Kugblenu, Carl; Vuorimaa, Petri; Keller, Barbara

Smart Contract Enabled Decentralized Reputation System for E-Commerce Reviews

Published in:
Internet of Things, Smart Spaces, and Next Generation Networks and Systems - 21st International Conference, NEW2AN 2021, and 14th Conference, ruSMART 2021, Proceedings

DOI:
10.1007/978-3-030-97777-1_3

Published: 01/01/2022

Document Version
Peer-reviewed accepted author manuscript, also known as Final accepted manuscript or Post-print

Please cite the original version:
Kugblenu, C., Vuorimaa, P., & Keller, B. (2022). Smart Contract Enabled Decentralized Reputation System for E-Commerce Reviews. In Y. Koucheryavy, S. Balandin, & S. Andreev (Eds.), *Internet of Things, Smart Spaces, and Next Generation Networks and Systems - 21st International Conference, NEW2AN 2021, and 14th Conference, ruSMART 2021, Proceedings* (pp. 22-34). (Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics); Vol. 13158 LNCS). Springer. https://doi.org/10.1007/978-3-030-97777-1_3

Smart Contract Enabled Decentralized Reputation System for E-commerce Reviews

Carl Kugblenu[1][0000−0002−3673−7720], Petri Vuorimaa[2], and Barbara Keller[3]

[1] Aalto University, Dept. of Computer Science, Espoo, Finland
carl.kugblenu@aalto.fi
[2] Aalto University, Dept. of Computer Science, Espoo, Finland
petri.vuorimaa@aalto.fi
[3] Aalto University, Dept. of Computer Science, Espoo, Finland
barbara.keller@aalto.fi

Abstract. E-commerce has seen a surge in growth in the wake of the ongoing pandemic and is gaining ground worldwide. Inherently, product reviews by customers have fueled purchasing decisions. Blockchain is a decentralized ledger technology where a history of transactions are managed in an immutable manner. This technology is gaining traction as a result of general distrust and fragmentation in centralized systems. This paper proposes a smart contract enabled decentralized reputation system on a permissioned blockchain for E-commerce reviews. We present an overview of the limitations of current reputation system. We show how our approach addresses the fragmentation and credibility issues of product reviews in current reputation systems.

Keywords: Blockchain · Reputation System · Smart Contracts · Hyperledger Fabric · E-Commerce.

1 Introduction

Global e-commerce was showing an unprecedented growth and has seen a surge in adoption due to the COVID pandemic. According to NASDAQ, it has been estimated that by 2040, over 95% of purchases will be by e-commerce services [8]. Customers are continually seeking verifiable and genuine reviews and over 60% read reviews in some form before making a purchasing decision [9].

There has been a proliferation of fraudulent reviews on the major online retailers like Amazon, Walmart and Alibaba and they are facing challenges in mitigating them despite their best efforts [14]. Additionally, the centralized nature of the existing review systems by the retailers leaves some level of mistrust in the reviews. Retailers occasionally employ techniques to label products as top rated without elaborating on the metrics used. As a result, healthy competition becomes a challenge as the methods of boosting certain products are opaque and thereby limiting the ability of the customer to make well informed purchasing decisions [13].

Blockchain is a technology that involves an immutable distributed ledger with committed transactions stored in a chain of blocks. It has garnered interest in industry and academia with some of its key features including transparency, decentralization and auditability [12]. A subsequent feature, smart contract support, has given it a broader appeal for more generalized use cases [4].

Research efforts on blockchain and reputation systems are gaining momentum in order to reduce the reliance on centralized reputation systems. These efforts have not been without their setbacks as decentralization also poses unique challenges including attack vectors such as Sybil based attacks [11]. Trade-offs in performance for transparency are necessitated especially for the use case of a decentralized reputation system.

In this paper, we present a smart contract enabled decentralized reputation system on a permissioned blockchain. Our proposed system combines review information of products purchased on recognized retailer platforms and aggregates them. There are multiple attacks that are possible on the e-commerce sites due to the centralized nature of the review systems being utilized. Due to the transparent nature of our approach, malicious activity [7] will be difficult to obscure. An example is review bombing where multiple identities are created and used to give high or low reviews after purchase. This becomes challenging in a centralized approach as they must mitigate all forms of malicious activity.

By utilizing smart contracts, we ensure similar capabilities of centralized reputations systems with the added element of transparency. Customers are guaranteed a high level of privacy by utilizing multiple pseudonymous identities, since reviews are connected to a verified proof of purchase. Reviews can be flagged by parties specialized in detecting fake reviews. A smart contract based state machine is designed to achieve this functionality. Customers now have the choice of the third party to trust for flagging anomalous reviews.

Our contributions are:

1. Design of a decentralized reputation system with local verification of proof of purchase
2. Smart Contract design and state transitions that leverages protocols over platforms
3. Implementation of a prototype using Hyperledger Fabric.

The remainder of the paper is structured as follows. In Section 2, we present the related work. In Section 3, we give an overview of our proposed architecture and design goals. In Section 4, we detail the smart contract design and state transitions. The product review process flow is discussed in this section. Section 5 details the implementation with Hyperledger Fabric blockchain. In Section 6, we discuss some limitations of our approach and possible solutions before finally concluding with main takeaways in Section 7.

2 Related Work

Dennis et al. [5] first proposed a novel generalized reputation system built atop the Bitcoin blockchain showing the benefits in comparison to centralized reputation systems. The paper highlights the issues of centralized reputation and the negative impacts of a single entity controlling the reputation information and making changes to how reputation is computed in an obscure manner. However, the system has limitations in transaction speed, block size and the choice of the Proof of Work [6] consensus algorithm.

Carboni [3] presents a blockchain reputation system based on an incentive model. The paper highlights key requirements a decentralized feedback management system needs and expands on how the Bitcoin blockchain helps in this regard. The decentralized approach highlights a key benefit of an architecture without a single point of failure. The possibility of a motivated malicious actor to set up multiple identities to boost reputation is mentioned. However, the incentive mechanism presented mitigates malicious activity only to an extent and other methods of highlighting abuse and fraud need to exist in a reputation system. The use of a public blockchain like Bitcoin does not take into consideration the stakeholders of a feedback reputation system.

Liu et al. [10] propose a blockchain based reputation system with a focus on preserving customer identities. The approach taken ensures that the high level reputation of the retailers is transparent while ensuring the privacy of the customers. Smart contracts are heavily utilized for retailer review aggregation unlike in [3]. The emphasis is placed on the importance of transparency, privacy and how blockchain enabled technologies achieve this within a reputation system. However, it does not take into consideration anomalous reviews that bypass the verified proof of purchase mechanism and the ability to flag such reviews in a decentralized fashion.

Wang et al. [15] present a decentralized review system that utilizes two Ethereum blockchains for on-chain and off-chain validation of reviews. The benefits of smart contracts to model centralized review systems are highlighted. The dependence of validation from a supply chain could pose a bottleneck to the system.

The existing research has shown the benefits of utilizing smart contracts and blockchains for designing reputation systems, but research is lacking in how fraudulent reviews are mitigated adequately. The system we propose presents a solution to this by providing a transparent mechanism for flagging reviews and supporting interested parties that have competencies in participating in the blockchain network.

3 Proposed Architecture

Our approach is a smart contract enabled reputation system that aggregates product ratings from multiple retailer platforms and mitigates attacks common on centralized reputation. The system will center around a permissioned blockchain, Hyperledger Fabric, as the stakeholders or participants of the system are known. The participants are online retailers, customers, sellers and interested parties.

1. Customer. A customer represents an individual capable of creating multiple pseudonymous identities to leave reviews of products, view reviews and update past reviews.
2. Retailer. A retailer represents the e-commerce platforms that hosts sellers for the purchase and delivery of products. The retailer is capable of validating reviews via proof of purchase and will flag reviews if there is evidence of malicious reviews.
3. Seller. A seller represents an individual or group that has listed products on multiple online retailers.
4. Interested Party. An interested party represents an individual or group that wishes to participate in the blockchain network to get access to the product review data in exchange for running a node. An example is a company that has competencies in detecting fake reviews using machine learning techniques.

As a result of the known entities participating in the blockchain network as shown in Fig.1, identity management and access control is managed via certificate authorities [2]. A root Certificate Authority (CA) issues Intermediate CAs to retailers and interested parties due to their specific access control. The retailers issue certificates to sellers as proof for being a seller on their specific platforms. Intermediate CAs issue certificates to customers as end users.

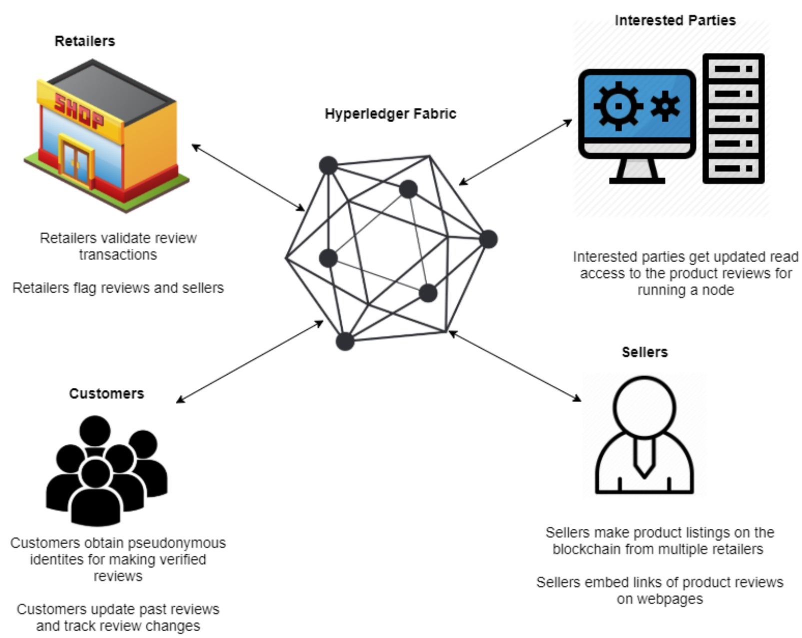

Fig. 1: Decentralized Reputation Architecture

The important elements of the design as follows:

- Multiple Identities. A customer has the ability to choose an identity from multiple pseudonymous identities to leave a review.
- Local Storage. All personal information of the customer is stored locally and only used to verify the purchase within the client application.
- Review Portability. The reviews of a product that exists on multiple recognized retailers are aggregated to give a full impression of customer satisfaction.
- Embedded Reviews. A customer has the ability to view and make reviews of purchased products on web-pages with embedded tags that have integrated the review system. These embedded tags on specific pages can give aggregated reviews about a product without visiting the ecommerce website.
- Review Chaining. A customer has the ability to update a past review and track past updates of a review to see the evolution of impressions made about the product.
- Flagged Reviews. A customer's review can be flagged if malicious intent or monitored threat models are detected. This is due to reputation systems being the target of malicious actors and coordinated attacks. It is with this functionality that customers can then choose to trust reviews based on the external reputation of the Interested Party.

3.1 Description of Our Approach

The main goals of our proposed system are two folds - to aggregate customer impressions of a product that exists on recognized retailer platforms in a decentralized fashion and to mitigate the majority of attacks leveled against reputation systems in a transparent manner. Retailers and product owners will play a key role in the system and serve as stakeholders. Due to the transparency considerations, assigned permissions and roles can be revoked if malicious activity is observed. We follow the major online retailers review data model; the numeric score and supporting review text. When a customer who has the web extension installed makes a purchase on a recognized retailer platform, the order information is associated with a selected pseudonymous identity. The customer can in the future leave a review with the selected identity, which will then be validated and submitted as a transaction on the blockchain. A permissioned blockchain is an ideal fit for our solution and the reasons are as follows:

1. Stakeholders contributing in a trust-less environment lends itself to a permissioned blockchain solution. The ability to use appropriate consensus algorithms like Proof of Stake and Proof of Authority instead of Proof of Work [6].
2. It has been observed that a permissioned blockchain delivers better performance than public blockchains since the stakeholders are known and their roles defined.

Retailers have the ability to flag questionable reviews in a transparent manner. It will be made possible by standardized smart contracts that are enforced specific to the retailer role. The reviews of a product that is available from multiple retailers are aggregated. Reviews are accessible on platforms that contribute a node to the blockchain with more of a read-only access control. Customers can update their review and track past reviews. Product owners and sellers can use embedded links to make their product reviews accessible in a decentralized fashion.

4 Smart Contract

This section details the process flows in the proposed system that are enabled by smart contracts [2]. The review life-cycle is presented followed by process flow of the customer and seller.

4.1 Review Life-cycle

Hyperledger Fabric models specific users as Participants who can interact with entities as Assets. An example of an asset pertaining to reviews is shown in Fig 2. These Assets are modifiable and transferable by Participants. In our proposed system, the Customer, Retailer, Seller and Interested Party are all Participants and have specific access controls and operations enforced by smart contracts.


```
{
  "reviewerID": "A2SUAM1J3GNN3B",
  "listingID": "ADHFEDSSWWF3B",
  "reviewText": "Works as expected",
  "overall": 5.0,
  "summary": "Positive",
  "reviewTimestamp": 1252800000,
  "status": "validated"
}
```


Fig. 2: Example of a review asset

Fig. 3 presents the full process of a product review made by a customer. Firstly, a review asset is submitted by a customer. Then, the review is validated by a retailer using a smart contract leveraging a proof of purchase. A customer can later make an update to the review using the same pseudonymous identity. A review can be flagged as fraudulent by a retailer and reason stated in a transparent manner. The flagged review can be revoked back to an updated state by a specific Interested Party.

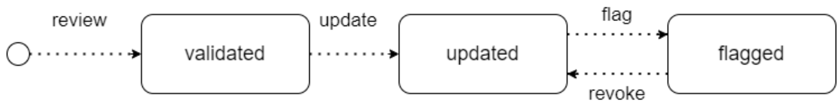

Fig. 3: Smart Contract State Diagram

4.2 Customer Process Flow

From the point of view of a customer, the customer goes through the process as shown in Fig.4. The customer has access to multiple pseudonymous identities to tie a review to. These identities are in a wallet application either running in a web extension or as an application on a phone. The customer can only make a review after a verified proof of purchase. In the proposed design, this occurs locally via a web extension retrieving the order information from an active session on the retailer's web page. The submitted review is checked and enforced by a smart contract before storage on the blockchain. The customer is then notified of a successful validation of their submitted review.

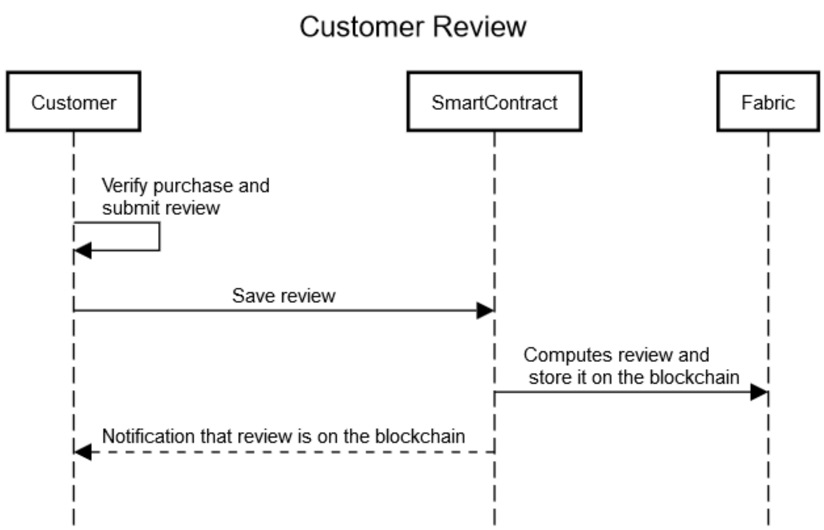

Fig. 4: Customer Flow

The blocks and transitions described in Fig. 3 are described at a high level to show the transactions and the smart contract logic that is executed.

4.3 Seller Process Flow

From the point of view of a seller, the seller goes through the process as shown in Fig.5. The seller can only make a listing after a verified proof of ownership. In

Algorithm 1: SubmitReview Transaction

```
Input: Review Asset
Result: Transaction Status
initialization with proof of purchase parameters;
if Proof of Purchase then
    Initialize connection to blockchain;
    set reviewState to Invalid;
    submit review asset to blockchain;
end
```

Algorithm 2: ValidateReview Transaction

```
Input: Review Asset
Result: Transaction Status
Verify proof of purchase;
set reviewState to Valid;
```

Algorithm 3: UpdateReview Transaction

```
Input: Review Asset
Result: Transaction Status
if Past Review exists then
    Initialize connection to blockchain;
    update review asset;
    set updatedState to True;
    submit updated asset to blockchain;
end
```

Algorithm 4: FlagReview Transaction

```
Input: Review Asset
Result: Transaction Status
Initialize connection to blockchain;
update review asset;
set flaggedState to True;
submit asset to blockchain;
```

the proposed design, this occurs if a supported retailer issues a CA to the seller. With these access rights, the seller can make a listing of products being sold on multiple retail platforms to be able to aggregate the reviews. When a seller submits a listing, a smart contract verifies ownership and checks for duplicates on the blockchain. The seller is then notified of a successful validation of their submitted review.

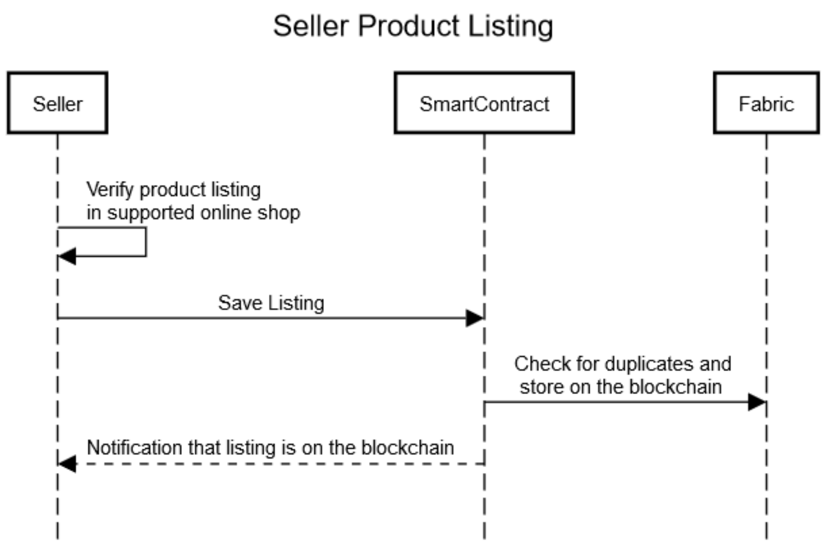

Fig. 5: Seller Process Flow

5 Implementation

The proposed design is implemented with the Hyperledger Fabric v1.4 and the smart contracts written as chaincode in golang. The system is evaluated based on the smart contract enabled review lifecycle testing the state transitions and Participant interactions. The blockchain test network was set up in Docker Engine 19.03 deployed on Google Cloud virtual instance e2-medium machine with 4GB of RAM. Each component runs as a container on the virtual machine and using one peer node for testing.

5.1 Experimental Setup

We leveraged Hyperledger Caliper, a performance testing tool used to run workloads on blockchain platforms including Hyperledger Fabric. A key advantage of this tool is that it abstracts away the complexity of the communication by the client and the blockchain to focus more on the test scenarios.

5.2 Measurements

We measure the latency and throughput of executing the smart contract and querying a review to compare the results. The workload specifies a fixed send rate, specified in transactions per second (tps) each round and gradually increase the rate to observe the performance at each step show in Table 1. The test scenario are executed for the "SubmitReview" chaincode and retrieving a review. Caliper collects the results for each fixed send rate.

Metrics	Send rate (tps)	Number of transactions
Latency	50, 100, 200, 300, 400tps	1000
Throughput	50, 100, 200, 300, 400tps	1000

Table 1: Metrics for Performance Evaluation.

6 Results and Discussion

Fig. 6 shows the average latency in seconds of the transaction types at different transaction send rates. The "SubmitReview" transaction has a higher latency in comparison with "GetReview" transaction due to the overhead of validation checks and writing to the Hyperledger Fabric blockchain. The latency is also constrained by the test environment shown by the increasing latency in "SubmitReview".

Fig. 7 shows the throughput in transactions per second (tps) at different transaction send rates. It can be observed from the results that the "SubmitReview" transactions had a throughput limit of 66 tps before leveling off. When the send rate is increased to 100 tps and beyond, the latency of continues to increase while the throughput remains the same or decreases slightly. This shows the limitations of the specific test environment ability to handle 66 tps of the "SubmitReview" transaction without impacting network latency significantly.

However, the "GetReview" transactions handled 173 tps with a delay of up to 0.03 seconds from 6. The low latency results are as a result of the relatively low overhead in querying the blockchain.

The key takeaway from the results are as follows:

- Performance of the blockchain network is impacted by the type of transactions and complexity of the smart contract
- Throughput levels out when it exceeds the maximum transaction send rate and is limited by the test environment.

7 Limitations

A key limitation is the incentive model of the stakeholders participating in the decentralized reputation system. A case could be made for sellers being incen-

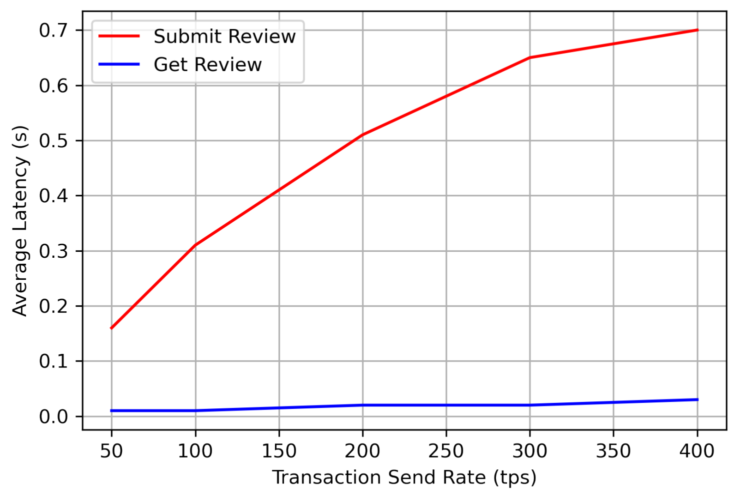

Fig. 6: Latency results

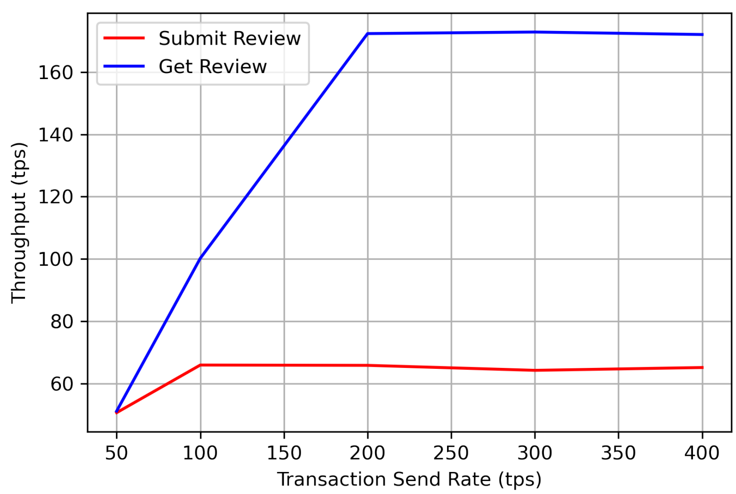

Fig. 7: Throughput results

tivized to make available the reviews of their products across multiple avenues. However, a clear incentive for retailers is a challenge as they are more incentivized to continue to improve their centralized platforms and be gatekeepers for the data.

Another challenge is the limited storage capabilities of the blockchain. Current centralized review systems include images and video. The decentralized reputation system in its current form cannot handle multimedia content and would need a backing store. The InterPlanetary File System (IPFS) [1] has shown potential as a possible decentralized storage, but more research is needed to ascertain the feasibility in a production environment.

A limitation of our system is that although it is effectively guards against objective attacks like bad-mouthing attacks and Sybil attacks on reputation systems [11], subjective or opinion based attacks are a major issue. However, the benefits of transparency on the permissioned blockchain will highlight coordinated review manipulation for it to be adequately flagged if enough evidence is present.

8 Conclusion

In this paper, we presented a smart contract enabled decentralized reputation system to solve the challenges of product reviews on centralized retailer platforms. The proposed approach details a decentralized solution that addresses the fragmentation of product reviews and how malicious attacks like bad-mouthing attacks, are mitigated as a result of utilizing a permissioned blockchain. We also present the architecture and smart contract state transitions. The system was implemented and tested with Hyperledger Fabric. The results showed that customers can submit verified reviews in a decentralized manner with pseudonymous identities. The throughput and latency results of the transaction types showed the impact of the system configuration of the test environment. We discussed some limitations and presented possible solutions to address these issues.

A possible future research direction is to conduct similar tests with multiple permissioned blockchains to evaluate their performance, robustness and scalability. Other approaches of identity management on a permissioned blockchain could be explored to test effectiveness and ease of use. Also, a standard for the smart contracts could be proposed to address the disparity in the ecosystem as it changes quickly and technologies get deprecated.

References

1. Benet, J.: Ipfs-content addressed, versioned, p2p file system. arXiv preprint arXiv:1407.3561 (2014)
2. Cachin, C.: Architecture of the Hyperledger Blockchain Fabric. Workshop on Distributed Cryptocurrencies and Consensus Ledgers (DCCL 2016) **URL:**, https://www.zurich.ibm.com/dccl/papers/cachin_dccl (2016), http://bytacoin.io/main/Hyperledger.pdf
3. Carboni, D.: Feedback based Reputation on top of the Bitcoin Blockchain (2015), http://arxiv.org/abs/1502.01504
4. Cong, L.W., He, Z.: Blockchain disruption and smart contracts. The Review of Financial Studies **32**(5), 1754–1797 (2019)

5. Dennis, R., Owen, G.: Rep on the block: A next generation reputation system based on the blockchain. 2015 10th International Conference for Internet Technology and Secured Transactions, ICITST 2015 pp. 131–138 (2016). https://doi.org/10.1109/ICITST.2015.7412073
6. Ferdous, M.S., Chowdhury, M.J.M., Hoque, M.A., Colman, A.: Blockchain consensuses algorithms: A survey. arXiv preprint arXiv:2001.07091 (2020)
7. Hoffman, K., Zage, D., Nita-Rotaru, C.: A Survey of attacks on Reputation Systems pp. 7–13 (2007), http://docs.lib.purdue.edu/cgi/viewcontent.cgi?article=2676&context=cstech
8. Kitonyi, N.: UK Online Shopping and E-Commerce Statistics for 2017 — Nasdaq, https://www.nasdaq.com/articles/uk-online-shopping-and-e-commerce-statistics-2017-2017-03-14, accessed on: Feb 02 2021
9. Lipsman, A.: Global Ecommerce 2019 - eMarketer Trends, Forecasts & Statistics, https://www.emarketer.com/content/global-ecommerce-2019, accessed on: Feb 02 2021
10. Liu, D., Alahmadi, A., Ni, J., Lin, X., Shen, X.: Anonymous reputation system for IIoT-enabled retail marketing atop PoS blockchain. IEEE Transactions on Industrial Informatics **15**(6), 3527–3537 (2019). https://doi.org/10.1109/TII.2019.2898900
11. Mohaisen, A.: The Sybil Attacks and Defenses: A Survey. The Smart Computing Review **3**(6) (2013). https://doi.org/10.6029/smartcr.2013.06.009
12. Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System (2008)
13. Palmer, A.: Amazon Choice badge recommends unsafe, fake products, https://www.cnbc.com/2019/12/23/amazon-choice-badge-recommends-unsafe-fake-products.html, accessed on: Feb 02 2021
14. Schoolov, K.: Amazon Reviews: Thousands are fake, here's how to spot them, https://www.cnbc.com/2020/09/06/amazon-reviews-thousands-are-fake-heres-how-to-spot-them.html, accessed on: Feb 02 2021
15. Wang, K., Zhang, Z., Kim, H.S.: ReviewChain: Smart Contract Based Review System with Multi-Blockchain Gateway. 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/Gree pp. 1521–1526 (2018). https://doi.org/10.1109/Cybermatics$_2$018.2018.00256