Blockchain-based Online Review System

Tanakorn Karode

A Thesis Submitted in Fulfillment of the Requirements for the

Degree of Master of Science in Computing

Prince of Songkla University

2021

Blockchain-based Online Review System

Tanakorn Karode

A Thesis Submitted in Fulfillment of the Requirements for the

Degree of Master of Science in Computing

Prince of Songkla University

2021

Thesis Title	Blockchain-based Online Review System
Author	Mr. Tanakorn Karode
Major Program	Master of Science in Computing

Major Advisor

.....

(Asst. Prof. Dr. Warodom Werapun)

Examining Committee :

.....Chairperson

(Asst. Prof. Dr. Rattana Wetprasit)

.....Committee

(Asst. Prof. Dr. Warodom Werapun)

.....Committee

(Prof. Dr. Kailas Ravsaheb Patil)

The Graduate School, Prince of Songkla University, has approved this thesis as fulfillment of the requirements for the Master ofScience Degree in Computing

.....

(Prof. Dr. Damrongsak Faroongsarng)

Dean of Graduate School

This is to certify that the work here submitted is the result of the candidate's own investigations. Due acknowledgement has been made of any assistance received.

.....Signature
(Asst. Prof. Dr. Warodom Werapun)
Major Advisor

.....Signature
(Mr. Tanakorn Karode)
Candidate

I hereby certify that this work has not been accepted in substance for any degree, and is not being currently submitted in candidature for any degree.

.....Signature

(Mr. Tanakorn Karode)

Candidate

Thesis Title Blockchain-based Online Review System
Author Mr. Tanakorn Karode
Major Program Master of Science in Computing
Academic Year 2020

ABSTRACT

An online review system is a tool that promotes the marketing strategies of tourism businesses. It also supports customers in product quality assessment. However, fraudsters exploit online reviews to gain more revenue or beat their competitors. Even though many tourism platforms have tried to handle the fake review problem, the results are not satisfying. Fake reviews are still concealing among authentic reviews. Customers have increased their concerns about untraceable management of platforms due to their questionable actions. Much literature suggested improving system transparency. People would increase their trust in a platform that they can keep track of actions behind it. Blockchain technology natively supports traceability. Thus, it has the potential to overcome problems related to trust. This work applies blockchain technology to the customer review use case. The author investigates the blockchain-based online review system in three aspects: usability, potential features, and problem-solving. The transaction cost and speed of the smart contract are tested to identify system usability. The experiment results indicate that a usable smart contract needs some techniques for minimizing its transaction cost. The potential features of the framework are accomplished by applying financial use cases and decentralized management to the system. Including payment generates supplies, which can be used to reward people for their contributions. The framework utilizes a community-driven ecosystem to handle fake reviews. It is a promising strategy for fake review management due to its flexibility. This work proposes a novel form of the online review system, which has the potential to improve the credibility of tourism online reviews.

Keywords: blockchain, smart contract, tourism online review system

ชื่อวิทยานิพนธ์ การใช้งานบล็อกเชนกับระบบรีวิวออนไลน์
ผู้เขียน นายธนากร ก้าโหรด
สาขาวิชา การคอมพิวเตอร์
ปีการศึกษา 2563

บทคัดย่อ

ระบบรีวิวออนไลน์เป็นเครื่องมือที่ส่งเสริมกลยุทธ์ทางการตลาดของธุรกิจการท่องเที่ยว อีกทั้งยังช่วยให้นักท่องเที่ยวสามารถพิจารณาคุณภาพสินค้า และบริการผ่านระบบออนไลน์ได้ อย่างไรก็ตาม มีผู้ใช้โอกาสจากความน่าเชื่อถือของระบบรีวิวออนไลน์ในการสร้างข้อมูลปลอมเพื่อเพิ่มยอดขายของตน หรือเพื่อเอาชนะคู่แข่งทางการตลาด ถึงแม้ผู้ให้บริการแพลตฟอร์มรีวิวออนไลน์มีการจัดการปัญหารีวิวปลอมแล้ว แต่ผลลัพธ์ไม่เป็นที่น่าพึงพอใจเนื่องจากยังคงมีรีวิวปลอมที่ซ่อนอยู่กับรีวิวจริงจำนวนมาก กลุ่มลูกค้ายังมีข้อกังวลที่เพิ่มขึ้นในเรื่องการจัดการที่ไม่สามารถตรวจสอบได้ของผู้ให้บริการ เนื่องจากมีการดำเนินการหลายประการที่ก่อให้เกิดความสงสัยแก่ผู้ใช้งานระบบ งานวิจัยหลายฉบับได้เสนอแนะให้มีการเพิ่มความโปร่งใสในการจัดการของระบบ ซึ่งจะส่งผลให้ลูกค้ามีความเชื่อถือต่อข้อมูลในระบบมากยิ่งขึ้นหากทุกความเคลื่อนไหวสามารถถูกตรวจสอบในภายหลังได้ เทคโนโลยีบล็อกเชนเป็นระบบที่ถูกออกแบบให้มีความโปร่งใสสูง ส่งผลให้บล็อกเชนมีความสามารถที่จะจัดการกับปัญหาที่เกี่ยวข้องกับความเชื่อมั่นได้ วิทยานิพนธ์เล่มนี้นำเสนอการประยุกต์ใช้เทคโนโลยีบล็อกเชนกับระบบรีวิวออนไลน์ ผู้เขียนได้ศึกษาระบบรีวิวออนไลน์บนฐานข้อมูลบล็อกเชนในสามมุมมอง ได้แก่ ความเป็นไปได้ในการใช้งาน ความสามารถของระบบ และความสามารถในการแก้ปัญหา โดยที่มีการทดสอบความเร็ว และค่าใช้จ่ายในการทำธุรกรรมของสัญญาอัจฉริยะเพื่อวิเคราะห์ความเป็นไปได้ในการใช้งานของระบบ ผลการทดลองได้ชี้ให้เห็นว่าสัญญาอัจฉริยะที่เหมาะกับการใช้งานจริงจำเป็นจะต้องมีการพัฒนาในรูปแบบที่สามารถลดค่าธุรกรรมให้ได้มากที่สุด ความสามารถของระบบถูกสร้างขึ้นโดยการประยุกต์ใช้เรื่องการเงิน และการจัดการแบบกระจายศูนย์เข้าด้วยกัน การเพิ่มระบบชำระเงินเข้ามาในระบบช่วยเพิ่มแหล่งเงินทุนที่จะสามารถนำไปใช้เป็นรางวัลให้แก่ผู้ที่สร้างประโยชน์แก่ระบบ ระบบมีการจัดการรีวิวปลอมโดยอาศัยการจัดสินใจจากผู้ใช้งานระบบเป็นหลัก วิธีการนี้เป็นวิธีการที่มีความเป็นไปได้ที่จะแก้ปัญหารีวิวปลอมเนื่องจากเป็นวิธีที่มีความยืดหยุ่นรองรับต่อการเปลี่ยนแปลงความคิดเห็นของผู้ใช้งานในระบบ วิทยานิพนธ์เล่มนี้นำเสนอระบบรีวิวออนไลน์รูปแบบใหม่ที่มีความเป็นไปได้สูงในการเพิ่มความน่าเชื่อถือให้กับรีวิวออนไลน์ของธุรกิจการท่องเที่ยว

คำสำคัญ: บล็อกเชน, สัญญาอัจฉริยะ, ระบบรีวิวออนไลน์สำหรับการท่องเที่ยว

ACKNOWLEDGEMENT

First and foremost, I am grateful to my advisor Asst. Prof. Dr. Warodom Werapun for his continuous supports and guidance of my research, I am very proud of being his student. I could not accomplish all of my works since undergraduate until master's degree without his supports. His dedication to research work deeply encourages me to keep working. In many times, he shaped my ideas and helped me to improve my works as well as my skills for the future life.

I would like to also thank Dr. Tanwa Arpornthip, Aj. Esther Sangiamkul, Dr. Norrathep Rattanavipanon, Asst. Prof. Dr. Rattana Wetprasit, Assoc. Prof. Dr. Apichat Heednacram, and all BLOCK research team members for helping me with my research. The BLOCK research team weekly meeting helps very much to keep me update to date on the blockchain technology. Many ideas in my work are extracted from the meeting and the BLOCK research team member's suggestions.

Furthermore, I greatly appreciate supports and suggestions of all lecturers who involve in my master's journey especially Asst. Prof. Dr. Aziz Nanthaamornphong, Asst. Prof. Dr. Nattapong Tongtep, Asst. Prof. Dr. Kitsiri Chochiang, Dr. Kwankamon Dittakan, Dr. Thitinan Kliangsuwan and Aj. Kullawat Chaowanawatee. I also thank to the assistance of our department staffs throughout my study at College of Computing.

Last but not least, I am grateful to have my lovely supporters, my family. They always help me for entire life. All of my hard working is also for their happiness.

Tanakorn Karode

CONTENT

	Page
ABSTRACT	v
บทคัดย่อ	vi
ACKNOWLEDGMENT	vii
CONTENT	viii
LIST OF TABLES	xii
LIST OF FIGURES	xiii
CHAPTER	
1 INTRODUCTION	1
1.1 Background and rationale	1
1.2 Scope of work	4
1.3 Objectives	5
1.4 Outcomes	5
1.5 Thesis outline	6
2 BACKGROUND KNOWLEDGE AND REVIEW OF LITERATURE	7
2.1 Blockchain	7
2.1.1 Bitcoin: the origin of blockchain	7
2.1.2 Smart contract: the programmable blockchain	10
2.1.3 IPFS: peer-to-peer file system	12
2.1.4 Token curated registry (TCR)	13
2.1.5 Blockchain applications	14
2.2 Problems in online review systems	15
2.2.1 Fake review spamming	15
2.2.2 Reputation score forging	17

CONTENT (Continued)

	Page
2.2.3 Review content tampering	18
2.3 Current methods and issues	19
2.3.1 Fake review spam protection	20
2.3.2 Fake review spam detection	21
2.3.3 Fake review spam handling	22
2.4 Similar projects	23
2.4.1 Revain	24
2.4.2 Lina.Review	25
2.4.3 Dentacoin	26
3 RESEARCH METHODOLOGY AND PROPOSED FRAMEWORK	28
3.1 Potential of a blockchain in online review systems	28
3.1.1 Tools	28
3.1.2 System design	29
3.1.3 Experiment	32
3.2 Blockchain-based online review system features	34
3.2.1 System design	34
3.2.2 Performance testing	41
3.2.3 Feature analysis	43
3.3 Robustness against fraudulent activities of a blockchain-based online review system	44
3.3.1 Proposed framework	45
3.3.2 Evaluation	48
4 RESULTS	55
4.1 Potential of a blockchain in online review systems	55
4.1.1 Review size and transaction cost	55

CONTENT (Continued)

	Page
4.1.2 Review size and response time	57
4.1.3 File size and uploading time	58
4.2 Blockchain-based online review system features	58
4.2.1 Performance	59
4.2.2 Features	60
4.3 Robustness against fraudulent activities of a blockchain-based online review system	67
4.3.1 Fake review spam robustness	68
4.3.2 Reputation score forging robustness	72
4.3.3 Review content tampering spam robustness	73
5 DISCUSSIONS	76
5.1 Potential of a blockchain in online review systems	76
5.1.1 Principles are needed for the blockchain-based online review system implementation	76
5.1.2 The price volatility is the main concern for the usability of the system	77
5.1.3 The financial process should be included on the blockchain-based online review system	77
5.2 Blockchain-based online review system features	78
5.2.1 Decentralization brings new form of online consumer review system	78
5.2.2 Transaction costs and unfamiliar interfaces are likely to be concerning issues	79
5.3 Robustness against fraudulent activities of a blockchain-based online review system	80

CONTENT (Continued)

Page

5.3.1 The proposed framework provides the better fake review management 80

5.3.2 Reputation score forging is intensively addressed by the proposed system 81

5.3.3 Review content tampering requires extremely high cost 82

6 CONCLUSIONS 83

6.1 Remarks and observations 83

6.2 Contributions 85

6.3 Limitations of the work 86

6.4 Further works 87

BIBLIOGRAPHY 88

VITAE 95

LIST OF TABLES

Tables	Page
3.1 Smart contract methods' details	42
3.2 Online review system features inherited from blockchain properties	43
4.1 Review posting transaction cost	56
4.2 Review posting speed	57
4.3 Uploading speed	58
4.4 Gas used for each method	60
4.5 Purchasing validation comparison	61
4.6 Information management comparison	63
4.7 Rewarding comparison	64
4.8 Cooperation capability comparison	66
4.9 voting compatibility comparison	67
4.10 Fake review spam cost	68
4.11 Fake review detection comparison	70
4.12 Fake review spam handling comparison	71
4.13 Reputation forging efforts	72
4.14 Reputation score forging robustness comparison	73
4.15 Review content tampering robustness comparison	75

LIST OF FIGTURES

Figure	Page
2.1 High-level Bitcoin transaction flow	8
2.2 Blockchain structure	9
2.3 Ethereum state transition function	12
3.1 Without IPFS contract's sequence diagram	30
3.2 With IPFS contracts' sequence diagram	31
3.3 System architecture	35
3.4 Use case diagram	36
3.5 Integrity checking tool	45
3.6 Transaction visualizer	46
3.7 Review grading tool	47
3.8 Off chain feeding strategy	50
4.1 Review posting transaction cost	56

CHAPTER 1

INTRODUCTION

1.1 Background and rationale

The first and main application of a blockchain is digital currency (Nakamoto, 2008). A blockchain was designed to be tamper-proof to keep financial information securely. After a few years that Bitcoin was introduced, Ethereum provided an environment that can apply a blockchain to non-financial use cases (Buterin, 2014). Since then, applications of a blockchain are investigated by researchers and industries. A blockchain provides immutable records of data, so the applications like provenance (Liang, et al., 2017), and tracking systems (Neisse, et al., 2017) are discovered. A blockchain can connect multiple different systems with its publicity characteristic. Personal health and traveler itinerary record systems (Roehrs, et al., 2019; Vinod, 2020) are examples of the public storage applications. A blockchain helps support many industries as mentioned in these examples. The tourism industry is one that could be improved by blockchain technology. A crucial tool that connects customers and businesses in the tourism domain is an online review system. It is a tool that has the potential to be enhanced by a blockchain since it is related to trust (Önder and Treiblmaier, 2018). Additionally, an online review system today is full of dubiousness because most platforms do not provide transparency on their service (Harris, 2018; Luca and Zervas, 2016; Mayzlin, et al., 2014).

In online review systems, three main problems are possible to be reduced or solved by utilizing blockchain technology. Firstly, the biggest problem in online reviews is the fake review spam problem because it directly declines the trustworthiness of the overall system (Luca and Zervas, 2016). Secondly, the reputation score forging problem is conducted by fraudsters in order to increase the credibility of fake information (Mayzlin, et al., 2014). This problem occurs when a fake reviewer posts a review and uses another fake account to give a "helpful" score to the fake review. The last is the review content tampering problem, which was mentioned by many customers (from web https://www.tripadvisor.com/ShowTopic-g1-i12105-k8465871-o60-Review_censorship-Tripadvisor_Support.html, 3 March 2021). This problem can be conducted by a hacker or a platform itself. Some posted reviews are edited or removed by others without acknowledgment of the review author and other users. In some cases, platforms inform the review authors with automatic messages for the reasons of review filtering. However, many of them are not sensible. These problems undermine the credibility of online review systems. Additionally, people do not freely express their actual opinion towards the products and services they experienced.

Much literature and platforms introduced methods to handle fake review spam. However, to the best of our knowledge, there are no works that address the reputation score forging and content tampering problems. Current platforms can catch many fake reviews by using methods whether manually and automatically. TripAdvisor analyses review content and user behavior patterns to spot suspected activities. If a review does not match the criterion constructed by the platform, it will be automatically removed. The platform employs specialists for some cases that the automatic system cannot classify the review. TripAdvisor claims that it can reduce a large number of fake reviews. However, a fake restaurant could still climb to the top list under this rigorous investigation (Orlikowski and Scott, 2019). Meanwhile, many people claimed that they honestly post a review on TripAdvisor, but the review was removed by the platform (from web https://www.tripadvisor.co.nz/ShowTopic-g1-i12105-k12618778-Sympathetic_to_review_manipulation_but_deleting_my_negative-TripadvisorSupport.html, 3 March 2021). According to the Australian Competition and

Consumer Commission (ACCC, 2015), the platform should allow only a real customer, who has purchased a product, to post a review. This guideline matches with the practice of booking platforms, such as Booking.com, and Expedia.com. As reported on many sources, the booking platforms contain a lower amount of fake reviews. Unfortunately, these booking platforms do not conduct the best practices of review investigation as the review platforms (e.g., TripAdvisor, and Yelp.com) do. Even though purchasing requirement produces high cost for fake negative review spamming, fraudsters do not have to spend much effort to generate fake positive reviews. Even worse, when the platform providers do not honestly provide the service by directly changing review score. On the other hand, they do not require purchasing before posting a review in some cases. While these cases are not apparently observed, there is no guarantee that the platforms will always be honest under the intensely competitive market. Additionally, it is difficult to trace movements behind the current platforms since the providers do not expose much information. As a result, people still question the platforms even they introduce many solutions because they lack transparency. This introduces an idea to apply the high transparent blockchain technology to an online review system.

A blockchain has been applied to online review systems by a few companies. They aim to improve the trust of online reviews by providing transparent systems. Additionally, the immutability of a blockchain ensures that posted reviews will not be changed or removed by hackers and platform providers. The most famous blockchain-based online review platform at the time of writing is Revain (Revain LLP, 2018). It is a crypto-community online review platform, which collects reviews about blockchain-related services. Revain uses the automatic filtration system to validate and remove suspect reviews. The platform introduces token-based incentives to reward reviewers. Lina.review is general product review platform (Lina Network, 2019). People can give scores and provide information about products, such as cars, houses, movies, computers, and many others, on these platforms. Dentacoin is the first blockchain-based online review system for the dentists (Switch, 2017). All mentioned platforms use similar methods like AI and automatic filtration to manage fake reviews. They

leverage the value of tokens in the blockchain economy to encourage users to properly interact with the systems. Even though the platforms provide customers with high transparency services, they still have some vulnerability due to lacking best practices of online review providers. Revain does not validate users' experience towards products or services they mention. Users can rewrite phrases presented on other reviews and create their own reviews (without any actual experiences) to get rewards. Furthermore, the automatic filtering system scopes the real opinion of users. People who have extreme experience with some products or services are inclined to post their experience because they will not pass the filtering process. The blockchain-based online review platforms today still rely on a central authority while they utilize a decentralized technology. The observable advantages of a blockchain in online review systems have not been presented on these projects. Thus, the results are possible to be the same as the centralized online review platforms.

This work attempts to apply unique features of a blockchain like immutability, decentralization, and smart contract to the online review systems. The proposed system will eliminate a central authority and returns all management responsibilities to users. This work investigates procedures and guidelines of a decentralized online review system implementation. The strengths and weaknesses of the system are discussed to determine its potential.

1.2 Scope of work

1.2.1 This work investigates a blockchain-based online review system for the tourism industry.

1.2.2 The proposed system is implemented on the public Ethereum blockchain and the test network.

1.3 Objectives

1.3.1 To determine the usability of a blockchain in online review applications

1.3.2 To explore potential features, which cannot be achieved by the centralized environment

1.3.3 To identify robustness against fraudulent activities of a blockchain-based online review system

1.4 Outcomes

This work gives an insight into a blockchain-based online review system implementation. The empirical results of performances in terms of the transaction cost and the response time are displayed. The guidelines to handle these issues are presented. Keeping data to be small reduces transaction costs. Each blockchain has different procedures to reduce the amount of data, for example, using an event instead of a state can reduce a huge amount of transaction cost on the Ethereum blockchain. Developers can refer to them for their further implementations. The unique features of the decentralized online review system are discovered. Decentralization introduces a new form of an online review system, which relies on the majority of users instead of the central authority. The system encourages good practices and punishes fraudulent activities with community-driven management. The public information on the blockchain can be shared among different systems. Moreover, the system opens opportunities for extended applications to be implemented on top of the available information.

The blockchain-based online review system can reduce the amount of fake review generating, provide crucial information to investigate suspected activities, and keep the integrity of reviews. The system provides a more flexible judgment by voting, which gives fairer management. Unsolved problems, reputation score forging, and content tampering are handled by the proposed system.

1.5 Thesis outline

The rest chapters are organized as follows: We research and discuss background knowledge and review of literature on Chapter 2. Chapter 3 provides the research methodology and proposed framework. We present the system design and evaluation method in this chapter. The experiment results are illustrated in Chapter 4. We discuss the experiment result in Chapter 5. The discussion will imply the adoption of the blockchain-based online review system. Eventually, we give observation, limitation, and further work in Chapter 6.

CHAPTER 2

BACKGROUND KNOWLEDGE AND REVIEW OF LITERATURE

2.1 Blockchain

This work utilizes blockchain technology as a core component since it has potential to cope with trust issues. This subsection introduces the origin of blockchain, the programmable blockchain, peer-to-peer file system, token curated registry, and blockchain application. These topics offer information that helps in understanding the backbone of the proposed system.

2.1.1 Bitcoin: The origin of blockchain

The first appearance of Blockchain was in 2008, where Satoshi Nakamoto proposed the “Bitcoin: A Peer-to-Peer Electronic Cash System” paper (Nakamoto, 2008). He aimed to create an electronic cash system that does not need a third party. The traditional financial institutions applied the process via electronic payments. They acted as a trusted center because there was no way to ensure the reversible state in the electronic cash system. Consequently, the cost of improving high trust and security raises transaction fees. Moreover, a certain amount of fraud still occurred unavoidably. The payment system needs cryptographic proof instead of trusting the third party to make peer-to-peer transactions. The double-spending

problem is solved by using distributed timestamp server to order transactions. Only the first transaction is valid.

At the high-level view, instead of recording a transaction history on a centralized database, the ledger is distributed and stored on every participant. A sender defines the receiver address and the amount of Bitcoin to be sent. He then signs his private key with the data and broadcast it over the network. After that, miners verify the transaction. The verification needs to confirm that the transaction is actually sent from the private key owner. Everyone can verify the agreement of the transaction by using the senders' public key, sent message, and signature. If the signature verification is failed, it means that the transaction was not send by the asset owner. Additionally, miners verify whether the sender holds sufficient amount of Bitcoin. The high-level workflow of Bitcoin transactions can be illustrated in Figure 2.1.

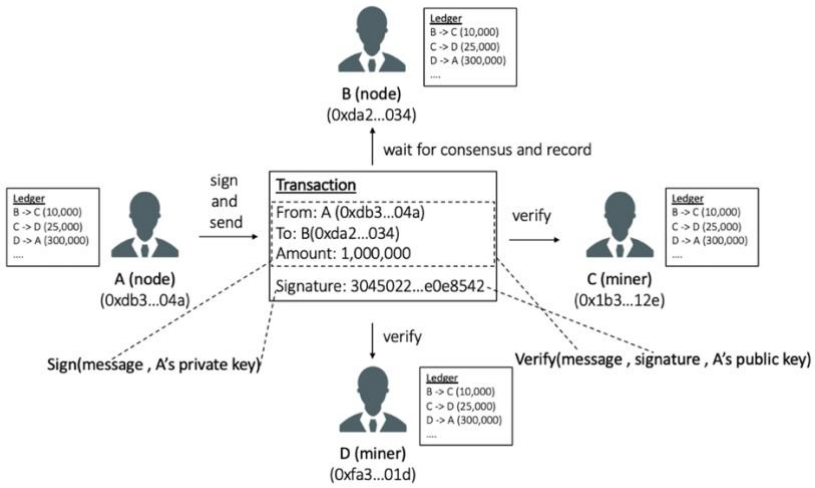

Figure 2.1 High-level Bitcoin transaction flow

The valid transactions are collected into a block that is being mined by a miner. The mining process is the crucial step for the distributed electronic cash system because any transaction needs to be synchronized among nodes in the networks. Only one version of a block from a miner is recorded in a row. Bitcoin uses a consensus algorithm called Proof-of-Work (POW) to select a miner who can broadcast the verified block. This maintains the consistency of data among nodes on the network.

The double-spending problem is also prevented by this method. However, there might be some chances that many nodes complete mining a block at the same time. According to the propagation delay of the network, some nodes might receive a block from one miner first while others might receive a block from the different miners. Such that, a recorded block is not be confirmed immediately but waits for several recorded blocks before confirming once. The POW consensus needs high computational performance to solve, which needs some time to complete each block. Therefore, it can minimize the probability of a concurrent mined block, which can be appropriately handled by waiting for the number of recorded blocks before confirming. The tradeoffs are the slower process and the larger energy consumption though. The structure of a blockchain can be represented in Figure 2.2.

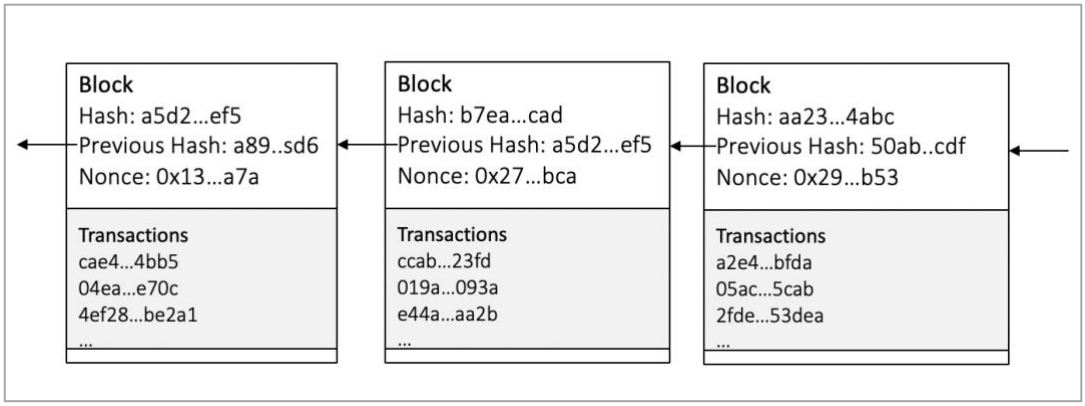

Figure 2.2 Blockchain structure

Each block contains its hash value, the previous block hash value, nonce, list of transactions, and other necessary details. The hash value can be derived by using the cryptographic technique. For Bitcoin, SHA256 is used to generate a hash value. Putting the data into the hash algorithm produces a fixed-length string that looks random, but it is not. The hash functions can always produce the same output for the same input. Changing a few inputs causes very different outputs. This ability can be used to keep track of data changing in a block. Every block has its hash value and the previous of them. Changing a piece of data in a block affects all of the later blocks. For this reason, editing the recorded block is tough work, and it is more difficult for the older block editing. Hence, Bitcoin is the first system that introduces the blockchain

structure. It can serve the following characteristics: secure, reliable, transparent, and immutable. The first version of a blockchain can only work with the financial application.

2.1.2 Smart contract: the programmable blockchain

Ethereum was proposed in 2015 by Vitalik Buterin, promising to be the world's leading programmable Blockchain (Buterin, 2015). It takes the concept of smart contract, which is the self-verifying computer program. It executes the term of the contract to satisfy it automatically. By combining with a blockchain, a smart contract can become an immutable peer-to-peer contract. Ethereum provides a turing-completeness script, where the developer can implement the applications on top of its blockchain. There are some possible applications mentioned in Ethereum white paper such as token systems, sub-currencies for assets representation, stable coins, digital identity, reputation system, and many others. All of the applications are unsatisfied in the centralized system, whether from an unreliable database, low trust authority, or high trust with high-cost authority, isolated, and uncollaborative systems. By using the Ethereum smart contract, those applications can be implemented easily with a few lines of code, reduce cost, improve security and transparency.

The Ethereum state is made up of objects called "accounts". Transferring value and information between accounts causes changing of states. There are two types of addresses in Ethereum. Firstly, the externally owned accounts, which are controlled by the private key. They can be inferred as a user account. Lastly, the contract accounts are controlled by their code. In Ethereum, messages and transactions are two different types of communication between accounts. Message can be created by either externally owned accounts or contract accounts. The data can be attached to the message. If the message is sent to a contract account and the attached data are relative to contract functions, it returns the response. The

transaction needs to be signed by using the externally owned private key before being sent. In addition, the sender needs to define the receiver's account, amount of Ether to transfer (if any), data (if any), a fee for each step of computation (*gas_price*), and the limit of computation fee (*gas_limit*). Ethereum uses a Gas mechanism to be the crypto-fuel. Any computation step needs some fee to reward the miner who performs the computation. The gas mechanism can maintain the Ethereum blockchain by incentivizing miners for keeping work and prevent the infinity loop in the smart contract function. If a sender has not enough Ether to pay for the computation, *the runs-out-of-gas* exception is thrown and terminates the computation. Sending transactions cause changing of state in Ethereum. The states are changed regarding the transaction. Ethereum state transition function has the steps as follows:

(1) Check if the data, signature, and nonce are valid. Otherwise, return an error.

(2) Calculate *max_fee = gas_limit x gas_price* and deduct the balance from the sender. If the sender has not enough balance, return an error.

(3) Every step of computation accumulates gas being used (*gas_used*) and monitors whether it is more than *max_fee*. If that is in the case, throw runs-out-of-gas exception.

(4) The balance is transfered from the sender to the receiver account. If there is not yet exist receiver account, create it. If the receiver account is a contract, run the contract code until complete or runs out of gas.

(5) If the transaction is failed because the sender has no enough balance to send or run out of gas, revert all changes except the transaction fee that has been deducted in the step (2) and pay to the miner.

(6) If the transaction is complete, save all state changed, calculate the remaining gas (i.e., *max_fee – gas_used*), return the remaining gas to the sender, and pay the transaction fee (*gas_used x gas_price)* to the miner.

While the Gas mechanism can maintain the stability of the Ethereum blockchain, it might cause an expensive transaction cost for the complex smart contract. Therefore, the developers need to be aware of this tradeoff and try to find some techniques to reduce the transaction cost. Ethereum state transition function is displayed in Figure 2.3.

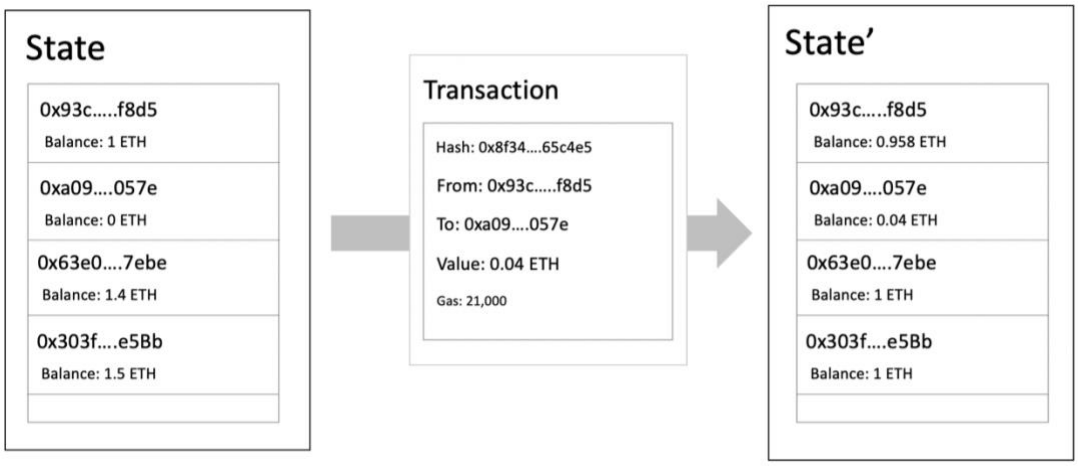

Figure 2.3 Ethereum state transition function

2.1.3 IPFS: peer-to-peer file system

The InterPlanetary File System (IPFS) is a peer-to-peer version-controlled file system that was proposed in 2015 by Juan Benet and Protocol Labs (Benet, 2015). It is an open source that issues high bandwidth data transferring and permanence state of file problems that cannot be solved by HTTP protocol. IPFS stores the metadata in the Distributed Hash Table (DHT), which is the array of key/value pairs stored spread in every participant node in the network. By using the hash function to generate a key, DHT offers fast looking up, excellent performance, and scalability. An IPFS node stores some object (i.e., files or other data structures) and maintains the DHT to refer to the node that can serve the requested objects.

2.1.4 Token curated registry (TCR)

After emerging of the smart contract concept, a TCR was introduced to be a decentralized quality assurance system. Participants can vote to agree or against an objective by staking their tokens (i.e., valuable assets) on a smart contract. With the potential of loss and gain, people have to be confident in their arguments. Thus, it increases the number of participants and protects the quality of the result. Real-world applications of a TCR have been rising today. The Ocean Protocol (Ocean Protocol Foundation, 2020) and Decentralized Data Marketplace (DDM) (Ramachandran, et al., 2018) utilize a TCR to maintain the quality of data sources in online marketing applications. FOAM, the consensus-driven map of the world, allows anyone to add location data (Foamspace Corp, 2018). The quality and correctness of data are maintained by using a TCR. The adChain registry works on digital advertising through the curated list of websites (Mike, et al., 2017). Recently, there has also been an increase in studies about TCRs in the research field. Asgaonkar and Krishnamachari (2018) explored the TCR from the game theory perspective. They found that a TCR result can be depended on various conditions, such as the quality of voters, the value of a TCR, and the TCR parameters. Wang and Krishnamachari (2019) enhance people's engagement towards a TCR by using an inflationary mechanism. Kosmarski and Gordiychuk (2020) applied a TCR as community-driven decisions on the academic paper reviewing. Ito and Tanaka (2019) worked on a TCR with academic literature using a citation graph. According to the on-going projects and literature, the TCR is a promising system for decentralized information quality maintenance. Thus, we apply this concept into the proposed system to provide the decentralized management, which is more suited than centralized decision.

2.1.5 Blockchain Applications

Blockchain technology has been adopted in many applications in both financial and non-financial domains. Werapun, et al. (2020) tokenized solar photovoltaic (PV) into tokens and use them as shares among investors. This project extends the investment sector to be global scale since the blockchain simplifies investing process. The system keeps track of electric consumption and revenue. Investors can trace the system operation in real-time. The revenue from solar PV is computed and distributed automatically each month. The blockchain-based solar PV project does not only generates higher revenue but also reduces the operation cost. Boonpeam, et al. (2020) introduced a blockchain-based student activity credit system. They issue a token named "PSU Coin" to represent the student activity credit in Prince of Songkla University, Phuket campus. The PSU Coin token motivates students to participate in activities more since they can get further benefit from it. For example, they can exchange it with a special product, redeem some promotions, and use it as a governance token. Blockchain technology enhances the activity credit system to be more secure, reliable, transparent, and scalable. External organizations can involve in the PSU Coin ecosystem by purchasing it from the student affair, who issues the token. They can pay the student PSU Coin tokens as rewards for joining their activities. The PSU Coin project extends the usefulness of student activity credits. It also improves cooperation with external organizations and universities.

The blockchain and tourism research propositions are mentioned by Önder and Treiblmaier (2018). Firstly, an online consumer review system with blockchain can provide individuals with traceable identities. It can confirm that a specific transaction comes from a particular user since all entities are signed with unique keys. Secondly, the adoption of cryptocurrencies leads to simpler customer-to-customer (C2C) markets. The tourism industries frequently involve the transfer of money across the country. They are usually charged a high commission by intermediaries, who work under the trust of customers. Utilizing cryptocurrency

payment eliminates intermediaries and thus reduces transaction costs. The C2C market is also simplified. Lastly, the largest impact of blockchain technology on the tourism industry is disintermediation. A small business has to bring itself be listed on famous online travel agencies (OTAs). While the OTAs support marketing advertisement, the business must be stuck on the stipulated rules and high amount of fees. Blockchain technology enables powers for businesses to distribute their information over the internet without dependencies on OTAs. The implemented system in this thesis is motivated by these research propositions.

2.2 Problems in online review systems

The ideal online review systems provide trusted information to customers. They support the online marketing strategies of businesses. Those advantages cannot be practically achieved due to fake reviews. Moreover, the untraceable managements of platforms cause uncertainty, which ends up with losing trust. This subsection collects occurrences and causes of problems in online review systems.

2.2.1 Fake review spamming

The occurrence of fake reviews are reported in various media (from web https://qz.com/india/1136043/misinformation-and-fake-reviews-are-flooding-indian-e-commerce/, 26 February 2021; Consumer News and Business Channel [CNBC], 2014), and industrial reports (Sussin and Thompson, 2012), about 15% or 30% of all online reviews are estimated to be fake. Furthermore, academic literature indicated the

prevalence of fraud reviews on popular platforms like Yelp, Expedia, Trip Advisor (Lee, et al., 2008). Mayzlin, et al. (2014) stated that there exist fake negative reviews in a hotel nearby the hotel that generates fake positive reviews for its own business.

Fake review spamming affects the overall scores of businesses. It misleads actual information people perceive from online reviews. Lappas, et al. (2016) illustrated that 50 reviews are enough to gain visibility over competitor businesses. In popular online review platforms, business rating manipulation does not require much effort to be conducted. A hotel in Phuket is attacked by negative review spamming on popular platforms (e.g., Google, TripAdvisor, Twitter, and Facebook) (from web https://www.posttoday.com/economy/news/633773, 26 February 2021). In Google, the number of reviews was rising from around 700 to 3,000 reviews and the rating was decreasing from 5 to 1.9 stars in two days. Even though the platforms can recover the hotel ratings after a few days, it can be implied that many popular platforms cannot resist reviewing spam.

The prevalence of fake reviews can cause a negative impact on at least two issues. Firstly, the information in online reviews is misleading. People can be fooled by fake advertising or attacking reviews. As a result, it reduces the efficiency of consumer product quality assessment. Lastly, the potential presence of fake reviews may lead consumers to mistrust reviews. People are aware of trusting all information in an online review system today (Zhao, et al., 2013). Customers are inconvenient to assess product quality since they have to consider review credibility at the same time. Concurrently, businesses encounter an unfair market environment, which allows rating manipulations.

The impacts are more serious with fake negative reviews. Many researchers investigated fake negative review impacts. An attacked business losses trust from customers (Lee, et al., 2008; Vermeulen and Seegers, 2009). Other studies observed that negative online reviews could decrease sales (Duan, et al., 2008). In the worst case, a business that does not struggle to maintain its competing position must

stop the service. However, many businesses choose to struggle. The businesses have the opportunity to argue by responding to misleading reviews on some platforms. The businesses that frequently reply to consumer feedbacks get more credibility. Even though responding to reviews can increase the credibility of the businesses, fake negative reviews still decrease the overall ratings. Because of this, businesses handle the situation by using the same strategy as attackers. On the one hand, they generate fake negative reviews to lose their competitor's credibility. On the other hand, they boost their ratings by fake positive review spamming. From these practices, fake reviews are widespread over the current online review platforms.

2.2.2 Reputation score forging

General online review systems provide a channel to evaluate the usefulness of a review (e.g., helpful score in Trip Advisor, useful, funny, and cool scores in Yelp.com). A reputation score reduces the cognitive load of review readers. They can screen only useful reviews to consider products quickly. Many researchers utilize the reputation score in their studies. Fang, et al. (2016) use it to understand how customers perceive the value of tourism reviews. Additionally, review writing guidelines are modeled using the reputation score (Chiriatti, et al., 2019; Hassan, et al., 2020). It can provide various benefits to online review systems. However, the benefit can be achieved only if the reputation score is given by real customers.

Nowadays, fake review spammers take serious actions in forging credibility. They use accounts that contain several previous activities to generate fake reviews. A component that can improve account credibility is the reputation scores of reviews (Mayzlin, et al., 2014). The current platforms do not protect reputation score forging. Therefore, fraudsters do not have to spend much effort to make their accounts to be credible. There exists a famous case in fake review forging. A freelance writer demonstrated that he could fool the number one tourism online review platform

(Orlikowski and Scott, 2019). He created a restaurant name “The shed at Dulwich” on Trip Advisor. The restaurant became the top restaurant in London within 6 months. However, the restaurant does not exist in reality. It means that all reviews posted to the restaurant were fake. However, people trusted reviews posted to this restaurant and contacted for reserving a table many times. The restaurant managers used many techniques to make his restaurant looks authentic. The reputation score faking is an essential part that makes people trust in the reviews posted to this restaurant.

Reputation score forging enhances the credibility of fake reviews. As a result, it further misleads information in online review systems. In addition, the reputation score cannot serve the full benefit if it is presented in vulnerable systems. The fake review problems become worse when reputation score forging exists. However, many online review platforms do not seriously handle this problem.

2.2.3 Review content tampering

A platform should not edit a posted review since it might affect facts provided by a reviewer. There exist many claims by reviewers about the suspicious practices of platforms. While they post reviews from real experiences, platforms silently edit them. (from web https://www.tripadvisor.com/ShowTopic--g1--i12105--k11664022--TripAdvisor--manipulating--reviews--TripadvisorSupport.html, 24 February 2021). In the current platforms, the posted reviews are possibly changed or removed by hackers or platform owners. Platform providers might get paid to boost or lose some businesses’ ratings. On the other hand, a business might hire hackers to manipulate their review scores. These cases can occur when the platform providers are dishonest, and the review data are stored in a low secure environment. Even though platforms claim that they honestly provide the services and keep data secure, there is no guarantee that those cases do not occur behind the systems. Therefore, customers have to reluctantly trust the platforms when they take services.

Inaccurate automatic filtration can be a sort of online review problem. Review filtering mechanism of many platforms hurt authentic reviewers (from web https://support.google.com/business/thread/1774636, 24 February 2021). People argued that they did not get acceptable reasons from platforms when their reviews are removed. The main criterion of review filtration is extreme tone content. Hence, people who have an extremely positive or negative experience with products are inclined to post a review on many popular platforms today (Mayzlin, et al., 2014). Thus, people cannot express real opinions as they experienced from products or services. The review scores are scoped down to be moderate. Moreover, people question the fake review management of platforms. The decision of platforms, which might not really know about the product or service, is less accurate than the real customer decisions.

Review tampering and removing are suspected if people do not acknowledge those actions. Moreover, those actions mislead information in the posted reviews. Consequently, the trustworthiness of reviews is undermined by those actions.

2.3 Current methods and issues

The fake review spam problem is a difficult task that needs some complex solutions to solve. There are steps to address the fake review spam problem: (1) protecting, (2) detecting, and (3) handling. We investigate how current platforms and researchers conduct these procedures. The effectiveness of these solutions is also discussed. To our best knowledge, no literature proposes solutions for reputation score forging and review content tampering problems.

2.3.1 Fake review spam protection

Current online review platforms inform terms and conditions in review writing. The terms and conditions include writing guidelines, law enforcement, and proper practice encouragement. New users might be aware of writing some reviews that do not meet those conditions. However, spammers get some ideas to avoid getting detected by considering those terms and conditions. Fake reviews are still able to get spammed under those conditions.

One way to prevent fake review spam is to construct a model that requires more cost for fake review generating (Dellarocas, 2006). Well-perform protection is to require purchasing before posting a review. Mayzlin, et al., 2014 found that TripAdvisor contains more amount of fake reviews than Expedia. Since it requires cost for review generating, a spammer has to pay more effort to conduct fraudulent actions. More specifically, the fake reviews that are posted to competitor businesses require much more cost. However, fake review spam to friendly or own businesses still requires much fewer costs. Spammers can purchase a product, post a review, and get money back from the targeted businesses. The worst-case in the centralized online review system is when the platform is dishonest. The platform can easily bypass the purchasing step without the acknowledgment of users. Additionally, any reviews can be edited and removed directly in the centralized database.

For honest centralized platforms, the current solutions can protect some online review problems. The fake negative review spam can be reduced by purchasing requirements. Review data can be protected by the secure storage system. However, fake positive review spam cannot be prevented. Detecting action is needed for further management. On the other hand, if the platform is dishonest, all problems cannot be simply protected and detected in the centralized online review system.

2.3.2 Fake review spam detection

Fake review detection is a popular topic in research. There exist many proposed techniques in fake review detection. Those techniques can be categorized into two types: (1) textual analysis and (2) behavioral analysis. The textual analysis considers the review content and analyzes its credibility. Asghar, et al. (2020) and Ott, et al. (2011) analyze the sentiment of review content. They found that fake reviews are likely to have an extremely positive or negative tone of sentiment. A reviewer who has only one tone of sentiment is suspected. Chiriatti, et al. (2019) stated that the reviews with the same content as other reviews are fake. Reviews that do not express their direction (i.e., positive or negative direction) are suspected (Li, et al., 2014; Li Jiwei, et al., 2013). It is still a challenging task for researchers to make textual analysis well-performed (Mayzlin, et al., 2014). Apart from textual analysis, behavioral analysis is a more effective approach. Li, et al. (2017) analyze the potential fake reviews by considering the frequency and period of reviews posting by a reviewer. Researchers also analyze user behaviors with available usage information. IP address, geolocation, and device information of reviewers are analyzed in (Li, et al., 2014). Authors in (Banerjee, et al., 2014; Monaro, et al., 2020) consider suspected activities by using keystroke and mouse movement of reviewers.

Industries and researchers have investigated fake review detection since the emerging of online review systems. Many methods can detect many fake reviews. However, fake review cases are still apparently and frequently occurred today. Especially in the case of “The Shed at Dulwich,” the fake restaurant was not caught by TripAdvisor until the manager reveals his action. Hence, it can be implied that the centralized online review system still lacks some crucial information to judge fake reviews.

2.3.3 Fake review spam handling

Many platforms like Google, Booking.com, and Amazon silently remove fake reviews after the detection process. Review platforms like TripAdvisor inform review authors when their reviews are filtered out from the platform. Yelp.com goes beyond one step by keeping detected reviews as “Not recommended reviews.” Most platforms do not reveal the actual percentage of fake reviews behind the systems. Exposing the number of fake reviews may highlight the prevalence of fraud. Customers might reduce their trust in the platforms when they perceive the presence of fake reviews. However, keeping the platform transparent is a key to improve credibility (Stevens, et al., 2018). Ananthakrishnan, et al. (2020) also suggest remaining suspected review accessible. People are likely to trust in platforms more when they can trace more information. An additional suggestion is to identify suspected reviews. Consequently, customers can easily distinguish between truth and fake reviews.

Most platforms rely on automatic filtration. It can remove many suspected reviews within a short time. However, the filtered reviews are not only fake reviews but also genuine reviews. Many customers claim that their reviews were filtered out, and the reasons they got were not sensible (Mayzlin, et al., 2014). While many automatic filtering systems rely on sentimental analysis, people are blocked from expressing extreme opinions. As a result, review scores are scoped to be moderate by the automatic filtrations. Perhaps, the terms “fake review” and “undesirable review” should be defined by users. Unfortunately, people do not have much authority over current platforms. The platform providers have the highest privilege to handle activities that do not follow their rules.

In some special cases, people might prefer to keep promotional or attacking reviews in the system. On the one hand, a business may get much impressed by customers. On the other hand, a business manager might make unforgivable mistakes. In the current platforms, promotional or attacking reviews are immediately

filtered out by platform providers. They cannot provide different judgment among participated businesses because such action is a biased service. In contrast, if there is no central authority, the system can provide flexibility in judgment. The majority of users have the highest privilege. Every participant has the same level of authority. The proposed framework can provide such an ecosystem by leveraging the decentralization of a blockchain.

The disadvantages of current platform solutions in fake review spam handling can be summarized into three aspects: (1) lacking transparency, (2) platform-centric ecosystem, and (3) non-flexible judgment. Our framework aims to increase online review credibility by providing high transparency. The majority of users can define criteria to judge undesirable reviews. Lastly, suspected reviews are still valid until users vote for them.

2.4 Similar projects

Currently, few projects are working on the blockchain-based online review system. The same objectives among the projects are to improve reliability, transparency, and user-motivation. The review data will be recorded permanently and exposed publicly in a blockchain. Some of the platforms utilize AI to extract the sentiment of review content and filter out the negative ones. They introduced token-based rewards, which utilize cryptocurrencies to incentivize users. The proposed projects are listed as follows.

2.4.1 Revain

This project is a blockchain-based review platform that tries to improve the quality of user reviews for any business. Revain utilizes IBM's artificial intelligence to suggest quality review writing to the reviewer (Revain LLP., 2018). If the reviews do not pass the rules, they cannot be posted. With this platform, the reviewers need to spend more effort and time to write a quality review, but they will be rewarded if they can post a review. The reviewers that make many quality reviews will be promoted to be experts, who will obtain more opportunities and rewards. Revain uses two tokens R and RVN to produce a less volatile token. R token is used for gathering funds and exchange purposes. As a result, the R token is volatile. RVN token is a stable token that will be mainly used internally in this platform, such as rewarding users for quality reviews, debiting companies for written reviews, penalizing users for non-compliance with the rules of the platform. Revain accomplishes RVN token to be 1 USD by using this formula:

$$1\,RVN = \frac{(1\,USDT + 1\,USDC + 1\,TUSD)}{3} \tag{2.1}$$

Eq. 2.1 uses the following stable coins to formulate the RVN token. USDT is a Tether coin, USDC is a USD coin, and TUSD is a TrueUSD coin. RVN cannot be exchanged externally, but the users can withdraw their reward using the R token. The reward from reviews comes from the reviewee companies. They have to pay a review fee in RVN for every review created by users. Users will be able to get the reward if and only if the companies accept a review. Users can dispute if they believe that their reviews should not be rejected. This case will be handled by using a decentralized oracle system, which is the group of high reputation users who can verify proof of users. If the users are right, they will get the reward, and the company will receive a warning by penalizing for 10 RF (i.e., Reward Fee). A company may receive up to 3 warnings. If there is a fourth, the company will be blocked from using the platform. The users can also receive the warning. The first case is if three of the user's

reviews in two weeks period are rejected by automatic filtration. The second is if five of the review in two weeks period are rejected by the reviewee company. The fourth warning leads to the users being blocked from using the platform and cannot withdraw the reward.

There are 2 steps for review filtrations in the Revain platform. The first is automatic filtration using the IBM Watson platform. It can analyze the tone of reviews in three components containing emotional, language style, and social tendencies. The second is manual company filtration. Once the reviews pass automatic filtration, the company can either approve or reject the reviews. However, the review will be shown regardless of the company's decision. If the company rejects the review, they need to leave a comment on that review. The comment will be visible publicly with the corresponding review. Thus, solving the issue of unconstructive reviews.

Revain platform only targets the crypto business reviews, which have some different practices with tourism reviews. There is no purchasing verification before posting a review in Revain. Anyone can still generate reviews without real consuming experiences. The platform contains automatic filtration, which mainly focuses on sentimental analysis. The extreme negative or positive reviews are always filtered out. As a result, the overall reviews in the platform are scoped to be moderate tone.

2.4.2 Lina.Review

Lina (Lina Network, 2019) is a platform that utilizes blockchain technology in various fields include review, supply chain, individual identity, healthcare, and education. Lina.Review is a module in the Lina platform. It stores the submitted review from the user in a secure manner and also rewards for quality reviews. Individuals or businesses can build their systems on Lina.review platform. To

produce more useful reviews, Lina.review employs experts or helpers, who proved their domain knowledge by providing CV to the platform or be promoted by other users by publishing many acceptable reviews. The experts and helpers write reviews to businesses regard to their knowledge domain. They are entitled to receive the reward from advertisement revenue and registration fee. However, they must satisfy a monthly quota of acceptable reviews. Otherwise, they will lose the expert or helper status. Lina.Review ensures that the reviews have come from the users who have consumed the products or services by storing transaction details in private blockchain to avoid the high cost of transaction in the Ethereum public blockchain.

Lina.review stores the review content in their private blockchain. As a result, the platform is under controlled by the Lina team. This point is the main difference between Lina and this work.

2.4.3 Dentacoin

Dentacoin (Switch, 2017) claimed to be the first blockchain-based online review system for dental services. The dentists can register their dental offices to get patient feedbacks and display them in public. Additionally, the patient can also register the dental clinics they have serviced. It uses the concept of “trusted reviews”, where only the patients who have received service from the corresponding dentists can post the review. These patients are verified by the dentists sent a link for posting reviews via email. The reviews posted via those links are marked as trusted reviews. The reviewer gets a reward in Dentacoin token (DCN) after posting a review. DCN can be used to get discounts or promotions for further treatment. Moreover, DCN tokens will be distributed through the industries which means that the users can use them as a cryptocurrency.

The trusted review concept proposed by Dentacoin can be vulnerable to fake positive review spamming. A dentist can send emails to his friends to allow them to post fake promotional reviews.

CHAPTER 3

RESEARCH METHODOLOGY AND PROPOSED FRAMEWORK

3.1 Potential of a blockchain in online review systems

This work firstly investigates the suitability of blockchain technology in the online review application. The blockchain tradeoffs such as transaction costs and speed are firstly investigated. This subsection introduces tools used in system implementation. The system design, which aims to minimize tradeoffs, is proposed. The testing methodologies are then explained in detail.

3.1.1 Tools

A smart contract is the core component of the system. It is implemented on the Ethereum blockchain by using the Solidity programming language. Remix online IDE is used in coding, compiling, and deploying processes. The smart contract is deployed to and tested on the Ropsten test network, which works similarly with the main network (uses the POW consensus algorithm). IPFS is used to reduce the transaction cost of the smart contract. The Web3js library is used for the smart contract interaction. A blockchain node is communicated through the Infura service.

3.1.2 System design

The implemented system records review data and authorship information on the blockchain storage. The review data contain title, content, ratings, timestamp, and graphical data (images and videos). The implemented system can be divided into 2 approaches. The first directly keeps review data on the blockchain storage. In contrast, the second approach stores data on IPFS and uploads the IPFS hash to the blockchain instead. The transaction cost can be reduced by minimizing the amount of transferred data. Thus, the second approach costs less than the first. However, it causes a slower process since there is an additional process of data transfer. The implemented systems are designed as follows:

3.1.2.1 Smart contract without IPFS

This approach stores actual review data on the blockchain. Even though users can directly upload graphical data to the smart contract, it produces extremely high costs due to a large amount of data. Thus, the system maintains graphical data on a centralized database. The centralized server returns hashes and URLs of graphical data to users after they upload that information. The users then submit review data (including hashes and URLs of graphical data) to the smart contract. The sequence diagram of the system can be illustrated in Figure 3.1.

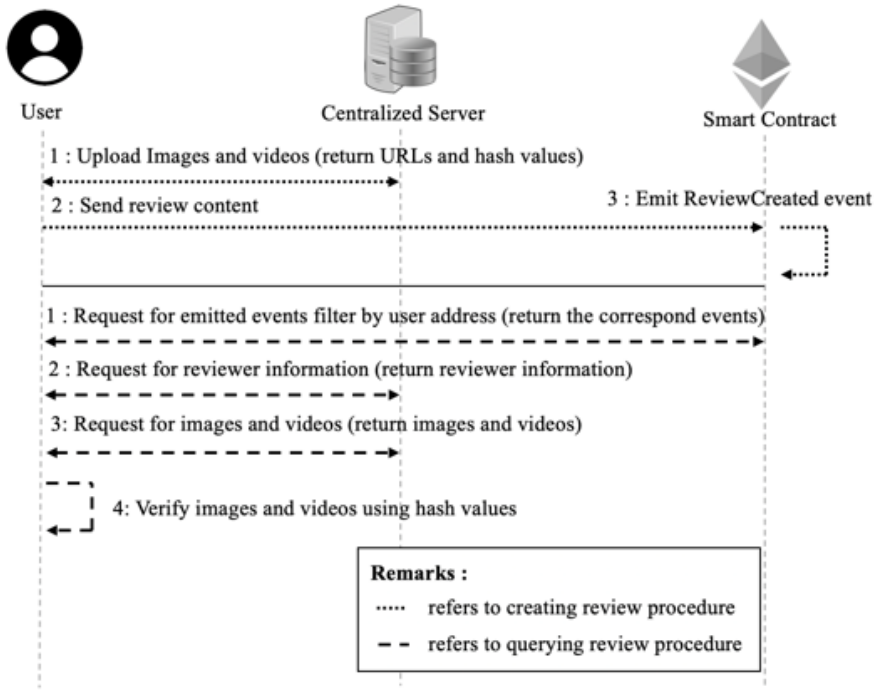

Figure 3.1 Without IPFS contract's sequence diagram

Inside this approach, the system can be divided into 2 sub-approaches. The first sub-approach records data on smart contract states. The another does not use the states but emit events to keep data in form of records instead. The stateful contract can further utilize review content inside the smart contract. On the other hand, the stateless contract just keeps the review data on the blockchain storage, but it cannot be used on-chain. However, the stateless contract reduces operations. As a result, the stateless contract costs less than the stateful contract.

Review data can be retrieved from the smart contract. The stateful contract provides getter methods for review data retrieving. The stateless contract needs a different way to fetch the review data. Users have to request the emitted events related to review posting. The results from both approaches are the same. They contain review data (title, content, ratings, and timestamp) and graphical information metadata (URLs and hashes). Users can request graphical data as well as author information from the centralized server. Eventually, users can validate the integrity of

images and videos by computing their hashes and comparing them with hashes retrieved from the smart contract.

3.1.2.2 Smart contract with IPFS

The second approach of the implemented smart contract utilizes IPFS to reduce the amount of data recorded on the blockchain storage. Thus, it reduces transaction costs. In this approach, users upload graphical data to the IPFS and get its hashes. The hashes are then uploaded with the review data into IPFS again. The hash of a review is uploaded to the smart contract. The IPFS hash is a 46-character string, which is significantly smaller than the raw review data. The sequence diagram of the smart contract with IPFS is illustrated in Figure 3.2.

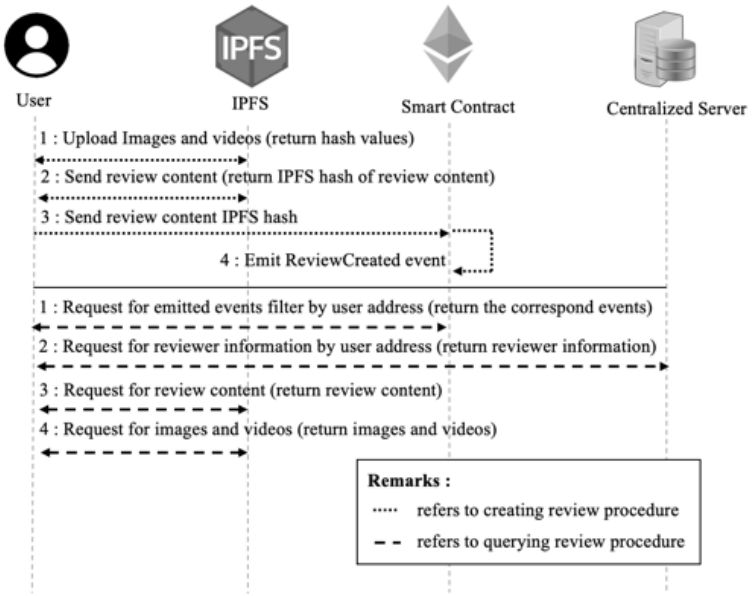

Figure 3.2 With IPFS contracts' sequence diagram

The smart contract with IPFS can be segregated into 2 sub-approaches as well. The first sub-approach keeps the IPFS hashes of reviews on the smart contract state. The second sub-approach emits events to record IPFS hashes instead. The

review authorships can be further applied on-chain for the stateful contract. Nevertheless, the stateful contract losses the ability to compute the review data on the smart contract. The stateful contract produces more transaction costs due to more operations.

3.1.3 Experiment

An experiment is constructed to demonstrate the empirical results of transaction costs and speeds of the blockchain-based online review systems. Moreover, the implementation principles of blockchain applications are studied. Controlled factors and testing methodology are described as follows:

3.1.3.1 Controlled factors

Sizes of graphical data used in the experiment are varied by 1MB, 5MB, 10MB, and 50MB. The review content size is in the range of 200 bytes to 2KB. The gas price is 3 GWEI (1 GWEI = 10^{-9} ETH), which is the cost for average speed transactions at the time of experimenting on January 12, 2020. ETH Gas station, which monitors the gas price on the Ethereum blockchain, is the reference of the average speed transaction cost. The centralized server used in the experiment is the cheapest Digital Ocean droplet, which has 1 GB RAM and 1 CPU.

3.1.3.2 Experiment 1: cost and response time

This experiment aims to find the relationship between review content size (input), and transaction cost and speed (output). The smart contacts with IPFS and without IPFS are tested their performances with the following procedures:

(1) Create a review with the size of 200 + (100*i*) bytes, where *i* denotes the round number, which is ranged from 0 to 18. Only metadata of graphical information (i.e., URLs, hashes, and IPFS hashes) is included in a review.

(2) Post a review to the system and note the input size, the transaction cost, and the response time (hash time).

(3) Repeat step (2) for 10 times to calculate the average results.

(4) Increase the round number (*i*) and repeat step (1) to step (3) until the final round.

3.1.3.3 Experiment 2: uploading time

The second experiment tests performances of the storages. The file size is used to be the input of the experiment. The output is the duration of the graphical data uploading. This experiment explores the usability of IPFS compared to the centralized database. The experiment is conducted with the following processes:

(1) Upload a file to the storage (i.e., the centralized database or IPFS). The file size is varied by 1MB, 5MB, 10MB, and 50MB with regarding the testing round.

(2) Record file size as input and uploading time as output.

(3) Repeat step (1) and step (2) for 20 times.

(4) Increase the file size and repeat step (1) to step (3).

3.2 Blockchain-based online review system features

According to the first study, blockchain technology is not suitable for the review-only application due to the possible expensive transaction cost. However, a blockchain natively supports financial use cases, which has the potential to provide many features over the traditional systems. Additionally, the transaction cost would be treated as a small amount compared to the product prices. Applying the financial use case is a way to maintain a good user experience. This subsection proposes a blockchain-based online review system with full features. The system is tested in performance and feature aspects.

3.2.1 System design

Currently, the centralized online review systems are working under the trust of users. Customers have to trust the centralized online review providers, which might not always be honest. However, there is no guarantee that platforms do not silently conduct suspected actions behind the system. Thus, some users are skeptical about trusting platforms. The proposed system eliminates a central authority with the capability of a smart contract. The smart contract enforces a set of rules, which encourage good practices. The rules and all information are securely protected by a blockchain. As a result, the review data cannot be tampered by anyone except the review authors. The system keeps every version of edited or removed reviews. They can be traced publicly. The system provides the fairest judgment by the user community. The majority of users has the highest privilege on the proposed system. The system design comprises architecture and protocols.

3.2.1.1 Architecture

There are 2 main components on the system, the smart contract, and users. The smart contract acts as an interface of the system. It contains functions, which can be called by a user for system interaction. The details of functions will be presented in the protocols section. Users can be divided into 3 roles: (1) customers, (2) sellers, and (3) third parties. The system architecture can be illustrated in Figure 3.3.

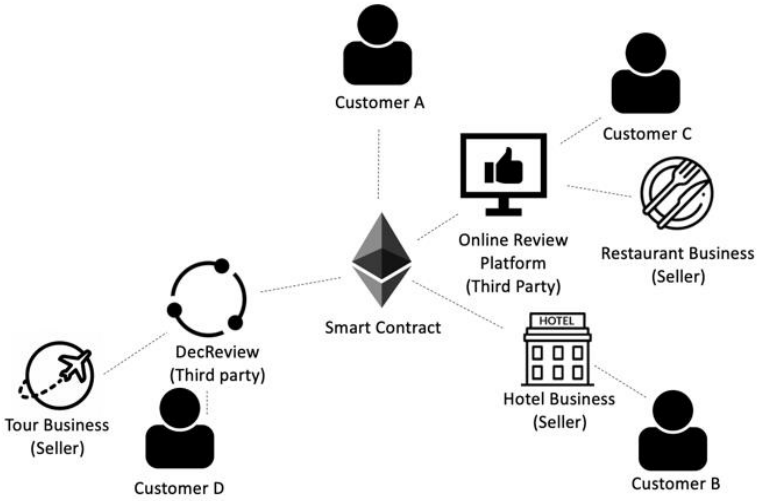

Figure 3.3 System architecture

Users have different purposes of system participation. Customers need some information to assess products' qualities. They can purchase a product through the smart contract. Sellers or businesses need review data to make credibility. They can also sell their products through the smart contract. Third parties provide services to customers, sellers, and even other third parties. They utilize the smart contract to build applications that benefit other users and can make profits from the system. System functionalities and use cases are illustrated in Figure 3.4.

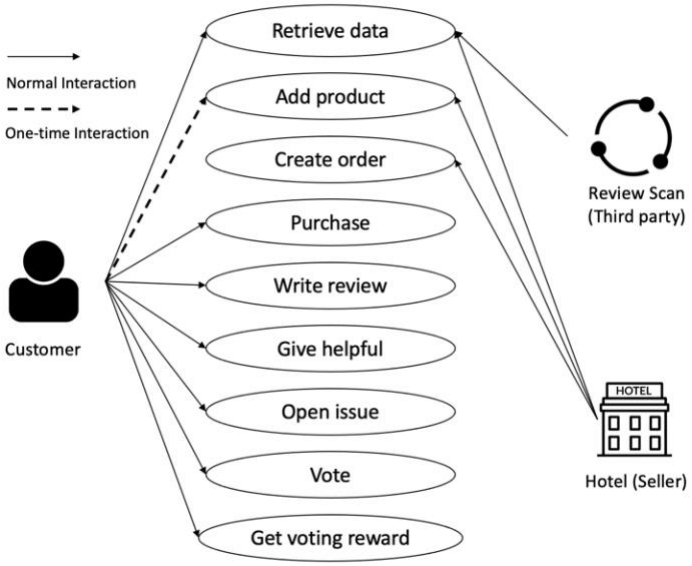

Figure 3.4 Use case diagram

All accounts are customers at the beginning state. Customers can purchase products, post reviews, give review helpful scores, and vote to point out fake reviews. Customers assess quality of products by reading reviews available on the blockchain storage. They can then purchase a selected product or service through the smart contract. Customers can post a review after they purchase a product. The system encourages people to give a helpful score to a review that the customers benefit from it. On the other hand, customers can vote for a suspicious review. If they succeed in voting, they get a reward for their contribution.

Once customer accounts upload product information into the smart contract, the accounts become seller accounts. Sellers can only manage their product information and operate selling. Other customer actions, such as purchasing, reviewing, helpful score giving, and voting, cannot be done by sellers. The system does not allow those actions as well as reverting seller accounts to customer accounts due to credibility reasons. According to guidelines, sellers should not be able to conduct actions that directly affect rating scores. Sellers have alternatives to display their reviews on their platforms or third-party platforms. With the advantage of a blockchain, the reviews are identically presented on every platform. Additionally, there is no cost or permission to retrieve and show reviews on multiple platforms.

Many third-party applications can be implemented on top of the proposed system. They utilize review data to provide some services, such as a ranking system, a tourist recommendation platform, a marketing analysis system, a review credibility assessment tool, and many others. A ranking system collects a list of local businesses in a particular area and supports their marketing. Customers and businesses can easier use a large amount of data by the recommendation systems. Fraudulent activity detections are more intense with the credibility assessment tool. There can be various opportunities from the public online data, which can be used to implement applications by any users.

3.2.1.2 Protocols

The system protocols are defined by using a smart contract. The declared protocols cannot be changed except with migration, which needs agreement among users. The source code of the smart contract is publicly available. Thus, people can consider the protocols before participating in the system. The protocols are designed to encourage good practices and discourage suspicious actions. All participants interact with the system under the following protocols:

(1) Product management: Sellers can record product information on the system. The raw product information has to be stored on IPFS and its IPFS hash is recorded on the smart contract. Product information schema can be varied, but it should be consistent. The simplest schema contains the product name and a URL link that provides more information. Since updating data in the smart contract requires cost, the rapidly changed data should not be stored on the smart contract. Sellers have to define a review value of each product. The review value is the amount of Ether that the sellers are willing to pay to incentivize quality reviews and handle fake reviews. Each time a product is purchased, the smart contract deducts and keeps the review value from the paid money. The remaining will be transferred to the

corresponding sellers. The product information and review value can be updated by the product owner. The general information can be edited anytime. However, the review value cannot be frequently changed to keep the motivation of users in review posting.

(2) User profile: At the beginning state, every account is anonymous. There is no personal information attached to any accounts. According to prior research, people will trust reviews more when the review authors disclose their personal information. The system provides options for users to be anonymous or identified (Park and Nicolau, 2015). Users can upload their personal information to IPFS and store the IPFS hash on the smart contract. Personal information can be edited anytime, but every version of it is available on the system. Thus, people can trace information about an account.

(3) Product purchasing: Trading procedures begin with order creation, which is conducted by sellers. Customers have to contact sellers and request order creation. Sellers define a product price, create an order on the smart contract, and get the order identification number (order id). The order id is then submitted to the requester. The customer refers to the order id to purchase the product. The protocol compares the amount of transferred balance with the product price defined on the order. If the condition is passed, the transaction is successful. The smart contract keeps an amount of review value from the transferred balance. The saved review value can be used to reward a reviewer who writes a quality review. The remaining balance will be transferred to the seller.

(4) Review management: Customers have to refer to a purchased order when they post a review. A purchased order can be used once to ensure that the opinion is expressed related to actual purchases. Raw review content is stored on IPFS and its IPFS hash is submitted to the smart contract. The smart contract then emits an event to record a review. This practice follows transaction cost minimizing guidelines, which are demonstrated in the previous work (Karode and Werapun, 2020). Review

authors can update or delete their reviews. The system keeps all versions of reviews. The updated or removed reviews can be kept track of every version. The smart contract code ensures that all reviews cannot be edited or deleted by other persons except their authors. Moreover, the high security of a blockchain protects the smart contract and data in the system.

(5) Review response: The system provides sellers with a review response channel. Sellers can reply to reviews to thanks customers or clarify misleading messages. The frequent, quick, and authentic response of sellers increases customers' trust towards the businesses. Raw review responses are stored on IPFS and their hashes are submitted to the smart contract. The smart contract then emits an event to record them.

(6) Review value: Each product has a review value, which is defined by the product owner. When there takes place a purchase, the smart contract deducts and keeps the review value on the system. The remaining money (i.e., paid money – review value) is eventually transferred to the seller. The stored review value is bound with an order. Customers can use an order to give a helpful score within a limited time. The review value will be transferred to the review authors who own reviews that receive a helpful score. If customers do not give a helpful score in time, the system will lock the review value on the particular orders. They will not be able to use the locked orders to give helpful scores. The review value is then moved to the reward pool, which will be additional rewards for voting.

(7) Issue creation: The protocol enables only users who have purchased a product to create an issue on it. Customers open an issue when they detect a suspicious review. The objective of issue creation is to handle fake reviews. A suspected review is selected on the step of issue creation. Issue creators define voting timeout, the maximum vote value, and the argument text (to point out review mistakes). The locked orders can be referred to as an additional reward. They can stake an amount of money (i.e., Ether in this system) to determine their voting scores at the

time of issue creation. After an issue is created, people can vote for the issue. When the issue time is up, it will be concluded and executed according to voting scores.

(8) Issue voting: Customers can participate in an issue opened on a product they have purchased. They decide to vote “agree” or “disagree” with the issuer’s arguments. Voters stake an amount of Ether on the side they vote. The amount of Ether determines the confidence of voters. While the real-time voting results are publicly available, there might occur the last-minute voting problem. Last-minute voting is done by a voter who stakes a large amount of Ether in a few minutes before the issue closes. The vote time extension is introduced to address the problem. If there still occur votes near the issue closing time, the voting time will be extended. The issue will close when there is no vote submitted on the extended time. The result of the voting is determined by comparing the summation of scores between both sides. If the issue contains more “agree” scores, the target review is marked as “undesired”. Otherwise, there has no change in the target review.

The voting mechanism is designed to motivate contribution. At the same time, it disincentivizes cheating. Voting winners get their staked money and the staked balance of the opposite side. The reward portion (P) is calculated by dividing the user’s voting amount (V_{own}) with the total voting amount on the same side ($V_{total\ same}$). If there exists the additional reward ($R_{addition\ total}$) from an unused order, it is shared among the winners by ($R_{addition}$) value. Finally, the voting reward (R) is the partition of total votes in the opposite side ($V_{total\ opposite}$) plus the voter’s vote amount (V_{own}) and the portion of additional reward ($R_{addition}$). The reward is distributed among the winners. Investing more Ether increases the portion of the earned reward. However, losing an issue means wasting all invested Ethers too. With this condition, voters need to be confident in their votes. The reward calculation can be illustrated as Eq. 3.1, Eq. 3.2, and Eq. 3.3.

$$P = \frac{V_{own}}{V_{total\_same}} \quad (3.1)$$

$$R_{addition} = P \text{ x } R_{total\_addtion} \quad (3.2)$$

$$R = P\ x\ V_{total\_oppisite} + V_{own} + R_{addition} \quad (3.3)$$

3.2.2 Performance testing

There are further implemented functions on the proposed framework. Performance testing is required to ensure their usability. Transaction costs and response speed of every method on the smart contract are examined. The experiment details are presented as follows:

3.2.2.1 Controlled factors

The Ethereum Ropsten test network is used in the experiment because it uses POW as a consensus algorithm. Thus, the result is closed to the main network. The gas price is set to 3 GWEI since it is the average transaction speed suggested by the Metamask wallet at the time of experimenting on January 12, 2020. The blockchain node is used through the Infura service. The experiment code is implemented with NodeJS. Web3.js is the library for smart contract interaction.

3.2.2.2 Methodology

The implemented smart contract contains a set of methods, which provide interactive interfaces for users. The experiment investigates transaction costs and the speed of the smart contract methods. Each method is tested by submitting 20 transactions and record their costs and speed. The method names and arguments are presented in Table 3.1.

Table 3.1 Smart contract methods' details

Method Name	Arguments
Add product	string ipfsHash, uint256 reviewValue
Update product	uint256 productId, uint256 reviewValue
Update user info	string ipfsHash
Create Order	Address customer, uint256 productId, uint256 price
purchase	uint256 orderId
Post review	uint256 orderId, string ipfsHash
Delete review	uint256 orderId
Update review	uint256 orderId, string ipfsHash
Reply review	uint256 targetId, string ipfsHash
Give helpful	uint256 orderId, uint256 targetId
Open issue	uint256 orderId, uint256 targetId, uint256 timeout, uint256 maxVal, string ipfsHash, uint256 unusedOrder
Vote	uint256 orderId, uint256 issueId, string ipfsHash
Get voting reward	uint256 issueId

3.2.3 Feature analysis

In this work, the unique features of the blockchain-based online review system are explored. Blockchain characteristics are applied to the online review application to find features that cannot be achieved by the centralized environment. The potential features of an online review system are matched with blockchain characteristics as displayed in Table 3.2.

Table 3.2 Online review system features inherited from blockchain properties

Online Review Features	Immutability	Decentralization	Smart Contract
Purchasing validation	✓		✓
Information management	✓		✓
Rewarding	✓		✓
Cooperation capability		✓	
User-centric operation		✓	✓

The system design does not only aim to find possible features of the framework but also to cope with problems in traditional online review systems. Further investigation on robustness against fraudulent activities of the proposed system is demonstrated in the next experiment.

3.3 Robustness against fraudulent activities of the blockchain-based online review system

The blockchain-based online review system publicly opens information. Many applications can extend features of the proposed system by utilizing public data. The system does not contain only review data but also user behaviors. Both of them are applied by prior research to identify fake reviews. Even though many excellent tools are proposed and applied on the centralized platforms, a number of fake reviews are still along with them. Moreover, genuine reviews of some users who have extreme experiences are removed by automatic filtering tools. Review platforms (e.g., Trip Advisor, Yelp.com) take serious actions to detect fake reviews. However, they do not validate customer's purchasing status before accepting a review. Lacking purchase validation causes systems vulnerable to be spammed. In contrast, booking platforms (e.g., Booking.com, Expedia), which require a purchase before review posting, do not earnestly investigate fake reviews. Combining good practices from both types can deal with many fake reviews. The proposed system can inherit methods from centralized review systems. This chapter further explores how the proposed system resists fraudulent activities. We focus on 3 fraudulent actions including fake review spamming, reputation forging, and review content tampering. Its capabilities to protect, detect, and handle problems are evaluated and compared to the centralized online review platforms.

3.3.1 Proposed framework

A third party can utilize the information available on the blockchain storage. A third-party application named “review scan” is proposed. The framework comprises 4 tools: (1) integrity checking tool, (2) transaction visualizer, (3) review grading tool, and (4) community label dataset.

3.3.1.1 Integrity checking tool

The system provides public data to platforms and businesses. They can retrieve and display such data. However, there is no guarantee that those services display the same data as retrieved from the blockchain. Ideally, customers can directly compare review data presented in platforms and blockchain. However, it is not convenient for ordinary users to directly check data in both sources. The integrity checking tool programmatically compares data on service with the blockchain data. It computes hashes of both versions and compares each other. A platform might include a badge on a review content to show the review integrity. The content integrity checking tool interface can be illustrated in Figure 3.5.

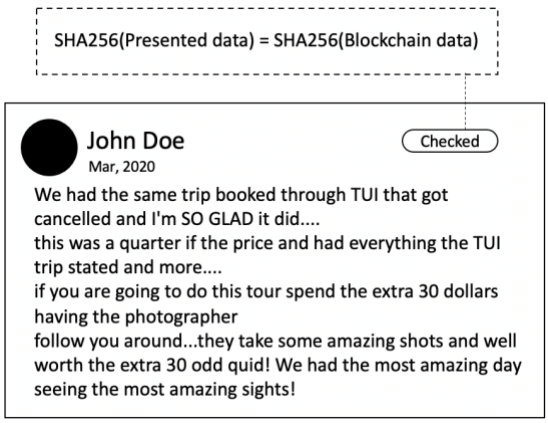

Figure 3.5 Integrity checking tool

3.3.1.2 Transaction visualizer

Transaction history available on a blockchain can be used to imply suspicious actions. For example, when a business transfers some money to its customers, then the customers post reviews to it in a short period. This practice can infer relationships between them. The posted reviews can be treated as paid reviews. The transaction data reflects users' behaviors, which are important information to point out suspected actions. However, the blockchain transaction history is stored in the form of records, which is not convenient for interpreting. The review scan framework collects transaction records and converts them into the graph structure. This work uses the Neo4j library to maintain the transaction graph database. Users can easier recognize suspected actions like paid reviews, self-reviews, and self-ratings. The relationship among spammer groups can also be detected. The transaction visualizer displays account relationships in a simple view as illustrated in Figure 3.6.

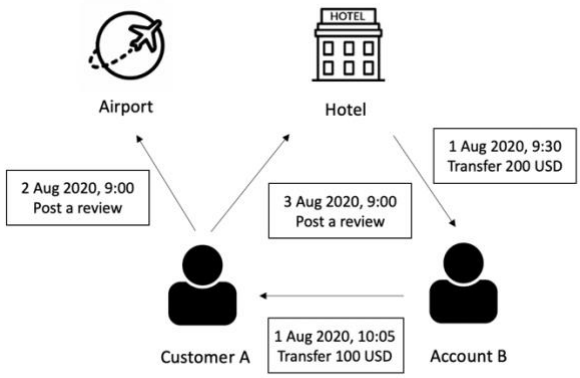

Figure 3.6 Transaction visualizer

3.3.1.3 Review grading tool

People might not be able to detect complex account relations by only using the transaction visualizer. Graph analysis is needed to indicate fraudulent actions. The transaction graph database created by Neo4j can be used to determine review authors' scores and credibility. The review grading tool analyzes not only transaction data but also review content. It computes and displays aggregated information, which reflects the review's trustworthiness. All previous methods in fake review detection can be applied in the review grading tool. Moreover, users can define terms of "fake" by the community agreement. The review grading tool only determines credibility scores, which help people to decide to trust in a review. The system lets users manage fake reviews by voting. They can utilize the review grading tool for quicker and smarter decisions. However, they can also leave a low score review if they prefer. Since the fake review problem is subjective, fixed criteria are not always accurate. As a result, the system offers the last decision based on the user community. This practice provides more flexible and fairer fraudulent action punishment. An example of a review grading tool interface that picks some criteria from Yelp.com (Mukherjee, et al., 2013) is presented in Figure 3.7.

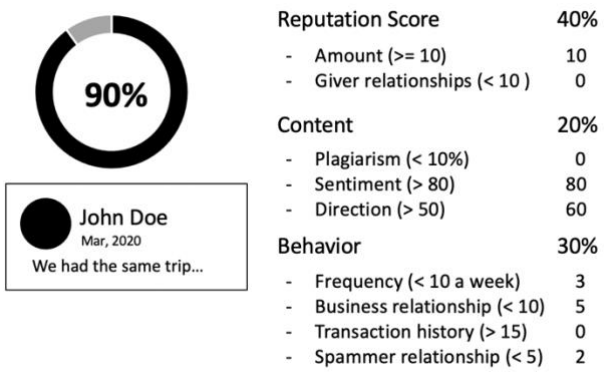

Figure 3.7 Review grading tool

3.3.1.4 Community label dataset

The machine learning method is the most popular approach for fake review detection. More specifically, supervised learning is applied with labeled datasets that contain fake and non-fake reviews. Fake review definition should be determined by customers and sellers, who are involved with online reviews (and their consequences). However, the centralized online review platforms classify fake and non-fake reviews by the platform decisions. Consequently, the labeled datasets available today might not correctly indicate fake reviews defined by users. Some genuine reviews can still get filtered out, and some fake reviews can remain in the system.

The proposed framework relies on the user community in fake review detection. When the majority of users agree, the targeted review is treated as a fake review. The labeled datasets of fake reviews can be created from fake review voting history. Fake review detection tools can be developed on top of the user-decision datasets. As a result, this approach can detect fake reviews with higher accuracy related to user decisions.

3.3.2 Evaluation

Robustness against fraudulent activities of the proposed system is evaluated by using scenario tests. The scenarios are applied to the current platform environment. They are also executed to test the proposed tools. The effectiveness of both approaches is then compared to evaluate the proposed framework.

3.3.2.1 Fake review spam scenario

A fake review spam scenario is constructed and applied to the current platform and the proposed framework environments. The objectives of the experiment are to evaluate the capability to protect, detect, and handle fake review spamming in both approaches. The fake review spam scenario is constructed with the following information:

(1) Review posting requires purchasing. A purchase can be used for one review posting.

(2) A fraud business asks spammers to boost its rating by posting N fake positive reviews of its products or services.

(3) The business wants to attack another business by generating N fake negative reviews.

(4) The business pays the initial cost to spammers. The initial cost is used to purchase products or services to unlock review posting.

(5) Spammers use N fake accounts to generate fake reviews.

(6) The business pays a service fee to spammers after they finish the work.

Suppose the business conducts the above scenario on the current booking platforms (e.g., Booking.com, Expedia.com). The cost for fake negative review spamming is relative to the product or service price and spam service fee as determined by Eq. 3.4, where $C_{product}$ represents product price and C_{spam} is spam fee. The cost for fake positive review spamming can be determined as Eq. 3.5. It is significantly lower than negative review spamming because the product price is returned to the business.

$$C_{c\_neg} = N\left(C_{product} + C_{spam}\right) \tag{3.4}$$

$$C_{c\_pos} = NC_{spam} \tag{3.5}$$

When the scenario is applied to the proposed framework, the spammers need to have a money-feeding strategy. Each account requires a cost for product purchasing and transaction sending. Difficulty in money feeding increases in the proposed framework environment, since the transaction visualizer can display transactions in a blockchain. People can notice the relationship between the business and the spammers. Thus, the business has to avoid sending transactions to the spammers, whether in direct or indirect ways, to conceal their relationships.

The only way to hide their relationship is off chain feeding. The business pays the spammers in cash. Then, the spammers spend the cash to exchange cryptocurrency (i.e., Ether in this case) from a buyer. Ideally, they might trade with a peer-to-peer buyer. The cost of exchanging is cheaper with peer-to-peer trading. However, it is difficult to find a peer-to-peer buyer locally. Hence, a cryptocurrency exchange platform (e.g., Binance, Kraken, BitMex) is the simpler choice. For their best practice, they have to avoid revealing relations among spammer accounts. Thus, each account directly withdraws Ether from the exchange platform and spends it for fake review spamming. Since withdrawal requires additional cost, they have to encounter high cost for money feeding. The off chain feeding strategy is illustrated in Figure 3.8.

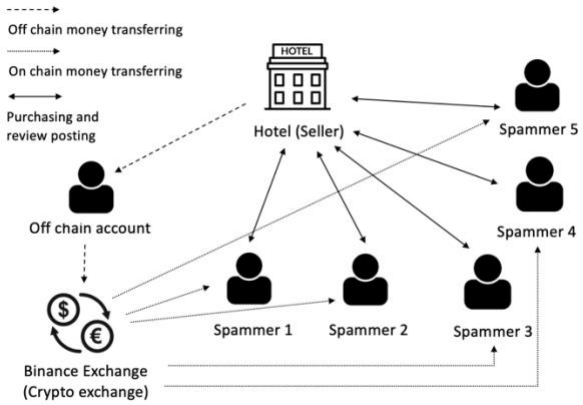

Figure 3.8 Off chain feeding strategy

The scenario is executed with the previous and the following conditions:

(1) Spammers deposit money to a cryptocurrency exchange platform. There is no cost for depositing money to the platform. However, the platform charges a fee for withdrawal ($C_{withdrawal}$).

(2) Transaction costs for product purchasing and review posting are required in the proposed system environment. The product purchasing and review writing transaction costs are referred to as $C_{tx\_purchase}$ and C_{tx_review} respectively.

Spammers must pay additional cost when they generate fake reviews in the proposed system. The additional cost can be calculated by using Eq. 3.6. Cost for fake negative review spamming in the framework can be determined as in Eq. 3.7, where $C_{addition}$ represents additional cost fraudsters have to spend more to generate fake reviews in the proposed system. Fake positive review spam cost can be determined by Eq. 3.8.

$$C_{additon} = C_{withdrawal} + C_{tx\_purchase} + C_{tx\_review} \quad (3.6)$$

$$C_{d\_neg} = N(C_{addition} + C_{product} + C_{spam}) \quad (3.7)$$

$$C_{d\_pos} = N(C_{addition} + C_{spam}) \quad (3.8)$$

3.3.2.2 Reputation score forging scenario

User contribution history is an important element that increases the credibility of reviewers. Users who post more reviews get more trust from others. Specifically, reviewers who receive many helpful scores on their reviews are the first

considered. As a result, reputation score forging is usually conducted by paid review services. We conduct scenarios of reputation score forging on the current platforms and the proposed system.

Spammers can forge reputation scores on the current platforms by using the following strategy:

(1) Generate fake accounts: The Spammers need many emails to generate N fake accounts on the current platforms. They might have to make the fake profiles (fake names and fake avatar images) to those accounts to maintain credibility. The difficulty of this step can be determined as $N(Email + Profile)$.

(2) Use an account to post reviews to products: The main account is used to generate M reviews to products. The spammers have to avoid using similar phrases among the reviews. Moreover, they must prevent posting multiple reviews in a short time. The effort needed in this step can be determined as $MReview$.

(3) Use other accounts to give helpful scores to the posted reviews: The current platforms do not require users to purchase a product before giving a helpful score. Some of them even do not need logging in to proceed. Thus, the following step does not require much effort to conduct. The overall efforts to forge a credible account on the current platforms can be determined as Eq. 3.9.

$$Effort = N(Email + Profile) + MReview \quad (3.9)$$

The proposed system requires an additional step for helpful score giving. Spammers have to purchase a product to unlock the action. Thus, spammers do the following steps to forge reputation score on the proposed system:

(1) Generate fake accounts: On the proposed framework, users can create an account by generating a key pair. They do not need to create emails.

However, every account is anonymous at the beginning state. Spammers have to upload the profile information to the smart contract, which requires a transaction cost. The effort needed in this step can be determined as $NProfile^*$, where * denotes the process that requires a transaction cost.

(2) Use an account to post reviews to products: The spammers use the main account to purchase products and post M reviews. In this step, the spammers have to be careful more than the current platform environment because they might reveal relations between them and the target businesses. Therefore, their best practice is to use the off chain feeding strategy to initialize costs. Concurrently, they have to avoid posting multiple reviews in a short period. The spammers have to generate credible review content. This step requires effort as $M(Feeding^* + Purchase^* + Review^*)$.

(3) Use other accounts to purchase T products regarding the purchase of the main account (same products): The proposed framework limits a helpful score for a purchased product. If the spammers want to forge T helpful scores, they have to purchase T products. Same as the previous step, the spammers need money-feeding strategy to transfer the initial cost to their accounts. Thus, the effort needed for this step can be determined as $T(Feeding^* + Purchase^*)$.

(4) Use other accounts to give helpful scores to the posted reviews: The spammers have to avoid rapidly giving helpful scores in a short time. Moreover, the system requires a transaction cost for reputation score gives. Thus, the effort needed in this step can be determined as $THelpful^*$.

The overall efforts needed for reputation forging are determined as Eq. 3.10.

$$Effort = NProfile^* + M(Feeding^* + Purchase^* + Review^*) + T(Feeding^* + Purchase^* + THelpful^*) \quad (3.10)$$

3.3.2.3 Review content tampering scenario

The simplest strategies to tamper data on centralized online review systems and the proposed system are investigated. The simplest way to change data on the centralized system can be proceeded by the database owners. As a result, there is no initial cost required to conduct review content tampering on the centralized systems. On the other hand, a central authority is eliminated on decentralized systems. As a result, hacking is the only way to change the recorded data on the proposed system.

In this section, cost calculation for the Ethereum blockchain attacking is illustrated. The objective is to compare efforts needed for content tampering in both environments. The cost needed for attacking the Ethereum blockchain network can be calculated as Eq. 3.11, Eq. 3.12, and Eq. 3.13, where $H_{network}$ represents the total hash rates of the network, H_{device} is the hash rates of a mining device, N is the number of devices needed for attacking, P_{device} denotes the price of a mining device, E_{device} represents electric power produced by a mining device, $P_{electric}$ is the electric price per hour, and T denotes time in hours.

$$N = \frac{H_{network}}{H_{device}} \tag{3.11}$$

$$C_{initial} = NP_{device} \tag{3.12}$$

$$C_{execution} = NE_{device}P_{electric}T \tag{3.13}$$

Attackers have to occupy more than half of network hash rates. Thus, they have to purchase N mining devices that can totally produce more than the current network hash rate. The difficulty increases for the number of prior blocks since the attackers have to recalculate blocks and catch up with the network.

CHAPTER 4

RESULTS

4.1 Potential of a blockchain in online review systems

According to the experiment, the review content size is linearly relative to the transaction cost. However, the content size is not apparently correlated with the response time due to the small input size. Lastly, increasing file size significantly raises uploading time, especially in the IPFS.

4.1.1 Review size and transaction cost

The transaction costs of the contracts without IPFS are raised for the larger input size. The smart contracts with IPFS produce constant transaction costs since the recorded data are fixed size. Using event emitting produces significantly fewer transaction costs than using the contract states. The correlation of review size and transaction cost is demonstrated in Figure 4.1.

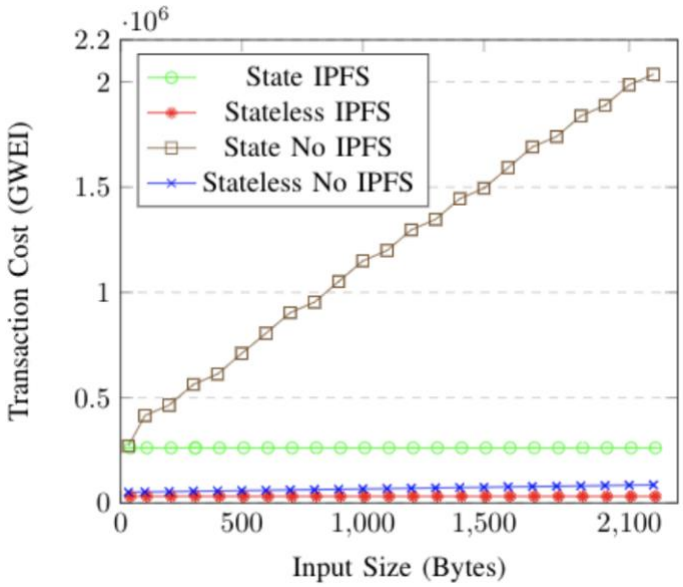

Figure 4.1 Review posting transaction cost

We pick the 500-byte input size, which is the typical size of reviews posted to Trip Advisor, Yelp.com, Lazada, Alibaba, and Amazon to create the empirical result. The Ethereum price at the time of experimenting on January 12, 2020 is 144.47 USD. This value is used to calculate the cost of review posting. The most expensive approach is the stateful contract without IPFS while the cheapest is the stateless contract with IPFS. It is a 24.44-fold difference between the most expensive and the cheapest approaches. The result is presented in Table 4.1.

Table 4.1 Review posting transaction cost

Approaches	Gas used	Cost in USD	Number of Reviews for 1 USD
State IPFS	261,402	0.03776	26
Stateless IPFS	31,342	0.00453	220
State No IPFS	710,204	0.1026	9
Stateless No IPFS	58,348	0.00843	118

4.1.2 Review size and response time

According to the sequence diagram, the response time is divided into 3 parts: the centralized server, the smart contract, and the IPFS response times. Users directly upload reviews to the centralized server for the centralized review approach. On the contract without IPFS systems, the images and videos are firstly uploaded to the centralized server and all data are published to the smart contract. In contrast, on the contract with IPFS systems, the graphical data are uploaded to IPFS and the review data are submitted to IPFS again before being sent to the smart contract.

Since review size is almost not correlated with the response time, we present its average value with its standard variation (in the parenthesis). Response time results are illustrated in Table 4.2.

Table 4.2 Review posting speed

Approaches	Response Time (seconds)			
	Centralized server	Smart contract	IPFS	Total
Centralized	0.13 (0.04)	0	0	0.13 (0.04)
State No IPFS	0.12 (0.03)	1.01 (0.11)	0	1.17 (0.11)
Stateless No IPFS	0.12 (0.04)	1.06 (0.1)	0	1.17 (0.11)
State IPFS	0	1.12 (0.2)	5.17 (7.25)	6.29 (7.29)
Stateless IPFS	0	1.42 (0.36)	4.53 (5.04)	5.95 (5.28)

4.1.3 File size and uploading time

Increasing file size raises uploading time. The IPFS has a higher growth rate. The difference in uploading time is much higher for the larger file size. The uploading speed result is presented in Table 4.3.

Table 4.3 Uploading speed

File Size	Uploading Time (seconds)	
	Centralized	IPFS
1MB	0.4 (0.4)	1.2 (0.4)
5 MB	1.3 (0.5)	4.3 (0.4)
10 MB	1.9 (0.5)	10.3 (1.8)
50 MB	10.5 (0.4)	70.2 (30)

4.2 Blockchain-based online review system features

The blockchain-based online review system is further implemented under guidelines from the first experiment. The performance of the system is tested. Moreover, the potential features of the system, which cannot be achieved in the centralized environment, are explored.

4.2.1 Performance

The system performances evaluated in this work are transaction speed and cost. The experiment results are illustrated as follows:

4.2.1.1 Response time

There are 2 phases of a response time: a hash time and a block time. A hash time is recorded when a transaction is submitted until it gets a hash value. Block time begins at the same point, but it ends when the transaction is recorded into a block. From the experiment, the average hash time ranges from 1 to 2 seconds. The block time is in the range of 20 to 30 seconds.

4.2.1.2 Transaction cost

The actual cost can be calculated by defining the gas price value and multiply it with the gas used value. For example, the gas price is 3 GWEI. The transaction cost of the “Add product” method is 78,379 x 3 GWEI, which is 235,137 GWEI (1 GWEI = 10^{-9} Ether). The transaction cost in fiat can be calculated by considering the Ether value comparing to fiat. For instance, the Ether value at the time of experimenting is 144.47 USD. As a result, the transaction cost for the “Add product” method in fiat is 235,137 x 10^{-9} x 144.47 USD, which is 0.03397 USD. Each method consumes different amount of costs as shown in Table 4.4.

Table 4.4 Gas used for each method

Method Name	Gas Used
Add product	78,379 (± 7,246)
Update product	26,024 (± 0)
Update profile	25,442 (± 0)
Create order	117,374 (± 16,807)
Purchase	81,233 (± 2,589)
Post review	50,216 (± 4,085)
Delete review	27,148 (± 0)
Update review	30,080 (± 0)
Reply review	27,725 (± 0)
Give helpful	50,203 (± 3,338)
Open issue	133,041 (± 16,432)
Vote	75,277 (± 7,131)
Get reward	71,743 (± 11,475)

4.2.2 Features

A blockchain enhances online review systems with its properties. The unique features that cannot be achieved by the centralized environment are demonstrated.

4.2.2.1 Purchasing validation

Travel booking platforms utilize third-party payment services to handle purchasing. They validate purchases from the transactions recorded on the payment services. However, they can ignore the validation process since they can rule everything on their systems. There is no guarantee and accurate detection methods to ensure that platforms will always be honest under the competitive market. In contrast, the proposed system ensures that the review authors have completely purchased a product through the smart contract. There are no alternatives to bypass the purchasing process on the proposed system. The purchasing validation of both environments are compared in Table 4.5.

Table 4.5 Purchasing validation comparison

Feature	Centralized System	Proposed System
Trustless	N/A (People have to trust that the platforms do not bypass purchasing validation process)	Any actions that validate purchasing will not be successful except with an actual purchase
Traceability	N/A (The financial information cannot be traced publicly because of privacy concerns)	The blockchain-based applications natively publish transactions, which can be further used for suspected activity investigation
Tamper-proof	N/A (Platform owners can forge, edit, and delete any data on their system including purchase information)	A blockchain requires extremely high costs and efforts to tamper with the recorded data

4.2.2.2 Information management

Centralized online review systems manage information on their databases. As a result, the information is bound to the platforms. They have the highest privilege on data generated by users. Reviews posted to centralized platforms are not actually owned by reviewers and businesses. People have to request permissions from the platforms to retrieve and use the data. Most platforms do not allow authors to edit or delete their reviews. They claim that the practice is conducted to avoid changing written experiences. Nevertheless, there are other solutions to detect misleading information, such as review version tracking. The data are available only if the systems operate.

The proposed system gives actual ownership to users. Reviews can be edited or deleted by their authors anytime. All versions of reviews are available on the system. Thus, people can notice if a review is suspiciously changed or deleted. The data are available as long as the corresponding blockchain works. Furthermore, the reviews are bound with customer and seller accounts. They can retrieve and display their reviews on any platform without permission. Reviews can be treated as a valuable property on a blockchain-based review system. Information management of both approaches is compared in Table 4.6.

Table 4.6 Information management comparison

Feature	Centralized System	Proposed System
Ownership	N/A (Platforms can update or delete any data on their databases. Users do not have the actual ownership of data they produce)	The system provides users to manage their own data as they want. All actions can be traced publicly.
Reliability	All data are not available when platforms stop their services. Businesses lose all review information on the platforms.	Data are not bound to any platforms. The only way to make them disappeared is to stop a blockchain, which is operated by thousands of computers.
Accessibility	Applications that want to utilize data from review platforms must request permissions. Otherwise, they have to do scrapping, which cannot guarantee the integrity of data.	Anyone can access the review data on the blockchain. Businesses have the opportunity to display reviews from the blockchain on their own websites.

4.2.2.3 Rewarding

Some of the online review platforms provide an incentive for users who post reviews. The reward system increases the number of reviews posted to the system. However, most of them do not benefit other customers. Centralized platforms incentivize scoped rewards, which are only valid on their platforms. The source of reward is the platforms, who get paid from the listed businesses and spend the revenue for the operation cost. Thus, they can only pay a fixed and small amount of reward to users.

The proposed system gives rewards to users through helpful giving. Thus, it encourages people to post quality reviews instead of spamming reviews for earning rewards. Token-based rewards can be used to incentivize users on blockchain-based applications. A token provides more opportunities to its owners, such as currency tokens, discount and promotion tokens, and governance tokens. Users can use currency tokens like Ether as a real currency. Some tokens can be used to get offers from shops. At the same time, those tokens can be exchanged for another token type. The governance tokens can be used in voting to change the system protocols. Businesses can directly give rewards to customers. Since the system eliminates operation costs, businesses can contribute a higher amount of reward compared to the centralized approach. Moreover, the businesses can flexibly adjust the amount of reward regarding their needs for feedbacks. The differences of rewarding in both environments are compared in Table 4.7.

Table 4.7 Rewarding comparison

Feature	Centralized System	Proposed System
Objective	Encourage review generating (In many cases, users post non-relevant content to earn a reward)	Encourage quality review posting (People have to get a helpful score to earn rewards)
Value scope	Centralized rewards are usually restricted to the platforms. The centralized environment is not suitable for financial applications.	Rewards can be directly paid to the beneficiaries' wallets. They can use the reward on other platforms without any restrictions.
Reward source	The central authority manages all processes of incentives. The amount of rewards is fixed. It is also declined from the operation the costs of the platforms.	Businesses can flexibly contribute their incomes for user incentives. The flexible rewards help businesses to motivate customers to post more reviews in some period. They can also decrease the reward amount when they are not willing to pay.

4.2.2.4 Cooperation

Centralized online review systems individually maintain data on their own databases and different practices. A business that participates in multiples platforms might have many versions of its reviews. It much improves their credibility, if all of those are the same trend. However, they are generally different. Platform practices directly affect rating differences. Some platforms keep attractive views of businesses while others do not intensively investigate reviews. Many concerns occur when they want to integrate their systems. An important concern is a trust among participants. They have to trust that their cooperators will always provide correct data. Tracing and validation are more difficult when there are many cooperators on the system.

The proposed system operates on the public blockchain database, which provides trustless cooperation. Keeping the review in one place helps consumers to focus on one point of trust. The businesses also get benefits from this practice. By using a blockchain as a global database, every platform can use the same version of the reviews. Businesses do not need to recreate their ratings when they move to a new platform. Moreover, it opens data for developers to create useful extended applications. The cooperation capability of both approaches is compared in Table 4.8.

Table 4.8 Cooperation capability comparison

Feature	Centralized System	Proposed System
System integration	The separated database makes systems difficult to be integrated	A blockchain publicly opens data, which can be utilized by different platforms without any permissions and concerns about trust
Extension	N/A (Centralized online review platforms do not provide public developers to extend their applications)	The proposed system opens data for the public. Many applications can be implemented on top of the available data

4.2.2.5 User-centric operation

Resolving a subjective problem like fake reviews is not a simple task. Currently, fake reviews are managed by automatic filtering systems or platform experts. It is not fair management to let people who did not have experience with the particular products or services decide the correctness of the information. Actual customers should have the highest right to assess the information. This approach can be treated as a user-centric operation. People can get different experiences from the same services. Thus, the majority of them can express the most accurate information. The majority opinion can be determined through voting. Voting can be interrupted by platform providers if it takes place in a centralized environment. The decentralized environment can prevent this issue. The majority voting might not be practical since it needs many people to participate in while the customers do not have the motivation to join voting. Instead, the Token Curated Registry (TCR) principle is utilized to decrease required participants and motivate users. TCR is executed by requiring stakes from voters. The number of stakes determines the confidence of voters. They cannot withdraw the stakes if they lose voting. On the other hand, they can get money back with opposite site stakes as rewards. While the financial use case like staking is not

suitable for the vulnerable centralized environment, it perfectly works on the blockchain environment. The voting compatibility of both environments are identified in Table 4.9.

Table 4.9 voting compatibility comparison

Feature	Centralized System	Proposed System
Voting protection	Platforms can interrupt user votes	Voting scores are securely protected
Staking	People have to trust that the platforms honestly keep stakes and protect them securely	Staking is automatically and securely executed.

4.3 Robustness against fraudulent activities of a blockchain-based online review system

The scenarios constructed in Chapter 3 are executed under these conditions:

(1) The product or service price is 16.50 USD, which is the price of medium level hotels in Trip Advisor.

(2) The spam service fee is 1.65 USD per review according to a review spam service (from web https://ปั้มรีวิว.com/, 26 February 2021).

(3) The price of Ether at the time of experimenting is 144.47 USD.

(4) Since the 3 GWEI gas price is used in the previous work, this experiment uses the same value to avoid biasing.

(5) The Binance exchange platform is selected to demonstrate a fraudster strategy. A 0.0103 ETH (1.5 USD) fee ($C_{withdrawal}$) is required for Ether withdrawal.

(6) Product purchasing produces 198,607 units of gas (which is equivalent to 0.0286 USD) ($C_{tx\_purchase}$). Review posting consumes 50,216 units of gas (which is equivalent to 0.00725 USD) (C_{tx_review}).

4.3.1 Fake review spam robustness

We use 50 reviews to substitute equations in Chapter 3 to find the empirical results. The costs for fake review spamming in the scenarios are displayed in Table 4.10.

Table 4.10 Fake review spam cost

Environments	Sentiments	Cost (USD)
Expedia.com / Booking.com	Negative	907.5
Expedia.com / Booking.com	Positive	82.5
Proposed system	Negative	987.29
Proposed system	Positive	162.29

Costs required for fake positive review spamming in the proposed framework are significantly higher than the cost of fake positive review spamming in the current platforms (i.e., 1.9672 folds). As a consequence, fraudsters have to pay much more effort to manipulate their ranking in the proposed system.

In contrast, costs for fake negative review spamming in both systems are not much different (i.e., 1.0879 folds). However, the results are only applied to the platforms that require purchasing before posting a review (e.g., Booking.com, Expedia.com). Spammers can still spam fake negative reviews in review platforms (e.g., Yelp.com, Trip Advisor) without any cost. In addition, the fake negative review cost calculated in Table 4.10 is only applied with honest platforms. Dishonest platforms can allow fraudsters to bypass purchasing steps to generate fake reviews. Even though

such cases do not apparently occur, there is no guarantee that platforms will always be honest. Unlike the current platforms, the proposed framework ensures that the purchasing status is generated by real purchasing. Breaking the defined rules is almost impossible and requires much effort because of the characteristics of blockchain technology.

While the systems can protect against many spammed fake reviews, there might remain some amount of them posted to the system. Fake review detection is a necessary procedure to address suspect reviews. The proposed system can inherit all fake review detection methods used by current platforms. Fake review detection strategies used in Trip Advisor and Yelp are applied in the framework. Trip Advisor uses its tracking system to identify fake reviews. The tracking system utilizes huge datasets of reviews and user activities to create classification models. The models are claimed to be accurate in identifying unusual patterns of fraudsters. The pieces of information such as locations, device details, offensive language, or plagiarized content are gathered to keep track of misbehaviors. Yelp.com uses similar methods to detect fake reviews. The reviewers' behaviors such as the maximum number of reviews posted by an author, percentage of positive reviews, review length and review score deviation are analyzed on both platforms.

Many researchers proposed brilliant solutions for fake review detection. However, those methods are not utilized by current platforms. Fortunately, every fake review detection method can be implemented by any developers in the proposed framework. The most effective methods will be evaluated by the user community when people get benefits from those tools.

Beyond the previous solutions, the framework further provides important information to catch fraudsters. Transaction history is recorded and exposed publicly in a blockchain. Useful information can be derived from the transaction records. Behavioral analysis is much improved with transaction history information. The account transactions can be used to investigate suspect accounts. An account is suspect when:

(1) it does not have previous transactions or only a few of them.
(2) it contains only transactions about review posting.
(3) it does not conduct any transactions after posting a review.
(4) it has strong relations with suspicious accounts.
(5) it directly gets paid by a business that is reviewed by it.

The review grading tool and user community datasets can be implemented on top of the features. People can detect fake reviews faster and more accurately with these tools. The capability to detect fake reviews and fraudulent behaviors are compared between current platforms (i.e., Trip Advisor and Yelp.com) and the proposed framework in Table 4.11.

Table 4.11 Fake review detection comparison

Features	**Current platforms**	**Proposed framework**
Review content analysis	Available	Available
Reviewer behavior analysis	Available only review related behaviors	Available with review related behaviors and all transactions
Spammer group detection (account relations)	Available only with pattern checking	Available with pattern checking and transaction history
Multiple tool integration	N/A (Restricted to a platform)	Anyone can implement efficient tools and integrate with others
Transaction pattern detection	N/A	Natively available

The differences between reputation score forging robustness of the current platforms and the proposed framework are identified in Table 4.12.

Table 4.12 Fake review spam handling comparison

Features	Current platforms	Proposed framework
Transparency	N/A	By exposing every action behind the system
Flexibility	N/A	User community define terms “fake” and “undesirable” reviews
User-centric	N/A	Majority of users have the highest privilege in suspected review handling

In the proposed framework, the detected fake reviews are not immediately removed. The review grading tool just suggests the potential of fake reviews. Taking action is decided by users. With this approach, the fake review handling is more flexible than in the current platforms that utilize automatic filters. The framework is compatible with the majority of user opinions. For instance, when reviews posted of a hotel are suggested to be fake, but people accept them because the hotel manager makes a huge mistake. Those reviews will not be filtered until people forgive the hotel manager and vote for downgrading those reviews.

In addition, people can know the actual percentage of the filtered reviews in the proposed system. They can decide to stop using the system or continue improving system credibility. The proposed system relies on the user community in maintaining system credibility. The terms “fake” and “undesirable” reviews are defined by the user community. The proposed system serves user-centric fake review handling. Consequently, it is suitable for subjective fake review problems.

4.3.2 Reputation score forging robustness

According to reputation forging scenarios, spammers need various steps to forge a credible account. The differences of efforts needed in reputation forging procedures in both environments are compare in Table 4.13.

Table 4.13 Reputation forging efforts

Activities	Current platforms	Proposed framework
Email registration	✓	✗
Profile forging	✓	✓
Review posting	✓	✓
Money feeding	✗	✓
Product purchasing	✗	✓
Review posting	✗	✓
Helpful score giving	✓	✓

The current platforms do not need cost to forge a credible account. Spammers do not have to spend any costs the proposed system requires transaction costs for actions. However, the proposed system requires transaction costs for every on-chain action. As a result, spammers have to spend much more costs to produces fake credible accounts.

Most platforms do not protect reputation score forging. Anyone can create new accounts and give reputation scores to raise account credibility. Even worse, some platforms do not require logging in before giving a score to a review. Thus, the review reputation scores do not reflect the actual usefulness of a review. In the proposed framework, the review reputation score is designed to present the real usefulness of a review perceived by readers. Customers can give a reputation score only if they have purchased a product. The customers will be asked to give a helpful score to the most useful review presented on that product.

With the defined conditions, fraudsters have only one way to forge their reputation score. They have to purchase products and give themselves a reputation score. To reduce the cost, they can use the spam accounts that have already posted reviews to give reputation scores among those accounts. However, such a strategy reveals relationships among the spammer accounts. To conceal the account relationship, they have to increase product purchasing and minimize repeating the same pattern. Eventually, they will encounter a large cost for reputation score forging. Furthermore, they might waste their effort when the relationships among the accounts are revealed and pointed out by the user community. The differences between reputation score forging robustness of the current platforms and the proposed framework are displayed in Table 4.14.

Table 4.14 Reputation score forging robustness comparison

Features	Current platforms	Proposed framework
Protection	N/A	Requiring high cost, and exposing every action
Detection	N/A	Using transaction history to analyze account relations
Handling	N/A	User community judgment

4.3.3 Review content tampering robustness

In the centralized database ecosystem, the database owners can change and delete data in their database as they prefer. People have to trust the current platforms they are using today since there is no guarantee by the platform providers. Ideally, people can keep track of changing reviews in the current platforms. Even though people can acknowledge review tampering or deleting actions, they cannot immediately stop using dishonest platforms. People still need the huge

amounts of data available in the current platforms. As a result, users do not have a choice to opt-out of using services by dishonest platforms.

The proposed framework stores information in the blockchain storage. The attackers have to dominate more than half of the network hashing power. According to NiceHash (NiceHash Miner, 2021), the current total hash rate of the Ethereum network is 253 TH/s. An ASIC device with 190 MH/s hash power has a 2,940 USD price. The attackers need a minimum of 1,331,579 ASIC devices (3.9 billion USD) to initiate their hack. They have to run all devices to manipulate the incoming blocks. If they want to change the prior blocks, they have to forge and mine the target block and all blocks after it. The attackers need to occupy more hashing power and spend a longer time on the older blocks. A million ASIC devices consume extremely high electricity. An ASIC device produces 0.707 kWh. The standard electricity price is 0.127 USD per hour. Thus, the attackers have to pay 119,561.14 USD per hour to run all ASIC devices.

Tampering data on the blockchain layer produces extremely high costs. It is unworthy for attackers to waste their cost just for changing a review content. However, platforms that display blockchain review data can still change it on the presentation layer. With help of the content integrity checking tool, platforms that utilize review data in a blockchain can present their honesty. The best advantage of the proposed framework is that people can immediately stop using the service of dishonest platforms. Since all data are available in the blockchain, they have alternatives to choose platforms that honestly provide the service without concerns about data ownership. The differences between the current platforms' and the proposed framework's robustness against review content tampering are summarized in Table 4.15.

Table 4.15 Review content tampering robustness comparison

Features	Current platforms	Proposed framework
Protection	N/A (Need trust)	The immutable characteristic of a blockchain
Detection	By capturing snapshot of reviews presented in platform	Integrity checking tool (only require for tampering in the presentation layer)
Handling	N/A (Users do not have choices to find other platforms that provide the same information)	Users can immediately stop using dishonest service and find another service that consumes reviews from the blockchain

CHAPTER 5

DISCUSSIONS

5.1 Potential of a blockchain in online review systems

The experiment results implied the potential of a blockchain in online review applications. This subsection discusses findings and implications on a simple blockchain-based online review system.

5.1.1 Principles are needed for the blockchain-based online review system implementation

The blockchain-based online review system can keep review content permanently without changing. People can trace every movement on the storage layer. This can ensure that the posted review will not be edited by platform providers or hackers. Moreover, online reviews are publicly available. People can retrieve and utilize the data easier comparing to the current centralized platforms.

However, applying a blockchain to an online review system requires some principles to achieve the applicable system. Storing raw review content on the smart contract costs more than using IPFS about 2 folds. Additionally, using event emitting to store review content reduces about 10 folds of transaction cost compared

to using contract state. Even though using IPFS raises the response time and the uploading time, there are some solutions to maintain user experience. Platforms can provide a buffer server, which stores uploaded information before passing it to the destination. Users just wait for the uploading time of the centralized buffer server. As a result, the longer uploading and response times are the less important tradeoffs compared to the transaction cost issue. Knowing this limitation supports developers for further implementations.

5.1.2 The price volatility is the main concern for the usability of the system

The experiment results illustrated the empirical study of the blockchain-based online review system transaction cost. The most practical way to measure the expensiveness of a transaction cost is to convert it to be the real-world currency (fiat). At the time of experimenting, the cheapest transaction cost for review posting (stateless with IPFS contract) was 0.00453 USD. A user can post 220 reviews by paying 1 USD. The transaction cost is nevertheless varied by the Ether price, which can be much higher or lower than the illustrated numbers. The volatility is the most concern issue for the non-financial application of a blockchain.

5.1.3 The financial process should be included on the blockchain-based online review system

According to the unavoidable transaction cost, a blockchain-based online review system is not suitable for a simple system that only stores review data. Since the traditional online review systems do not require any cost for review posting, people do not have reason to use the more expensive system. As a result, a blockchain-based online review system should involve financial use cases, such as

booking, purchasing, and incentives. Blockchain technology natively supports financial applications, which may provide further benefits over the centralized online review systems. Applying the financial use cases to the system stimulates the market and generates a money supply. The available supply can be used to incentivize people. The larger number of supplies minimizes the transaction cost issue due to their huge differences. Moreover, on-chain purchasing information can be used to validate purchasing status and user experience in a product or a service. It is interesting to further explore the usability of a blockchain in online review systems with the obtained information.

5.2 Blockchain-based online review system features

After applying the financial use cases to the proposed system, many potential features over the traditional systems were found. This subsection discusses opportunities from the findings and some concerning issues.

5.2.1 Decentralization brings new form of online consumer review systems

Utilizing a blockchain in an online review system leads to the new form of electronic word-of-mouth (eWOM) (Karode, et al., 2020). While a central authority is eliminated, there are many benefits provided to users. Verification processes are automatically accomplished by the smart contract. The system provides correct validations without any bias. The global-scale and permanent database conduct real ownership of data and action history. Multiple platforms can display the same version of reviews by subscribing to data from the smart contract. Businesses do not need to recreate their ratings on different platforms. The subjective fake review problem is

managed by the majority of users who have the same experiences. This practice provides the fairest solution since real customers know the truth of products or services. Eliminating a central authority returns a huge cost to the market. The returned costs can be used to incentivize people for their contributions. The decentralized online review system minimizes costs for businesses' marketing. The businesses only pay for the user community when their products or services are purchased. Customers are encouraged to contribute to the system. The financial use cases such as transferring, and staking can be easily developed with the smart contract. More interestingly, the system can be seamlessly integrated with the other smart contracts. This feature leverages the abilities of the token-based reward system. People are more motivated by the reward system with more utilities. These are advantages of a blockchain-based online review system, which have not been proposed by previous literature or industrial reports.

5.2.2 Transaction costs and unfamiliar interfaces are likely to be concerning issues

According to emerging of Decentralized Finance (DeFi), people flock to the Ethereum blockchain. Transaction costs significantly increase due to the crowded network. People accept expensive transaction costs because of high returns from the DeFi investments. However, general propose applications, which do not focus on financial use cases, are impacted by high transaction costs. People are not willing to pay a high fee for posting a review. The transaction cost issue is being discussed and addressed by the blockchain community. Currently, there are proposed scalable blockchains, which aim to solve transaction cost and speed problems. Near protocol (Near protocol, 2021), Solana (Yakovenko, 2017), Polkadot (Wood, 2016), and Terra (Evan Kereiakes, et al., 2018). are examples of on-progress scalability blockchains. The Ethereum 2.0 is also being improved its scalability.

The target group of the online review applications is ordinary users. Most of them need some time to get familiar with new technologies. There are plenty of concepts people have to understand before using a blockchain application. They should realize how wallets work. Currently, an Ethereum wallet address is on a hexadecimal form, which is seen by ordinary users as a random text. People might take some time to understand the concept of public and private keys. However, those backgrounds are important because they might be at risk if their private keys are not securely kept. Like other new technologies, people have to spend time learning about them. There are a number of blockchain projects constantly launched today. Additionally, people are more involved in those platforms. Thus, this issue will be eventually solved when people are familiar with blockchain technology.

5.3 Robustness against fraudulent activities of a blockchain-based online review system

According to the scenario tests, the proposed system offers the higher level of robustness against fraudulent activities in online review systems. This subsection discusses findings from the research.

5.3.1 The proposed framework provides the better fake review management

The current platforms can ignore the purchasing steps. Some platforms do not even require purchases before posting reviews. On the other hand, the proposed system ensures that spammers pay some money to generate fake reviews. Requiring product purchasing disincentivizes fake review spamming. Thus, spammers encounter a high amount of cost to generate fake negative reviews. The cost for

generating fake positive reviews on the proposed system is much higher than on the current platforms due to the transaction costs. Spammers have to manage more processes to conceal their suspicious actions. The proposed system provides transaction history, which is a crucial clue to point out fraudulent activities. Since all actions are exposed publicly, people can help each other investigate fake reviews. Fraudsters have to be more cautious because of the higher intense inquisition from the user community. The proposed system provides more flexible management by relying on the user community. A suspicious review is handled only if the majority of users agree. The system environment is operated under the fairer judgment, which is executed by most customers. The overall system is controlled by the majority of users. They own a system together. As a result, it is their responsibility to maintain system credibility by helping each other to point out suspicious actions. Otherwise, they will not benefit from the system.

5.3.2 Reputation score forging is intensively managed by the proposed system

Apart from the fake review spamming problem, reputation score forging is a problem handled by the proposed framework. Fraudsters need various steps to build a credible fake account. Moreover, they have to purchase any products to unlock helpful scores and give them to the target account. The fraudsters are discouraged with the more steps and higher costs needed. Initializing a credible account is not only a difficult task but also maintaining it. The fake credible account can be pointed out by the user community any time when they reveal some clues. In their worst case, people will mistrust them and all related accounts. This means that they waste all costs to build their credibility and people lose trust towards that account. While the current platforms do not seriously manage this problem, the proposed system provides solutions. The pointed-out fake account and their cooperators can be listed on some third-party platforms (e.g., a blacklist platform). Moreover, people can vote to manage fake reviews posted by those accounts to maintain system credibility.

5.3.3 Review content tampering requires extremely high cost

The proposed system protects all information with blockchain technology. The smart contract allows review owners to manage their reviews. People cannot directly change or delete reviews of others. The only way to change the posted reviews is to attack the blockchain. However, tempting to change the recorded data on the blockchain requires an extremely high cost as demonstrated in the previous chapter. The attackers have to invest in a million mining devices. Moreover, operating all devices consumes a huge amount of electricity. It is not worth it for them to waste a huge amount of costs just for changing online review content. Consequently, people can consider online reviews on the blockchain-based online review system without concerning about the distorted data.

CHAPTER 6

CONCLUSIONS

6.1 Remarks and observations

In this work, the usability of a blockchain in the online tourism review application was explored. Potential features that cannot be achieved by centralized systems are discovered. The capability to address current platform problems is also examined. The findings provide insights into the blockchain-based online review system, which is possibly the new form of electronic word-of-mouth (eWOM).

The simple blockchain-based online review systems were implemented to determine the usability of a blockchain in the online review application. The experiment demonstrated the importance of blockchain development disciplines. The transaction cost is significantly reduced with data minimizing and state usage avoidance. Even though using IPFS causes a slower process, there are some solutions to keep well-user experiences. The transaction cost is the unavoidable tradeoff for blockchain applications. Thus, some valuable procedures should be included in the system. The incentive was introduced to compensate transaction costs and motivate proper contributions.

The decentralized online review system was implemented under guidelines from the first experiment and best practices from centralized review systems. Furthermore, the blockchain characteristics are applied to the proposed system. The implemented system replaces a central authority to be a smart contract. The smart contract automatically handles system interaction with the unbreakable

rules, which are publicly exposed. People can consider the rules before participating in the system. Users can consider reviews without concerning about biased management. Customers have to purchase a product before posting a review to a particular business. When there is a purchase, the smart contract keeps an amount of money to be a supply for incentivizing user contributions. The amount of deducted money can be flexibly adjected by the business owners. The system ensures that every review is written by customers who purchased a product. Moreover, all reviews are protected from suspicious tampering or deleting. Only review authors can manage their reviews and all of their versions are available publicly. When a customer gives a helpful score to a review, the review author gets a reward from the smart contract. This strategy motivates users to post a quality review instead of posting a useless review. The system provides a fairer fake review management, which relies on the majority of customers. We applied TCR voting, which uses stakes as voting scores. Losers cannot withdraw the stakes, and winners get those stakes as rewards. If the issuer wins voting, the target review is treated as an undesirable review. The most advantage of the blockchain-based online review system is the global storage. The same version of data can be utilized by many different platforms. Customers can focus on one trusted source of information. Businesses do not have any concern when they move to another platform because their ratings are globally available on the blockchain. More importantly, there can be many possible extended applications from third parties, who can develop a useful system that supports online marketing.

The traditional online review platforms were investigated under the decentralized online review ecosystem. This work focused on fake review spamming, reputation score forging, and review content tampering problems. The results indicated that the system can discourage fraudsters by requiring various processes to conduct those actions. They have to spend significantly more costly compared to the centralized platforms. The system provides more information to investigate fraudulent activities. Concurrently, the investigation can be more intense since every user can trace all activities on the system. Fake review detection methods used by traditional platforms can be applied to the proposed system. Furthermore, those methods can

be more efficient because of the important information, transaction history. The proposed framework provides the user-centric operation. People can flexibly manage fake reviews regarding the majority votes. As a result, the overall system is controlled by users, which is a fairer solution for the subjective fake review problem.

6.2 Contributions

To the best of our knowledge, the decentralized online review system is the first proposition based on blockchain technology. The guidelines of blockchain-based online review system implementation are useful for developers. The work points out the disadvantages of blockchain technology in the online review application and possible ways to handle them.

Potential features discovered in this work encourage adoptions of the tourism industry. While blockchain technology offers higher transparency and benefits, customers would move away from the untraceable systems. Businesses are motivated to be updated on technologies that can serve the highest benefits for them and their customers.

The analysis of system features and robustness against fraudulent activities identifies the effectiveness of the framework. This exposes opportunities for developers and platform providers to build such an ecosystem.

6.3 Limitations of the work

This work does not cover the following issues:

6.3.1 Implementing on new scalable blockchains. This work began with the Ethereum blockchain, which has problems with transaction cost and speed. We use the same environment throughout the project to keep the consistency of the results. In practice, using other new blockchains might provide better performances compared to this work. Moreover, there might be some development guidelines on the specific blockchains.

6.3.2 Testing with real users. All information related to traditional online review systems including their problems, guidelines, and previous methods has been collected from news, articles, and research. Thus, the proposed system is implemented by considering that information. The effectiveness of the system is implied from the gathered information. We have not tested the system with real users. The scope of this work is to discover potential features of the blockchain-based online review system.

6.3.3 Solving the fake review problem. This work does not guarantee to solve the fake review problem. The experiment result indicated that spammers have to spend much more effort to generate fake reviews. Moreover, the spammers encounter difficulties in concealing their actions under the transparent system. We use this information to implies that the number of fake reviews on the proposed system can be reduced. Additionally, the fake review management is implied to be fairer because it is decided by multiple parties instead of only one party as the current platforms.

6.4 Further works

This work can be extended for further research as following topics:

6.4.1 Finding a suitable blockchain for the online review application. Currently, many scalable blockchains are working, such as Near Protocol, Solana, Polkadot, Terra network, and many others. The novel blockchains focus on reducing transaction costs and speeding up the operation. Even though those blockchains produce an acceptable transaction cost for a while, there is no guarantee that they will not be affected by their token price. Thus, finding a suitable blockchain for non-financial application is an interesting topic.

6.4.2 Testing with real users. The best way to answer the effectiveness of the online review system is to execute it with real users. The real execution will provide information related to user trusts and their needs.

6.4.3 Upgradeable protocols. A smart contract is upgradeable with migrations. However, the migrations must be issued on the smart contract code. The fixed rules might not be suitable for the online review system, since people need to change all-time. The proposed system smart contract can be further implemented to compatible with migrations. People can vote to change some rules enforced by the smart contract.

BIBLIOGRAPHY

Ananthakrishnan, U. M., Li, B., and Smith, M. D. (2020). "A Tangled Web: Should Online Review Portals Display Fraudulent Reviews?" *Information Systems Research*, 31(3), 1-64.

Anatoly, Y. (2017). "Solana." (Online) Available on https://solana.com/solana-whitepaper.pdf (27 February 2021).

Asgaonkar, A., and Krishnamachari, B. (2018). "Token Curated Registries - A Game Theoretic Approach." *arXiv preprint arXiv:1809.01756*.

Asghar, M. Z., Ullah, A., Ahmad, S., and Khan, A. (2020). "Opinion spam detection framework using hybrid classification scheme." *Soft Computing*, 24(5), 3475–3498.

Australian Competition and Commission. (2013). "WHAT YOU NEED TO KNOW ABOUT: Online reviews—a guide for business and review platforms." (Online) Available on https://www.accc.gov.au/system/files/Online%20reviews%E2%80%94a%20guide%20for%20business%20and%20review%20platforms.pdf (27 February 2021).

Avilon. (2021). "Pump Review." (Online) Available https://ปั้มรีวิว.com/ (27 February 2021).

Banerjee, R., Feng, S., Kang, J. S., and Choi, Y. (2014). "Keystroke Patterns as Prosody in Digital Writings: A Case Study with Deceptive Reviews and Essays." *Proceeding of the 2014 Conference on Empirical Methods in Natural Language Processing (EMNLP)*, Association for Computational Linguistics, Doha, Qatar: 26-28 October, 2014.

Bhattacharya, A. (2017). "Trust no one: Reviews and ratings mean little to India's online shoppers." (Online) Available on https://qz.com/india/1136043/misinformation-and-fake-reviews-are-flooding-indian-e-commerce/ (26 February 2021).

Boonpeam, N., Werapun, W., and Karode, T. (2020). "Student Activity Credit Framework (PSUCOIN)." *Proceeding of the 5th International Conference on Information*

Technology (InCIT), Burapha University, Chonburi, Thailand: 21-22 October, 2020.

Buterin, V. (2015). "Ethereum White Paper." (Online) Available on https://ethereum.org/en/whitepaper/ (26 February 2021).

Chiriatti, G., Brunato, D., Dell'Orletta, F., and Venturi, G. (2019). "What Makes a Review Helpful? Predicting the Helpfulness of Italian TripAdvisor Reviews." *Proceeding of Italian Conference on Computational Linguistics,* Bari, Italy: 13-15 November, 2019.

CliveNicol. (2015). "Review censorship!" (Online) Available on https://www.tripadvisor.com/ShowTopic-g1-i12105-k8465871-o60-Review_censorship-Tripadvisor_Support.html (27 February 2021).

Community Specialist. (2019). "Why was my review removed?" (Online) Available on https://support.google.com/business/thread/1774636?hl=en (2 March 2021).

Consumer News and Business Channel. (2014). "TripAdvisor fined $600,000 for fake reviews." (Online) Available on https://www.cnbc.com/2014/12/23/tripadvisor-fined-600000-for-fake-reviews.html (11 January 2020).

Copperpot_uk. (2019). "TripAdvisor manipulating reviews?" (Online) Available on https://www.tripadvisor.com/ShowTopic-g1-i12105-k11664022-TripAdvisor_manipulating_reviews-Tripadvisor_Support.html (27 February 2021).

Dellarocas, C. (2006). "Strategic Manipulation of Internet Opinion Forums: Implications for Consumers and Firms." *Management Science*, 52(10), 1577–1593.

Duan, W., Gu, B., and Whinston, A. (2008). "The dynamics of online word-of-mouth and product sales—An empirical investigation of the movie industry." *Journal of Retailing*, 84(2), 233–242.

Evan, K., Do, K., Marco, D. M., and Nicholas, P. (2019). "Terra Money: Stability and Adoption" (Online) Available on https://terra.money/Terra_White_paper.pdf (2 March 2021)

Fang, B., Ye, Q., Kucukusta, D., and Law, R. (2016). "Analysis of the perceived value of online tourism reviews: Influence of readability and reviewer characteristics." *Tourism Management*, 52, 498–506.

Foamspace Corp. (2018). “FOAM Whitepaper” (Online) Available on https://foam.space /publicAssets/FOAM_Whitepaper.pdf (2 March 2021).

Gavin Wood. (2016). “Polkadot: Vision for a Heterogenous Multi-chain Framework” (Online) Available on https://polkadot.network/PolkaDotPaper.pdf (2 March 2021).

Harris, C. G. (2018). “Decomposing TripAdvisor: Detecting Potentially Fraudulent Hotel Reviews in the Era of Big Data.” *Proceeding of 2018 IEEE International Conference on Big Knowledge (ICBK)*, Nanyang Technological University, Singapore: 17-18 November, 2018.

Hassan, I., Azmi, M. N. L., and Abdullahi, A. M. (2020). “Evaluating the Spread of Fake News and its Detection. Techniques on Social Networking Sites.” *Romanian Journal of Communication and Public Relations*, 22(1), 115-125.

Ito, K., and Tanaka, H. (2019). “Token-Curated Registry with Citation Graph.” *Ledger*, 4(1), 1-16.

Juan, B. (2015). “IPFS - Content Addressed, Versioned, P2P File System.” (Online) Available on https://ipfs.io/ipfs/QmR7GSQM93Cx5eAg6a6yRzNde1FQv7u L6X1o 4k7zrJa3LX/ipfs.draft3.pdf (27 February 2021).

Karode, T., and Werapun, W. (2020). “Performance Analysis of Trustworthy Online Review System using Blockchain.” Proceeding of *the 17th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON 2020)*, Virtual Conference Hosted by College of Computing, Prince of Songkla University Phuket Campus, Thailand: 24-27 June, 2020.

Karode, T., Werapun, W., and Arpornthip, T. (2020). “Blockchain-based Global Travel Review Framework.” *International Journal of Advanced Computer Science and Applications*, 11(8), 90-99.

Kharrazi. (2020). “Sympathetic to review manipulation but deleting my negative.” (Online) Available on https://www.tripadvisor.co.nz/ShowTopic-g1-i12105-k12618778-Sympathetic_to_review_manipulation_but_deleting_my_negative-Tripadvisor_Support.html (28 February 2021).

Kosmarski, A., and Gordiychuk, N. (2020). “Token-curated registry in a scholarly journal: Can blockchain support journal communities?” *Learned Publishing*, 33(3), 333–339.

Lappas, T., Sabnis, G., and Valkanas, G. (2016). “The Impact of Fake Reviews on Online Visibility: A Vulnerability Assessment of the Hotel Industry.” *Information Systems Research*, 27(4), 940–961.

Lee, J., Park, D.-H., and Han, I. (2008). “The effect of negative online consumer reviews on product attitude: An information processing view.” *Electronic Commerce Research and Applications*, 7(3), 341–352.

Li, H., Chen, Z., Liu, B., Wei, X., and Shao, J. (2014). “Spotting Fake Reviews via Collective Positive-Unlabeled Learning.” *Proceeding of 2014 IEEE International Conference on Data Mining (ICDM)*, Shenzhen, China, 14-17 December, 2014.

Li, H., Fei, G., Wang, S., Liu, B., Shao, W., Mukherjee, A., and Shao, J. (2017). “Bimodal Distribution and Co-Bursting in Review Spam Detection.” *Proceeding of the 26th International Conference on World Wide Web*, International World Wide Web Conferences Steering Committee, Perth Australia: 3-7 May, 2017.

Li, J., Cardie, C., and Li, S. (2013). “TopicSpam: a Topic-Model based approach for spam detection.” *Proceedings of the 51st Annual Meeting of the Association for Computational Linguistics*, Sofia, Bulgaria: 4-9 August, 2013.

Li, J., Ott, M., Cardie, C., and Hovy, E. (2014). “Towards a General Rule for Identifying Deceptive Opinion Spam.” *Proceeding of the 52nd Annual Meeting of the Association for Computational Linguistics*, Association for Computational Linguistics, Baltimore, Maryland: 23-25 June, 2014.

Liang, X., Shetty, S., Tosh, D., Kamhoua, C., Kwiat, K., and Njilla, L. (2017). “ProvChain: A Blockchain-Based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability.” *Proceeding of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID)*, Madrid, Spain: 14-17 May, 2017.

LINA Network (2019). “(LINA) Blockchain Based Application for Innovation LINA Network.” (Online) Available on https://whitepaper.io/document/487/lina-whitepaper (28 February 2021).

Luca, M., and Zervas, G. (2016). “Fake It Till You Make It: Reputation, Competition, and Yelp Review Fraud.” *Management Science*, 62(12), 3412–3427.

Mayzlin, D., Dover, Y., and Chevalier, J. (2014). “Promotional Reviews: An Empirical Investigation of Online Review Manipulation.” *American Economic Review*, 104(8), 2421–2455.

Mike, G., Ameen, S., and James, Y. (2017). “The AdChain Registry.” (Online) Available on https://blockchain-x.eu/wp-content/uploads/2018/02/The_adChain_Registry_ENG.pdf (2 March 2021).

Monaro, M., Cannonito, E., Gamberini, L., and Sartori, G. (2020). “Spotting faked 5 stars ratings in E-Commerce using mouse dynamics.” *Computers in Human Behavior*, 109(1), 1-7.

Mukherjee, A., Venkataraman, V., Liu, B., and Glance, N. (2013). “What Yelp Fake Review Filter Might Be Doing?” *Proceedings of the 7th International Conference on Weblogs and Social Media (ICWSM),* Boston, USA: 8-11 July, 2013.

Nakamoto, S. (2008). “Bitcoin: A Peer-to-Peer Electronic Cash.” (Online) Available on https://bitcoin.org/bitcoin.pdf (27 February 2021).

Near Protocol. (2021), “Near protocol.” (Online) Available on https://near.org/papers/the-official-near-white-paper/ (28 February 2021).

Neisse, R., Steri, G., and Nai-Fovino, I. (2017). “A Blockchain-based Approach for Data Accountability and Provenance Tracking.” *Proceeding of the 12th International Conference on Availability, Reliability and Security (ARES)*, Reggio Calabria, Italy: 29 August - 1 September, 2017.

NiceHash (2021). “NiceHash Miner.” (Online) Available on https://www.nicehash.com/mining-hardware (2 March 2021).

Ocean Protocol Foundation. (2020). “Ocean Protocol: Tool for the Web3 Data Economy.” (Online) Available on https://oceanprotocol.com/tech- whitepaper.pdf (2 March 2021).

Önder, I., and Treiblmaier, H. (2018). “Blockchain and tourism: Three research propositions.” *Annals of Tourism Research*, 72(1), 180–182.

Orlikowski, W. J., and Scott, S. V. (2019). “Performing Apparatus: Infrastructures of Valuation in Hospitality.” *Research in the Sociology of Organizations*, 62(1), 169–179.

Ott, M., Choi, Y., Cardie, C., and Hancock, J. T. (2011). “Finding Deceptive Opinion Spam by Any Stretch of the Imagination.” *Proceeding of the 49th Annual Meeting of the Association for Computational Linguistics,* Portland, Oregoen: 19-24 June, 2011.

Park, S., and Nicolau, J. L. (2015). “Asymmetric effects of online consumer reviews.” *Annals of Tourism Research*, 50(1), 67-83.

Post Today. (2020). “Chan Isara is collecting evidence to catch netizens who spammed negative reviews #Ban Sri Panwa.” (Online) Available on https://www.posttoday .com/economy/news/633773 (26 February 2021).

Ramachandran, G. S., Radhakrishnan, R., and Krishnamachari, B. (2018). “Towards a Decentralized Data Marketplace for Smart Cities.” *Proceeding of 2018 IEEE International Smart Cities Conference (ISC2)*, Kansas City, MO, USA: 16-19 September, 2018.

Revain LLP. (2018). “Revain Full Whitepaper.” (Online) Available https://whitepaper.io/ document/107/revain-whitepaper (2 March 2021).

Roehrs, A., da Costa, C. A., da Rosa Righi, R., da Silva, V. F., Goldim, J. R., and Schmidt, D. C. (2019). “Analyzing the performance of a blockchain-based personal health record implementation.” *Journal of Biomedical Informatics*, 92(1), 1-9.

Stevens, J., Spaid, B., Breazeale, M., and Esmark-Jones, C. (2018). “Timeliness, transparency, and trust: A framework for managing online customer complaints.” *Business Horizons*, 61(3), 375-384.

Sussin, J., and Thompson, E. (2012). "*The Consequences of Fake Fans, 'Likes' and Reviews on Social Networks."* (Online) Available on https://www.gartner.com/ en/documents/2091515/the-consequences-of-fake-fans-likes-and-reviews-on-socia (2 March 2021).

Switch, T. M. (2017). “Dentacoin: The Blockchain Solution for the Global Dental Industry.” (Online) Available on https://dentacoin.com/assets/uploads/white paper.pdf (1 March 2021).

Vermeulen, I. E., and Seegers, D. (2009). “Tried and tested: The impact of online hotel reviews on consumer consideration.” *Tourism Management*, 30(1), 123–127.

Vinod, B. (2020). “Blockchain in travel.” *Journal of Revenue and Pricing Management*, 19(1), 2–6.

Wang, Y. L., and Krishnamachari, B. (2019). “Enhancing Engagement in Token-Curated Registries via an Inflationary Mechanism.” *Proceeding of 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, Seoul, Korea (South): 14-17 May, 2019.

Werapun, W., Arpornthip, T., Sangiamkul, E., Wetprasit, R., and Karode, T. (2020). “A Blockchain-based Renewable Energy Investment Management Platform: Decentralized Sustainable Development (DeSDev).” *Journal of Computer Science*, 16(11), 1657–1668.

Zhao, Y., Yang, S., Narayan, V., and Zhao, Y. (2013). “Modeling Consumer Learning from Online Product Reviews.” *Marketing Science*, 32(1), 153–169.

VITAE

Name Mr. Tanakorn Karode

Student ID 6230622001

Educational Attainment

Degree	Name of Institution	Year of Graduation
Bachelor of Engineering (Department of Computer Engineering)	Prince of Songkla University Phuket Campus	2018

Scholarship Awards during Enrolment

College of Computing Graduate Scholarship

List of Publication and Proceeding

N. Boonpeam, W. Werapun, T. Karode, "Student Activity Credit Framework (PSUCOIN)", The 5th International Conference on Information Technology: InCIT2020, 21-22 October 2020 (IEEE Library)

T. Karode, W. Werapun, T. Arporntip, "Blockchain-based Global Travel Review Framework", The International Journal of Advanced Computer Science and Applications (IJACSA), Volume 11, No 8, August 2020 (ISI / Scopus Index)

T. Karode, W. Werapun, "Performance Analysis of Trustworthy Online Review System using Blockchain", The 17th International Conference on Electrical Engineering/ Electronics, Computer, Telecommunications and Information Technology (ECTI-CON 2020), 24-27 June 2020

W. Werapun, T. Arpornthip, E. Sangiamkul, R. Wetprasit, and T. Karode, (2020). A Blockchain-based Renewable Energy Investment Management Platform: Decentralized Sustainable Development (DeSDev). Journal of Computer Science, 16(11), 1657-1668. https://doi.org/10.3844/jcssp.2020.1657.1668