coin is the private Blockchain. One of the pros is that it is controlled by a central authority, which enables them to be more efficient and scalable. Private blockchains are not open to everyone, which means that data stored on the network can be kept private and confidential. Private blockchains can be more easily governed and regulated by a central authority.

Private Blockchain also has its cons. Private blockchains are centralized networks that are controlled by a central authority or group of authorities. This can make them less transparent and trustworthy than public blockchains. It may not be as secure as public blockchains, as they may rely on fewer nodes to validate transactions. It can be more expensive to set up and maintain than public blockchains.

Private blockchains are controlled by a central authority or group of authorities. They are not open to everyone and require permission to join and participate. Private blockchains can be used to store data that is confidential and not visible to everyone. Private blockchains can be more easily governed and regulated by a central authority. They can be more scalable than public blockchains.

Setting up a private blockchain can require significant upfront costs, including hardware, software, and personnel. Private blockchains require ongoing maintenance and updates to ensure security and performance, which can lead to ongoing costs. Private blockchains require a central authority or group of authorities to govern the network, which can lead to additional costs associated with governance and administration. Building DApps on private blockchains can require specialized expertise and development costs.

The costs of public blockchain and private blockchain can vary significantly based on the specific use case, network size, and complexity of the application. However, in general, public blockchains may be more cost-effective for smaller applications or those with limited budgets, while private blockchains may be more suitable for larger, enterprise-level applications that require more control and customization. As presented in Table 2:

Table 2 - Which is the Best Blockchain? Source: www.blockchain-council.org

Aspect	**Private Blockchain**	**Public Blockchain**	**Consortium Blockchain**
Access Control	Restricted access	Open to anyone	Limited access
Participants	Known and permissioned	Anonymous and open	Known and permissioned
Consensus Mechanism	Faster, less energy-intensive	Slower, energy-intensive	Variable, depends on consensus model
Decentralization	More centralized	Fully decentralized	Intermediate level
Speed and Scalability	Faster and scalable	Slower and less scalable	Moderate speed and scalability
Example	Hyperledger Fabric, Corda	Bitcoin, Ethereum	Quorum, R3 Corda

5.5 The appropriate blockchain for reputation models on e-commerce[5]

With this understanding, the public, decentralized, and linear reputation model seems to be the right path to take. It costs less, it is suitable for reputation scores, making it easy to rate, and the decision-making authority and control are spread out among different individuals, groups, or nodes in a network, and decisions are made through a consensus or democratic process.

To maintain the privacy of the users, tokens and a digital fingerprint shall be used, keeping in mind the need to have some sort of identity in store. Creating a token on blockchain software requires some information.

[5] https://www.blockchain-council.org/blockchain/types-of-blockchains-explained-public-vs-private-vs-consortium/

The user's wallet address is a unique identifier that allows the user to receive, store, and send tokens on the blockchain. It is important to ensure that the user's wallet address is accurate and secure.

It's necessary to collect some personal information from the user, such as their name, email address, and date of birth. This information can be used to verify the user's identity and comply with regulatory requirements.

Detailing the token is needed; information such as its name, symbol, total supply, and decimal places are important, for these details will determine how the token functions on the blockchain.

You will need to develop or deploy a smart contract that defines the token's behaviour and rules for interactions with the blockchain. This may include the transfer of tokens between users, token burn or mint functions, and any other functionalities specific to the token.

The use of tokens is another reason why smart contracts are important in the development of the reputation model. A public blockchain has some templates that can be used to help new users get started.

So, the information needed to create a token on a blockchain will depend on the specific blockchain and token being created, as well as any regulatory requirements that may apply. It is important to ensure that all user information is collected and stored securely and that any necessary regulatory compliance measures are followed.

At the present time, it's believed, after reading several articles about reputation models, that scoring the purchase and commenting on the product is more effective in assuring a more reliable trust in the product/seller.

5.6 Reputation model Guidelines

With that said, we believe that a reputation model that uses a one to four score prevents people from feeling the comfort of choosing the middle mark. The comments are also important. The more recent comments and scoring must have a bigger weight, especially the last six months.

The buyer's return is also important. An algorithm that can track the many times a buyer returned to that seller is important, and it gives credibility to the products. The

token can be a way to control every time a buyer purchases from a specific seller. It is also important to track how many times the buyer returned the seller's products.

Also, in the present time, where social media has such a significant impact, and influencers are a new marketing product, Endorsement has a saying when addressing reputation. Having public statements, testimonials, and social media posts linked to the seller's marketplace is a plus.

Keep in mind that people will comment and score in purchase when they have something to gain. Few or no buyers will leave a comment or score a purchase just because they really liked the product. However, when given a little treat, the buyer is more compelled to leave feedback. Most times, it is given discounts or points to be traded in a future purchase. It is safe to say that if the purchase does not meet the buyer's expectations, the buyer will not purchase again. So, the points given must have an expiration date of up to three or four months and, if not used, count as negative feedback for the seller since the buyer did not return and no feedback is given.

All of this seems simple, but the problem is that the user can create several accounts or have several accounts in different marketplaces.

It's a goal to have a reputation system that works for all marketplaces, possibly using the public and decentralized blockchain. So, we present several strategies that can be used to make it more difficult or to discourage users from doing so.

Implement a verification process. This requires the users to verify their identity through a phone number or email address to create an account. This can make it more difficult for users to create multiple accounts.

Set a limit on how many accounts can be created from a single device or IP address. This can help prevent users from creating multiple accounts on the same device or location.

Train machine learning algorithms to detect patterns that may indicate fraudulent activity, such as multiple accounts being created from the same device or IP address. Keep track of user behaviour and flag suspicious activity, such as multiple accounts being created from the same device or IP address. This can help you identify users who are trying to cheat the system. Make it clear in your terms of service that creating multiple

accounts is not allowed and will result in penalties, such as account suspension or termination.

By using a combination of these strategies, it's more difficult for users to create multiple accounts on the marketplace.

Summarizing, the algorithm must have the following information to create a more effective reputation model that can face a large sum of attacks:

1. One to four score, where up to two is negative, three up is positive. A score of one to four is used, where up to two is negative, and three up is positive.
2. Aging, recent comments have more impact on the reputation than the one from six months ago.
3. Returning the product. How many times has the buyer returned one or more products?
4. The repurchase at that seller's marketplace. How many times does a buyer return?
5. Endorsement and positive comments on social media.
6. Awarding feedback is where the award has a due time.
7. Assure that the user cannot create several accounts.
8. Financial system where being dishonest doesn't pay off
9. Use of AI to identify platform use patterns

Studies have yet to continue. The technological development and the capacity to overcome the system make this scientific area a moving area, so it is believed that a constant need to update and investigate is necessary. Even though the base of a reputation model, having in mind the literature ate the present time, shows that these variables are important and need to be present, in a few months more variables might be added. Even blockchain is in development and must always be updated.

Trust is essential in e-commerce because buyers and sellers need to rely on each other to complete transactions. If buyers do not trust sellers, they are unlikely to make purchases, which can lead to a decrease in sales for businesses. Similarly, if sellers do not trust buyers, they may be hesitant to sell their goods or services, which can lead to a decrease in the availability of goods and services online.

Trust issues can also lead to fraudulent activities, such as online scams, phishing attacks, and identity theft, which can damage the reputation of e-commerce platforms and deter customers from using them.

In addition, trust issues can lead to a lack of transparency in e-commerce transactions, which can make it difficult for buyers and sellers to resolve disputes. This can lead to legal issues and further damage the reputation of e-commerce platforms.

Overall, the problem of trust in e-commerce can have a significant impact on the industry. It can lead to a decrease in sales, a lack of availability of goods and services online, fraudulent activities, legal issues, and damage to the reputation of e-commerce platforms. This is why building trust in e-commerce is essential, and reputation plays a crucial role in achieving this goal.

Our study shows some of the problems that e-commerce platforms encounter, and we find that bad-mouthing and ballot-stuffing are common attacks that one can find. Collusion, constant attacks on a specific target, possibly a direct competitor, whitewashing, and Sybil attacks are commonly present in daily transactions.

In e-commerce, reputation is built through feedback and ratings provided by buyers and sellers.

Positive feedback and high ratings indicate that a seller is trustworthy and reliable, while negative feedback and low ratings indicate the opposite. Similarly, buyers who have a good reputation are more likely to be trusted by sellers.

There appears to be agreement on the variables that a reputation model requires one must have a rating score, human behaviour has a say in it, whether in the absence or as a user's mode of operation, the information of the users is the most relevant variable, and that information must be private, and anonymity must be ensured.

Another point of agreement is that costs may play a role in determining whether the model is appropriate or not; the more information we have, the more storage we

require, and to provide anonymity, we will need to provide each user with a unique digital identity, which can be extremely expensive.

Furthermore, awarding rewards will have an impact on the seller's profit and may influence the buyer. People react to prizes, and no matter how small the discount is, they are always appreciated. Price reductions may increase customer loyalty to the seller, but it is not a guarantee that the seller is a good seller; it may give him a good reputation percentage, but this could also be only because the prices are low.

On the other hand, the return policy can be used as a key point in developing a more trustworthy model. The greater the number of returns, the less reliable the products, e.g., the seller. It is undeniable that the more information we have, the more we can ensure a more reliable reputation model. However, the security of those data is not explicitly stated, and there is a lack of information on how they will prevent data breaches.

Some reputation models attempted to address the collusion issues of reputation models by allowing the seller to calculate the reputation score based on parameters that they set. This type of model cannot solve all problems because there is no impartial party; if the seller sets the parameters, the seller controls the outcome.

Nonetheless, it is critical to consider psychological factors to improve the reliability of a reputation model that is associated with other data. Emotions, sociocultural factors, inborn or acquired factors, and friend-to-friend information are important, but they are not sufficient, even though we trust people we know and people with similar backgrounds. All of this must be considered when discussing a reputation model.

For that, most authors present Blockchain as a potential platform to store data and contribute to the decentralization of information. A public blockchain is cheaper, and one with large storage can be used. Transparency and privacy are still there, mostly through the tokens. However, as previously mentioned, more studies must be conducted, and it is necessary to pay attention to continuous technological development. (Habib et al., 2022)

Blockchain presents itself to mitigate some problems, but as it has been shown, it is not bulletproof.

More research is needed to understand how one can use blockchain technology advantages and how to mitigate the issues that the current reputation system has.

The use of some variables discussed here, and the understanding of the mathematical algorithm are needed to create or conceptualize a stronger reputation model that one can use to implement and construct a reputation system that can overcome most of these attacks due to its characteristics. Blockchain is a potential technology that can enhance reputation systems.

Being blockchain and the reputation systems technologies that are in constant evolution, more readings and more studies need to be conducted, and is a strong belief that these studies have to be continuous and keep up with the technological evolution.

1. Ahn, J., Park, M., & Paek, J. (2018). Reptor: A Model for Deriving Trust and Reputation on Blockchain-based Electronic Payment System. At 2018 International Conference on Information and Communication Technology Convergence (ICTC). IEEE. https://doi.org/10.1109/ictc.2018.8539641
2. Ali, S., Wang, G., White, B., & Cottrell, R. L. (2018). A Blockchain-Based Decentralized Data Storage and Access Framework for PingER. In 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE). IEEE. https://doi.org/10.1109/trustcom/bigdatase.2018.00179
3. Analyses: The PRISMA Statement," Phys Ther, vol. 89, no. 9, pp. 873–880, 2009, doi: 10.1093/ptj/89.9.873.
4. Arner, D. W., Barberis, J. N., & Buckley, R. P. (2015). The evolution of fintech: A new post-crisis paradigm? University of Pennsylvania Journal of International Law, 36(2), 203-282.
5. Atif, Y. (2002). Building trust in e-commerce. *IEEE Internet Computing*, *6*(1), 18–24. https://doi.org/10.1109/4236.978365
6. B. Kitchenham, "Procedures for performing systematic reviews (Joint technical report No. Keele university technical report TR/SE-0401 // NICTA technical report 0400011T.1; p. 27)," *https://www.inf.ufsc.br/~aldo.vw/kitchenham.pdf.* 2004.
7. Bhumika, T., Jyoti, Neha, G., & Santosh, K. (2022). Overview of Electronic commerce (E-commerce). i-manager's Journal on Information Technology, 11(2), 29. https://doi.org/10.26634/jit.11.2.18955
8. Brereton, P., Kitchenham, B. A., Budgen, D., Turner, M., & Khalil, M. (2007). Lessons from applying the systematic literature review process within the software engineering domain. Journal of Systems and Software, 80(4), 571–583. https://doi.org/10.1016/j.jss.2006.07.009
9. C. Dellarocas., "Mechanisms for coping with unfair ratings and discriminatory behaviour in online reputation reporting systems," *Proceedings of the twenty first international conference on Information systems (ICIS '00)*, pp. 520–525, 2000.
10. C. Kugblenu and P. Vuorimaa, "Decentralized Reputation System on a Permissioned Blockchain for E-Commerce Reviews." pp. 177–182, 2020. doi: 10.1007/978-3-030-43020-7_24.
11. Cardoso, T., Alarcão, I., & Celorico, J. (2010). Revisão da literatura e sistematização do conhecimento (P. Editora Ed. 2010 ed.): Porto Editora.

12. D. Liu, A. Alahmadi, J. Ni, X. Lin, and X. Shen, “Anonymous Reputation System for IIoT-Enabled Retail Marketing Atop PoS Blockchain,” *IEEE Trans Industr Inform*, vol. 15, no. 6, pp. 3527–3537, Oct. 2019, doi: 10.1109/TII.2019.2898900.
13. Dennis, R., & Owen, G. (2015). Rep on the block: A next generation reputation model based on the blockchain. In 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST). IEEE. https://doi.org/10.1109/icitst.2015.7412073
14. Dhakal, A., & Cui, X., (2019). DTrust: A Decentralized Reputation model for E-commerce Marketplaces.
15. Druschel, P., Kaashoek, F., & Rowstron, A. (Eds.). (2002). Peer-to-Peer Systems. Springer Berlin Heidelberg. https://doi.org/10.1007/3-540-45748-8
16. E. Koutrouli and A. Tsalgatidou, “Taxonomy of attacks and defense mechanisms in P2P reputation systems—Lessons for reputation system designers,” *Comput Sci Rev*, vol. 6, no. 2–3, pp. 47–70, 2012, doi: 10.1016/j.cosrev.2012.01.002.
17. Engineering Technical report, Ver. 2.3 EBSE Technical Report. EBSE.
18. F. Hendrikx, K. Bubendorfer, and R. Chard, “Reputation systems: A survey and taxonomy,” *J Parallel Distrib Comput*, vol. 75, pp. 184–197, 2015, doi: 10.1016/j.jpdc.2014.08.004.
19. Fornaciari, M., & Rus, V. (2021). Blockchain-based reputation management systems for e-commerce: A systematic literature review. Journal of Cleaner Production, 283, 125369. doi: 10.1016/j.jclepro.2020.125369
20. G. F. Camilo, G. A. F. Rebello, L. A. C. de Souza, and O. C. M. B. Duarte, “A Secure Personal-Data Trading System Based on Blockchain, Trust, and Reputation,” in *2020 IEEE International Conference on Blockchain (Blockchain)*, Oct. 2020, pp. 379–384. doi: 10.1109/Blockchain50366.2020.00055.
21. Ghandour, “Ecommerce website value model for SMEs. Int J. Electron Commerce,” pp. 203–222, 2015.
22. Gonçalves, M. J. A., Pereira, R. H., & Coelho, M. A. G. M. (2022). User Reputation on E-Commerce: Blockchain-Based Approaches. Journal of Cybersecurity and Privacy, 2(4), 907–923. https://doi.org/10.3390/jcp2040046
23. Grigg, I. (2019). Triple-entry accounting using blockchain technology. The Journal of the British Blockchain Association, 2(1), 1-8.
24. Gu, S., Ślusarczyk, B., Hajizada, S., Kovalyova, I., & Sakhbieva, A. (2021). Impact of the COVID-19 Pandemic on Online Consumer Purchasing Behaviour. Journal of Theoretical

and Applied Electronic Commerce Research, 16(6), 2263–2281. https://doi.org/10.3390/jtaer16060125

25. Habib, G., Sharma, S., Ibrahim, S., Ahmad, I., Qureshi, S., & Ishfaq, M. (2022). Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing. Future Internet, 14(11), 341. https://doi.org/10.3390/fi14110341
26. Hoffman, K., Zage, D., & Nita-Rotaru, C. (2009). A survey of attack and defense techniques for reputation systems. ACM Computing Surveys, 42(1), 1–31. https://doi.org/10.1145/1592451.1592452
27. J. Ahn, M. Park, and J. Paek, "Reptor: A Model for Deriving Trust and Reputation on Blockchain-based Electronic Payment System," in *2018 International Conference on Information and Communication Technology Convergence (ICTC)*, Oct. 2018, pp. 1431–1436. doi: 10.1109/ICTC.2018.8539641.
28. J. Ahn, M. Park, H. Shin, and J. Paek, "A Model for Deriving Trust and Reputation on Blockchain-Based e-Payment System," *Applied Sciences*, vol. 9, no. 24, p. 5362, Oct. 2019, doi: 10.3390/app9245362.
29. J. R. Douceur, "The Sybil Attack. In: Druschel, P., Kaashoek, F., Rowstron, A. (eds) Peer-to-Peer Systems.," *Lecture Notes in Computer Science, vol 2429. Springer, Berlin, Heidelberg*, vol. 2429, 2002.
30. J. Sänger, C. Richthammer, A. Rösch, and G. Pernul, "Reusable Defense Components for Online Reputation Systems," 2015, pp. 195–202. doi: 10.1007/978-3-319-18491-3_15.
31. J. Thomas, D. Gough, and S. Oliver, *Introduction to Systematic Reviews*, 2nd ed. Los Angeles: SAGE Publications, Limited., 2017.
32. Jøsang, A., Ismail, R., & Boyd, C. (2007). A survey of trust and reputation systems for online service provision. Decision Support Systems, 43(2), 618–644. https://doi.org/10.1016/j.dss.2005.05.019
33. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," Decis Support Syst, pp. 618–644, 2007.D. Moher, A. Liberati, J. Tetzlaff, and D. G. Altman, "Reprint—Preferred Reporting Items for Systematic Reviews and Meta-
34. Joshi, P., & Kumar, A. (2020). A Novel Framework for Decentralized C2C E-commerce using Smart Contract. In 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT). IEEE. https://doi.org/10.1109/icccnt49239.2020.9225377

35. K. C. Laudon and C. G. Traver, E-commerce : business, technology, society. 2019.
36. K. Christidis and M. Devetsikiotis, “Blockchains and smart contracts for the internet of things,” pp. 2292–2303, 2016.
37. K. Hoffman, D. Zage, and C. Nita-Rotaru, “A survey of attack and defense techniques for reputation systems,” *ACM Comput Surv*, vol. 42, no. 1, pp. 1–31, 2009, doi: 10.1145/1592451.1592452.
38. Keele, S. (2007). Guidelines for performing systematic literature reviews in software engineering Technical report, Ver. 2.3 EBSE Technical Report. EBSE.
39. Kugblenu, C., & Vuorimaa, P. (2020). Decentralized Reputation model on a Permissioned Blockchain for E-Commerce Reviews. In Advances in Intelligent Systems and Computing (pp. 177–182). Springer International Publishing. https://doi.org/10.1007/978-3-030-43020-7_24
40. L. Mui, M. Mohtashemi, and A. Halberstadt, “Notions of reputation in multi-agents systems: a review.,” pp. 280–287, 2002.
41. L. Sherman, “A Decentralized Reputation System. How Blockchain Can Restore Trust In Online Markets,” 2018.
42. L. Zeynalvand, T. Luo, E. Andrejczuk, D. Niyato, S. G. Teo, and J. Zhang, “A Blockchain-Enabled Quantitative Approach to Trust and Reputation Management with Sparse Evidence,” *Proceedings of the 20th International Conference on Autonomous Agents and MultiAgent Systems (AAMAS ’21).*, 2021.
43. Laudon, Kenneth & Traver, Carol (2020). E-Commerce 2019 (15th Edition): Business, Technology, Society. Boston, USA: Pearson-Prentice Hall.
44. Li, J., Chen, X., & Wu, J. (2019). A blockchain-based e-commerce reputation model. Future Generation Computer Systems, 92, 720-727.
45. Li, M., Zhu, L., Zhang, Z., Lal, C., Conti, M., & Alazab, M. (2021). Anonymous and Verifiable Reputation model for E-commerce Platforms based on Blockchain. IEEE Transactions on Network and Service Management, 1. https://doi.org/10.1109/tnsm.2021.3098439
46. Li, X., Li, Y., Li, J., & Wu, F. (2017). E-commerce reputation management based on blockchain technology. In Proceedings of the 14th International Conference on e-Business Engineering (pp. 64-69). ACM. doi: 10.1145/3168254.3168280
47. Li, Z., Li, J., & Zhang, X. (2019). A blockchain-based reputation model for e-commerce systems. In Proceedings of the 13th International Conference on Ubiquitous Information Management and Communication (pp. 1-6).

48. Liu, D., Alahmadi, A., Ni, J., Lin, X., & Shen, X. (2019). Anonymous Reputation model for IIoT-Enabled Retail Marketing Atop PoS Blockchain. IEEE Transactions on Industrial Informatics, 15(6), 3527–3537. https://doi.org/10.1109/tii.2019.2898900
49. Liu, X., & Ma, J. (2018). A reputation model for e-commerce based on blockchain and smart contract. Journal of Physics: Conference Series, 1021(1), 012082.
50. Liu, Y., Zhou, X., & Yu, H. (2021). 3R model: A post-purchase context-aware reputation model to mitigate unfair ratings in e-commerce. Knowledge-Based Systems, 231, 107441. https://doi.org/10.1016/j.knosys.2021.107441
51. M. Dixon-Woods and R. Fitzpatrick, "Qualitative research in systematic reviews: Has established a place for itself.," *Br Med J*, vol. 323, pp. 765–766, 2001.
52. M. Li, L. Zhu, Z. Zhang, C. Lal, M. Conti, and M. Alazab, "Anonymous and Verifiable Reputation System for E-Commerce Platforms Based on Blockchain," *IEEE Transactions on Network and Service Management*, vol. 18, no. 4, pp. 4434–4449, Oct. 2021, doi: 10.1109/TNSM.2021.3098439.
53. M. Petticrew and H. (Roberts, *Systematic reviews in the social sciences: A practical guide (1 edition*, 1st ed. Oxford: Wiley-Blackwell, 2005.
54. M. Zulfiqar *et al.*, "EthReview: An Ethereum-based Product Review System for Mitigating Rating Frauds," *Comput Secur*, vol. 100, p. 102094, Oct. 2021, doi: 10.1016/j.cose.2020.102094.
55. Noyes, J., Booth, A., Flemming, K., Garside, R., Harden, A., Lewin, S., Pantoja, T., Hannes, K., Cargo, M., & Thomas, J. (2018). Cochrane Qualitative and Implementation Methods Group guidance series—paper 3: methods for assessing methodological limitations, data extraction and synthesis, and confidence in synthesized qualitative findings. Journal of Clinical Epidemiology, 97, 49–58. https://doi.org/10.1016/j.jclinepi.2017.06.020
56. P. S. Aithal A, "Review on Various E-Business and M-Business Models & Research Opportunities," International Journal of Management, IT and Engineering, vol. 6, no. 1, pp. 275–298, 2016.
57. Panagopoulos, E. Koutrouli, and A. Tsalgatidou, "Modeling and evaluating a robust feedback-based reputation system for e-commerce platforms," *ACM Trans. Web 11, 3*, vol. 18, p. 55, 2017.
58. Panagopoulos, A., Koutrouli, E., & Tsalgatidou, A. (2017). Modeling and Evaluating a Robust Feedback-Based Reputation System for E-Commerce Platforms. *ACM Transactions on the Web*, *11*(3), 1–55. https://doi.org/10.1145/3057265

59. Pereira, R. H., Gonçalves, M. J., & Magalhães, M. A. G. (2023). Reputation Systems: A framework for attacks and frauds classification. Journal of Information Systems Engineering and Management, 8(1), 19218. https://doi.org/10.55267/iadt.07.12830
60. Petersen, K., Vakkalanka, S., & Kuzniarz, L. (2015). Guidelines for conducting systematic mapping studies in software engineering: An update. Information and Software Technology, 64, 1–18. https://doi.org/10.1016/j.infsof.2015.03.007
61. R. B. Briner, D. Denyer, and D. M. Rousseau, "Evidence-Based Management: Concept Cleanup Time?," *Academy of Management Perspectives*, vol. 23, no. 4, pp. 19–32, 2009, doi: 10.5465/AMP.2009.45590138.
62. R. Dennis and G. Owenson, "Rep on the Roll: A Peer to Peer Reputation System Based on a Rolling Blockchain," *International Journal for Digital Society*, vol. 7, no. 1, Oct. 2016, doi: 10.20533/ijds.2040.2570.2016.0137.
63. Ramachandiran, R., (2018). Using Blockchain Technology to Improve Trust In eCommerce Reviews. 10.13140/RG.2.2.29324.00646.
64. Resnick, P., Kuwabara, K., Zeckhauser, R., & Friedman, E. (2000). Reputation models. Communications of the ACM, 43(12), 45–48. https://doi.org/10.1145/355112.355122
65. S. Goyal, B. S. Sergi, and M. Esposito, "Literature review of emerging trends and future directions of e-commerce in global business landscape," World Review of Entrepreneurship, Management and Sustainable Development, vol. 15, no. 1–2, pp. 226–255, 2019, doi: 10.1504/WREMSD.2019.098454
66. S. M. Shafer, H. J. Smith, and J. C. Linder, "The power of business models, Business Horizons," vol. 48, no. 3, pp. 199–207, 2005.
67. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System." [Online]. Available: www.bitcoin.org
68. Saeed, S. (2023). A Customer-Centric View of E-Commerce Security and Privacy. Applied Sciences, 13(2), 1020. https://doi.org/10.3390/app13021020
69. Schaub, A., Bazin, R., Hasan, O., & Brunie, L. (2016). A Trustless Privacy-Preserving Reputation model. In ICT Systems Security and Privacy Protection (pp. 398–411). Springer International Publishing. https://doi.org/10.1007/978-3-319-33630-5_27
70. Settey, J. Gnap, D. Beňová, M. Pavličko, and O. Blažeková, "The Growth of E-Commerce Due to COVID-19 and the Need for Urban Logistics Centers Using Electric Vehicles: Bratislava Case Study," Sustainability, vol. 13, no. 10, p. 5357, Oct. 2021, doi: 10.3390/su13105357.

71. Soleimani, M. (2021). Buyers' trust and mistrust in e-commerce platforms: a synthesizing literature review. Information Systems and e-Business Management, 20(1), 57–78. https://doi.org/10.1007/s10257-021-00545-0
72. Soleimani, M. Buyers' trust and mistrust in e-commerce platforms: a synthesizing literature review. Inf Syst E-Bus Manage 20, 57–78 (2022). https://doi.org/10.1007/s10257-021-00545-0
73. Sun, Y., Zhang, R., Xue, R., Su, Q., & Li, P. (2020). A Reputation Based Hybrid Consensus for E-Commerce Blockchain. In Web Services – ICWS 2020 (pp. 1–16). Springer International Publishing. https://doi.org/10.1007/978-3-030-59618-7_1
74. Swamynathan, G., Almeroth, K. C., & Zhao, B. Y. (2010). The design of a reliable reputation system. Electronic Commerce Research, 10(3-4), 239–270. https://doi.org/10.1007/s10660-010-9064-y
75. Swan, M. (2015). Blockchain: Blueprint for a new economy. O'Reilly Media, Inc.
76. T. Karode, W. Werapun, and T. Arpornthip, "Blockchain-based Global Travel Review Framework," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 8, 2020, doi: 10.14569/IJACSA.2020.0110813.
77. Wang, J., Peng, Y., & Chen, H. (2018). A reputation model for e-commerce based on blockchain and multi-agent systems. In Proceedings of the 14th International Conference on Computational Intelligence and Security (pp. 278-282).
78. Webster, J., & Watson, R. (2002). Analyzing the past to prepare for the future: Writing a literature review. Management Information Systems Quarterly, 26(2), 3.
79. Y. Liu, X. Zhou, and H. Yu, "3R model: A post-purchase context-aware reputation model to mitigate unfair ratings in e-commerce," *Knowl Based Syst*, vol. 231, p. 107441, 2021, doi: 10.1016/j.knosys.2021.107441.
80. Y. Yao, S. Ruohomaa, and F. Xu, "Addressing Common Vulnerabilities of Reputation Systems for Electronic Commerce," *Journal of theoretical and applied electronic commerce research*, vol. 7, no. 1, pp. 3–4, 2012, doi: 10.4067/S0718-18762012000100002.
81. Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology?—A systematic review. PloS one, 11(10), e0163477. doi: 10.1371/journal.pone.0163477
82. Yuan, Y., Bi, J., & Wang, Y. (2021). Design of a blockchain-based reputation system for e-commerce. Journal of Information Science and Engineering, 37(3), 717-734.
83. Z. Zhou, M. Wang, C.-N. Yang, Z. Fu, X. Sun, and Q. M. J. Wu, "Blockchain-based decentralized reputation system in E-commerce environment," *Future Generation*

Computer Systems, vol. 124, pp. 155–167, Oct. 2021, doi: 10.1016/j.future.2021.05.035.

84. Zhang, X., Wen, Y., Li, X., & Huang, Y. (2018). A reputation-based trust mechanism for e-commerce in the age of blockchain. International Journal of Information Management, 39, 80-88. doi: 10.1016/j.ijinfomgt.2017.12.006
85. Zhao, Y., Li, L., & Zhang, C. (2018). A blockchain-based reputation model for e-commerce. In Proceedings of the 4th International Conference on Frontiers of Educational Technologies (pp. 120-124).
86. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. IEEE International Congress on Big Data (pp. 557-564). IEEE. doi: 10.1109/BigDataCongress.2017.85
87. Zibari, B., Abu-Tayeh, G., Alsmadi, M. K., & Tarhini, A. (2021). Blockchain-based reputation management in e-commerce: A systematic literature review. Sustainability, 13(4), 2104. doi: 10.3390/su13042104

1. https://simplicable.com/new/reputation-systems, viewed on January 29th 2023

2. https://itlaw.fandom.com/wiki/Reputation-based_system, viewed on January 29th 2023

3. https://library.serviceinnovation.org/Intelligent_Swarming/Practices_Guide/50_Intelligent_Swarming_Practices/20_Recognize/15_Reputation_Models_Badging, viewed on January 29th 2023

4. https://www.investopedia.com/terms/b/blockchain.asp, viewed on Mars 5th 2023

5. https://www.ibm.com/topics/smart-contracts, viewed on Mars 5th 2023

6. https://www.statista.com/outlook/dmo/ecommerce/worldwide, viewed on May 27th 2023

7. https://www.blockchain-council.org/blockchain/types-of-blockchains-explained-public-vs-private-vs-consortium/, viewed on May 27th 2023

8. https://medium.com/@bsse0914/prisma-framework-for-systematic-literature-review-ec8b54872bf1, viewed on June 24th 2023

APPENDAGE I – COMPLETE ARTICLES LIST

Web of Science

Authors	*Article Title*
Gong, YW; van Engelenburg, S; Janssen, M	*A Reference Architecture for Blockchain-Based Crowdsourcing Platforms*
Sun, Y; Xue, R; Zhang, R; Su, QQ; Gao, S	*RTChain: A Reputation System with Transaction and Consensus Incentives for E-commerce Blockchain*
Ahn, J; Park, M; Shin, H; Paek, J	*A Model for Deriving Trust and Reputation on Blockchain-Based e-Payment System*
Kundu, D	*Blockchain and Trust in a Smart City*
Ahn, J; Park, M; Paek, J	*Reptor: A Model for Deriving Trust and Reputation on Blockchain-based Electronic Payment System*
Schaub, A; Bazin, R; Hasan, O; Brunie, L	*A Trustless Privacy-Preserving Reputation System*
de Graaf, TJ	*From old to new: From internet to smart contracts and from people to smart contracts*
Shrestha, AK; Vassileva, J; Joshi, S; Just, J	*Augmenting the technology acceptance model with trust model for the initial adoption of a blockchain-based system*
Chen, CL; Deng, YY; Weng, W; Zhou, M; Sun, HY	*A blockchain-based intelligent anti-switch package in tracing logistics system*
Kaal, WA	*Decentralized Autonomous Organizations: Internal Governance and External Legal Design*
Kabir, MR	*Behavioural intention to adopt blockchain for a transparent and effective taxing system*
Sung, HC	*Can Online Courts Promote Access to Justice? A Case Study of the Internet Courts in China*
Gil-Cordero, E; Cabrera-Sanchez, JP; Arras-Cortes, MJ	*Cryptocurrencies as a Financial Tool: Acceptance Factors*

Thiebes, S; Lins, S; Sunyaev, A	*Trustworthy artificial intelligence*
Li, M; Shao, SJ; Ye, QW; Xu, GY; Huang, GQ	*Blockchain-enabled logistics finance execution platform for capital-constrained E-commerce retail*
Badi, S; Ochieng, E; Nasaj, M; Papadaki, M	*Technological, organisational and environmental determinants of smart contracts adoption: UK construction sector viewpoint*
Ferrer-Gomila, JL; Hinarejos, MF	*A 2020 perspective on A fair contract signing protocol with blockchain support*
Su, X; Liu, YM; Choi, C	*A Blockchain-Based P2P Transaction Method and Sensitive Data Encoding for E-Commerce Transactions*
Wamba, SF; Queiroz, MM	*Blockchain in the operations and supply chain management: Benefits, challenges and future research opportunities*
Parekh, J; Jaffe, A; Bhanushali, U; Shukla, S	*Disintermediation in medical tourism through blockchain technology: an analysis using value-focused thinking approach*
Talamo, M; Arcieri, F; Dimitri, A; Schunck, CH	*A Blockchain based PKI Validation System based on Rare Events Management*
Hong, WC; Chen, YC; Yang, RK; Li, B; Lee, JS	*Efficient Peer-to-Peer E-Payment Based on Asynchronous Dual Blockchain*
Mut-Puigserver, M; Cabot-Nadal, MA; Payeras-Capella, MM	*Removing the Trusted Third Party in a Confidential Multiparty Registered eDelivery Protocol Using Blockchain*
Cao, SZ; Wang, F; Lang, XL; Wang, R; Liu, XY	*Multi-party Contract Signing Protocol Based on Certificateless*
Mileros, MD; Lakemond, N; Forchheimer, R	*Towards a Taxonomy of E-commerce: Characterizing Content Creator-Based Business Models*
Ferrer-Gomila, JL; Hinarejos, MF; Isern-Deya, AP	*A fair contract signing protocol with blockchain support*
Le, HT; Le, NTT; Phien, NN; Duong-Trung, N; Son, HX; Huynh, TT; Nguyen, TP	*Introducing Multi Shippers Mechanism for Decentralized Cash on Delivery System*
Liu, CC; Xiao, YH; Javangula, V; Hu, Q; Wang, SL; Cheng, XZ	*NormaChain: A Blockchain-Based Normalized Autonomous Transaction Settlement System for IoT-Based E-Commerce*
Kamble, S; Gunasekaran, A; Arha, H	*Understanding the Blockchain technology adoption in supply chains-Indian context*
Mao, DH; Hao, ZH; Wang, F; Li, HS	*Novel Automatic Food Trading System Using Consortium Blockchain*

Yeh, JY; Liao, SC; Wang, YT; Chen, YJ	*Understanding Consumer Purchase Intention in a Blockchain Technology for Food Traceability and Transparency context*
Toleva-Stoimenova, S; Christozov, D; Rasheva-Yordanova, K	*Introduction of Emerging Technology into Higher Education Curriculum: The Case of Blockchain Technology as Part of Data Science Master Program*
Zhu, XX; Wang, D	*Research on Blockchain Application for E-Commerce, Finance and Energy*
Mehrwald, P; Treffers, T; Titze, M; Welpe, IM	*Application of Blockchain Technology in the Sharing Economy: A Model of Trust and Intermediation*
Fleischmann, M; Ivens, BS	*Exploring the Role of Trust in Blockchain Adoption: An Inductive Approach*
Hawlitschek, F; Notheisen, B; Teubner, T	*The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy*
Li, B; Wang, YJ	*RZKPB: A Privacy-preserving Blockchain-Based Fair Transaction Method for Sharing Economy*
Xie, WL; Zhou, W; Kong, LJ; Zhang, XD; Min, XP; Xiao, ZS; Li, QZ	*ETTF: A Trusted Trading Framework Using Blockchain in E-commerce*
Dixit, A; Norta, A	*A Self-Aware Contract For Decentralized Peer-To-Peer (P2P) Commerce*
Xie, C; Guo, HY; He, DF	*Research on the Construction of Traceability System for E-commerce Agricultural Products Quality and Safety in China Based on Blockchain*
Chen, YH; Chen, SH; Lin, IC	*Blockchain based Smart Contract for Bidding System*
Dai, MJ; Zhang, SL; Wang, H; Jin, S	*A Low Storage Room Requirement Framework for Distributed Ledger in Blockchain*
Zamani, ED; Giaglis, GM	*With a little help from the miners: distributed ledger technology and market disintermediation*
Grover, P; Kar, AK; Ilavarasan, PV	*Blockchain for Businesses: A Systematic Literature Review*
Patsonakis, C; Samari, K; Roussopoulos, M; Kiayias, A	*Towards a Smart Contract-Based, Decentralized, Public-Key Infrastructure*
Zhang, N; Zhong, S; Tian, L	*Using Blockchain to Protect Personal Privacy in the Scenario of Online Taxi-hailing*
Ryan, P	*Smart Contract Relations in e-Commerce: Legal Implications of Exchanges Conducted on the Blockchain*

Jarvenpaa, S; Teigland, R	*Trust in Digital Environments: From the Sharing Economy to Decentralized Autonomous Organizations*
Min, XP; Li, QZ; Liu, L; Cui, LZ	*A Permissioned Blockchain Framework for Supporting Instant Transaction and Dynamic Block Size*
Ateniese, G; Faonio, A; Magri, B; de Medeiros, B	*Certified Bitcoins*
Zulfigar, M; Tarig, F; Janjua, MU; Mian, AN; Qayyum, A; Qadir, J; Sher, F; Hassan, M	*EthReview: An Ethereum-based Product Review System for Mitigating Rating Frauds*
Karode, T; Werapun, W; Arpornthip, T	*Blockchain-based Global Travel Review Framework*
Huang, HH; Cai, J; Xie, SC	*Implementing an Asset Trading System Based on Blockchain and Game Theory*
Asgaonkar, A; Krishnamachari, B	*Solving the Buyer and Seller's Dilemma: A Dual-Deposit Escrow Smart Contract for Provably Cheat-Proof Delivery and Payment for a Digital Good without a Trusted Mediator*
Hassija, V; Bansal, G; Chamola, V; Saxena, V; Sikdar, B	*BlockCom: A Blockchain based Commerce Model for Smart Communities using Auction Mechanism*
Yang, CN; Chen, YC; Chen, SY; Wu, SY	*A Reliable E-commerce Business Model Using Blockchain Based Product Grading System*
Hasan, HR; Salah, K	*Blockchain-Based Proof of Delivery of Physical Assets With Single and Multiple Transporters*
Gupta, S; Gupta, S; Mathew, M; Sama, HR	*Prioritizing intentions behind investment in cryptocurrency: a fuzzy analytical framework*

Scopus

Title	*Source title*
Blockchain-Based Fog Computing Model (BFCM) for IoT Smart Cities	*International Journal of Information Management*
International Conference on Emerging Technologies and Intelligent Systems, ICETIS 2021	*Electronic Commerce Research and Applications*

A blockchain-based trust system for decentralised applications: When trustless needs trust	*Electronics (Switzerland)*
A novel framework of collaborative early warning for COVID-19 based on blockchain and smart contracts	*ACM Transactions on Internet Technology*
A peer-to-peer verifiable and secure energy trading framework based on blockchain technology	*Lecture Notes in Networks and Systems*
A Distributed Fewer Environment for the Use of Blockchain IoT Device Sharing	*Proceedings of the International Joint Conference on Autonomous Agents and Multiagent Systems, AAMAS*
Application of Blockchain Technology in Used Vehicle Market: A Review	*Computers and Security*
The impact of blockchain on e-commerce: A framework for salient research topics	*Proceedings - 2020 IEEE International Conference on Blockchain, Blockchain 2020*
A blockchain-based intelligent anti-switch package in tracing logistics system	*Journal of Intelligent and Fuzzy Systems*
Trustless Virtual PON Sharing for 5G Services	*Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*
Towards event-driven decentralized marketplaces on the blockchain	*Advances in Intelligent Systems and Computing*
Defs—data exchange with free sample protocol	*International Journal of Computers and their Applications*
A multi-party contract signing solution based on blockchain	*Applied Sciences (Switzerland)*
Digitalizing land administration: The geographies and temporalities of infrastructural promise	*IEEE Transactions on Industrial Informatics*

A systematic literature review on applications of information and communication technologies and blockchain technologies for precision agriculture development	*IFIP Advances in Information and Communication Technology*
ITrade: A Blockchain-based, Self-Sovereign, and Scalable Marketplace for IoT Data Streams	*EAI/Springer Innovations in Communication and Computing*
The sharing economy is in real estate, from the institute of trust to the decentralized solutions	*Journal of Physics: Conference Series*
Blockchain technology and trust relationships in trade finance	*2021 International Conference on Information Technology, ICIT 2021 - Proceedings*
Anti-collusion data auction mechanism based on smart contract	*25th International Conference on Optical Network Design and Modelling, ONDM 2021*
The Reconstruction of Accounting Information Disclosure System Based on Blockchain Technology	*DEBS 2021 - Proceedings of the 15th ACM International Conference on Distributed and Event-Based Systems*
Modeling and Analysis of Data Trading on Blockchain-Based Market in IoT Networks	*Geoforum*
Research on Enterprise Trust Relationship of Jilin Province Agricultural Products Supply Chain Based on Big Data Blockchain Logistics	*Journal of Cleaner Production*
Architecture design and application of distributed power trading system based on blockchain asynchronous consensus	*Information Sciences*
A Review on Trust and Reputation Management Systems in e-commerce and P2P Network	*Journal of Physics: Conference Series*
The effect of thickness-based dynamic matching mechanism	*IEEE Internet of Things Journal*

on a hyperledger fabric-based timebank system	
Block Chain Based Supply Chain Financial Risk Management Research	*Proceedings - 2021 4th International Conference on Advanced Electronic Materials, Computers and Software Engineering, AEMCSE 2021*
Proxy re-encryption enabled secure and anonymous IoT data sharing platform based on blockchain	*Proceedings - 2nd International Conference on E-Commerce and Internet Technology, ECIT 2021*
Discussion on Payment Application in Cross-border E-Commerce Platform from the Perspective of Blockchain	*Future Internet*
Capitalization and Trading System Design of Power Data Based on Blockchain	*Journal of Physics: Conference Series*
RTChain: A Reputation System with Transaction and Consensus Incentives for E-commerce Blockchain	*Journal of Network and Computer Applications*
A privacy-preserving consensus mechanism for an electric vehicle charging scheme	*E3S Web of Conferences*
A Trustworthy Food Resume Traceability System Based on Blockchain Technology	*Dongbei Daxue Xuebao/Journal of Northeastern University*
The impact of blockchain technology on consumer behavior: a multimethod study	*Journal of Network and Computer Applications*
Agora: A Privacy-Aware Data Marketplace	*International Conference on Information Networking*
A Robust and Efficient Micropayment Infrastructure Using Blockchain for e-Commerce	*Journal of Management Analytics*
Increasing privacy and security by integrating a Blockchain Secure Interface into an IoT	*IEEE Transactions on Dependable and Secure Computing*

Device Security Gateway Architecture	
A blockchain-enabled quantitative approach to trust and reputation management with sparse evidence	*Energy Reports*
8th International Conference on HCI in Business, Government and Organizations, HCIBGO 2021, Held as Part of the 23rd HCI International Conference, HCII 2021	*Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*
Trusted Player Transfer Evaluation for Sport Markets based on Blockchain and Locality-Sensitive Hashing	*Personal and Ubiquitous Computing*
Transformation the Business of eCommerce Through Blockchain	*Computer Systems Science and Engineering*
A Transaction Model of Bill Service Based on Blockchain	*42nd Australian Society of Sugar Cane Technologists Conference 2021, ASSCT 2021*
Drug traceability and transparency in medical supply chain using blockchain for easing the process and creating trust between stakeholders and consumers	*Wireless Communications and Mobile Computing*
Using blockchain technology in mobile network to create decentralized home location registry (HLR)	*Lecture Notes in Networks and Systems*
Anonymous and Verifiable Reputation System for E-commerce Platforms based on Blockchain	*Proceedings of the Annual Hawaii International Conference on System Sciences*
Can blockchain technology show provenance and increase value for Australian sugar?	*Mobile Information Systems*
Blockchain-Based Trust Auction for Dynamic Virtual	*IEEE Transactions on Engineering Management*

Machine Provisioning and Allocation in Clouds	
Designing Bidding Systems in Supply Chain Management Using Blockchain Technology	*Complexity*
Blockelm - A public blockchain freight exchange protocol	*Lecture Notes in Electrical Engineering*
Analysis of the Negative Relationship between Blockchain Application and Corporate Performance	*Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*
The Choice Strategy of Authentication Technology for Luxury E-Commerce Platforms in the Blockchain Era	*Smart Innovation, Systems and Technologies*
Distributed Power Trading System Based on Blockchain Technology	*Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*
2nd International Conference on Emerging Trends and Advances in Electrical Engineering and Renewable Energy, ETAEERE 2020	*International Journal of Innovation Science*
OBFP: Optimized Blockchain-Based Fair Payment for Outsourcing Computations in Cloud Computing	*Communications in Computer and Information Science*
Adopting Blockchain in Supply Chain – An Approach for a Pilot	*Transportation Research Part E: Logistics and Transportation Review*
Slaying the Crypto Dragons: Towards a CryptoSure Trust Model for Crypto-economics: Blockchain Versus Trust: The Expert's View of the Crypto Scammers	*Advances in Intelligent Systems and Computing*
Digitizing Physical Assets on Blockchain 2.0: A Smart Contract Approach to Land Transfer and Registry	*ACM International Conference Proceeding Series*

Using blockchain technology in credit rating industry to promote an innovative bond-pays model	*2020 International Conference on Internet of Things and Intelligent Applications, ITIA 2020*
A Case Study for Blockchain in OTC: "BATN": A Prototype for Bid and Ask Trading Network	*iSPEC 2020 - Proceedings: IEEE Sustainable Power and Energy Conference: Energy Transition and Energy Internet*
Should multinational firms implement blockchain to provide quality verification?	*Transportation Research Interdisciplinary Perspectives*
EthReview: An Ethereum-based Product Review System for Mitigating Rating Frauds	*Computer Law and Security Review*
Guided Analytics Software for Smart Aggregation, Cognition, and Interactive Visualisation	*IEEE Network*
Traceability of agricultural product quality and safety based on blockchain – taking fresh e-commerce as an example	*Proceedings of the International Conference on Anti-Counterfeiting, Security and Identification, ASID*
EBEE 2020 - 2020 2nd International Conference on E-Business and E-Commerce Engineering	*2020 IEEE International Smart Cities Conference, ISC2 2020*
Blockchain anonymous trading system based on multi-hop payment	*2020 International Conference on Computer Science and Its Application in Agriculture, ICOSICA 2020*
Block-chain based Energy Tracing Method for Electric Vehicles Charging	*2020 IEEE International Conference on Power Systems Technology, POWERCON 2020*
A Secure Personal-Data Trading System Based on Blockchain, Trust, and Reputation	*ACM International Conference Proceeding Series*
City logistics: Towards a blockchain decision framework for collaborative parcel deliveries in micro-hubs	*2020 International Conference on Technology and Entrepreneurship, ICTE 2020*

Can Online Courts Promote Access to Justice? A Case Study of the Internet Courts in China	*Dianli Zidonghua Shebei/Electric Power Automation Equipment*
Blockchain-Assisted Spectrum Trading between Elastic Virtual Optical Networks	*Computers and Chemical Engineering*
IP Trading System with Blockchain on Web-EDA	*Proceedings - 21st IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, WoWMoM 2020*
BIT: A Blockchain Integrated Time Banking System for Community Exchange Economy	*Technology in Society*
A proof-of-concept of farmer-to-consumer food traceability on blockchain for local communities	*DEBS 2020 - Proceedings of the 14th ACM International Conference on Distributed and Event-Based Systems*
Real-time peer to peer energy trade with blockchain offline channels	*Electronic Commerce Research and Applications*
Performance analysis of blockchain-based systems for industry applications	*IOP Conference Series: Earth and Environmental Science*
Servitization in the Era of Blockchain: The Ice Cream Supply Chain Business Case	*Proceedings of the 12th International Conference on Electronics, Computers and Artificial Intelligence, ECAI 2020*
Energy transaction method of microgrid based on blockchain and improved auction algorithm	*2020 European Conference on Networks and Communications, EuCNC 2020*
A Smart Contract-based agent marketplace for the J-Park Simulator - a knowledge graph for the process industry	*2020 International Wireless Communications and Mobile Computing, IWCMC 2020*
Supply-Chain Management System for Plastic Pipes Market Based on Open Blockchain Framework	*ACM International Conference Proceeding Series*

COST: A Consensus-Based Oracle Protocol for the Secure Trade of Digital Goods	*Proceedings - 2020 IEEE 34th International Parallel and Distributed Processing Symposium Workshops, IPDPSW 2020*
Smart contract-based computing resources trading in edge computing	*IEEE Vehicular Technology Conference*
Blockchain as a confidence machine: The problem of trust & challenges of governance	*IEEE Transactions on Industrial Informatics*
Accepting financial transactions using blockchain technology and cryptocurrency: A customer perspective approach	*IEEE Internet of Things Journal*
Mechanisms for outsourcing computation via a decentralized market	*ACM International Conference Proceeding Series*
A Novel Framework for Decentralized C2C E-commerce using Smart Contract	*Future Internet*
Enhancing E-Commerce through Blockchain (DLTs): The Regulatory Paradox for Digital Governance	*International Journal of Information Management*
A 2020 perspective on "A fair contract signing protocol with blockchain support"	*ICETE 2020 - Proceedings of the 17th International Joint Conference on e-Business and Telecommunications*
A Blockchain-Based P2P Transaction Method and Sensitive Data Encoding for E-Commerce Transactions	*ICETE 2020 - Proceedings of the 17th International Joint Conference on e-Business and Telecommunications*
Research and Application of Adjustable Load Measurement Technology Based on Blockchain	*Lecture Notes in Business Information Processing*
Using Blockchain in the agri-food sector following SARS-CoV-2 pandemic	*Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*

5G network slice brokering: A distributed blockchain-based market	*Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*
Efficient Data Trading and Storage in Internet of Vehicles using Consortium Blockchain	*Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*
Blockchain in the operations and supply chain management: Benefits, challenges and future research opportunities	*Proceedings of the European Conference on Innovation and Entrepreneurship, ECIE*
Towards Trust Enabled Commodity Market for Farmers with Blockchain Smart Contracts	*Journal of Internet Technology*
Pinocchio: A blockchain-based algorithm for sensor fault tolerance in low trust environment	*Mathematical Problems in Engineering*
Blockchain based Power Transaction Asynchronous Settlement System	*IEEE Access*
Achieving Intelligent Trust-Layer for Internet-of-Things via Self-Redactable Blockchain	*IEEE Access*
BitCom: A Commerce Model on Blockchain	*Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*
Blockchain-Based Hierarchical Trust Networking for JointCloud	*Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*
A 2020 perspective on "The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy"	*FEMIB 2020 - Proceedings of the 2nd International Conference on Finance, Economics, Management and IT Business*
A Design and Implementation of Macro Prevention Ticket	*Communications in Computer and Information Science*

Booking System Using Blockchain	
A blockchain based PKI validation system based on rare events management	*Advances in Intelligent Systems and Computing*
A framework for analysing blockchain technology adoption: Integrating institutional, market and technical factors	*2020 IEEE 17th Annual Consumer Communications and Networking Conference, CCNC 2020*
Deconstructing the decentralization trilemma	*Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*
Prov-Trust: Towards a trustworthy sgx-based data provenance system	*Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*
The Impact of Blockchain on Medical Tourism	*Lecture Notes in Business Information Processing*
18th International Conference on Service-Oriented Computing, ICSOC 2020	*IEEE Access*
The bitcoin hunter: Detecting bitcoin traffic over encrypted channels	*Advances in Intelligent Systems and Computing*
A game-based secure trading of big data and iot services: Blockchain as a two-sided market	*2020 International Conference on COMmunication Systems and NETworkS, COMSNETS 2020*
Development of a reliable supply chain system using blockchain	*Advances in Intelligent Systems and Computing*
Improving food transparency through innovation and blockchain technology	*Energies*
Efficient peer-to-peer E-payment based on asynchronous dual blockchain	*Advances in Intelligent Systems and Computing*

A Blockchain Prediction Model on Time, Value, and Purchase Based on Markov Chain and Queuing Theory in Stock Trade	*Dianwang Jishu/Power System Technology*
A Reputation Based Hybrid Consensus for E-Commerce Blockchain	*Proceedings - 2019 IEEE Intl Conf on Parallel and Distributed Processing with Applications, Big Data and Cloud Computing, Sustainable Computing and Communications, Social Computing and Networking, ISPA/BDCloud/SustainCom/SocialCom 2019*
Energy Transaction for Multi-Microgrids and Internal Microgrid Based on Blockchain	*2019 2nd IEEE International Conference on Hot Information-Centric Networking, HotICN 2019*
Cross-Certification towards Distributed Authentication Infrastructure: A Case of Hyperledger Fabric	*2019 2nd International Seminar on Research of Information Technology and Intelligent Systems, ISRITI 2019*
Experiencing the Conditions of Trust: A Practice-Based Exploration of Trust Formation Through an Artificial Society Environment	*2019 IEEE Globecom Workshops, GC Wkshps 2019 - Proceedings*
Enabling medical research through privacy-preserving data markets	*Proceedings of 2019 IEEE 4th Advanced Information Technology, Electronic and Automation Control Conference, IAEAC 2019*
A commons-compatible implementation of the sharing economy: Blockchain-based open source mediation	*Asia-Pacific Power and Energy Engineering Conference, APPEEC*
Decentralized e-learning marketplace: Managing authorship and tracking access to learning materials using blockchain	*Proceedings of the International Conference on Cloud Computing Technology and Science, CloudCom*
Blockchain Technology Transforms E-Commerce for Enterprises	*GIS: Proceedings of the ACM International Symposium on Advances in Geographic Information Systems*
17th International Conference on Information Technology: New Generations, ITNG 2020	*3rd International Conference on Innovative Computing, ICIC 2019*
Decentralized Reputation System on a Permissioned	*Dianzi Yu Xinxi Xuebao/Journal of Electronics and Information Technology*

Blockchain for E-Commerce Reviews	
PEX: Privacy-Preserved, Multi-Tier Exchange Framework for Cross Platform Virtual Assets Trading	*IOP Conference Series: Materials Science and Engineering*
19th IFIP WG 6.11 Conference on e-Business, e-Services, and e-Society, I3E 2020	*Proceedings of the IEEE Symposium on Reliable Distributed Systems*
TIDES: A Trust-Aware IoT Data Economic System with Blockchain-Enabled Multi-Access Edge Computing	*15th International Conference on Network and Service Management, CNSM 2019*
A Framework for the Adoption of Blockchain-Based e-Procurement Systems in the Public Sector: A Case Study of Nigeria	*SIBIRCON 2019 - International Multi-Conference on Engineering, Computer and Information Sciences, Proceedings*
A smart distributed marketplace	*Proceedings - 2019 Innovations in Intelligent Systems and Applications Conference, ASYU 2019*
Blockchain-Based Agri-Food Supply Chain: A Complete Solution	*Computer Law and Security Review*
Synergy of Trust, Blockchain and Smart Contracts for Optimization of Decentralized IoT Service Platforms	*IEEE Transactions on Services Computing*
Blockchain-Based Reputation System in Agri-Food Supply Chain	*2019 17th International Conference on Privacy, Security and Trust, PST 2019 - Proceedings*
Blockchain Enabled Trustless API Marketplace	*IOP Conference Series: Earth and Environmental Science*
IT Security for Measuring Instruments: Confidential Checking of Software Functionality	*2019 International Conference on High Performance Computing and Simulation, HPCS 2019*
Blockchain technology for information security of the energy internet: Fundamentals,	*Proceedings - 2019 2nd IEEE International Conference on Blockchain, Blockchain 2019*

features, strategy and application	
ETSB: Energy Trading System Based on Blockchain	*Proceedings - Companion of the 19th IEEE International Conference on Software Quality, Reliability and Security, QRS-C 2019*
Transaction Model for Electric Vehicle Charging Based on Consortium Blockchain	*Electronic Commerce Research and Applications*
Situational trust and reputation in cyberspace	*IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*
Perishable digital goods trading mechanism for blockchain-based vehicular network	*2019 IEEE International Black Sea Conference on Communications and Networking, BlackSeaCom 2019*
Intelligent Eco Networking (IEN) II: A Knowledge-Driven Future Internet Infrastructure for Value-Oriented Ecosystem	*IEEE Transactions on Industrial Informatics*
The Design and Implementation of Trade Finance Application based on Hyperledger Fabric Permissioned Blockchain Platform	*Trust and Distrust in Digital Economies*
A distributed bilateral resource market mechanism for future telecommunications networks	*Blockchain: The Advent of Disintermediation*
Research on the Influential Factors of Blockchain-based traceable products Purchase Intention	*2019 IEEE Canadian Conference of Electrical and Computer Engineering, CCECE 2019*
Research on Power Transaction Information Security of Microgrid Blockchain Network	*2019 IEEE International Conference on Communications Workshops, ICC Workshops 2019 - Proceedings*
Trust modeling for blockchain-based wearable data market	*ICBC 2019 - IEEE International Conference on Blockchain and Cryptocurrency*

A model for deriving trust and reputation on blockchain-based e-payment system	*E3S Web of Conferences*
A privacy-preserving, accountable and spam-resilient geo-marketplace	*IEEE Vehicular Technology Conference*
A journey of WEB and Blockchain towards the Industry 4.0: An Overview	*Arabian Journal for Science and Engineering*
Multi-party Contract Signing Protocol Based on Certificateless	*Proceedings - 16th IEEE International Symposium on Parallel and Distributed Processing with Applications, 17th IEEE International Conference on Ubiquitous Computing and Communications, 8th IEEE International Conference on Big Data and Cloud Computing, 11th IEEE International Conference on Social Computing and Networking and 8th IEEE International Conference on Sustainable Computing and Communications, ISPA/IUCC/BDCloud/SocialCom/SustainCom 2018*
Research on Blockchain Technology in Promoting Environmental Protection Development of Agricultural Products E-commerce Model in Jilin Province	*Zhongguo Dianji Gongcheng Xuebao/Proceedings of the Chinese Society of Electrical Engineering*
Building Ad-hoc clouds with cloudagora	*2019 IEEE 5th International Conference for Convergence in Technology, I2CT 2019*
TradeMap: A FINMA-compliant Anonymous Management of an End-2-end Trading Market Place	*2019 Innovations in Power and Advanced Computing Technologies, i-PACT 2019*
Decentralized Labor Record System Based on Wavelet Consensus Protocol	*Environment and Urbanization ASIA*
Implementing an asset trading system based on blockchain and game theory	*Proceedings - 2018 15th International Symposium on Pervasive Systems, Algorithms and Networks, I-SPAN 2018*
Blockchain Based Confidential Communication and Authorization Model for IoT Devices	*Computer Law and Security Review*

From old to new: From internet to smart contracts and from people to smart contracts	*2018 2nd Cyber Security in Networking Conference, CSNet 2018*
Block-chain technology - security, platforms	*Proceedings - 2018 IEEE 3rd International Workshops on Foundations and Applications of Self* Systems, FAS*W 2018*
Blockchain for Large-Scale Internet of Things Data Storage and Protection	*Proceedings of the Annual Hawaii International Conference on System Sciences*
Blockchain-based Marketplace for Software Testing	*AEE World Energy Engineering Congress 2019*
Research on Blockchain Application for E-Commerce, Finance and Energy	*Managing Technology for Inclusive and Sustainable Growth - 28th International Conference for the International Association of Management of Technology, IAMOT 2019*
Open Data Market Architecture and Functional Components	*EPiC Series in Computing*
A hybrid blockchain architecture for privacy-enabled and accountable auctions	*IEEE Access*
Towards Transparency and Trustworthy: A Used-Car Deposit Platform Based on Blockchain	*IEEE Access*
A fair contract signing protocol with blockchain support	*Communications in Computer and Information Science*
Blockchain enabled AI marketplace: The price you pay for trust	*Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*
Challenges and opportunities using multichain for real estate	*Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*
Anonymous reputation system for IIoT-enabled retail marketing atop PoS blockchain	*Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*

Building redactable consortium blockchain for industrial internet-of-things	*International Journal of Advanced Computer Science and Applications*
Trust and Distrust in Digital Economies	*Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*
Blockchain: The advent of disintermediation	*Energy Procedia*
Demonstrating Blockchain-Enabled Peer-to-Peer Energy Trading and Sharing	*International Journal of Innovative Technology and Exploring Engineering*
BlockCom: A blockchain based commerce model for smart communities using auction mechanism	*Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*
Solving the Buyer and Seller's Dilemma: A Dual-Deposit Escrow Smart Contract for Provably Cheat-Proof Delivery and Payment for a Digital Good without a Trusted Mediator	*2nd IEEE Conference on Energy Internet and Energy System Integration, EI2 2018 - Proceedings*
Blockchain as a trust layer for more efficient finance market	*Technology and Economics of Smart Grids and Sustainable Energy*
Blockchain combined with smart contract to keep safety energy trading for autonomous vehicles	*2018 5th International Conference on Internet of Things: Systems, Management and Security, IoTSMS 2018*
Novel Automatic Food Trading System Using Consortium Blockchain	*IEEE 4th International Forum on Research and Technologies for Society and Industry, RTSI 2018 - Proceedings*
A blockchain based online trading system for DDoS mitigation services	*Sensors (Switzerland)*
Research on Intelligent Trading and Cooperative Scheduling System of Energy Internet Based on Blockchain	*Proceedings of the International Joint Conference on Neural Networks*
AgroVita using Blockchain	*International Conference on the European Energy Market, EEM*

Implementation of Blockchain technology for Energy Trading with Smart Meters	*Proceedings - 2018 IEEE International Conference on Smart Internet of Things, SmartIoT 2018*
Blockchain and Trust in a Smart City	*MATEC Web of Conferences*
Proceedings - 2018 15th International Symposium on Pervasive Systems, Algorithms and Networks, I-SPAN 2018	*Computer Law and Security Review*
Creating markets in no-trust environments: The law and economics of smart contracts	*IEEE/IFIP Network Operations and Management Symposium: Cognitive Management in a Cyber World, NOMS 2018*
Concept for Controlled Business Critical Information Sharing Using Smart Contracts	*9th International Conference on Intelligent Systems 2018: Theory, Research and Innovation in Applications, IS 2018 - Proceedings*
A self-aware contract for decentralized peer-to-peer (p2p) commerce	*Proceedings - IEEE 2018 International Congress on Cybermatics: 2018 IEEE Conferences on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, iThings/GreenCom/CPSCom/SmartData/Blockchain/CIT 2018*
Buyers of lemons: Addressing buyers' needs in the market for lemons with blockchain technology	*IEEE Cloud Computing*
Session L1: Blockchain application in energy performance contracting	*Proceedings of the 2018 19th International Carpathian Control Conference, ICCC 2018*
Applications of blockchain technology in the Brazilian government	*Proceedings of 4th IEEE International Conference on Applied System Innovation 2018, ICASI 2018*
Elevating beneficence in cyberspace with situational trust	*International Journal of Environmental Research and Public Health*
A Survey on Using Blockchain in Trade Supply Chain Solutions	*ACM International Conference Proceeding Series*
Smart Contract-Based Data Commodity Transactions for Industrial Internet of Things	*IEEE Access*

Sensitive Data Encoding in Blockchain-Based P2P Trading System	*IET Conference Publications*
The International Register of Ideas and Innovations. A Visionary Social Network to Develop Innovation and Protect IP Using Blockchain and Proof-of-Originality Algorithm	*Proceedings of the International Conference on Industrial Engineering and Operations Management*
An HCI Perspective on Distributed Ledger Technologies for Peer-to-Peer Energy Trading	*Proceedings of the International Astronautical Congress, IAC*
Explainable multi-agent systems through blockchain technology	*Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*
Introducing multi shippers mechanism for decentralized cash on delivery system	*Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*
A Blockchain-Based Digital Advertising Media Promotion System	*26th European Conference on Information Systems: Beyond Digitization - Facets of Socio-Technical Change, ECIS 2018*
Trusted Data's Marketplace	*Wireless Communications and Mobile Computing*
Applied engineering programs of energy blockchain in US	*Industrial Management and Data Systems*
An evaluation of barriers to E-Procurement in Turkish construction industry	*Proceedings - 14th IEEE International Conference on E-Business Engineering, ICEBE 2017 - Including 13th Workshop on Service-Oriented Applications, Integration and Collaboration, SOAIC 207*
11th International Conference on Wireless Internet , WiCON 2018	*2017 IEEE Power and Energy Society Innovative Smart Grid Technologies Conference, ISGT 2017*
Research on the Application of Blockchain Technology in Energy Internet	*Proceedings of the International Conference on Electronic Business (ICEB)*
Peer to Peer Energy Trade Among Microgrids Using Blockchain Based Distributed Coalition Formation Method	*Proceedings of the International Conference on Electronic Business (ICEB)*

Fog Computing as enabler for blockchain-based IIoT app marketplaces-A case study	*Proceedings of the International Conference on Electronic Business (ICEB)*
E-Fairs: A Cyber-Physical System for Aggregation and Economy of Scale in e-Commerce	*Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*
Reptor: A Model for Deriving Trust and Reputation on Blockchain-based Electronic Payment System	*ICETE 2017 - Proceedings of the 14th International Joint Conference on e-Business and Telecommunications*
Smart contract-based review system for an IoT data marketplace	*Dianwang Jishu/Power System Technology*
Commercial Property Tokenizing with Smart Contracts	*Journal of Supercomputing*
The reserve sharing mechanism among interconnected power grids based on block chain	*Electronics (Switzerland)*
Application of blockchain technology in smart city infrastructure	*Proceedings of the IM 2021 - 2021 IFIP/IEEE International Symposium on Integrated Network Management*
The Prospects for the Use of Digital Technology "blockchain" in the Pharmaceutical Market	*IOP Conference Series: Earth and Environmental Science*
From Rai stones to Blockchains: The transformation of payments	*Technological Forecasting and Social Change*
Setting up flexible and light weight trading with enhanced user privacy using smart contracts	*Journal of Physics: Conference Series*
Towards Blockchain-Based Robonomics: Autonomous Agents Behavior Validation	*IEEE Access*
Exploring Blockchain Technology for Capital Markets: A Case of Angel Fund	*Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*

Trust chain: Establishing trust in the iot-based applications ecosystem using blockchain	*Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*
Decentralized transactive energy management system for distribution systems with prosumer microgrids	*IEEE Transactions on Information Forensics and Security*
Blockchain based smart contract for bidding system	*Advances in Intelligent Systems and Computing*
Governance on the drug supply chain via gcoin blockchain	*Proceedings - 2020 IEEE International Conference on Decentralized Applications and Infrastructures, DAPPS 2020*
Research and application of block chain technology in crowdsourcing platform	*IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC*
A Low Storage Room Requirement Framework for Distributed Ledger in Blockchain	*2020 11th International Conference on Computing, Communication and Networking Technologies, ICCCNT 2020*
A novel generation right trade in blockchain-enabled continuous double auction system	*IEEE Consumer Electronics Magazine*
Blockchain technology for efficient management of supply chain	*2020 6th International Conference on Signal Processing and Communication, ICSC 2020*
Blockchain for on-demand small launch vehicle supply chain	*Electronic Commerce Research and Applications*
Economic incentive structure for blockchain network	*Communications in Computer and Information Science*
A blockchain based data management system for energy trade	*IEEE Access*
Blockchain for businesses: A systematic literature review	*Advances in Intelligent Systems and Computing*

Blockchain technology impacting the role of trust in transactions: Reflections in the case of trading diamonds	*Proceedings - 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, CyberC 2019*
A Peer-to-Peer Architecture for Distributed Data Monetization in Fog Computing Scenarios	*Advances in Intelligent Systems and Computing*
With a little help from the miners: distributed ledger technology and market disintermediation	*Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*
A Blockchain-Based Supply Chain Quality Management Framework	*Technology in Society*
Smart contract-based campus demonstration of decentralized transactive energy auctions	*Global Jurist*
Blockchain technology acceptance in electronic medical record system	*9th International Conference on Information and Communication Technology Convergence: ICT Convergence Powered by Smart Intelligence, ICTC 2018*
RegTech evolution: The TrustChain	*Lecture Notes in Networks and Systems*
The acceptance of the application of blockchain technology in the supply chain process of the Thai automotive industry	*Future Generation Computer Systems*
Trustless intermediation in blockchain-based decentralized service marketplaces	*Information Sciences*
PB-PKI: A privacy-aware blockchain-based PKI	*Proceedings of the 2021 5th World Conference on Smart Trends in Systems Security and Sustainability, WorldS4 2021*
Electricity transactions and congestion management based on blockchain in energy internet	*IEEE Transactions on Network and Service Management*
A trustless privacy-preserving reputation system	*International Journal of Recent Technology and Engineering*

Google Scholar

Authors	*Article Title*
Zhili Zhou a,b,∗, Meimin Wanga,b, Ching-Nung Yang c, Zhangjie Fu a,b, Xingming Sun a,b, Q.M. Jonathan Wud	*Blockchain-based decentralized reputation system in E-commerce environment*
	Reptor: A Model for Deriving Trust and Reputation on Blockchain-based Electronic Payment System
	3R model: A post-purchase context-aware reputation model to mitigate unfair ratings in e-commerce
	Anonymous and Verifiable Reputation System for E-commerce Platforms based on Blockchain
	A Model for Deriving Trust and Reputation on Blockchain-Based e-Payment System †
	DTrust: A Decentralized Reputation System for Ecommerce Marketplaces
	A Blockchain-Enabled Quantitative Approach to Trust and Reputation Management with Sparse Evidence
	Using Blockchain Technology To Improve Trust In eCommerce Reviews
Horst Treiblmaier a,, Christian Sillaber b*	*The impact of blockchain on e-commerce: A framework for salient research topics*
	NormaChain: A Blockchain-Based Normalized Autonomous Transaction Settlement Systemfor IoT-Based E-Commerce
	Blockchain based Confidentiality and Integrity Preserving Scheme for Enhancing E-commerce Security
	Blockchain-Based Distributed Trust and Reputation Management Systems: A Survey
	A Blockchain-Based P2P Transaction Method and Sensitive Data Encoding for E-Commerce Transactions
	A Review on Trust and Reputation Management Systems in e-commerce and P2P Network
	BLOCKCHAIN TECHNOLOGY IN E-COMMERCE PLATFORM

	Smart Contract Relations in e-Commerce: Legal Implications of Exchanges Conducted on the Blockchain
Richard Dennis and Gareth Owen	*Rep on the block : A next generation reputation system based on the blockchain*
	RTChain: A Reputation System with Transaction and Consensus Incentives for E-commerce Blockchain
	Rep on the Roll: A Peer to Peer Reputation System Based on a Rolling Blockchain
	TrustChain: Trust Management in Blockchain and IoT supported Supply Chains

APPENDAGE II – GLOSSARY

Centralized:

Centralized refers to a system or organization in which decision-making authority is concentrated in a single, central location or entity. In a centralized system, all power and control are held by a single authority, and decisions are made and implemented from the top down. This contrasts with decentralized systems, in which power and decision-making authority is distributed across multiple actors.

Examples of centralized systems include traditional hierarchical organizations, centralized governments, and centralized computer networks. In each of these cases, a central authority makes decisions and exerts control over the entire system.

Decentralized:

Decentralized refers to a system or organization in which decision-making authority and power are distributed among multiple actors, rather than concentrated in a single, central location or entity. In a decentralized system, decision-making authority and control are spread out among different individuals, groups, or nodes in a network, and decisions are made through a consensus or democratic process.

Decentralization can take many forms, such as decentralized organizations, decentralized governments, and decentralized computer networks. Examples of decentralized systems include blockchain networks, peer-to-peer file sharing networks, and decentralized autonomous organizations (DAOs). In these systems, decision-making authority and control are distributed among multiple nodes or users, which helps to promote transparency, accountability, and resilience. Decentralization can also help to reduce the risk of single points of failure, as multiple nodes are involved in decision-making and control.

Community Driven:

"Community driven" typically refers to a concept or initiative that is driven by the collective efforts and interests of a community, rather than being led or controlled by a single individual or organization. In a community-driven model, decisions are made, and actions are taken based on the input and involvement of the members of the community, creating a sense of ownership and investment in the outcome. This approach can be seen in various settings, such as open-source software projects, neighborhood improvement initiatives, and online forums and communities.

Endorsement:

An endorsement is a statement of support or approval for a product, service, candidate, or idea. Endorsements can come in many forms, including written testimonials, public statements, advertisements, or even social media posts. They can be given by individuals, organizations, or celebrities, and are often used to build credibility, increase visibility, and persuade others to support or try something.

Endorsements can be a powerful tool for marketing and can help to build trust and credibility with potential customers. However, they can also be misleading if they are not genuine or if the endorser has a conflict of interest, such as being paid to endorse a product. As a result, it's important to consider the source of the endorsement and whether it aligns with your own values and interests before deciding based on it.

Aging and endorser at reputation models:

"Ageing" refers to the process of change that occurs over time to a person's reputation or credibility. As time passes, people may gain more experience and expertise, or they may experience changes in their behavior or circumstances that affect their reputation positively or negatively.

An "endorser" is someone who supports or recommends a particular product, service, or idea. In the context of reputation models, endorsers can have a significant impact on an individual's or organization's reputation by publicly endorsing or criticizing them.

Trusted Third Party (TTP):

An entity, other than the buyer or seller that is trusted by both parties to facilitate the interaction (transaction).

B2C:

Business to consumer (transaction between business and final client)

C2C:

Consumer to consumer (Transaction between to consumers, aid by an online platform)

B2B:

Business to Business (transaction between two businesses)

Cryptographic:

Cryptography is a method of protecting information and communications using codes, so that only those for whom the information is intended can read and process it.

In computer science, cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms, to transform messages in ways that are hard to decipher. These deterministic algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on the internet and confidential communications such as credit card transactions and email.

P2P (peer-to-peer):

A peer-to-peer (P2P) service is a decentralized platform whereby two individuals interact directly with each other, without a third-party intermediary. A group of computers are linked together with equal permissions and responsibilities for processing data, it allows computers to communicate directly; person-to-person.

Nodes:

A network node can be defined as the connection point among network devices such as routers, printers, or switches that can receive and send data from one endpoint to the other. In peer-to-peer or other types of distributed networks, nodes are comprised of the servers, clients and/or peers. Peers themselves can act both as servers and clients, while nodes that route data for other devices within the network are defined as "supernodes."

Token:

A token, in reputation models, is a code given to the user, in this way the identity of the user is preserved, but, if needed, he can be identified. The node is a fingerprint for that user and stores all information needed. A programming token is the basic component of source code. Characters are categorized as one of five classes of tokens that describe their functions (constants, identifiers, operators, reserved words, and separators) in accordance with the rules of the programming language.

Smart Contract:

Smart contracts are simply programs stored on a blockchain that run when predetermined conditions are met. They typically are used to automate the execution of an agreement so that all participants can be immediately certain of the outcome, without any intermediary's involvement or time loss. They can also automate a workflow, triggering the next action when conditions are met. Smart contracts work by following simple "if/when…then…" statements that are written into code on a blockchain. A network of computers executes the actions when predetermined conditions have been met and verified. These actions could include releasing funds to the appropriate parties, registering a vehicle, sending notifications, or issuing a ticket. The blockchain is then updated when the transaction is completed. That means the transaction cannot be changed, and only parties who have been granted permission can see the results.

Within a smart contract, there can be as many stipulations as needed to satisfy the participants that the task will be completed satisfactorily. To establish the terms, participants must determine how transactions and their data are represented on the blockchain, agree on the "if/when...then…" rules that govern those transactions, explore all possible exceptions, and define a framework for resolving disputes.

Then the smart contract can be programmed by a developer – although increasingly, organizations that use blockchain for business provide templates, web interfaces, and other online tools to simplify structuring smart contracts.

Trust:

The extent to which one party is willing to depend on something or somebody in each situation with a feeling of relative security, even though negative consequences are possible.

On e-Commerce trust is what a buyer is searching for when going through the reviews and feedback of others. It's very important to try to maintain reliable feedbacks from other users. Unfortunately, as is known, we can expect certain attacks and frauds, bad-mouthing, collusion, sybil attacks, made with the intent to lower the rating of a seller and/or product.

Attacks:

Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself. In case of e-Commerce the attacks have the intention of degrading a sellers/product reputation. These attacks decrease the ratings in that marketplace.

Frauds:

Using other means to gain reputation that are not real, true. Misinformation. Like attacks, frauds have one intent, to decrease the reputation of a seller or product (being the seller the part focused on this dissertation, but, it must be said, that the buyer can also be at the receiving end of attacks and frauds, making them untrusty for the seller).

Sybil Attack:

An entity forges multiple identities in the system, using it in collusion as a mean to increase his influence.

It is important to have a way to guarantee that a user can't create several accounts, making sure that the user has only one identity.

Sybil attacks are typically used in conjunction with Collusion assaults.

Whitewashing:

An e-commerce user with a bad reputation, can easily create a new identity and continue his activity without any consequences of his past transactions.

As mentioned above, this is a common way to bend the rules and continue the activity, this knowledge bring very little security when online shopping.

Ballot-stuffing:

Attack where members positively rate themselves on fake and unfair transactions to inflate their reputation.

It is important to guarantee that the transaction information is accurate and that can’t be adulterer, and one shouldn’t be able to rate themselves.

Bad Mouthing:

The opposite of Ballot-stuffing, in a way to destroy a user’s reputation, other user’s give false information about the seller or a product.

Traitor attack:

Members exploit their reputation by tricking others until their reputation dissolves.

Collusion:

The seller strategically provides a good service to a group of users and bad services to others, to get benefits of that asymmetry of product/service quality.

Whether in traitor attacks or collusion attacks, this happens because the information is centralized, is necessary that one user has the information on every marketplace to guarantee a certain good repute.