Summer 2024

Leveraging Blockchain for Trust Enhancement in Decentralized Marketplaces: A Reputation System Perspective

Meshari Mohammd Aljohani
Old Dominion University

LEVERAGING BLOCKCHAIN FOR TRUST ENHANCEMENT IN DECENTRALIZED MARKETPLACES: A REPUTATION SYSTEM PERSPECTIVE

by

Meshari Mohammd Aljohani
B.S. May 2003, Teachers College, Jeddah, Saudi Arabia
M.S. May 2013, California Lutheran University

A Dissertation Submitted to the Faculty of
Old Dominion University in Partial Fulfillment of the
Requirements for the Degree of

DOCTOR OF PHILOSOPHY

COMPUTER SCIENCE

OLD DOMINION UNIVERSITY
August 2024

Approved by:

Stephan Olariu (Co-Director)

Ravi Mukkamala (Co-Director)

Shuai Hao (Member)

Sachin Shetty (Member)

ABSTRACT

LEVERAGING BLOCKCHAIN FOR TRUST ENHANCEMENT IN DECENTRALIZED MARKETPLACES: A REPUTATION SYSTEM PERSPECTIVE

Meshari Mohammd Aljohani
Old Dominion University, 2024
Co-Directors: Dr. Stephan Olariu
Dr. Ravi Mukkamala

Centralized marketplaces provide reliable reputation services through a central authority, but this raises concerns about single points of failure, user privacy, and data security. Decentralized marketplaces have emerged to address these issues by enhancing user privacy and transparency and eliminating single points of failure. However, decentralized marketplaces face the challenge of maintaining user trust without a centralized authority. Current blockchain-based marketplaces rely on subjective buyer feedback. Additionally, the transparency in these systems can deter honest reviews due to fear of seller retaliation. To address these issues, we propose a trust and reputation system using blockchain and smart contracts. Our system replaces unreliable buyer feedback with objective transaction assessments. Performance challenges of blockchain-based systems are tackled through three innovative schemes, resulting in a substantial improvement over the baseline approach. Furthermore, we proposed a decentralized marketplace utilizing blockchain-based smart contracts to address privacy concerns in buyer reviews that arise from the transparency of decentralized marketplaces. This enables buyers to use one-time identities for reviews to promote anonymity. This system ensures that buyers provide reviews by requiring a review fee, which is fully refunded after the review is submitted. Moreover, we proposed a trust and reputation service based on Laplace's Law of Succession, where trust in a seller is defined as the subjective probability that they will fulfill their contractual obligations in the next transaction. This method

accommodates multi-segment marketplaces and time-varying seller performance, predicts trust and reputation far into the future, and discounts older reputation scores. In addition, we propose SmartReview, an automated review system utilizing blockchain smart contracts to generate objective, bias-free reviews. The review module is designed as a smart contract that takes the contract terms and the evidence provided by the buyer and seller as inputs. It employs advanced computer vision and machine learning techniques to produce quantitative and qualitative reviews for each transaction, ensuring objectivity and eliminating reviewer bias. Lastly, we introduce a structured blockchain architecture featuring a layered approach. This architecture includes mechanisms for secure transaction recording and efficient query retrieval through auxiliary indexing, demonstrating significant advancements in decentralized data management.

In the name of God, the most gracious, the most merciful

I dedicate my dissertation first and foremost to my parents, my role models in life, the primary contributors to achieving this accomplishment through their support and encouragement of my education. Their boundless love and sacrifices have shaped who I am today.

To my dearest wife, Abrar Alali, who has been my devoted partner and my greatest supporter. Your patience and understanding have made it possible for me to pursue my dreams although you were busy with your PhD. This journey would have been much harder without your constant encouragement and endless love. Thank you for being my companion, my confidante, and my love. This achievement is as much yours as it is mine.

To my sons, Mohammed and Abdulrahman, who bring endless joy and inspiration into my life. Watching you grow and explore the world with curious eyes motivates me every day to be the best I can be. I hope this dissertation not only makes you proud but also inspires you to chase your dreams, no matter the challenges you might face. And, to my twin sons, Ziad and Moath, your laughter and playfulness fill our home with happiness. You remind me of the pure joy of life and the importance of balancing dedication with fun. This dedication is a promise to you both that every moment spent away, working on this dissertation, was to build a better future for you.

To my brothers and sisters, thank you for your endless support and encouragement. Our shared memories and experiences have provided a foundation of strength and companionship that I have leaned on throughout my academic journey, and I am immensely grateful for it.

To everyone who offered prayers, support, and well-wishes throughout my journey, I extend my heartfelt thanks to each of you.

ACKNOWLEDGMENTS

In the name of Allah, the Most Gracious, the Most Merciful. All praise and thanks are due to Allah, the Almighty God, for granting me the strength, patience, and knowledge to complete this dissertation. Without His guidance and blessings, this achievement would not have been possible.

Then, I want to express my heartfelt gratitude to my advisor, Dr. Stephan Olariu. His constant support, insightful guidance, and immense expertise have been essential in completing this work. Dr. Olariu's dedication to excellence and his encouragement during tough times have had a profound impact on my academic journey. His constructive feedback and patience have helped shape this dissertation, and for that, I am forever grateful.

I am also deeply grateful to my co-advisor, Dr. Ravi Mukkamala. His deep knowledge and expertise have greatly enriched this work. Dr. Mukkamala's continuous encouragement, detailed reviews, and thoughtful advice have been a source of inspiration and have significantly contributed to the quality of this research. His mentorship has been incredibly valuable.

I would also like to extend my sincere gratitude to my committee members Dr. Shuai Hao and Dr. Sachin Shetty for their invaluable feedback and contributions. Their perspectives and advice have greatly enhanced the quality of this research. I appreciate their time, effort, and dedication in reviewing my work and providing constructive criticism, which has been helpful in refining this dissertation.

TABLE OF CONTENTS

Page

LIST OF TABLES

LIST OF FIGURES

Figure Page

Figure Page

CHAPTER 1

INTRODUCTION

Retail e-commerce sales have seen tremendous growth since COVID-19. According to the U.S. Department of Commerce, total U.S. e-commerce sales for 2023 were estimated at $1.1 trillion, an increase of 7.6 percent from 2022 [74]. Popular online shopping sites include Amazon.com, eBay.com, Alibaba.com, and Overstock.com. Similarly, several online review sites such as Yelp.com, Tripadvisor.com, and BBB.com provide platforms for existing customers to rate businesses, helping potential customers make informed decisions.

In global markets, buyers and sellers often engage in transactions with little or no prior interaction. This introduces significant risks for both parties. To mitigate these risks, marketplaces maintain individual reputation scores for each seller (and sometimes buyer) [43], [70], [89], [96]. These scores capture statistical information about the past behavior of users registered with the platform.

The goal of a trust and reputation service is to provide buyers with a robust framework that allows them to select transaction partners based on a combination of objective and subjective trust measures distilled from accumulated evidence of past behavior in the marketplace. The quality of a trust and reputation service fundamentally depends on the quality of the feedback it receives from buyers.

Most existing reputation systems are centralized, making them prone to data tampering, lack of transparency, single points of failure, and potentially high fees for their services. Additionally, users may find it difficult to verify the basis of a rating or the legitimacy of the customers who

provided it. There is clear evidence in the literature showing the prevalence of false reputations in online markets ([103]).

Moreover, reputation systems typically do not focus on the privacy of reviewers. When buyers provide feedback on a purchase, their identities are often exposed, which can lead to several issues. For instance, sellers could discriminate against buyers based on their reviews. On eBay, a user who posted a negative review reported that the seller threatened them and vowed to have the feedback removed [3]. Identity revelation may also influence sellers' behavior in future transactions, leading them to provide better service to buyers who give positive feedback and worse service to those who leave negative reviews [21]. As demonstrated in [77], buyer feedback affects seller behavior; positive buyer feedback correlates with positive future seller behavior 99.8% of the time, while neutral or negative feedback correlates with positive seller behavior only 39.3% of the time.

Due to these issues, decentralized marketplaces are becoming more attractive ([9]). Blockchain technologies can provide the desired transparency and tamper-proof evidence for reputation system users ([9], [15], [44], [53]). Blockchain-based reputation systems can guarantee the immutability of stored historical reviews and help with reputation verifiability issues, eliminating the need for a single controlling authority. In these systems, the marketplace authority provides infrastructure for transactions without direct intervention or control.

1.1 MOTIVATION

Current decentralized marketplaces still rely on buyers' subjective feedback. Being a subjective measure, the quality of buyer feedback is notoriously hard to assess [39], [86], [94]. The fundamental problem is that different buyers may rate similar experiences with the same seller vastly differently. When feedback is provided by buyers from around the world, who may value

different aspects of the same transaction differently, it is very hard to know if a buyer provides truthful feedback.

Moreover, several issues persist in current reputation systems: Lack of finer granularity in reputation scores: A single reputation score per seller is often inadequate. For example, a seller may perform well in the low-price range but not in the high-price range. Reputation score not being current: Scores are not frequently updated, leading to outdated information. Poor performance: Accessing reputation scores quickly is often challenging. Lack of verifiability: Customers cannot validate the legitimacy of a reputation score [31], [32], [35], [48], [101].

In addition, several researchers have suggested decentralized review systems that prioritize user privacy and reviewer anonymity. Bazin et al. [12] and Li et al. [48] proposed decentralized review systems using blind signatures to ensure reviewer anonymity. In their systems, a seller needs to send consent through a signature for a buyer to provide feedback. If the seller refuses to cooperate, the buyer cannot provide feedback. Additionally, the transaction and feedback processes are disjoint, meaning that even if a buyer decides not to complete a transaction, they can still provide a review once they obtain the seller's signature. These systems, however, still require a trusted third party to generate system parameters, cryptographic keys for users, and digital certificates. The trusted third party itself could become a single point of failure or a source of centralized control.

Sosoka et al. [89] proposed a different solution for managing reviewer anonymity in decentralized marketplaces. Here, users' reviews are linked to transactions using non-interactive zero-knowledge proofs and linkable ring signatures to protect their anonymity. To prevent Sybil attacks, the system charges reviewers a fee. However, imposing new fees may discourage consumers from providing feedback. These proposed systems use primitive cryptographic methods, which increase the complexity of the systems.

Moreover, the current blockchain structure's low efficiency in retrieving sellers' reputation scores is problematic due to the necessity of visiting all blocks in the blockchain.

Recognizing these gaps, a comprehensive smart contract-based decentralized marketplace system that manages buyer reviews and seller reputation is still required to accurately assess and reflect the trustworthiness of marketplace participants. Such a system should not only be immune to common threats but also scalable, efficient, and adaptable to changes in market conditions. Addressing these requirements enhances user confidence in decentralized marketplaces, leading to greater adoption and a more secure and efficient digital economy.

1.2 RESEARCH QUESTION

We identify the challenges and limitations of the current decentralized marketplaces and reputation systems. Therefore, our goal is to address the following question: Can blockchain and smart contracts (SCs), which are "digital contracts stored on a blockchain that are automatically executed when predetermined terms and conditions are met," [99] be used to build a strong, efficient, and secure reputation system in decentralized marketplaces? This question addresses the fundamental issue of trust in decentralized environments and aims to investigate novel solutions. To answer this question, we have to answer the following questions:

RQ1: How do blockchain-based SCs enhance the reliability and efficiency of feedback mechanisms in transaction systems in different marketplaces?

RQ2: What are the impacts of specialized data structures on the scalability and efficiency of computing and retrieving reputation scores within blockchain-based systems?

RQ3: How do SCs use multiple identities to promote reviewer anonymity in decentralized market-

places, and what impact does this anonymity have on the quality of feedback?

RQ4: How do SCs within blockchain-based trust and reputation services specifically address and improve quality in buyer feedback in decentralized marketplaces, and what impact does this have on transaction reliability?

RQ5: How does an SC-based review system address the shortcomings of traditional buyer-sourced reviews in marketplaces?

RQ6: How can a structured blockchain architecture optimize data integrity, security, efficiency, and query retrieval across various applications

1.3 DISSERTATION OUTLINE

The rest of this dissertation is organized as follows:

- **Chapter 2**: We introduce the background.
- **Chapter 3**: We provide related work.
- **Chapter 4**: We introduce three schemes to manage reputation scores in a blockchain-based decentralized marketplace.
- **Chapter 5**: We design an SC-based decentralized marketplace system to promote reviewer anonymity.
- **Chapter 6**: We design a blockchain-based trust and reputation service to address uncertainties in buyer feedback for decentralized marketplaces.

- **Chapter 7**: We design SmartReview, an automated system that uses blockchain and SCs to evaluate transactions automatically.

- **Chapter 8**: We develop an innovative blockchain architecture that improves data integrity, security, and efficient query retrieval across various applications.

CHAPTER 2

BACKGROUND

This chapter offers a concise overview of the fundamental concepts relevant to this dissertation.

2.1 ONLINE MARKETPLACES

An online marketplace, also known as an online e-commerce marketplace, is a form of e-commerce site that aggregates product or service details from multiple third-party sellers [100]. Serving as a key example of multichannel e-commerce, online marketplaces, henceforth referred to simply as "marketplaces," facilitate a more efficient production process. Within these platforms, the marketplace operator handles the processing of consumer transactions, while the delivery and fulfillment duties are performed by participating retailers or wholesalers. These websites allow users to register and offer products ranging from single items to multiple items, typically charging a post-sale fee.

2.1.1 Centralized Marketplaces

Centralized marketplaces are digital platforms in which a single authority controls transaction processing, data management, and rule enforcement [10]. This single authority oversees all important marketplace functions, such as participant entry and exit, transaction security, and dispute resolution. The structure of centralized markets ensures that all data is stored and processed by a single node, which maintains order and trust within the platform. This structure not only offers a

more streamlined user experience and strong security constraints but also centralizes data, increasing exposure to data breaches and reducing user control over personal information.

2.1.2 Decentralized Marketplaces

Decentralized marketplaces are digital platforms that use a distributed network architecture, often powered by blockchain technology. Unlike traditional marketplaces, that rely on a single authority to conduct transactions, enforce regulations, and ensure data integrity, decentralized marketplaces divide these tasks among all network participants (Avyukt, 2021). This structure eliminates the need for a central governing body, putting power and authority in the hands of the users themselves. Each network participant serves as a node, ensuring data integrity, security, and redundancy in transaction processing.

2.2 BLOCKCHAIN TECHNOLOGY

Blockchain technology is essentially a distributed ledger system. It records transactions across a network of computers, making sure that each transaction is recorded safely and permanently. This is achieved by using a decentralized structure that is completely different from standard centralized databases. Each block on the blockchain has a record of several transactions, and each new transaction is added to the ledger of each network participant [55].

The fundamental qualities of the blockchain, such as decentralization, immutability, and transparency, are critical to addressing trust and security concerns. Blockchain not only provides a secure and transparent environment for transactions but also ensures that these transactions are not under the control of a single party, reducing the risks associated with centralized systems [97].

The decentralized nature of the blockchain is critical to its security and flexibility. Changing

any record on a blockchain requires unanimity across the entire network, making data tampering and fraud extremely difficult. This feature identifies the blockchain as a great option for applications that require a permanent, secure, and accessible record keeping mechanism.

Although blockchain is well known for its role in powering cryptocurrencies such as Bitcoin, its potential uses are widespread. In decentralized marketplaces, the blockchain can provide an immutable and transparent record of transactions, which is critical for participant confidence.

2.3 SMART CONTRACT

Smart contracts (SCs) are self-executing contracts that have the conditions of the agreement stated in the code [55]. These contracts, hosted on blockchain platforms, are automatically triggered when predetermined criteria are met, removing the need for intermediaries.

SCs play an important role in this ecosystem. These self-executing contracts, with the terms of the agreement directly written in code, run on the blockchain network. They automate and enforce transaction rules, which is especially useful in decentralized marketplaces without traditional enforcement methods. By incorporating SCs, blockchain-based systems can efficiently handle reputation scores and transactional agreements without the need for a central authority. This integration greatly improves the integrity and dependability of reputation data by ensuring that transactional feedback and ratings are accurately captured and tamper-proof [54], [55], [62].

SCs in decentralized markets automate a wide range of transactional activities, including payment processing and term enforcement. They can also be programmed to manage reputation systems by updating scores based on transaction results, resulting in a fair and transparent system.

2.4 TRUST IN MARKETPLACES

In online marketplaces, trust is fundamental to the success of these marketplaces as it builds confidence in the buyers to transact with the sellers. In this work, it is usually derived from the accumulated evidence of the seller's past behavior in the marketplace. In this work, trust in a seller is defined as the probability that she will fulfill her obligations in the next transaction. The quality of such a trust and reputation system depends on the quality of feedback provided by buyers.

2.5 REPUTATION IN MARKETPLACES

In order to assist buyers and sellers with the process of choosing a trustworthy trading partner, the marketplace maintains, in a decentralized fashion, individual reputation scores for each buyer and seller registered with the platform. These reputation scores capture, in various forms, statistical information about the past behavior of buyers and sellers. The reputation score in the marketplaces is the number of successful transactions versus the total number of transactions for each participant.

CHAPTER 3

RELATED WORK

The development of blockchain technology has brought about significant changes in digital marketplaces, leading to the emergence of decentralized platforms. An assessment of traditional reputation systems in these emerging decentralized environments is necessary for this change. Decentralized reputation systems are essential when transactions move away from centralized platforms, where trust is usually established through the platform itself. These systems, which play a vital role in maintaining trust, integrity, and security in peer-to-peer transactions without a central governing authority, must adapt to the decentralized nature of blockchain technology. While traditional reputation systems have demonstrated their effectiveness in controlled situations, their application in decentralized marketplaces faces additional obstacles. The blockchain's transparent and unchangeable ledger provides a unique solution to these issues. However, it also presents several challenges and concerns when it comes to creating reputation systems that can promote trust among users in this emerging digital domain.

This chapter explores the existing research and literature on Reputation Systems, Blockchain-based Decentralized Marketplace, and Decentralized Reputation Systems.

3.1 REPUTATION SYSTEMS

The authors in [38] described a unique reputation system that combines topic modeling with Latent Dirichlet Allocation (LDA) for topic modeling, criteria-based weights utilizing typed dependency relation representation, and reputation ratings computed using Bayesian approaches. Their

approach aggregates weighted criteria-based evaluations from user reviews to determine reputation scores by mining reviews written in Hindi. With a more sophisticated reputation ranking provided by this method, merchants with comparable high feedback scores can be distinguished from one another. The system has drawbacks despite its advances, such as the possibility of difficulties in precisely parsing and comprehending the semantic subtleties of user-generated content in Hindi, a language with intricate syntax and a wealth of morphological traits. Furthermore, the system's reliance on human preprocessing of reviews to ensure translation correctness and eliminate special characters may prevent it from scaling or being applicable in real-time. The paper notes that extrapolating results from one language or domain to another is challenging, and it recommends more research to expand the system's application in multi-language review mining and other online transaction domains.

The authors in [29] suggested a reputation system for marketplaces based on pairwise comparison to address concerns like the subjectivity of ratings, inequality of transactions, multi-context reputation, and dynamic user behavior. They introduced a model in which the context, value, and pricing fairness of each transaction are taken into account, and each transaction is linked to a score differential. The objective of this approach is to enhance the accuracy of users' reputations by reducing biases and accounting for context and transaction value. The algorithm uses temporal weighting to make sure recent transactions have a higher influence on reputation scores to take into account users' dynamic behavior. Multi-agent simulations with real-world data are used to evaluate the approach, demonstrating its potential to outperform conventional numerical rating-based systems. One problem with the suggested reputation system is that it might be hard to set up and keep up with a pairwise comparison model, especially in marketplaces with millions of transactions. Because the model depends on correctly classifying transactions and making changes

for context and fairness, it might be hard to make sure that all evaluations are consistent and fair. Also, because marketplace behaviors change all the time and the system relies on recent transaction weighting, it might not fully reflect how trustworthy users are in the long run.

3.2 BLOCKCHAIN-BASED DECENTRALIZED MARKETPLACE

Prasad et al.[75] suggested a decentralized marketplace application utilizing the Ethereum blockchain. Their primary objective is to eliminate centralized control and prevent owners of central marketplaces from rejecting users and charging excessive fees. The authors claim that, when compared to eBay and other marketplaces, their system may offer increased earnings for sellers.

Shakila and Sultana [82] have also proposed a decentralized marketplace prototype built on Ethereum SCs. They attempt to solve problems including listing fees, centralized power, user data ownership, and user privacy. They employed Solidity and the Truffle framework to develop their application.

3.3 DECENTRALIZED REPUTATION SYSTEM

In [56], the authors introduced a revolutionary dynamic, decentralized reputation system created for settings like wireless sensor networks (WSNs) and mobile ad hoc networks (MANETs). Due to their need to rely on a central authority, traditional reputation systems fail in such decentralized situations. The suggested method, however, gets around this problem by utilizing secure multiparty computation (SMC) and blockchain technology. The technology ensures privacy even in the presence of dishonest parties and enables all nodes to participate in both providing and receiving evaluations. The reputation system combines SMC methods with blockchain technology to keep individual ratings private while making the aggregated reputation scores available to the

public. Without a centralized authority, this system makes it possible to preserve information on reputation. Any network participant is able to rate and be rated; hence, the system is flexible and not just applicable in situations where there is a buyer and a seller or a provider and a customer. With an off-chain phase, it also lowers storage and computes costs. The system's SMC component enables participants to jointly compute a function over their private inputs without disclosing them. Each party can compute a value according to a correctness and privacy protocol without providing any information about their input other than the outcome. The proposed system is structured in three phases: join, rate, and update. Each participant submits a joint transaction at first, and when it is validated, they are each assigned to a subgroup. The majority of the reputation calculation takes place during the subsequent step. To jointly calculate a reputation rating without disclosing individual inputs, each subgroup uses the SMC protocol. In the last stage, miners carry out the rate transaction and update the final reputation score on the blockchain, making it accessible to everyone. However, the system does have several drawbacks and challenging areas. The system is secure when parties follow the protocol but allows for the possibility that they might attempt to glean additional information from its execution in a semi-honest adversarial paradigm. It might not work as effectively under other adversarial models, such as a malicious adversarial model where participants are free to arbitrarily break from the protocol.

In [51] introduced VRepChain, a reputation system for the Social Internet of Vehicles (SIoV) that uses blockchain technology to overcome rating privacy concerns. Ratings, which are used to evaluate the integrity of the entities within SIoV, may reveal personal information about users, including their activity and location, demanding security measures. Blockchain technology is used by VRepChain to protect rating privacy during transmission and storage. By employing the homomorphic encryption algorithm, they are able to maintain the privacy of the evaluations.

In their system, each vehicle (or entity) in their system model has a communication device and an onboard identification device (OBID) for managing traffic and facilitating social communication. In a peer-to-peer network, Road Side Units (RSUs), which have both public and private keys, facilitate communication and keep track of ratings and blocks. In the system, a vehicle that is moving can connect online with other moving vehicles on its friend list and share information with them, such as a report of an accident at a specific location. These communications, which only contain a small amount of sensitive information, are encrypted for transfer using the recipient's public key. Vehicles can also openly broadcast a message to other roadside devices nearby without encryption. This makes it possible for the RSUs to communicate with incoming vehicles. A vehicle may evaluate a message's validity based on its truthfulness and helpful accuracy after receiving it. These evaluations, or ratings, are considered for extra privacy protections since they involve more sensitive data. The ratings are protected by encryption using the rating provider's public key in order to guarantee this. The RSUs securely gather and aggregate ratings. Using the recipient's public key, the communication between RSUs and vehicles is encrypted, protecting the reputation values from eavesdropping. Upon request from another vehicle "i," a reliable RSU uses the following procedure to determine the reputation of a vehicle "t": The RSU obtains 't' ratings that have been encrypted from the blockchain. The rating provider and reliable vehicles are then sent encrypted random values relating to each rating that was generated by the system. The rating provider determines a value that has been weighted. In order to deliver the values back to the RSU in an encrypted form, the rating provider sums up the received values. The values received from the RSU are summed together and encrypted. The RSU computes the reputation value, decrypts the total values, and sends them to the querying vehicle.

REPUTABLE [8], is a decentralized reputation system built on blockchain technology, is in-

troduced in this paper. With the help of this system, users and service providers in ecosystems built around blockchain technology can engage in trustworthy ways. In order to protect user privacy and reputation values and to keep overhead to a minimum, REPUTABLE use of both on-chain and off-chain components. The main elements of REPUTABLE include token generation, user engagement, reputation calculation, a dashboard, and on-chain and off-chain storage. Token generation, which serves as an indicator of a user's eligibility to offer feedback, is a critical component of REPUTABLE. Tokens are issued by the seller against each legitimate transaction. Although they identify it as a potential area for future improvement, the authors acknowledge that this method may be vulnerable to collusion assaults. Allowing users to hide their ratings using cryptograms—encrypted feedback values with user-generated encryption keys—improves user engagement and NIZk proofs. This approach enhances privacy and avoids any centralized authority collusion. The component that calculates reputation combines each user's feedback to determine the seller's reputation. To calculate the final aggregated reputation of corporate entities or sellers, a beta reputation system is employed. Consumers and other interested parties can query reputation scores using the dashboard component's interface. They aim to build this service off-chain, possibly using the cloud services and offering a web-based endpoint and configurable interface. With regards to storage, REPUTABLE makes use of blockchain for on-chain storage, which offers reputation data end-to-end decentralization and tamper-proof storage, boosting the reliability and verifiability of the reputation data. Both the aggregate reputation ratings and the feedback from specific users are stored on-chain with the reputation data. To increase scalability and establish a specialized security layer for securing access to REPUTABLE interfaces, raw user feedback is stored off-chain. An oracle, which is the Reputation Data Oracle Service (RDOS), is used for efficient communication and linking between on-chain and off-chain storage. Following the rep-

utation model, RDOS controls the process of interacting with consumers to collect feedback and produce encrypted feedback data.

Dimitriou [23] proposed a blockchain-based decentralized reputation system to protect users' anonymity. To maintain unlinkability, users can employ as many pseudonyms as they like, and they can aggregate reputation among these identities. However, to maintain the uniqueness of user identities and the trustworthiness of reputation, user registration relies on a Registrar, which can be a single server or a decentralized group of nodes.

Li et al.[48] also proposed a reputation system for e-commerce applications based on the Ethereum blockchain. They create anonymous credentials using zero-knowledge proofs (ZKPs) and two-step blind signatures. They demonstrate that their system can detect and isolate aberrant rating attacks. Their approach satisfies requirements for rating privacy, identity privacy, and unlinkability. In this system, users are registered and given IDs by a single certification authority (CA).

The paper [95] described a blockchain-based and InterPlanetary File system (IPFS)-based decentralized publication system for open science. The proposed approach aims to make communications easier throughout the peer review process, from the submission of a manuscript to its acceptance or rejection. Additionally, it encourages peer review ratings, creating a network of reviewers. They utilize the IPFS and the Ethereum blockchain in the system. In order to keep track of system interactions, SCs are used along with the Ethereum blockchain, which operates as a public, decentralized ledger. IPFS is used as a distributed file system to store the content of the peer review process, ensuring that the data registered on the platform is persistent, free, accessible, and independent of a centralized server. Their system works as follows: In order to submit a paper, you must first upload it to the IPFS network, get its unique IPFS address, and then make an Ethereum

SC using the addresses of the paper's authors. Then, this SC generates a unique Ethereum address for the paper and records it on the blockchain, proving that the authors submitted it. The system also allows for a situation where a journal editor requests a reviewer for a particular paper, thereby creating review tasks in the SC for that paper. The transaction stores the reviewer's Ethereum address and, if chosen, the deadline for submitting the review. The decision of the invited reviewer to accept or refuse the review task is stored on the blockchain as well. When submitting a review, the reviewer creates a transaction that includes the detailed review's IPFS address, acceptance or rejection, and other information. A penalty is applied to the reviewer's system reputation if a review is submitted after the due date. The reputation system also enables ratings for reviews. The addresses of the rated review and reviewer, as well as the sender's address and rating, are all recorded in the blockchain transaction. However, there are various problems with this suggestion. Privacy risk is the most important problem since peer review is open and public and does not protect reviewers' identities. Furthermore, under such a system, problems like bias, rivalry, or retaliation present serious difficulties. Finally, the system doesn't manage different levels of openness and copyright regimes.

[24] introduced new, locally perceived behavioral reputation parameters designed for a distributed evaluation of a vehicle's reputation in the Internet of Vehicles (IoV) network. With a focus on protecting against Sybil and Denial of Service attacks in the context of Vehicular ad-hoc networks (VANET), these parameters attempt to remove malicious or unreliable vehicles from the network. These features are part of a reputation management system that works fully decentralized without the need for a centralized authority. The paper also presents a decentralized reputation management framework intended to protect VANETs from the risks caused by malicious nodes. Based on the behaviors of the vehicles, it offers parameters such as vehicle identity, size, direc-

tion, location, speed, acceleration, transmission range, and transmission frequency for determining locally perceived reputation and reliability, which are then integrated into a distributed reputation system. There are two phases to the system architecture. In the discovery phase, beacon packets are sent to scan the network and test the initial credibility of the data released by the visiting node. The system verifies data correctness and provides reputation scores after analyzing each parameter throughout the verification phase. If the total result is helpful, the node is considered trustworthy and permitted to communicate with other nodes in the network. To ensure that the values produced by a vehicle are reasonable and compatible with expectations, a set of restrictions is created for each parameter used in the calculation of these ratings. These restrictions are employed to identify a variety of malicious actions, such as DoS attacks and the injection of fake data. Additionally, each host node keeps track of the nodes it has interacted with, along with information like their reputation scores and other details. In subsequent interactions, this information is utilized to decide whether or not to trust a node. Nodes with a poor reputation are excluded from the network and placed on a blacklist until they can establish their reliability. The local reputation score, which is established by the host node, and the indirect reputation score, which is based on feedback from the closest nodes, are combined to form a node's total reputation. This hybrid approach is useful in preventing more complex attacks where several vehicles collude to trick the system. The system meets with several types of problems even though it offers a way to manage vehicle reputations on a decentralized level. In particular, in densely populated networks, its multi-layered, multi-parameter approach may result in significant processing and communication overhead. Furthermore, because it depends so heavily on accurate data from nodes, any inaccuracies in the parameters could have an impact on reputation scores. Collusion attacks, in which several vehicles share fake information to influence reputation scores, could still be able to exploit the system. Its functionality depends

on the timely and constant exchange of information; any pauses or disruptions could reduce its efficacy. It might also struggle with incorrect classifications of good and bad nodes, which would undermine user confidence. The system's importance could be affected in areas with poor or obstructed GPS signals, affecting its reliability for location-based metrics. Finally, the authors do not discuss blockchain or distributed ledger technologies.

The paper [11] proposed PrivBox system aims to improve buyers' security and privacy during interactions with service providers or sellers by securely computing sellers' reputations based on user feedback using homomorphic cryptographic methods and non-interactive ZKPs. The system's design assures user privacy without the need for a trusted setup or a third party. The system consists of three main parts: the buyer, the sellers, and the public bulletin board, which stores cryptograms of buyers' ratings. Buyers rate sellers on a binary scale and post their ratings to the Bulletin Board (BB). In a secure multi-party computing approach, the reputation of a specific seller is estimated by simply multiplying the cryptograms from the public bulletin board. Buyers generate private and public keys, which they use to send encrypted comments to a public bulletin board. This protects buyer feedback's privacy while also allowing it to be used to calculate the seller's overall reputation. The process is as follows: After a transaction, users receive a token from the marketplace, which is used to produce cryptographic parameters (private and public keys). They then encrypt their feedback (0 for negative, 1 for positive) and post it to the bulletin board, along with their public key and a non-interactive zero-knowledge (NIZK) proof proving that the encrypted feedback is either 0 or 1. These cryptograms are then used by the marketplace or any interested parties to compute the aggregated reputation of the sellers by multiplying the cryptograms. This provides an aggregated score that may be decrypted using a brute-force search to find the sum of positive feedback. Negative feedback is calculated by subtracting the positive ratings from the overall num-

ber of ratings. However, based on the type of system PrivBox appears to be, issues could include: These systems often require additional processing resources, which may not be practical for large-scale or real-time applications. While these technologies improve privacy, they may bring new weaknesses that malicious parties might use, such as self-promotion. Whitewashing one's reputation Badmouthing. Moreover, user feedback is dependent on the token generated by the seller, resulting in a single point of failure. However, the proposed system is vulnerable to several issues: it can be compromised through collusion if only one participant provides a unique score; it is at risk of Sybil attacks in which attackers create multiple identities; it mainly depends on participants completing the protocol, with disruptions possible if they don't; the protocol can be intentionally harmed as a form of a DoS attack.

This article [42] introduced a blockchain-based reputation system with edge intelligence that is specifically developed for the IIoT data environment. The single point of failure (SPOF) that is common in decentralized blockchain systems that rely on a single certificate authority is one of the key difficulties addressed by this solution. To mitigate this, the system relies on the Raft consensus process, increasing its resistance to possible system failures. The system uses advanced cryptographic techniques such as the blind elliptic curve digital signature (ECDSA) and a noninteractive zero-knowledge proof (ZKP) to ensure its security. The protections provided not only enhance its security but also ensure user anonymity. The system is robust due to its base in the Raft consensus mechanism, ensuring constant, smooth operation. To improve its resilience, particularly against link failures, a unique policy called RepGossip, based on the gossip protocol, has been integrated. The system's operational framework is made up of data providers, who market data records generated by IIoT devices, and data consumers, who buy and then explore these records. A central authority (CA) simplifies registration, verification, and overall operations. When data providers

initiate a transaction, the transaction is submitted to the CA for validation. The CA issues a rating token to the data consumer after they have been authenticated. This approach ensures that tokens are only released after a transaction has been confirmed, confirming the relationship between authentic transactions and the reviews that come with them.

The article [50] offered an anonymous reputation system ARS-PS that aims to overcome the multiple challenges of preserving user privacy while keeping the review process reliable. To provide security and privacy, the system relies on the PS signature, Bulletproof system, and non-interactive zero-knowledge proof approaches. The ARS-PS consists of three key players: customers, retailers, and an identity management entity (IDM). After registering with the IDM, consumers have an anonymous identity. They can make purchases from retailers and provide anonymous feedback, which is then aggregated to determine the retailer's reputation. Security is crucial, with the IDM playing a critical and trustworthy function. Initially, the IDM provides public parameters and security parameters for both consumers and retailers. Consumers and retailers both go through a registration process to receive anonymous credentials or public keys. A consumer can acquire an anonymous rating token from the retailer after completing a purchase, which confirms their eligibility to submit feedback. This token is then used by the consumer to make an anonymous review, which is later verified by a committee of selected retailers. The members of the committee gather legitimate reviews and compute a final aggregated rating score for each retailer. The process also functions to detect and track any misbehaving consumer who writes several reviews for a single transaction, maintaining system integrity. The proposed solutions, such as the use of ZKPs, encryption, and the inclusion of a retailer committee, provide a strong approach to anonymous reviews. Furthermore, with measures in place to detect and address misbehaving consumers, the system preserves the platform's legitimacy and fairness, making it a possible model for fu-

ture reputation systems that value privacy without compromising the authenticity of user feedback. The ARS-PS faces issues despite its important approach to privacy and reviews authenticity. The system depends on the IDM entity as a trustworthy agent raising issues about centralized control and potential abuse of power. Furthermore, the practice of addressing reviews through a chosen committee may result in potential biases or conflicts of interest. The system's approach to monitoring the misbehavior of customers, although necessary for credibility, may also be considered a potential misuse of the very privacy it aims to protect. Finally, the complexity of its operations, which include many security techniques, may make it less user-friendly and difficult to implement on a large scale.

The authors in [65] presented a privacy-preserving reputation system that hides individual feedback to maintain privacy while still allowing accurate reputation score computation. This decentralized system, which is based on blockchain technology, employs multiparty computation (MPC) that is improved by a verified secret-sharing scheme. While individual feedback is kept private, it still contributes to the total computation, making the reputation system both private and reliable. The framework consists of three main parts: service providers, customers, and the participating nodes that serve as the system's backbone. The mechanism that allows only customers to rate service providers is important to this framework, similar to traditional e-commerce businesses. Blind signatures are used to validate transactions, preventing service providers from identifying feedback from specific customers. Following a transaction, customers can request a blinded token, which keeps their identity hidden from the service provider. This token serves as verified proof of the customer-service provider transaction. When a customer decides to rate a service provider after the fact, they hash their pre-generated public key (the unique token for that specific transaction) and request a blind signature. This technique assures that the token is unrelated to the original

transaction, ensuring the customer's privacy.

The authors in [89] provided the Proof of Reputation (PoR) consensus approach. This solution eliminates the need for coin-based incentives and miners, instead relying on reputation as a motivator for virtuous behavior and as the basis for publishing blocks. PoR has been built for permissioned blockchains with an access control layer because of the inherent link between reputation and identification. The protocol can be integrated into a variety of peer-to-peer applications, providing a safe and non-manipulative way to track and evaluate participants' transaction reputation. PoR uses a trustworthiness mechanism similar to Bitcoin's Proof of Work for consensus, in its consensus goal, in which the participant with the greatest trust value puts several transactions into a block and sends it for others to verify. Unlike Bitcoin, PoR does not reward participants with money or transaction fees; instead, it rewards players with trustworthiness, a type of reputation that indicates that participants with greater trust values deliver better services. This method is less expensive because it avoids the complex mathematical challenges present in consensus methods. PoR consists of three major phases. First, after each interaction, the service requester generates feedback and broadcasts it with its signature. When a certain number of transactions have been completed, the next stage is to generate a block, which will be signed and released if the node is at the top of the trustworthiness ranking. Finally, before adding the block to the blockchain, nodes that receive it will check the sender's trustworthiness and the veracity of each transaction. Aside from these processes, the PoR incorporates transaction filters to prevent malevolent nodes from distributing fraudulent transactions or dishonest ratings. Furthermore, the processes for publishing and verifying blocks are defined, with measures set up to assure the reliability of transactions and block producers. The PoR method has significant drawbacks. If third-party verifiers become major players, linking blockchain identities to real-world IDs raises privacy concerns and the risk

of centralization. The system's dependence on reputation might lead to potential biases in which honest actors suffer from incorrectly poor reputations or manipulative actors abuse the reputation measurements. [26]

The paper [89] presented a Decentralized Anonymous Marketplace (DAM). DAM is resistant to Sybil's attacks on vendor reputation while maintaining user anonymity.DAM consists of up of several elements, including Customers, Vendors, Items, Reviews, and a Ledger. Customers buy items from sellers and provide feedback later. Vendors promote items for sale. Customers in the system do not require publicity because of the system's design and the nature of DAMs. However, sellers require a public identity that is linked to the products they sell and serves as the major reputation vector. To preserve customer anonymity and prevent her from signing multiple times, Linkable ring signatures are used. She must first make a purchase before they can submit a review. A transaction is recorded in the public ledger once the purchase is completed. An anonymity set is established after a particular number of transactions (specified by the parameter K) for a particular item. This collection includes all customers who bought the item. The exact number K makes sure the identity of the particular customer is hidden in a suitably big group. When a customer decides to write a review, the ring signature process is used. The ring for this signature contains all of the public keys connected with the anonymity set's K transactions. When the client signs their review, they utilize the private key associated with their public key in the group, but the final signature does not show which key was used. Anyone who wants to validate the review's credibility can do so by comparing the ring signature to the anonymity set's public keys. If the signature is valid, it confirms that one of the group's customers wrote the review, promoting both its authenticity and the reviewer's anonymity. Miners append the review to the public ledger after validating the ring signature, allowing it to be permanently accessible and verifiable by anybody in

the system. There is also an option in the system. Customers can link numerous reviews together if they choose. They can use Non-Interactive ZKPs of Knowledge (NIZKPoKs) to explicitly link numerous reviews together. This can be useful for building a reputation across multiple reviews while retaining privacy. While The Beaver system ensures review integrity and user privacy, it faces several challenges. Its dependency on transaction and review fees may put customers away due to the additional costs, thus limiting broad acceptance. Moreover, the size of the anonymity set determines the system's privacy, as misconfiguration might expose users to privacy problems or make the platform economically undesirable. Lastly, while the method attempts to reduce Sybil attacks by enforcing costs, smart adversaries with large resources may still be able to exploit it.

This paper [81], proposed a decentralized, trustless system that uses blind signatures on a blockchain to maintain anonymity. Customers receive blinded rating tokens from service providers (SP), which are then unblinded and anonymously published. To prevent ballot stuffing, SPs must spend restricted blockchain currency to issue tokens. The system claims to be resistant to attacks such as slander and fraudulent ratings. Customers can generate temporary key pairs for each transaction using the new system. To receive a rating token, they ask the SP for a blind signature on their public key, which they then unblind and convert into an anonymous token. Tokens provide proof of a transaction while maintaining anonymity using blind signatures. Customers broadcast ratings, coins, text reviews, and signatures on the blockchain for public verification and reputation score aggregation. However, a few weaknesses exist in the prevention of all ballot stuffing or Whitewashing. SPs can still self-issue tokens to increase their reputation but at a cost.

Hasan et al. [33] proposed A system based on additive homomorphic cryptography semantics and ZKPs. The system guarantees user privacy even in the context of a large number of bad users. The system requires a pre-selected pool of users to protect users' privacy.

CHAPTER 4

MANAGING REPUTATION SCORES IN A BLOCKCHAIN-BASED DECENTRALIZED MARKETPLACE

In this chapter, our goal is to answer the following research questions:**RQ1:** How do blockchain-based SCs enhance the reliability and efficiency of feedback mechanisms in transaction systems in different marketplaces? and **RQ2:** What are the impacts of specialized data structures on the scalability and efficiency of computing and retrieving reputation scores within blockchain-based systems?

Section 4.1 details the assumed blockchain-based decentralized marketplace. Section 4.2 describes the management of reputation scores in the assumed marketplace. Section 4.3 investigates the efficiency of our scheme for managing reputation queries. Section 4.4 specifies our simulation model and presents the simulation results. Finally, Section 4.5 provides concluding remarks.

4.1 THE BLOCKCHAIN-BASED DECENTRALIZED MARKETPLACE

In this chapter, we assume a blockchain-based marketplace similar to Agora [43], Beaver [89], and Wibson [96] where the transactions between buyers and sellers are maintained as individual blocks that, once added to the blockchain, keep immutable information about the transaction. We maintain statistical information about the buyers' and sellers' performance as part of the blockchain. Refer to Figure 1 or a high-level view of our system.

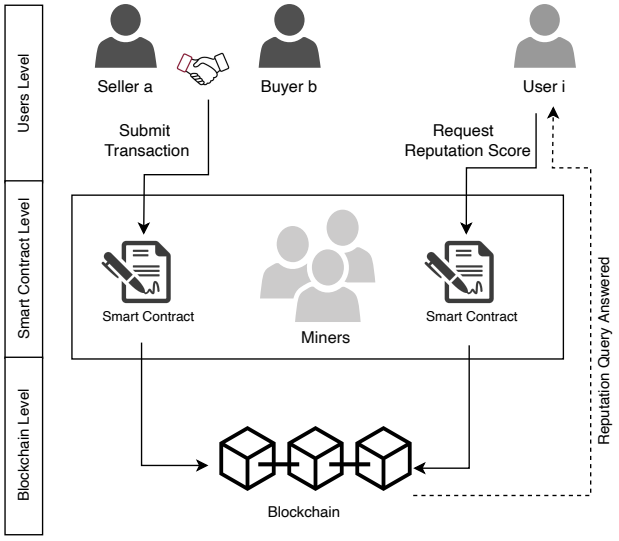

Figure 1. A high-level view of our system.

4.1.1 Buyers, Sellers, and Miners

We assume that the marketplace is populated by buyers, sellers, and miners, as we are about to describe.

Before participating in transactions, buyers and sellers register themselves with the marketplace by publishing their *public key*. As a consequence, the marketplace maintains a permissioned blockchain to store buyer and seller reputation scores. We assume that both buyers and sellers are *lightweight* clients using their cellphones and/or tablets to initiate transactions and to launch queries. Consequently, they cannot be assumed to have the capability to store large amounts of data. At most, they are expected to store the headers of all the transaction blocks in which they have participated. We assume that the buyers are able to see all the sellers that bring merchandise of interest to the market. Importantly, a lightweight user can act in the marketplace both as a buyer and as a seller, but not in the same transaction.

Entities within the marketplace, the so-called *miners*, possess high computational capabilities.

As in [70], we assume that the miners have sufficient resources to store the whole blockchain. The miners are in charge of several tasks, of which the most important one is to execute SCs. As part of executing SCs, the miners perform the following actions:

- add transaction blocks to the blockchain;
- verify blocks to be added by other miners;
- keep reputation scores in the blockchain up-to-date;
- answer user queries.

The miners are paid for their services from *transaction fees* associated with individual transactions and from *query fees* associated with individual queries.

When a buyer enters into a transaction with a seller, a SC is agreed upon. The SC is responsible for providing feedback at the end of each transaction, replacing the buyer feedback by a more objective assessment of how well, the buyer and the seller have fulfilled their contractual obligations towards each other.

4.1.2 Advantages of Using Smart Contracts

There are several advantages of putting an SC in charge of a transaction to provide feedback about the behavior of both buyer and seller:

- Each transaction is associated with objective feedback, reflecting accurately the behavior of the buyer and seller;
- Buyers and sellers cannot leave fake feedback for transactions in which they have not participated;

- Even in transactions in which they have participated, the buyers and sellers cannot leave glowing feedback with the intention to boost their own reputation scores or those of their associates. By the same token, they cannot leave derogatory feedback with the intention to harm the reputation of their competitors;

- Offers a consistent and complete summary of buyer and seller performance in the marketplace. In an environment where buyers and sellers know that the reputation scores maintained by the marketplace are accurate reflections of their behavior, even isolated and sporadic interactions between buyers and sellers take on attributes of long-term relationships and, as a result, the reputation scores maintained by the marketplace become a high-quality substitute for the more traditional, community-based, reputation;

- Promotes trust and confidence in the reputation system. The net effect is that more and more buyers and sellers will rely on the reputation system when it comes to selecting their business partners.

As we shall describe next, the role played by the SC in our marketplace is fundamental. Specifically,

- We assume simple transactions, each involving one buyer and one seller. The SC stipulates, in legally binding terms, the contractual obligations of both parties;

- At the conclusion of the transaction, the SC takes the following actions:

  - determines if the transaction was successful or unsuccessful. We say that a transaction is *successful* if both buyer and seller have fulfilled their contractual obligations;

  - if the transaction was not successful, the SC determines and documents which party has defaulted on their contractual obligations;

- Sets up a *transaction block* containing information about the transaction itself. The transaction block has a *header* and a *body*. The header contains information that identifies the buyer and seller by their public keys, the date and time of the transaction, the price range, numerical scores δ_B and δ_S, a litigation bit, and other metadata about the transaction. The litigation bit is set if one of the parties has defaulted on their obligations, and a full report is available in the data part of the block. The numerical scores, δ_B and δ_S, are intended to capture the behavior of both buyer and seller. Specifically,

  - $\delta_S = 1$ if seller S has fulfilled her contractual obligations, and 0 otherwise;
  - $\delta_B = 1$ if buyer B has fulfilled his contractual obligations, and 0 otherwise.

4.2 SCHEMES FOR MANAGING REPUTATION SCORES

The main goal of this section is to offer a detailed description of the data structure and methods used to manage reputation scores in our blockchain-based marketplace.

The buyers and sellers are not allowed to access or change their reputation scores. The reputation scores can be accessed by miners acting on behalf of buyers and sellers, as we discuss later. The buyers and sellers can issue queries about their own reputation scores (for verification purposes) or about the reputation scores of their potential transaction partners. In our marketplace, each such query is implemented as a SC (between the user and the blockchain) and executed by a miner.

In order to incentivize responsible behavior in the marketplace, query fees are refunded under

certain conditions:

- if a buyer who has requested the reputation score of a seller engages in a transaction with that seller and fulfills his contractual obligations, the query fee is refunded;
- if a user issues a query to verify his/her own reputation score, the query fee is refunded if the reputation score is maintained by the blockchain is incorrect.

We assume that a user may behave differently when acting as a buyer from the way they act as a seller. Therefore, the marketplace maintains separate reputation scores for buyers and sellers. Specifically, for a generic seller S registered with the marketplace, the blockchain stores in an implicit form her *seller reputation score* at time t, in the form of an ordered tuple (a,b,t) that specifies at time t

- the total number, b, of transactions in which S was involved (as a seller) up to and including time t;
- the total number, a, of these transactions in which S fulfilled her contractual obligations.

Similarly, for a generic buyer B, the blockchain stores his *buyer reputation score* at time t, in the form of an ordered tuple (c,d,t) that keeps track of

- the total number, d, of transactions in which B acted as a buyer up to and including time t;
- the total number, c, of these transactions in which B fulfilled, as a buyer, his contractual obligations.

4.2.1 Scheme 1: A Basic Reputation Management Scheme

Referring to Figure 2, It is useful to think of the blockchain that maintains seller reputation scores as an append-only data structure that contains one entry for each registered seller with the platform. Of course, new sellers can be added as needed. However, the entries corresponding to sellers that have departed the system have not deleted.

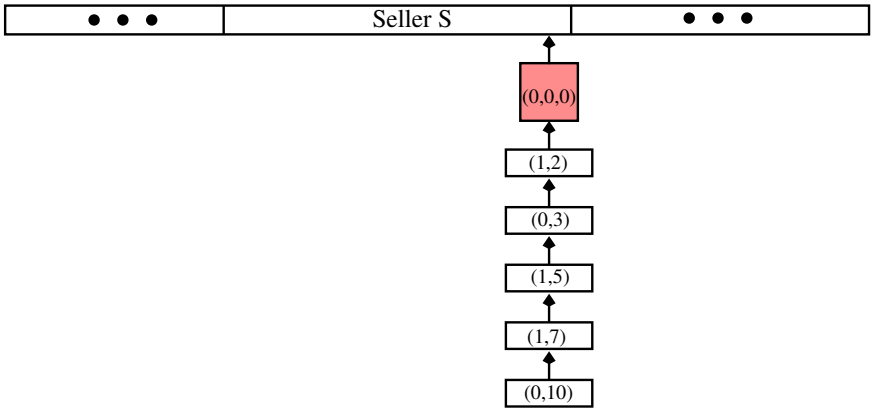

Figure 2. Illustrating the assumed reputation score blockchain.

Now, assume that seller S was involved in five transactions. The corresponding blocks were added to the blockchain as illustrated in Figure 2. Notice that each block contains the performance of the seller in the corresponding transaction along with a time stamp. Indeed, the first transaction has a score of $(1,2)$ indicating that in the transaction that carries the time stamp $t = 2$, the seller has fulfilled her contractual obligation; the next transaction carries a score of $(0,3)$ indicating that in the transaction with time stamp $t = 3$ seller S defaulted on her contractual obligation. Finally, the fifth transaction in Figure 2 tells us that in the transaction with timestamp $t = 10$, the seller has again defaulted on her contractual obligations.

Suppose that at time $t = 12$ a potential buyer issues a query about the reputation score of seller S. The corresponding SC is executed by a miner. Referring to Figure 3, the actions performed by the miner are as follows:

- traverses the list of blocks, including the most recent summary block, aggregating the corresponding scores;
- creates a summary block that contains the aggregated scores, along with the time stamp of the query;
- makes the summary block point to the previous summary block,[1] to the last block in the list of blocks and to the entry S in the array.
- returns the aggregated reputation score to the user who had requested it.

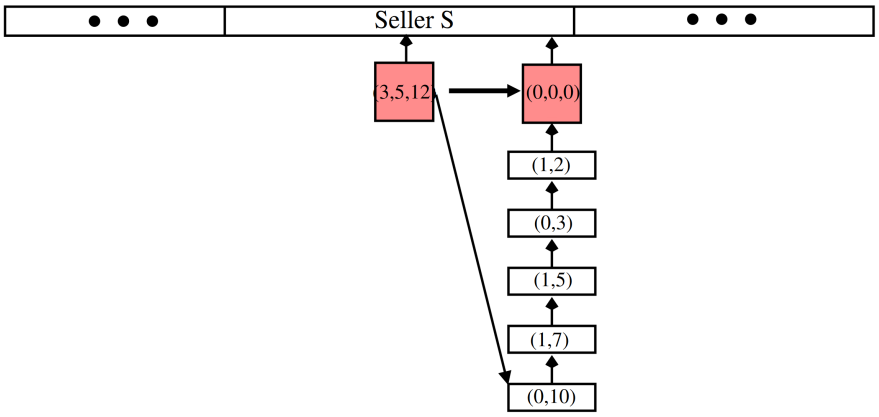

Figure 3. Illustrating the execution of the first query.

Assume now that a second query was to follow immediately after the first. In this case, the

[1] In this case, the previous summary block was added by default when the seller was added to the marketplace.

miner executing the query would access immediately the most recent summary block (the last block in the list of blocks) and would return the reputation score and the relevant time stamp without having to create a new summary block.

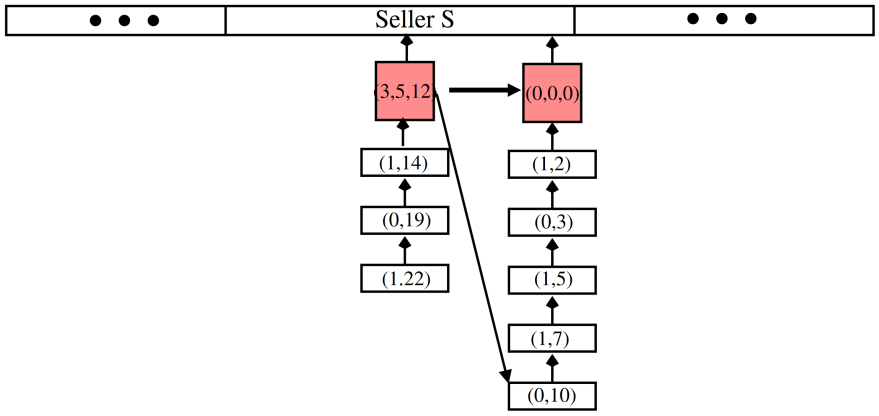

Figure 4. Illustrating more blocks added after the first query.

Suppose that, as illustrated in Figure 4, after the second query, seller S was involved in three more transactions. At time $t = 25$, a third query comes, finding the sequence of blocks as in Figure 4. The miner executing the query will traverse the list of recently added blocks, including the most recent summary block, and will aggregate the reputation scores. It will then create a new summary block, as illustrated in Figure 5, and will set pointers as discussed previously. With this done, the answer to the query is returned to the user.

In other words, the blockchain used in this chapter is an extension of the sequential blockchain structure used in Bitcoin, Ethereum, etc. Here, we have one sequential blockchain consisting of the summary blocks and another multiple transaction chains between successive summary blocks. This is a unique structure useful not only for storing transactions and reputation scores in a marketplace

but also for managing banking and inventory management systems, where transactions related to customers and inventory items, respectively, could be stored. Here, queries correspond to balance queries or a forced system query to compute the current balance.

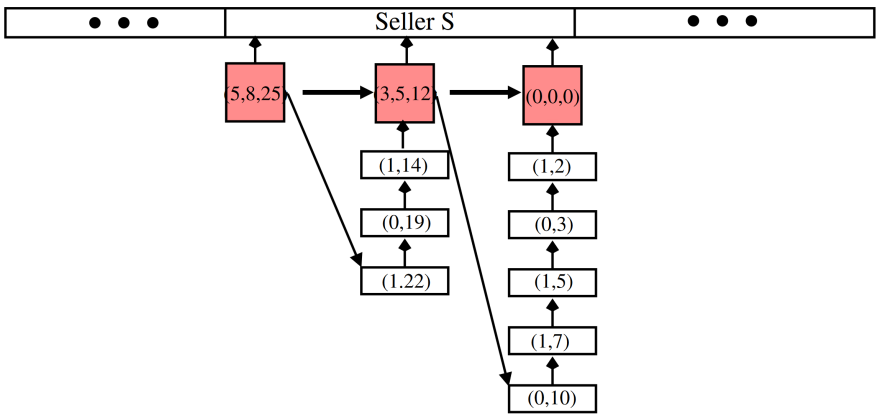

Figure 5. Illustrating the execution of the second query.

For efficiency purposes, the summary blocks form a *logical array* that supports binary searches based on time stamps, which occur in sorted order. It is important to notice that since the summary blocks are linked together, it is easy to produce historical information about the evolution, over time, of the reputation scores of seller S. For an illustration of how historical queries are handled refer to Figure 6.

Assume that at time $t = 42$ some buyer is interested in the reputation score of seller S at time $t = 17$. We briefly outline some of the tasks the miner in charge of this query will perform (the list is incomplete):

- By binary searching through the logical array of summary blocks, the miner will identify the first summary block whose time stamp exceeds 17. in Figure 6 this summary block is drawn

in blue. The timestamp of this summary block is 25, which exceeds 17.

- Starting at this summary block, the miner will follow the links to previous blocks until a timestamp less than 17 is found;
- The scores in all the blocks traversed (see in blue in the figure) are removed from the score in the summary block to yield $(4, 6, 17)$;
- This is to say, up to time $t = 17$ seller S was involved in a total of six transactions of which 4 were successful. This is the answer to the query and will be returned to the requester.

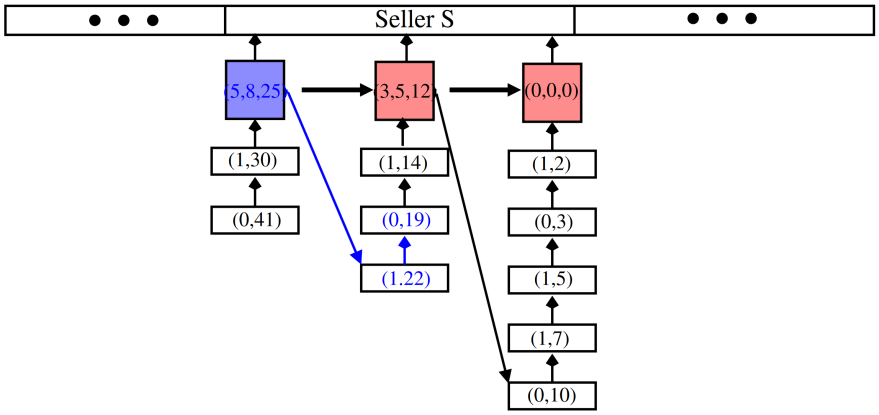

Figure 6. Illustrating answering a reputation query.

4.2.2 Scheme 2: Adaptive Reputation Management Scheme

In this section, we present details of our first reputation management scheme. The efficiency of our scheme is measured in terms of the number of blocks that need to be accessed to answer a user query. This scheme guarantees a maximum bound on the number of blockchain blocks to be

accessed in a query execution.

This scheme supports two types of operations: the addition of new reputation blocks to the blockchain and answering user (reputation) queries. After a transaction has been completed, the reputation SC generates a reputation block reflecting its transaction rating. New reputation blocks are added sequentially, with the latest block pointing to the previously added block. These are part of the blockchain. Whether or not the reputation blockchain should be part of the remaining transaction and buyer/seller information blockchain, or an independent one, is an implementation issue. The queries that need to be supported by the reputation blockchain and the associated SCs efficiently are of the type: "What is the current reputation score of seller S?"

Our scheme (similar to [58]), distinguishes two types of block additions: transaction outcome blocks to add the outcome of a buyer-seller transaction and summary blocks representing the reputation of sellers (buyers) at different times. However, since [58] allows an arbitrary number of transaction outcome blocks to be added on top of a summary block, it may result in large reputation query response times, especially when the rate of queries is much lower than the actual transactions. This may be the case in a real-world situation.

The proposed adaptive scheme overcomes this weakness by limiting the number of transaction outcome blocks that may be added on top of a summary block. We begin by setting a system parameter n, such that the chain of new blocks in between any two consecutive summary blocks cannot exceed n. In our adaptive scheme, a request for the addition of a new block is handled as follows:

- if the addition of the new transaction outcome block results in a chain shorter than or equal to $n-1$ blocks on top of the latest summary block, then the new transaction outcome block

is added and made to point to the previous block (see Figure 7, with $n = 5$);

- if the addition of the new transaction block would result in a chain longer than $n-1$ blocks, the new transaction block is added (the n^{th} transaction outcome block) and, at the same time, a new summary block is created and made to point to the newly added transaction outcome block (see Figure 8, with $n = 5$).

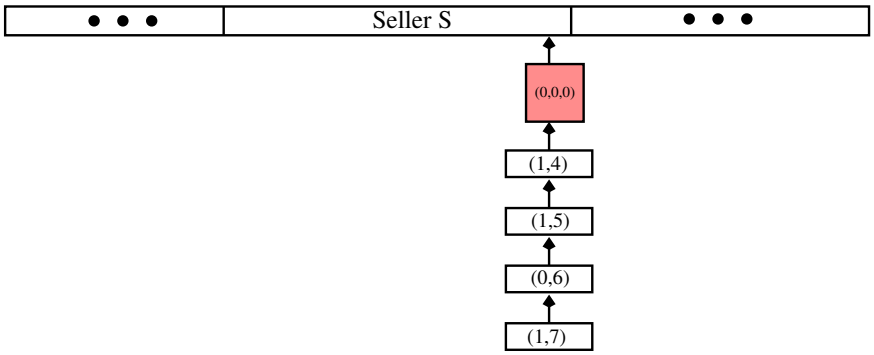

Figure 7. Illustrating the addition of a new block to the blockchain of reputation scores.

Notice that, initially, there is only one dummy summary block containing the tuple $(0,0,0)$, which indicates that at time $t = 0$, the seller was involved in no transactions. Each transaction block contains the performance of the seller in the corresponding transaction, along with a time stamp. Thus, for example, the first transaction has a score of $(1,4)$, indicating that in the transaction that carries the time stamp $t = 4$, the seller has fulfilled her contractual obligation; the next transaction carries a score of $(1,5)$ indicating that in the transaction with time stamp $t = 5$ seller S has fulfilled her contractual obligation. The third transaction has a score of (0,6) indicating that in the transaction with time stamp t=6, seller has failed to fulfill her contractual obligations. Finally,

the fourth transaction in Figure 7 tells us that in the transaction with a time stamp $t = 7$, the seller has fulfilled her contractual obligations. Now suppose that a fifth transaction block has to be added

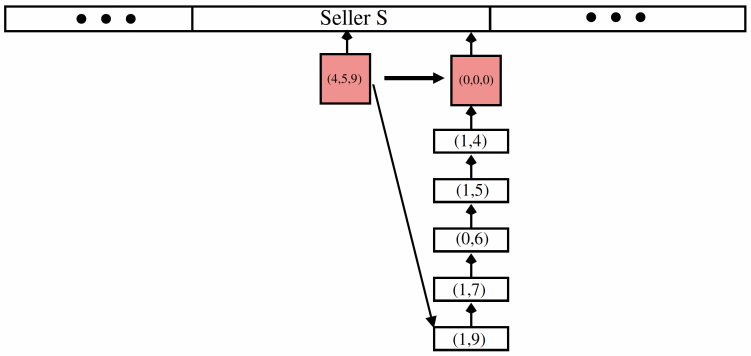

Figure 8. Illustrating the creation of a new summary block because of reaching the system limit $n = 5$

at time $t = 9$ and refer to Figure 8. Since $n = 5$ is our system limit, the actions performed by the miner in charge of the transactions are as follows:

- the miner traverses the list of blocks on top of summary block $(0,0,0)$ aggregating the corresponding scores;
- creates a *new summary block*, $(4,5,9)$, that contains the aggregated scores thus far, along with the time stamp, $t = 9$, of the last transaction that triggered the creation of the summary block;
- makes the new summary block point to the previous summary block, as well as to the last transaction block.

To set the stage for handling our first user query, notice that, as illustrated in Figure 9, two more

blocks were added on top of the last summary block, $(4,5,9)$. Referring to Figure 10, suppose that at time $t = 21$, a potential buyer issues a query about the reputation score of seller S. The corresponding SC is executed by a miner. The actions performed by the miner are as follows:

- the miner traverses the two blocks on top of the last summary block, $(4,5,9)$, aggregating the corresponding scores;
- creates a *summary block*, $(6,7,21)$ that contains the aggregated scores, along with the time stamp of the query;
- makes the new summary block point to the previous summary block and to the last transaction block;
- returns the aggregated reputation score to the user who had requested it.

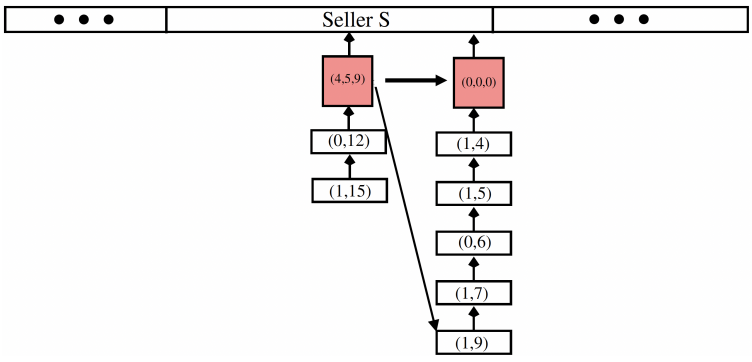

Figure 9. Illustrating the data structure just before the first query

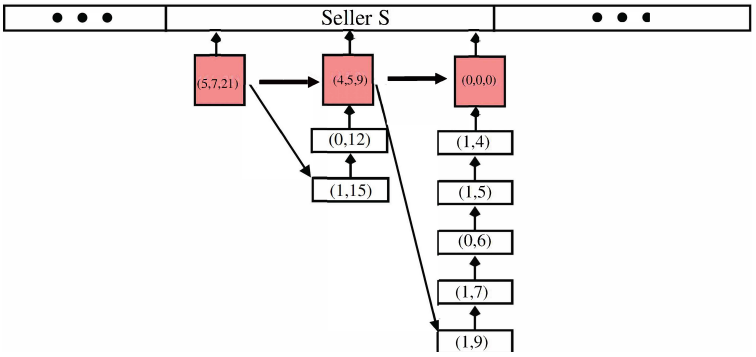

Figure 10. Illustrating handling the first query

4.2.3 Scheme 3: Randomized Reputation Management Scheme

We now discuss our second scheme for reputation management. A request for a transaction block addition is handled as follows:

- The miner in charge of adding the block flips a coin;
- If the coin turns up Heads (H), the transaction outcome block is added to the end of the list of blocks;
- If the coin comes up Tails (T), the transaction block is added, and a new summary block is also created. Pointers are set as described in Section 4.2.2.

As an illustration, refer to Figures 11, 12, and 13.

Now assume a transaction block addition request at time $t = 22$. The miner handling the addition flips a coin and assumes that H shows up. In this case, the block is added to the blockchain as illustrated in Figure 12.

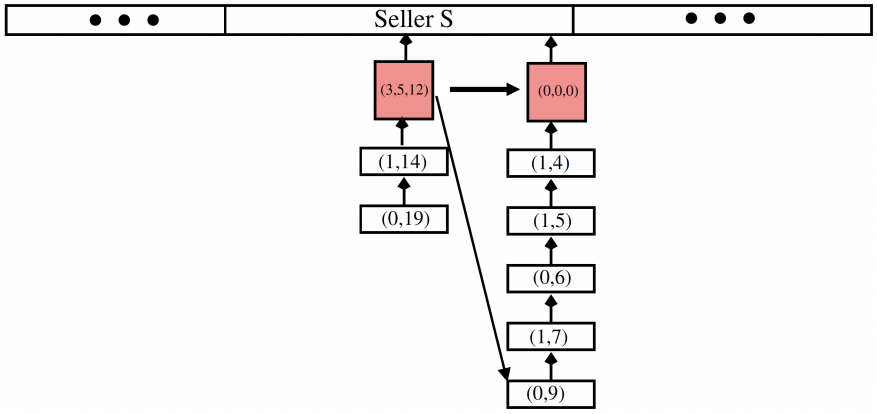

Figure 11. Illustrating the blockchain just before the transaction block addition.

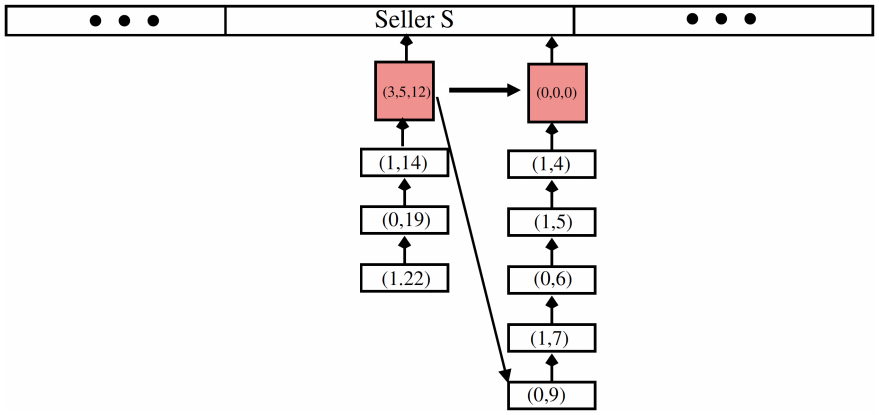

Figure 12. Illustrating the blockchain after block addition assuming an H was tossed.

On the other hand, if the coin tossed by the miner turns up T, the transaction block is added and a new summary block aggregating the previous scores is created by the miner. as illustrated in Figure 13.

A query is handled exactly as discussed in Section 4.2.2 wherein a query results in a new summary block unless the very previous block was a summary block.

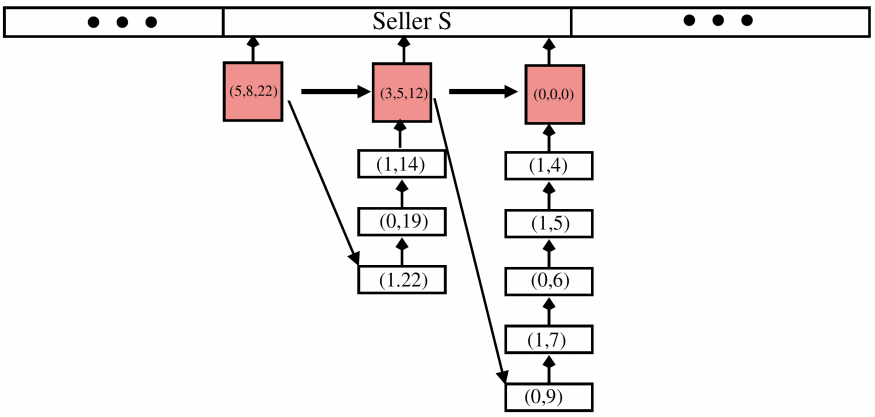

Figure 13. Illustrating the blockchain after block addition assuming a T was tossed.

4.3 PROBABILISTIC ANALYSIS

4.3.1 Scheme 1: Basic Reputation Management Scheme

Assume that requests for the addition of new blocks and queries arrive as independent Poisson processes with parameters $\lambda > 0$ and $\mu > 0$. We assume that new blocks are added to the data structure, while queries result in changing the data structure by adding a new summary block, unless the last block is itself a summary block.

We begin by asking the question: what is the probability that the next request to arrive is a query? We will solve this problem in a general setting. Consider independent Poisson processes $\{B(t)|t \geq 0\}$ and $\{Q(t)|t \geq 0\}$ with parameters λ and μ, respectively. Consider the *merged* process. It is well known that the merged process is itself a Poisson process with parameter $\lambda + \mu$.

Let τ be the next arrival of the merged process. We are interested in the probability of the event that τ is an arrival point of the process $\{Q(t)|t \geq 0\}$. We denote this event by $\{\tau \text{ is a query}\}$.

Let γ_B and γ_Q be random variables that keep track of the time until the next arrival in $\{B(t)|t \geq 0\}$

and $\{Q(t)|t \geq 0\}$, respectively. we write

$$\begin{aligned}
\Pr[\{\tau \text{ is a query}\}] &= \int_{u=0}^{\infty} \Pr[\gamma_B > \gamma_Q | \gamma_Q = u] \mathrm{d}F_{\gamma_Q}(u) \\
&= \int_{u=0}^{\infty} \Pr[\gamma_B > \gamma_Q | \gamma_Q = u] \mu e^{-\mu u} \mathrm{d}u \\
&= \mu \int_{u=0}^{\infty} \Pr[\gamma_B > u] e^{-\lambda_B u} \mathrm{d}u \\
&= \mu \int_{u=0}^{\infty} e^{-\lambda u} e^{-\lambda u} \mathrm{d}u \\
&= \mu \int_{u=0}^{\infty} e^{-(\lambda+\mu)u} \mathrm{d}u \\
&= \frac{\mu}{\lambda+\mu}. \qquad (1)
\end{aligned}$$

Notice that (1) tells us that the probability of the next arrival being a query is *independent* of τ, that is, of the time of the next arrival. The probability that the next arrival is a request for a block addition must be $1 - \frac{\mu}{\lambda+\mu} = \frac{\lambda}{\lambda+\mu}$.

Our goal is to investigate the *expected* number of *block accesses* involved in answering a reputation-score query. For this purpose, we note that if the last block in the chain of blocks to traverse, then the number of such accesses is one. In general, if the number of fresh blocks added to the latest summary block is k, for some $k \geq 0$, then the number of accesses is $k+1$. We model the dynamics of the query system using the Markov chain in Figure 14. The states of this Markov chain are $0,\ 1,\ 2,\ \ldots,\ k,\ \ldots$. We say that the Markov chain is in state $k,\ (k \geq 0)$, if the number of blocks on top of the latest summary block is k. It is important to note that the number of states of this Markov chain is countably infinite.

Let us take a closer look at the various transition probabilities in our Markov chain. To be specific, assume that, at some point, the Markov chain is in state k, namely, there are k blocks on top of the

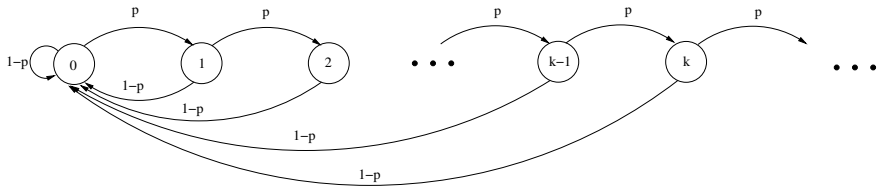

Figure 14. Illustrating the Markov chains modeling the query problem.

latest summary block. What can happen next?

If the next request is for a new block to be added, then there will be $k+1$ blocks on top of the latest summary block and, naturally, the Markov chain makes a transition to state $k+1$. By (1) the probability of such a transition is $p = \frac{\lambda}{\lambda+\mu}$;

If, on the other hand, the next request is a query, k drops to 0.[2] In this case, our Markov chain makes a transition to state 0, as illustrated in Figure 14. The probability of this latter event is $1-p = 1-\frac{\lambda}{\lambda+\mu} = \frac{\mu}{\lambda+\mu}$.

The transition matrix of the Markov Chain in Figure 14 is:

	0	**1**	**2**	$\cdots$	$\mathbf{k-1}$	**k**	$\cdots$
0	$1-p$	p	0	$\cdots$	0	0	$\cdots$
1	$1-p$	0	p	$\cdots$	0	0	$\cdots$
2	$1-p$	0	0	$\cdots$	0	0	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$	$\vdots$	$\vdots$
$\mathbf{k-1}$	$1-p$	0	0	$\cdots$	0	p	$\cdots$
k	$1-p$	0	0	$\cdots$	0	0	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$	$\vdots$	$\vdots$

[2] If $k \neq 0$, a new summary block is created. Otherwise, no summary block is created.

It is straightforward to see that our Markov chain is *ergodic* and so the steady-state probabilities exist and are unique. Indeed, let $\pi_0,\ \pi_1, \pi_2,\ \cdots,\ \pi_{k-1},\ \pi_k,\ \ldots$ denote these steady-state probabilities. It is well-known that these steady-state probabilities are the unique solutions of the following system of equations:

$$\begin{cases} \pi_0 = (1-p)\pi_0 + (1-p)\pi_1 + (1-p)\pi_2 + \cdots \\ \pi_1 = p\pi_0 \\ \pi_2 = p\pi_1 \\ \ldots\ldots \\ \pi_k = p\pi_{k-1} \\ \ldots\ldots \end{cases}$$

Elementary algebraic manipulations (omitted) confirm that the generic solution of this system of equations is

$$\pi_k = (1-p)p^k, \tag{2}$$

that holds for all $k,\ k \geq 0$.

In order to assess the expected amount of "work", as defined above, involved in answering a query we proceed as follows. Let W be the random variable that keeps track of the steady-state number of block accesses involved in answering a query. We are interested in the expected value,

$E[W]$, and the standard deviation, $\sigma(W)$, of W. To compute $E[W]$, we write

$$\begin{aligned} E[W] &= \sum_{k=0}^{\infty}(k+1)\pi_k \\ &= \sum_{k=0}^{\infty}(k+1)(1-p)p^k \\ &= (1-p)\sum_{k=0}^{\infty}(k+1)p^k \\ &= (1-p)\frac{1}{(1-p)^2} = \frac{1}{1-p} \\ &= \frac{\lambda+\mu}{\mu} = 1+\frac{\lambda}{\mu}. \end{aligned} \tag{3}$$

Now, using the fact that $\sum_{k=0}^{\infty}(k+1)^2\pi_k = \frac{1+p}{(1-p)^3}$, we write

$$\begin{aligned} Var[W] &= E[W^2]-E[W]^2 = \sum_{k=0}^{\infty}(k+1)^2\pi_k - \left(1+\frac{\lambda}{\mu}\right)^2 \\ &= (1-p)\sum_{k=0}^{\infty}(k+1)^2p^k - \left(1+\frac{\lambda}{\mu}\right)^2 \\ &= (1-p)\frac{1+p}{(1-p)^3} - \left(1+\frac{\lambda}{\mu}\right)^2 \\ &= \frac{\lambda}{\mu}\left(1+\frac{\lambda}{\mu}\right). \end{aligned} \tag{4}$$

Finally, by (4), the standard deviation $\sigma(W)$ can be written as

$$\sigma(W) = \sqrt{Var(W)} = \sqrt{\frac{\lambda}{\mu}\left(1+\frac{\lambda}{\mu}\right)}. \tag{5}$$

4.3.2 Scheme 2: Adaptive Reputation Management Scheme

We now perform a probabilistic analysis to evaluate the efficacy of the proposed scheme. As-

sume that new transaction blocks and queries arrive as independent Poisson processes with parameters $\lambda > 0$ and $\mu > 0$, respectively.

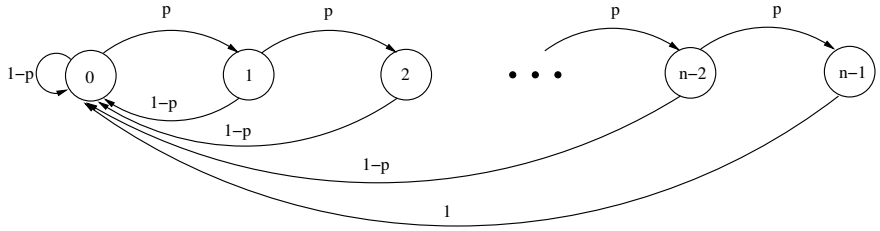

Figure 15. Illustrating the Markov chain modeling our query problem.

We begin by asking the following question: What is the probability that the next request will arrive as a query (and not a transaction)? We will solve this problem in a general setting. Consider independent Poisson processes $\{B(t)|t \geq 0\}$ and $\{Q(t)|t \geq 0\}$ with parameters λ and μ, respectively. Consider the *merged* process. It is well known that the merged process is itself a Poisson process with parameter $\lambda + \mu$. Let τ be the next arrival of the merged process. We are interested in the probability of the event that τ is an arrival point of the process $\{Q(t)|t \geq 0\}$. We denote this event by $\{\tau \text{ is a query}\}$. From here, we can derive an expression for the probability that the next arrival is a request for a transaction block addition as $p = 1 - \frac{\mu}{\lambda+\mu} = \frac{\lambda}{\lambda+\mu}$.

Our goal is to investigate the *expected* number of *block accesses* involved in answering a user query. In general, if the number of transaction blocks added to the latest summary block is k, for some $k \geq 0$, then the number of accesses is $k+1$. We model the dynamics of the query system using the Markov chain in Figure 15. The states of this Markov chain are $0,\ 1,\ 2,\ \ldots,\ n-1$. We say that the Markov chain is in state $k,\ (0 \leq k \leq n-1)$, if the number of blocks on top of the latest

summary block is k.

Let W be the random variable that keeps track of the steady-state number of block accesses in answering a query. From the Markov chain, we can derive the expected value of W ($E[W]$) and standard deviation of W ($\sigma(W)$), as follows (details omitted)

$$E[W] = \frac{1}{1-p} - \frac{np^n}{1-p^n} \tag{6}$$

$$\sigma(W) = \sqrt{Var[W]} = \sqrt{\frac{p}{(1-p)^2} - \frac{n^2 p^n}{(1-p^n)^2}} \tag{7}$$

These are plotted for different values of p and n in Figures 16 and 17. From here, it may be observed that the effect of the system parameter is much more prominent at larger values of p, since this is where the rate of transactions(λ) is higher than the rate of queries (μ). However, this is the most typical case, since in any online marketplace, transactions are much more frequent than reputation queries. Reputation queries generally occur when a buyer encounters the seller for the first time. In fact, for small values of p (e.g., $p \leq 0.4$), $E[W] \approx \frac{1}{1-p}$ and $\sigma(W) \approx \frac{\sqrt{p}}{(1-p)}$, and hence independent of the system parameter n, as can be seen from Figures 16 and 17, respectively.

In section 4.4, we compare the analytical expressions for $E[W]$ and $\sigma(W)$ with results obtained from simulations.

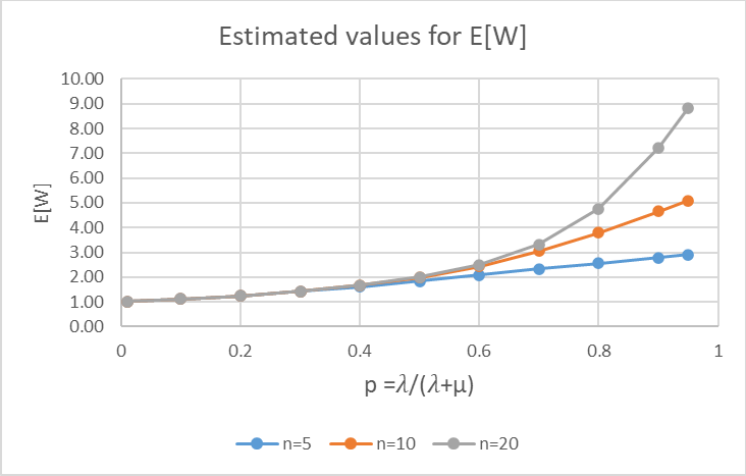

Figure 16. Estimated E[W] with the Adaptive Scheme

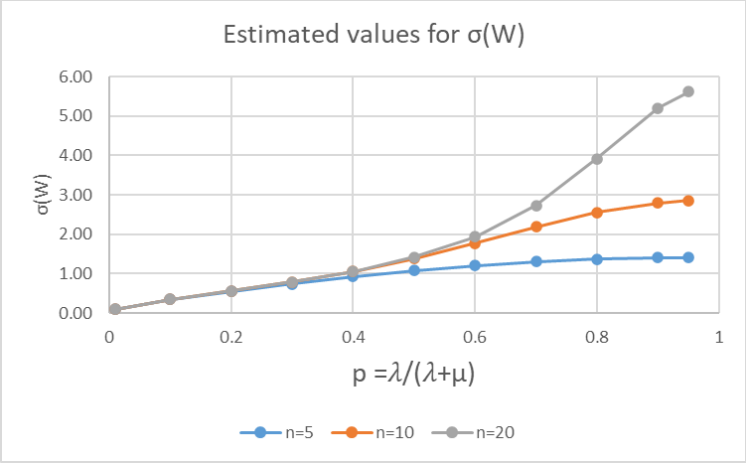

Figure 17. Estimated $\sigma(W)$ with the Adaptive Scheme

4.3.3 Scheme 3: A Randomized Scheme

As in scheme 1, our goal is to investigate the expected number of block accesses and their standard deviation involved in answering a user query. In general, if the number of blocks added to the latest summary block is k, for some $k \geq 0$, then the number of accesses is $k+1$. We model the dynamics of the query system using the Markov chain in Figure 18. The states of this Markov

chain are $0,\ 1,\ 2,\ \ldots,\ k,\ \ldots$. We say that the Markov chain is in state $k,\ (k \geq 0)$, if the number of blocks on top of the latest summary block is k. It is important to note that, a priori, the number of states of this Markov chain is *countably infinite*.

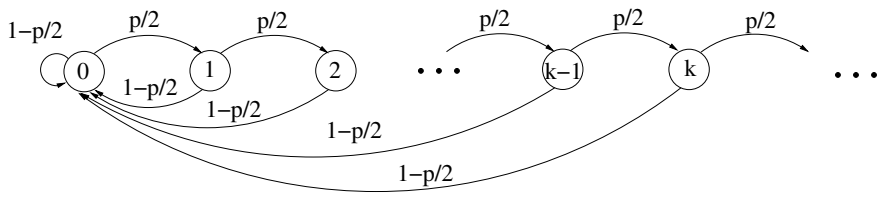

Figure 18. Illustrating the Markov chain modeling our randomized block addition/query strategy.

Assuming a fair coin flip, using Markov chain modeling, we obtain (details omitted)

$$E[W] = 1 + \frac{p}{2-p} \tag{8}$$

$$\sigma(W) = \frac{\sqrt{2p}}{2-p} \tag{9}$$

In figure 19, we plot $E[W$ and $\sigma(W)$ for different values of p. Obviously, since it is a fair coin, more summary blocks are created, and hence the lower values for $E[W]$ and $\sigma(W)$. This will change when the probability of a tail "T" is lower than the probability of a head "H." As p approaches 1 (where the rate of queries is insignificant as compared to the rate of transactions), the value of $E[W]$ approaches 2, and $\sigma(W)$ approaches $\sqrt{2}$. In the following section, we compare the analytical expressions for $E[W]$ and $\sigma(W)$ with results obtained from simulations.

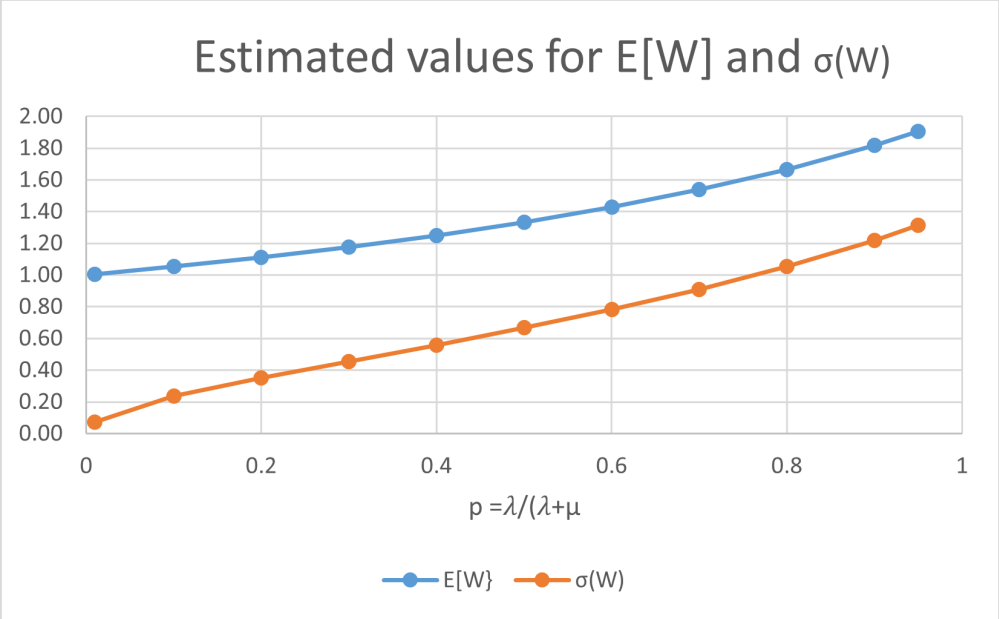

Figure 19. $E[W]$ and $\sigma(W)$ for the Randomized Scheme

4.4 SIMULATION MODELING AND EXPERIMENTAL RESULTS

In the previous sections, we have proposed three schemes to efficiently manage transaction outcome records in a blockchain and to answer user queries regarding sellers' reputation scores. This was achieved by proposing new data structures and algorithms to manage the data structures. The objective was to store buyer-seller transaction outcomes as well as a way to respond to reputation queries quickly. The data structures and the three query execution methods were then modeled using Markov chains, resulting in mathematical expressions for the expected number, $E[W]$, of blockchain blocks that are accessed in executing a query as well the corresponding standard deviation $\sigma(W)$. In this section, we use simulation methods to validate our analytical results. In the above models, we used λ and μ to represent the parameters of the Poisson processes representing the arrival of transactions and queries, respectively. We use the same in the simulation model, with $\lambda{:}\mu$ representing the ratio of transactions to queries. We experiment with the ratios of

$0.9:0.1,\ 0.8:0.2,\ \cdots,\ 0.1:0.9$. With each ratio, we generate transactions and queries with the appropriate distribution, build the blockchain structure, and determine the number of blocks, W, accessed by each query. For any given ratio, in each simulation run, we generated 50,000 events, a combination of transactions and queries. Each simulation run was repeated 10 times, for a given ratio. The combined statistics of these simulations for each of the methods are summarized in Table 1, Tables 2, and 3 below.

Table 1. Simulation results for W.

Simulation Results for W				
	$E[W]$		$\sigma(W)$	
$\lambda:\mu$	Analytical	Simulated	Analytical	Simulated
0.9 : 0.1	10.0	10.012	9.48	9.52
0.8 : 0.2	5.0	5.032	4.47	4.61
0.7 : 0.3	3.33	3.31	2.78	2.78
0.6 : 0.4	2.5	2.5	1.93	1.92
0.5 : 0.5	2.00	2.008	1.41	1.42
0.4 : 0.6	1.66	1.654	1.05	1.05
0.3 : 0.7	1.42	1.422	0.78	0.78
0.2 : 0.8	1.25	1.252	0.55	0.56
0.1 : 0.9	1.11	1.111	0.35	0.35

As the relative rate of queries increases, the relative number of summary blocks also increases in the blockchain data structure. This implies that the number, W, of blocks accessed by a miner to execute a query decreases. This is reflected in Table 1 where for different ratios of λ:μ, we show the average $E[W]$ obtained from simulations as well as (8) derived above. From here, we can observe that the analytical estimations of $E[W]$ are very close to those measured from simulations. This confirms the correctness of the analytical results. In addition, it may be observed that

the standard deviation of W decreases significantly as the relative rate of queries increases. The analytical results (see (5)) for the standard deviation also closely match those measured from the simulations. In addition, we have also measured the frequency distribution of W for different λ:μ ratios. Figure 20 shows the probability distributions of W for several λ:μ ratios.

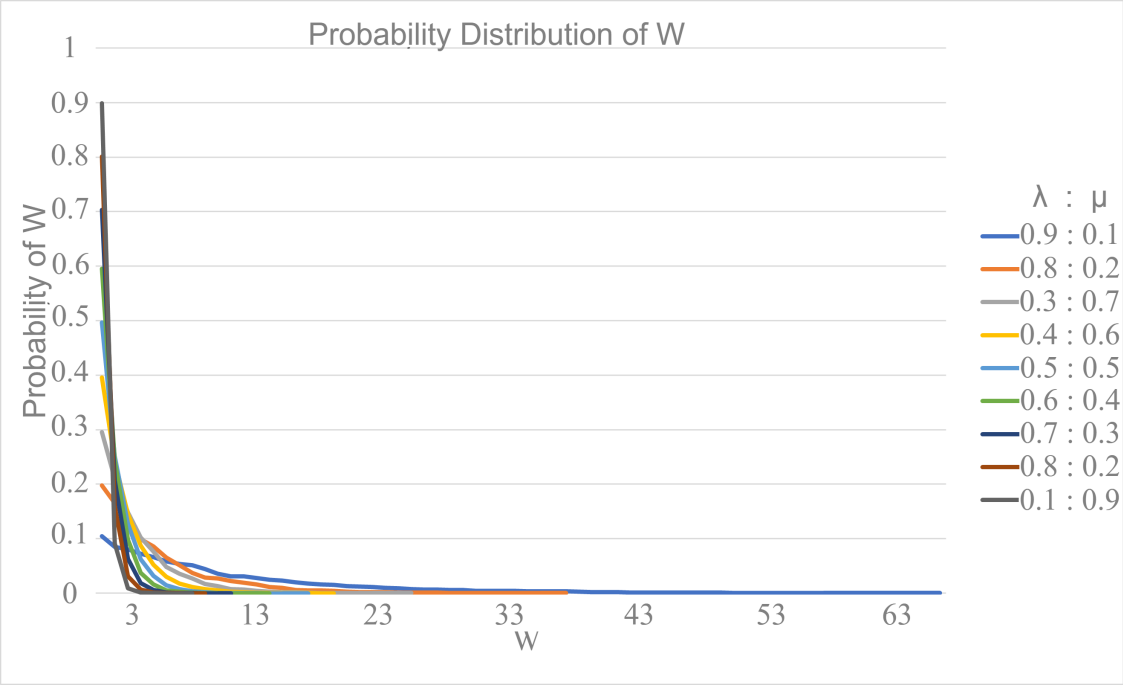

Figure 20. Probability distributions of W for different λ and μ

It is clear that as the proportion of queries increases, the ranges of values of W decreases significantly. In other words, the efficacy of adding summary blocks in the proposed blockchain data structure significantly increases with the frequency of the queries. Thus, the additional storage cost of maintaining summary blocks, which is linearly proportional to the queries, is found to significantly reduce the cost of query execution.

In this context, we compare the efficiency of the second and third schemes against the first scheme [58]. As the relative rate of queries increases (i.e., μ/λ increases), the relative number of summary blocks also increases in the blockchain data structure. This implies that the number, W, of blocks accessed by a miner to execute a query decreases. This is reflected in both schemes as seen in Tables 2 and 3 where for different ratios of λ:μ, we compare $E[W]$ and $\sigma(W)$ predicted and those obtained from simulation.

Table 2. Comparison of simulation and analytical results for W for Adaptive Reputation Management Scheme with n=10

Simulation Results for W with n=10				
	$E[W]$		$\sigma(W)$	
$\lambda : \mu$	Analytical	Simulation	Analytical	Simulation
0.9 : 0.1	4.65	4.65	2.79	2.80
0.8 : 0.2	3.80	3.80	2.55	2.56
0.7 : 0.3	3.04	3.05	2.19	2.20
0.6 : 0.4	2.44	2.44	1.77	1.77
0.5 : 0.5	1.99	1.99	1.38	1.38
0.4 : 0.6	1.67	1.66	1.05	1.04
0.3 : 0.7	1.43	1.43	0.78	0.78
0.2 : 0.8	1.25	1.25	0.56	0.56
0.1 : 0.9	1.11	1.11	0.35	0.35

It is clear that the analytical estimations of $E[W]$ are very close to those measured from simulations. This confirms the correctness of the analytical results. In addition, it may be observed that the standard deviation $\sigma(W)$ decreases significantly as the relative rate of queries increases. The analytical results for $\sigma(W)$ also closely match those measured from the simulations.

It is also interesting to note that the randomized management scheme results in more efficient

Table 3. Comparison of simulation and analytical results for W for Randomized Reputation Management Scheme

Simulation Results for W				
	$E[W]$		$\sigma(W)$	
$\lambda : \mu$	Analytical	Simulation	Analytical	Simulation
0.9 : 0.1	1.82	1.82	1.21	1.22
0.8 : 0.2	1.67	1.67	1.05	1.06
0.7 : 0.3	1.54	1.54	0.91	0.90
0.6 : 0.4	1.43	1.43	0.78	0.78
0.5 : 0.5	1.33	1.34	0.66	0.67
0.4 : 0.6	1.25	1.25	0.55	0.56
0.3 : 0.7	1.18	1.18	0.45	0.46
0.2 : 0.8	1.11	1.11	0.35	0.35
0.1 : 0.9	1.05	1.05	0.24	0.23

queries than the adaptive reputation management scheme. We have compared the performance of our two reputation management schemes with that in [58]. The results are summarized in Table 4. When compared to their scheme, the adaptive scheme shows the highest decrease in $E[W]$ of 53.5% for $\lambda : \mu$ of 0.9:0.1. This reduces as the proportion of queries increases, since each query (in both methods) results in a new summary block.

Similarly, the adaptive scheme results in a reduction of 70.57% in $\sigma(W)$ as compared to their method. We find similar or better improvements due to the randomized method. This is clear evidence that suggested methods are much desired, especially when the proportion of queries is much smaller than that of the transactions.

4.5 SUMMARY

In this chapter, we assumed a blockchain-based decentralized marketplace where an SC is associated with each transaction. To reduce the uncertainty linked to notoriously unreliable buyer

Table 4. Performance comparison of scheme 2 and scheme 3 with scheme 1

% Improvement of proposed methods over [58] for W				
	$E[W]$		$\sigma(W)$	
$\lambda : \mu$	Adaptive	Randomized	Adaptive	Randomized
0.9 : 0.1	53.50	81.80	70.57	87.13
0.8 : 0.2	24.00	66.60	42.95	76.51
0.7 : 0.3	8.71	53.75	21.22	67.27
0.6 : 0.4	2.40	42.80	8.29	59.59
0.5 : 0.5	0.50	33.50	2.13	53.19
0.4 : 0.6	0.00	24.70	0.00	47.62
0.3 : 0.7	0.00	16.90	0.00	42.31
0.2 : 0.8	0.00	11.20	0.00	36.36
0.1 : 0.9	0.00	5.41	0.00	31.43

feedback, we introduced a novel approach suggesting that the SC associated with each transaction should provide feedback at the end. This strategy replaces buyer feedback with a more objective assessment of how well the buyer and seller have fulfilled their contractual obligations toward each other. Furthermore, we proposed three schemes to enhance reputation management and query responses. Our first scheme is basic, the second is adaptive, and the third is randomized. We provided analytical performance predictions and verified them empirically through extensive simulation, demonstrating the accuracy of our predictions. Additionally, we compared the performance of our schemes.

CHAPTER 5

SMART CONTRACT-BASED DECENTRALIZED MARKETPLACE SYSTEM TO PRESERVE REVIEWER ANONYMITY

In this chapter, our goal is to answer the following research question: **RQ3:** How do SCs use multiple identities to promote reviewer anonymity in decentralized marketplaces, and what impact does this anonymity have on the quality of feedback?

We begin by outlining the key properties and characteristics that our system aims to achieve in Section 5.1. Following this, Section 5.2 presents a detailed model of our system, including its architecture and operational mechanics.Section 5.3 covers the implementation details, highlighting the tools and technologies used, as well as the development process. In Section 5.4, we present and analyze the results obtained from our experiments and simulations, demonstrating the system's performance and effectiveness. Finally, Section 5.5 provides a summary of the chapter, highlighting the main findings and their implications for the field.

5.1 SYSTEM PROPERTIES

In this section, we look at two salient features of the proposed system—promoting reviewer anonymity and incentivizing buyers to provide feedback.

5.1.1 Promoting Reviewer Anonymity

As illustrated above, a dishonest seller may cause damage to a buyer, when he/she provides negative feedback. Such a possibility might deter buyers from providing negative feedback and

hence result in implicit censorship. This may be avoided by providing reviewer anonymity. According to Tadelis [92], the average positive feedback on eBay is approximately 99.4% because sellers on eBay match the expectations of buyers regarding the product, or positive feedback ratings on eBay may be caused by the fear of retaliation. Li [47] also indicated that the lack of negative feedback is related to a fear of revenge.

In our system, a buyer can buy a product with his/her public identity, and submit a review corresponding to this purchase with another public identity. The SC assures that the buyer provided a hashed key upon committing to the purchase transaction. The buyer then uses a different public key as a reviewer to submit the review. The SC, likewise, requests the secret key (i.e. the origin of the hashed key) from the reviewer upon submitting the review. This process generally aids in upholding the validity of the review and aims to promote the reviewer's anonymity associated with each transaction.

5.1.2 Incentivizing Buyer Feedback

One of the most important components of marketplaces is reputation systems since they increase buyers' confidence and assist them in choosing a suitable seller to make a purchase. Existing systems, on the other hand, do not require users to provide feedback. Users may be discouraged from submitting feedback due to fear of retaliation or a lack of motivation. Avoiding providing feedback by buyers causes frustration on the sellers' side. Hence, sellers sometimes need to contact buyers directly asking them to provide feedback on them or their products.[1] Reviews help potential buyers in choosing reliable sellers and hence are invaluable for the sustenance of the marketplaces. However, this also may be a time-consuming task for the reviewer, and without

[1]The seller asked this question on the eBay forum.[88]

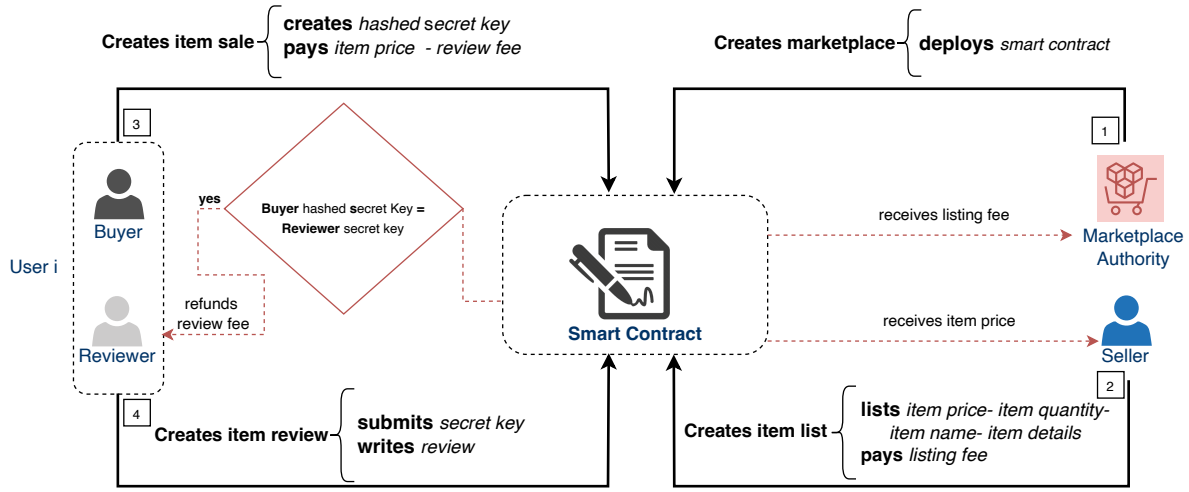

Figure 21. The architecture of the proposed decentralized marketplace

any additional incentives, buyers tend to ignore providing feedback. To encourage users to submit feedback, Simpson [84] recommended rewarding honest reviewers.

In this chapter, we present a novel mechanism to incentivize buyers to provide feedback at each transaction. As part of their transaction, buyers pay a review fee imposed by the SC. The SC will hold the review fee until the feedback is submitted, at which point the fee will be returned to the reviewer. The scheme could be further modified by providing additional financial or other incentives.

5.2 SYSTEM MODELING

Functionally, our system resembles a conventional marketplace, such as Amazon and eBay, where sellers and buyers collaborate to transact business. However, it is entirely decentralized, in contrast to traditional markets. Figure 21 illustrates the proposed system.

In this section, we describe the system definitions, system design, a threat model.

5.2.1 Terminology

Marketplace Authority is an e-commerce business that creates the marketplace. It is the marketplace authority's responsibility to link buyers and sellers in order to enhance sales via a high-quality multi-seller platform. It is responsible for regulating marketplace operations and deploying SCs. In exchange, the marketplace earns a commission on each item listed by the sellers. The sellers and buyers engage in transactions without any direct involvement of the market authority. A **seller** is an entity that makes available any type of goods, services, or financial assets available for purchase. A **buyer** is an entity that accepts a seller's offer and purchases goods, services, or financial assets in exchange for money. A **reviewer** is an entity that, after purchasing a product through the marketplace, provides reviews (feedback) after a transaction is executed. A **transaction** is a media for the exchange of goods, services, or financial assets for money in a financial transaction between two parties. There are three different types of transactions in the proposed marketplace. Listing transactions describe the contractual arrangement in which a seller pays the marketplace authority a fee in exchange for listing a product on the marketplace. Sale transactions describe the exchange of goods and money between buyers and sellers. Review transactions describe the feedback. A review fee must be included with the sale transaction by the buyer. Buyers must submit their review using a different identity in order to receive their review fee back.

5.2.2 System Design

In this section, we describe the functionality of the proposed marketplace. All symbols used in the rest of this chapter are illustrated in Table 5.

Table 5. Variable definitions

Variable	Definition
sc_{add}	Smart contract address
ma_{add}	Marketplace Authority address
$seller_{add}$	Seller address
$buyer_{add}$	Buyer address
$reviewer_{add}$	Reviewer address
$item_c$	Listed items counter
$item_{id}$	Unique number for each item
hs_{key}	Hashed Secrete key
$item_p$	Item price
$item_q$	Item quantity
$item_n$	Item name
$item_d$	Item details
$list_p$	Listing price
$review_f$	Review fee
$item_p$	Item payment
$item_{rev}$	Item review

Creating Marketplace

The marketplace authority first establishes the rules, the fee structure, etc. in the marketplace. It also develops and deploys an SC according to the type types and rules in the marketplace. The market authority's responsibility should be limited to developing and deploying the SC; it should not be used as an excuse to mediate disputes between buyers and sellers during a transaction. As a reliable party, the SC itself will take on this role.

Once the SC has been deployed, the market authority's address ma_{add} will be used to receive listing prices that are sent by sellers. In addition, the SC's address sc_{add} will be used to receive and hold the review fee sent by buyers and transfer it once their feedback is submitted. The SC sets a counter to track the number of listed items in the marketplace $item_c$. This counter is also used to assign an ID to the listed items. Each time a new item is listed, the counter $item_c$ increments, and

its new value is assigned to the listed item as in ID $item_{id}$. In addition, the SC sets the listing price $list_p$ to be paid by the seller and the review fee $review_f$ to be paid by the buyer.

Listing Transactions

In this transaction, the seller creates an item list that includes the marketplace address, item id, item price, item quantity, item name, and item description. The seller submits this list along with their prices $list_p$ to the market authority. The $item_{id}$ is unique for each item that has been added to the marketplace and is generated by the SC. $item_{id}$ to necessary to complete the purchase.

The procedure a seller takes to create an item list is described in Algorithm 1. The following actions are taken by the SC to implement the list creation procedure after the seller creates the item list:

(a) The SC verifies if the seller sent the exact listing price $list_p$.

(b) If the listing price $list_p$ is correct, the SC will check if the item price $item_p$ is greater than zero.

(c) If the $item_p$ is greater than zero, the SC creates the item instance and changes the SC's status.

(d) The SC transfers the listing price $list_p$ from $seller_{add}$ to ma_{add}.

Sale Transactions

Buyers can purchase an item by selecting the item id $item_{id}$ for that item and paying the required price. By exploring the marketplace, picking the item id $item_{id}$ for that item, and making the necessary payment, a buyer can start sales and buy an item. The buyer then enters a one-time

Algorithm 1 Item List

```
1:  procedure CREATEITEMLIST(sc_add,item_p,item_q,item_n,item_d)
2:      seller_add ← msg.sender
3:      if msg.value == list_p then                ▷ Check if the seller sent the exact listing price
4:          if item_p > 0 then          ▷ Check if the seller set a price for the item greater than zero
5:              item_c ← item_c + 1
6:              item[item_c].item_id ← item_c
7:              item[item_c].item_s ← seller_add
8:              item[item_c].item_p ← item_p
9:              item[item_c].item_q ← item_q
10:             item[item_c].item_n ← item_n
11:             item[item_c].item_d ← item_d
12:             List the market item in the marketplace
13:             Transfer the listing price from seller_add to ma_add
14:         else
15:             Show message: Item price cannot be empty
16:     else
17:         Show message: Listing price must be sent
```

hashed secret key and prepares a purchase payment that includes the cost of the item $item_p$ and the review fee $review_f$, and delivers it. She will use the same hashed secret key she has made to submit a review under a new identity after which she will refund the review fee.

To implement item purchases, Algorithm 2 is used. When a buyer triggers the SC after selecting an item, it initiates the item purchase process by following the steps outlined below.

(a) The SC verifies if the buyer sent the exact item price and review fee and the hashed secret key hs_{key}.

(b) If the total value sent is equal to the item price plus the review fee, and the buyer sent the hs_{key}, the SC will do the following:

(1) Transfers the item price to the seller's account

(2) Holds the review fee in the SC account

(3) Store the hashed secret key entered by the user in the item's data

---

Algorithm 2 Item Sale

1: **procedure** CREATEITEMSALE($item_{id}, item_q, hs_{key}$)
2: $buyer_{add} \leftarrow msg.sender$
3: **if** $item[item_{id}].sold_q > 0$ **then**
4: **if** $msg.value == item_p \times item_q + review_f$ and $hs_{key} != null$ **then**
5: Transfer the item price from $buyer_{add}$ to $seller_{add}$
6: Transfer the item review fee from $buyer_{add}$ to sc_{add}
7: $item[item_{id}].sold_q += item_q$
8: $item[item_{id}].hsKey.push(hs_{key})$
9: **else**
10: Show message: Please submit the item price and the review fee to complete the purchase
11: **else** Show message: This item is sold out

Review Transactions

The buyer generates a one-time hashed secret key when she creates a sale transaction. When she decides to submit her review for that specific item, she can utilize it under a new identity.

The review transaction process is described in Algorithm 3. The buyer activates the SC using her hashed secret key with a different identity. The SC begins the process by performing the following actions:

(a) Receives the secret key s_{key} and the review text *Review* from the reviewer.

(b) Generates the hashed secret key *hskey*.

(c) Searches through the stored hashed secret keys of the item.

(d) If it finds a match, the following actions are also performed by the SC:

(1) Generates a new random string and concatenates it with the existing matched hashed secret key and decodes it again.

(2) Replaces the matched stored *hskey* with the generated random string. This process ensures that the seller cannot know what is the original *hskey* of the reviewed items. In addition, this method prevents multi-review attacks.

(3) After replacing the existing hash number, it stores the new hash number and stores the entered review of the item.

(4) Transfers the paid review fee that is stored in the sc_{add} account balance back to the reviewer address.

(e) If no match is found it will show a message to the user that the entered hashed secret key is not registered and revert the transaction.

Algorithm 3 Item Review

```
1:  procedure CREATEITEMREVIEW(s_key,Review)
2:      found ← false
3:      matchInd ← 0
4:      matchKey ← 0
5:      hs_key ← hash(s_key)
6:      for i ← 0 to itemCount do
7:          if item[i+1].sold_q > 0 then
8:              for j ← 0 to len(item[i+1].hsKey) do
9:                  if item[i+1].hsKey[j] == hs_key then
10:                     found ← true
11:                     rnd ← randomString
12:                     newKey ← concatenate(item[i+1].hsKey[j], rnd)
13:                     item[i+1].hsKey[j] ← hash(newKey)
14:                     matchInd ← i+1
15:                     break
16:     if found then
17:         item[matchInd].review.push(Review)
18:         reviewer_add ← msg.sender
19:         item[matchInd].reviewer.push(reviewer_add)
20:         Transfer the review fee back to reviewer_add
21:     else:
22:         Show message: The entered secret key is either not registered, or has been used before.
    Please enter a registered secret key
```

5.3 IMPLEMENTATION

Our SC, which is intended to create an SC on the Ethereum blockchain, was created using Solidity. Remix IDE has been used to develop and test our SC. It is an open-source tool to create Solidity SCs from a desktop IDE or browser. It comes with a number of accounts by default with 100*Ether* as illustrated in Figure 22. To test our SC, we simply utilized the first four accounts.

The marketplace authority, sellers, buyers, and reviewers are the four primary participants in our SC. Every individual has a different account. First, we must use the Remix compiler to translate

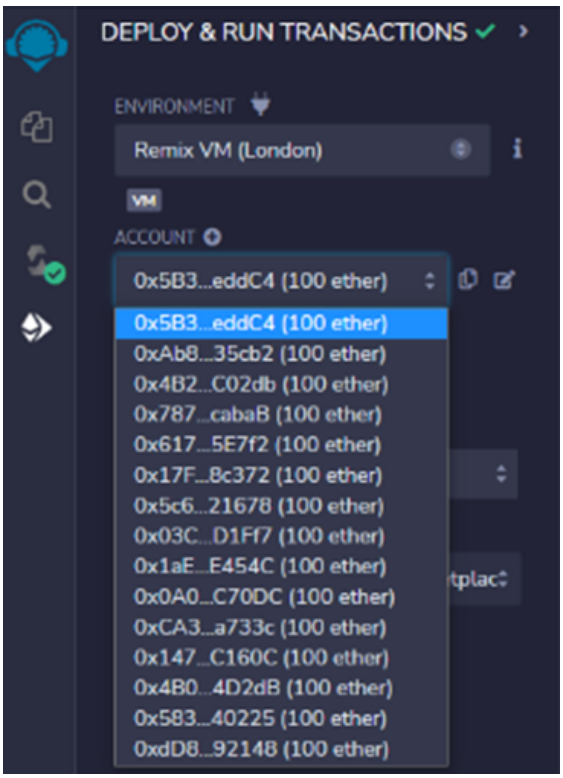

Figure 22. Default addresses provided by Remix IDE

the code into bytecode for the Ethereum virtual machine (EVM). Following that, we receive byte code and an ABI (application binary interface) that lets us communicate with the features of the SC.

The marketplace owner will first deploy the SC. Then, the seller starts to list her items as described in Algorithm1. The buyer, using her account mentioned above, starts to create sales using algorithm 2. Then, the buyer, to hide her identity, will use another account (we call it a reviewer account), which is mentioned above to write her feedback and then refund her review fee using algorithm3.

5.4 RESULTS

In this section, we provide examples of how the SC participants communicate with one another and how all functions are performed properly. We tested our SC using Remix IDE. To guarantee that the logic and state of the SC perform properly, all functions are tested. We are using the account addresses in the table 6 for all the participants, the marketplace authority, the seller, the buyer, and the reviewer.

Table 6. Users account addresses

User Role	User Address
Marketplace	0x5B38Da6a701c568545dCfcB03FcB875f56beddC4
Seller	0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2
Buyer 1	0x4B20993Bc481177ec7E8f571ceCaE8A9e22C02db
Buyer 2	0x78731D3Ca6b7E34aC0F824c42a7cC18A495cabaB
Buyer 3	0x617F2E2fD72FD9D5503197092aC168c91465E7f2
Buyer 4	0x17F6AD8Ef982297579C203069C1DbfFE4348c372
Reviewer 1	0x1aE0EA34a72D944a8C7603FfB3eC30a6669E454C
Reviewer 2	0x0A098Eda01Ce92ff4A4CCb7A4fFFb5A43EBC70DC
Reviewer 3	0x5c6B0f7Bf3E7ce046039Bd8FABdfD3f9F5021678
Reviewer 4	0x03C6FcED478cBbC9a4FAB34eF9f40767739D1Ff7

Each function is carried out in a specific manner in accordance with SC logic. For testing purposes, our marketplace contains one seller, four buyers, and four reviewers. Each one of them has her own account, as shown in Table 6.

Figure 23 shows all functions are executed successfully and all events were triggered and the console log will show the following messages: For creating an item list: *"Your item has been listed and the marketplace authority has received the listing price!"*; For the item sale *"Item purchase has been completed !"*; For creating item review *"Item review has been added and the review fee has been returned to the reviewer !"*.

Figure 23. Logs showing the performance of SC participants and the executed functions

All four buyers' transactions and all four reviewers' transactions include the following processes: when the seller creates an item list, the *msg.sendr* is assigned to the $seller_{add}$, and the $list_p$ is assigned to the *msg.value* (lines 2-3 in algorithm 1). The marketplace authority received the $list_p$. After the seller performed the transaction, and for testing purposes, the $list_p$ is $2ETH$. When the buyer performs her transaction to buy an item, the *msg.sendr* assigned to the $buyer_{add}$ and the $item_p$, and $review_f$ in one- time payment will be assigned to the *msg.value* (lines 2-3 in algorithm 2). As shown in (lines 3-4 of algorithm 2), the $item_p$ and $review_f$ will be calculated. The seller will

receive his payment after the buyer completes her transaction, and the SC will hold the $review_f$ in sc_{add}. Figure 24 shows the SC holds the $review_f$ for all buyers, waiting for their reviews to be submitted.

Figure 24. A screenshot showing the SC account holds buyers $reviews_f$.

Finlay, the reviewer, starts to initiate her transaction by submitting her review with her hs_{Key} that she created using her identity as a buyer. The SC will check on the hs_{key} she provided, and refund her the $review_f$ as shown in algorithm 3. Figure 25 shows the participant accounts have

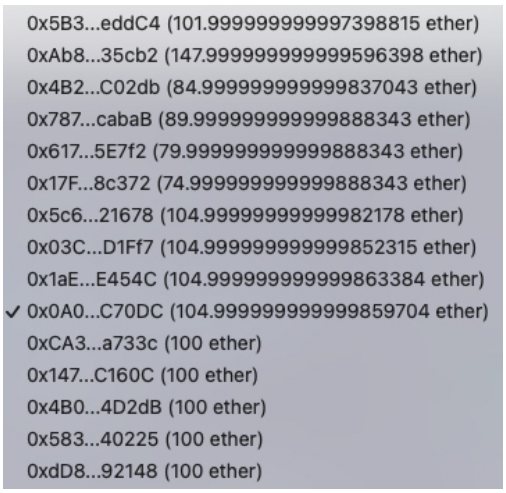

Figure 25. Participants' balance after all transactions occurred.

been changed after all transactions occurred. The seller was paid in full, the buyers purchased items, and they returned their review fees using their other identities.

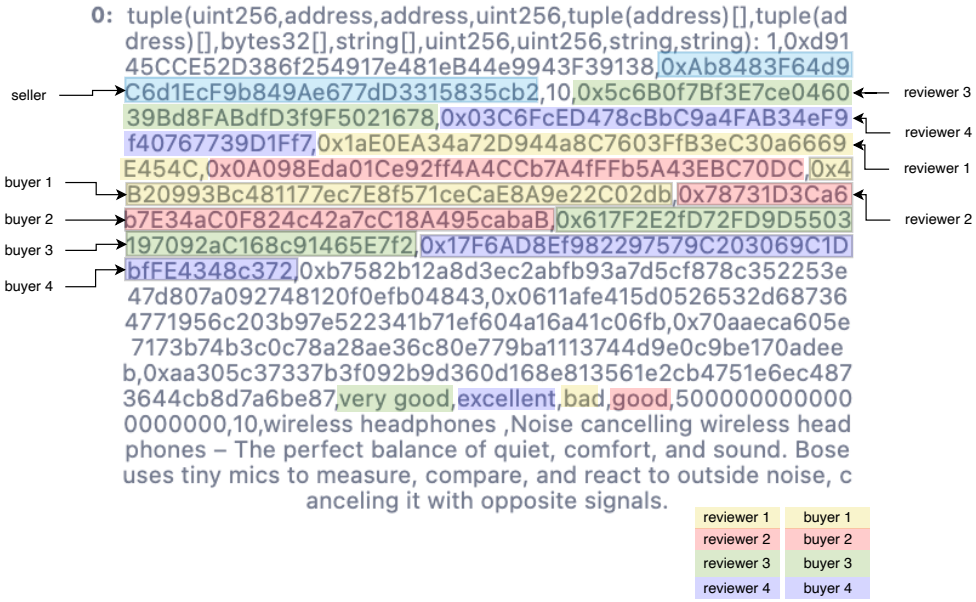

Figure 26. A screenshot shows the output of the marketplace transactions.

Figure 26 provides a thorough representation of the output of the market made possible by the usage of the *GetMarketItem* method. This particular function has been specifically constructed to have the ability to gather and retrieve all market items that users have generated and uploaded to the marketplace, providing a thorough picture of the items now in circulation.

We have added a special color-coding scheme to the representation to improve clarity and make it easier to use. This means giving each participant in the market a unique and independent color. This visual differentiation serves two purposes: first, it makes it easier to quickly and accurately identify certain users and the activities that go along with them; and second, it makes it simpler

to track and monitor user interactions in the marketplace. Thus, it is much easier for the reader to understand and interpret the figure because they can quickly tell which market products belong to which users.

5.5 SUMMARY

In this chapter, we propose and prototype a review system specifically designed to operate well in a completely decentralized marketplace. Our system allows buyers to employ multiple identities while submitting their reviews to promote trust. We outline blockchain technology and SCs' role in the marketplace, provide motivating instances from everyday life, offer a unique technique to ensure that buyers leave feedback, and show a detailed prototype using REMIX IDE.

CHAPTER 6

TOWARDS TRUST AND REPUTATION AS A SERVICE IN SOCIETY 5.0

In this chapter, our goal is to answer the following research question: **RQ4:** How do SCs within blockchain-based trust and reputation services specifically address and improve quality in buyer feedback in decentralized marketplaces, and what impact does this have on transaction reliability?

We begin by outlining the key properties and characteristics that our system aims to achieve in Section 6.1. Following this, Section 6.2 presents a detailed model of our system, including its architecture and operational mechanics. Section 6.3 shows how the trust measure introduced in Section 6.2 is updated over time. Section 6.4 illustrates three applications of the trust and reputation service introduced in Section 6.2. Section 6.5 aims to present the results of our empirical evaluation of the trust and reputation service discussed analytically in Sections 6.2 – 6.4. Finally, section 6.6 provides a summary of the chapter, highlighting the main findings and their implications for the field.

6.1 SYSTEM OVERVIEW

If a reputation system is to be successful, several conditions must be satisfied: first, the decentralized marketplace must collect, aggregate, and disseminate seller reputation scores accurately and in a timely manner; second, buyers provide truthful feedback of their buying experience; and, third, buyers base the choice of their future transaction partners (i.e. sellers) solely on reputation scores.

The first and third conditions are relatively easy to enforce or to incentivize. The second con-

dition is far more problematic. It has been argued that if buyers consistently provide truthful feedback, isolated interactions between buyers and sellers take on attributes of long-term relationships and, as a result, the reputation scores tallied by the marketplace become a high-quality substitute of community-based reputation [76].

In this work, we assume a blockchain-based marketplace similar to [22], [43], [70], [89], [96], [104], where the transactions between buyers and sellers are maintained as individual blocks that, once added to the blockchain, keep immutable information about the transaction. We maintain statistical information about the buyers' and sellers' performance as part of the blockchain.

6.2 SYSTEM MODELING

The main goal of this section is to introduce our trust and reputation service.

6.2.1 Terminology and Definitions

Consider a decentralized marketplace and a new seller S who just joined the marketplace at time 0. We associate with the seller an urn containing an unknown number, N, of balls and an unknown composition in terms of the number of black balls it contains. The intention is for the urn of unknown composition to represent the total number of transactions in which seller S will be involved during her career in the marketplace. Each transaction in which seller S is involved is associated with a ball extracted from the urn *without replacement*. If the extracted ball is black, we say that the seller has fulfilled her obligations in the corresponding transaction. The motivation for this is that every time a ball is extracted from the urn without replacement, the probability of obtaining a black ball on the next extraction changes. This is intended to capture, to some extent, the uncertainties and vagaries of seller behavior.

We define the *reputation score* of the seller at time t as an ordered triple whose first and second components are, respectively, the total number of transactions in which the seller was involved up to time t and the number of transactions in which the seller has fulfilled her contractual obligations up to time t. The third component is $(0,t)$ or, simply, t if no confusion can arise. Thus, initially, the seller's reputation score is $(0,0,0)$.

Let I be the random variable denoting the *initial* number of black balls in the urn. Let $H_i = \{I = i\},\ (0 \leq i \leq N)$, be the *hypothesis* that the initial composition of the urn is $(i, N-i)$, in other words, the urn initially contains i black balls, while the remaining $N-i$ balls have other colors.

Since nothing is known *à priori* about the past history, skill level, and integrity profile of the seller, it makes sense to assume, as an *initial prior*, that all compositions of the urn are equiprobable (see [28] for a good discussion) and so

$$\Pr[H_i] = \frac{1}{N+1}. \tag{10}$$

We define $\rho_S(0,t)$, the *trust measure* in seller S at time t, to be the probability that the seller will fulfill her contractual obligations on the next transaction following t. In terms of the underlying urn, this means that the next ball extracted from the urn is black. For example, let B_0 be the event that on the very *first* transaction the seller will fulfill her contractual obligations. Equivalently, B_0 is the event that, on the first extraction a black ball will appear. For reasons that will become clear

later we write $\rho_S(0,0)$ for $\Pr[B_0]$. We can write

$$\begin{aligned}
\rho_S(0,0) &= \Pr[B_0] \\
&= \sum_{i=0}^{N} \Pr[B_0|H_i]\Pr[H_i] \\
&= \frac{1}{N+1}\sum_{i=0}^{N}\frac{i}{N} \quad \text{[by (10)]} \\
&= \frac{1}{N(N+1)}\sum_{i=0}^{N} i \\
&= \frac{1}{N(N+1)}\frac{N(N+1)}{2} = \frac{1}{2}, \qquad (11)
\end{aligned}$$

which makes intuitive sense, since we have no à priori knowledge of the seller's past behavior in the marketplace and, therefore, the trust we place in her is $\frac{1}{2}$.

6.2.2 Updating the Prior

Now, suppose that our seller has accumulated, in the time interval $[0,t]$, a reputation score of (n,k,t). Recall that this means that out of a total of n transactions in which the seller was involved up to time t, she has fulfilled her obligations in k of them. Equivalently, this says that from the urn mentioned above, a sample of n balls was extracted *without replacement* and that k of them were observed to be black.

In order to update the trust measure in our seller, we need to update our belief in the original composition of the associated urn. For this purpose, let A be the event that in a sample of n balls extracted without replacement from the urn, k black balls were observed. Once the event A is known, we update the prior in a Bayesian fashion by setting

$$
\begin{aligned}
& \Pr[H_i|n,k] = \Pr[H_i|A] = \frac{\Pr[H_i \cap A]}{\Pr[A]} \\
= & \frac{\Pr[A|H_i]\Pr[H_i]}{\sum_{j=0}^{N}\Pr[A|H_j]\Pr[H_j]} \\
= & \frac{\Pr[A|H_i]}{\sum_{j=0}^{N}\Pr[A|H_j]} \text{ [by (10)]} \\
= & \frac{\frac{\binom{i}{k}\binom{N-i}{n-k}}{\binom{N}{n}}}{\sum_{j=0}^{N}\frac{\binom{j}{k}\binom{N-j}{n-k}}{\binom{N}{n}}} = \frac{\binom{i}{k}\binom{N-i}{n-k}}{\sum_{j=0}^{N}\binom{j}{k}\binom{N-j}{n-k}} \\
= & \frac{\binom{i}{k}\binom{N-i}{n-k}}{\binom{N+1}{n+1}} \text{ [by (31) in Appendix A.]} \qquad (12)
\end{aligned}
$$

To summarize, the expression of the updated prior $\Pr[H_i|n,k]$ reflects our updated belief in the *initial* composition of the urn, as a result of seeing k black balls out of n balls extracted. In terms of our seller, upon seeing that the seller has fulfilled her obligations in k out of the first n transactions, we update the perceived intrinsic performance profile of our seller. At the risk of mild confusion, we continue to write $\Pr[H_i]$ for the updated prior, instead of more cumbersome $\Pr[H_i|n,k]$.

6.2.3 Modeling the Trust Measure

Recall that we define a seller's (subjective) trust measure, $\rho_S(0,t)$, at time t as the probability of the event that on the next transaction the seller will fulfill her contractual obligations.

Theorem 1. *Assuming that seller S has accumulated, in the interval* $(0,t)$*, a reputation score of* (n,k,t)*, the trust measure in S at time t is*

$$\rho_S(0,t) = \frac{k+1}{n+2}.$$

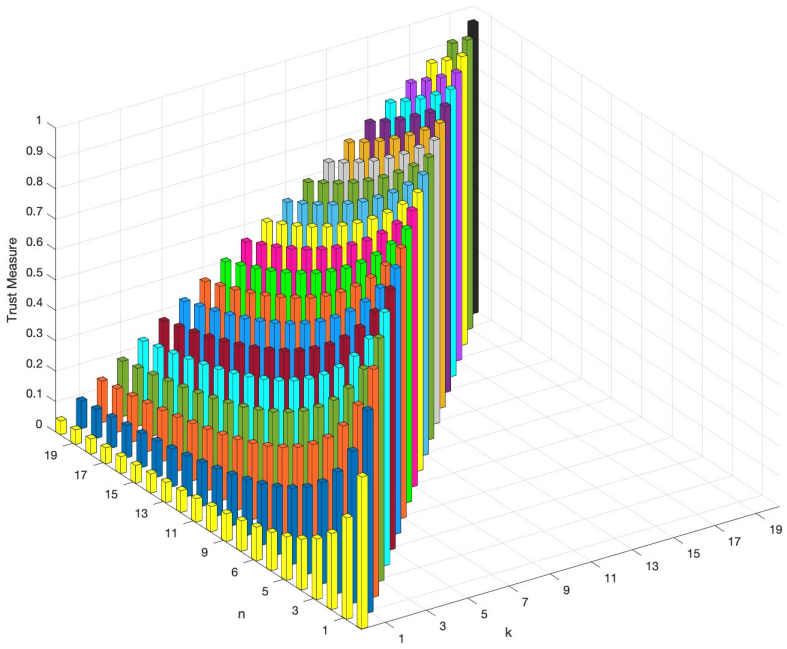

Figure 27. Illustrating $\rho_S(0,t)$ for small values of n and k.

Proof. Consider the urn associated with seller S and assume that out of the urn a sample of n balls was extracted and k of them were observed to be black. Let B be the event that the next ball extracted from the urn is black. In terms of our marketplace, $\Pr[B]$ is precisely $\rho_S(0,t)$. By the Law of Total Probability,

$$\Pr[B] = \sum_{i=0}^{N} \Pr[B|H_i] \Pr[H_i]. \tag{13}$$

Observe that $\Pr[B|H_i] = \frac{i-k}{N-n}$ and recall that, by (12), $\Pr[H_i] = \frac{\binom{i}{k}\binom{N-i}{n-k}}{\binom{N+1}{n+1}}$.

With this, (13) can be written as

$$\begin{aligned}
\rho_S(0,t) = \Pr[B] &= \sum_{i=0}^{N} \frac{i-k}{N-n} \frac{\binom{i}{k}\binom{N-i}{n-k}}{\binom{N+1}{n+1}} \\
&= \frac{\sum_{i=0}^{N}(i-k)\cdot \frac{i!}{k!(i-k)!}\binom{N-i}{n-k}}{(N-n)\frac{(N+1)!}{(n+1)!(N-n)!}} \\
&= \sum_{i=0}^{N} \frac{(k+1)\binom{i}{k+1}\binom{N-i}{n-k}}{(N+1)\binom{N}{n+1}} \\
&= \frac{k+1}{N+1} \sum_{i=0}^{N} \frac{\binom{i}{k+1}\binom{N-i}{n-k}}{\binom{N}{n+1}} \\
&= \frac{k+1}{N+1} \frac{\binom{N+1}{n+2}}{\binom{N}{n+1}} \quad \text{[by (31)]} \\
&= \frac{k+1}{n+2},
\end{aligned}$$

and the proof of Theorem 1 is complete. □

Somewhat surprisingly, the expression of the trust measure is independent of N and depends only on n and k. It is very important to note that the expression of the trust measure specified in Theorem 1 is very easy to remember and to compute. Specifically, if a certain seller has accumulated a reputation score (n,k,t), evaluating the corresponding trust measure in the seller at time t is very simple. This is one of the significant advantages of our trust and reputation service.

To summarize this discussion, we refer the reader to Figure 27 illustrating the trust measure $\rho_S(0,t)$ for small values of n and k. For a better visual efect, the values of $\rho_S(0,t)$ for different values of k are depicted in different colors. Figure 27 also reveals that $\rho_S(0,0) = \frac{1}{2}$, as we found in (11).

6.3 UPDATING THE TRUST MEASURE

The main goal of this section is to show how the trust measure introduced in Section 6.2 is updated over time.

Theorem 2. *Assume that in the time interval $(0,t]$, seller S was involved in n transactions and that she has fulfilled her contractual obligations in k of them. If in the time interval $(t,t']$ seller S is involved in n' additional transactions and that she fulfills her contractual obligations in k' of them, then the seller's trust measure, $\rho_S(0,t')$, at time t' is*

$$\rho_S(0,t') = \frac{k+k'+1}{n+n'+2}. \tag{14}$$

Proof. Let A' be the event that in a subsequent sample of size n', k' balls were observed to be black. Once the event A' is known to have occurred, it is necessary to update our prior. Proceeding, in a Bayesian fashion, we write

$$\begin{aligned} \Pr[H_i|n,k,n',k'] &= \Pr[H_i|A'] = \frac{\Pr[H_i \cap A']}{\Pr[A']} \\ &= \frac{\Pr[A'|H_i]\Pr[H_i]}{\sum_{j=0}^{N}\Pr[A'|H_j]\Pr[H_j]}. \end{aligned} \tag{15}$$

Notice that

- by (12), $\Pr[H_i] = \frac{\binom{i}{k}\binom{N-i}{n-k}}{\binom{N+1}{n+1}}$; and,
- $\Pr[A'|H_i] = \frac{\binom{i-k}{k'}\binom{N-i-(n-k)}{n'-k'}}{\binom{N-n}{n'}}$;
- by the Law of Total Probability $\Pr[A'] = \sum_{j=0}^{N}\Pr[A'|H_j]\Pr[H_j]$;

- by (35) in Appendix A.0.1,

$$\Pr[A'] = \sum_{j=0}^{N} \Pr[A'|H_j]\Pr[H_j] = \frac{\binom{k+k'}{k}\binom{n-k+n'-k'}{n-k}}{\binom{n+n'+1}{n+1}},$$

Consequently, equation (15) becomes

$$\Pr[H_i] = \Pr[H_i|n,k,n',k'] = \frac{\binom{i}{k+k'}\binom{N-i}{n-k+n'-k'}}{\binom{N+1}{n+n'+1}}. \tag{16}$$

As before, in order to simplify notation, we continue to refer to $\Pr[H_i|n,k,n',k']$ as $\Pr[H_i]$. The expression of the prior $\Pr[H_i]$ in (16) reflects our updated belief in the composition of the urn, as a result of seeing k' black balls out of n' balls in the second sample extracted.

Let B' be the event that the next ball extracted from the urn is black. In terms of our marketplace, $\Pr[B']$ is $\rho_S(0,t')$.

$$\begin{aligned}
\Pr[B'] &= \sum_{i=0}^{N} \Pr[B'|H_i]\Pr[H_i] \\
&= \sum_{i=0}^{N} \frac{i-k-k'}{N-n-n'} \frac{\binom{i}{k+k'}\binom{N-i}{n-k+n'-k}}{\binom{N+1}{n+n'+1}} \\
&= \frac{1}{(N-n-n')\binom{N+1}{n+n'+1}} \sum_{i=0}^{N} (i-k-k') \cdot \frac{i!}{(k+k')!(i-(k+k'))!} \binom{N-i}{n-k+n'-k} \\
&= \frac{k+k'+1}{(N-n-n')\binom{N+1}{n+n'+1}} \sum_{i=0}^{N} \binom{i}{k+k'+1} \binom{N-i}{n-k+n'-k} \\
&= \frac{k+k'+1}{(N-n-n')\binom{N+1}{n+n'+1}} \binom{N+1}{n+n'+2} \\
&= \frac{k+k'+1}{n+n'+2}.
\end{aligned} \tag{17}$$

□

Notice that, in spite of the laborious derivation, the final result is extremely simple and *easy* to compute. This is a definite advantage of our scheme.

An interesting question is to determine under what conditions the trust measure $\rho_S(0,t')$ is at least as large as $\rho_S(0,t)$. The answer to this question is provided by the following result.

Lemma 3.

$$\rho_S(0,t') \geq \rho_S(0,t) \iff \frac{k'}{n'} \geq \frac{k+1}{n+2}.$$

Proof. Follows by Lemma 7 in the Appendix with $a = k+1$, $b = n+2$, $a' = k'$ and $b' = n'$. □

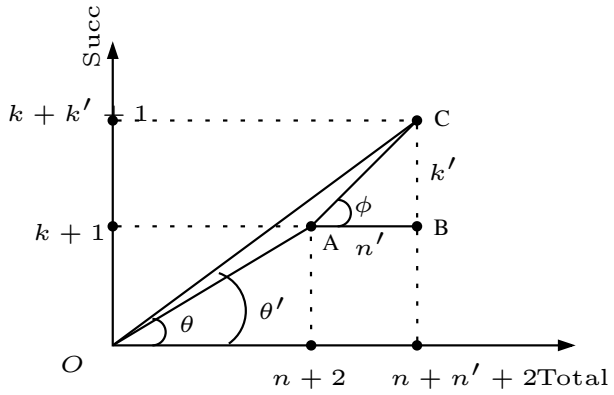

Figure 28. A geometric interpretation of Lemma 3.

Refer to Figure 28 for a geometric illustration of Lemma 3. Consider a two-dimensional coordinate system where the horizontal and vertical axes capture, respectively, the total number of transactions and the number of transactions in which the seller has fulfilled her contractual obligations. Consider, further, the points A, B, C of coordinates $(n+2, k+1)$, $(n+n'+2, k+1)$, $(n+$

$n'+2, k+k'+1)$. It is easy to see that $\rho_S(0,t) = \tan\theta = \frac{k+1}{n+2}$, and $\rho_S(0,t') = \tan\theta' = \frac{k+k'+1}{n+n'+2}$. Finally, is is easy to confirm that $\rho_S(0,t') \geq \rho_S(0,t)$ if and only if the angle ϕ determined by the sides AB and AC of the triangle determined by the points A, B, C satisfies $\frac{k'}{n'} = \tan\phi \geq \tan\theta = \frac{k+1}{n+2}$, exactly as claimed in Lemma 3.

Theorem 2 can be readily generalized.

Theorem 4. *For an arbitrary positive integer r, consider r successive time epochs* $(t_0,t_1]$, $(t_1,t_2]$, $\cdots$, $(t_{i-1},t_i]$, $\cdots$, $(t_{r-1},t_r]$, *such that in epoch* $(t_{i-1},t_i]$, $(1 \leq i \leq r)$, *our seller was involved in* n_i *transactions and has fulfilled her contractual obligations in* k_i *of them. Then the seller's reputation score at time* t_r *is* $(\sum_{i=1}^r n_i, \sum_{i=1}^r k_i, (t_0,t_r))$ *and her associated trust measure is*

$$\rho_S(0,t_r) = \frac{\sum_{i=1}^r k_i + 1}{\sum_{i=1}^r n_i + 2}. \tag{18}$$

Proof. Assume, without loss of generality, that $t_0 = 0$ and let t and t' denote, respectively, t_{r-1} and t_r. In the time interval $(0,t]$ the seller was involved in $\sum_{i=1}^{r-1} n_i$ transactions and has fulfilled her obligations in $\sum_{i=1}^{r-1} k_i$ of them. In the time interval $(t,t']$ our seller was involved in n_r transactions and has fulfilled her contractual obligations in k_r of them.

By definition, in the interval $(0,t']$, the seller's reputation score is $(\sum_{i=1}^r n_i, \sum_{i=1}^r k_i, (t_0,t_r))$. Similarly, by Theorem 2 her trust measure is

$$\begin{aligned} \rho_S(0,t_r) &= \frac{k+k'+1}{n+n'+2} \\ &= \frac{(\sum_{i=1}^{r-1} k_i) + k_r + 1}{(\sum_{i=1}^{r-1} n_i) + n_r + 2} \\ &= \frac{\sum_{i=1}^r k_i + 1}{\sum_{i=1}^r n_i + 2}, \end{aligned}$$

and the proof of Theorem 4 is complete. □

Theorem 4 has a number of consequences:

- the updated trust measure is related to the updated reputation scores, exactly as specified in Theorem 1;
- the updated trust measure does not change if
  - **Associativity:** the seller has fulfilled her obligations in 0 of the first $\sum_{i=1}^{r-1} n_i$ transactions and in $\sum_{i=1}^{r} k_i$ out of the next n_r transactions, provided $\sum_{i=1}^{r} k_i \leq n_r$.
  - **Commutativity:** for any choice of subscripts i, j, with $(1 \leq i \neq j \leq r)$, the n_j transactions in epoch j have occurred before or after the n_i transactions in epoch i;
  - **Interchangeability:** the seller has fulfilled her obligation in k_j of the n_i transactions in epoch i and in k_i of the transactions in epoch j, provided that $k_j \leq n_i$ and $k_i \leq n_j$.

6.4 APPLICATIONS OF THE LAPLACE TRUST ENGINE

The main goal of this section is to illustrate three applications of the trust and reputation service introduced in Section 6.2. Specifically, in Sections 6.4.1 and 6.4.2 we discuss two applications to a multi-segment marketplace, where a malicious seller may establish a stellar reputation by selling cheap items or by providing some specific type of service, only to use their reputation score to defraud buyers in a different market segment.

Next, in Section 6.4.3, we apply the results of Section 6.2 in the context of sellers with time-varying performance due to, say, overcoming an initial learning curve. With this in mind, we provide a discounting scheme, wherein older reputation scores are given less weight than more

recent ones. Finally, in Section 6.4.4 we show how to predict trust and reputation scores far in the future, based on currently available information.

6.4.1 Price-Range Specific Trust and Reputation

We assume that the transactions in the marketplace are partitioned, by monetary value of the goods transacted, into non-overlapping price ranges $0 < R_1 < R_2 < \cdots < R_s$ for some positive integer s. These ranges determine *s market segments* $M_1, M_2, \cdots, M_s$ where market segment M_j involves all the transactions within the price range R_j.

In all marketplaces of which we are aware [4], [13], [27], [32], [39], [43], [70], [89], [94], [96], seller reputation is *global*, being established irrespective of their performance in different market segments.

However, this may lead to insecurities. For example, imagine a seller who has established an enviable reputation score by selling cheap items, all in the market segment corresponding to range R_1. Suppose that our seller decides to get involved in a different market segment, say corresponding to price range R_{10}. Should her reputation score established in R_1 carry over to R_{10}? We believe that the answer should be in the negative. One reason is that, as pointed out by [41] and other workers, dishonest sellers establish stellar reputation scores by selling cheap items and use the resulting reputation score to *hit-and-run* in a different market segment.

To prevent this kind of attack from being mounted, we associate with each market segment a distinct reputation score and, consequently, a distinct trust measure. Also, with each market segment, we associate a *different* urn as discussed in the previous sections of this work. For example, if our seller has never transacted in the market segment corresponding to the price range R_{10}, her reputation score in that market segment is $(0,0,t)$ and, not surprisingly, her corresponding trust

measure will be $\frac{0+1}{0+2} = \frac{1}{2} = 50\%$, capturing the idea that nothing is known about the performance of the seller in that market segment.

Consider a generic market segment M_i, $(1 \leq i \leq s)$, and assume that up to time t, our seller has accumulated a reputation score of (n_i, k_i, t) in R_i. Consistent with our definition, the trust measure that our seller enjoys in M_i is $\frac{k_i+1}{n_i+2}$. This trust measure is *local* to M_i and is independent of the seller's trust measure in other market segments.

It is worth noting that, as an additional benefit, our approach provides *resistance* to Sybil attacks. It is well known that malicious users involve their Sybils in augmenting their reputation scores [19], [60], [79], [90]. However, the fact that by assumption SCs are responsible for providing transaction feedback (including the market segment in which the transaction took place), this feedback will be, per force, local to one market segment, minimizing the effect of the attack. Indeed, as a result of the Sybil attack, the malicious user's reputation may well increase in one market segment, her reputation in other market segments will not be affected. This provides for very desirable resistance to Sybil attacks.

6.4.2 Service-Specific Trust and Reputation

In Section 6.4.1 we argued that reputation scores and, therefore, the trust measure of a seller should not be global but should, instead, be specific to individual price ranges. Specifically, we made the point that reputation scores acquired by doing business in one market segment (by dollar amount) should not carry over to a different market segment.

In this Section we extend the same idea to the types of services provided. The intuition is that a service provider (i.e. seller) may behave differently when providing different services. Thus, the best indicator of how the service provider will perform in the future depends on their past

performance in the context of the type of services contemplated. This motivates assessing the trustworthiness of a service provider by the type of individual service of interest.

As an illustrative example, consider a plumbing contractor who may act in the marketplace as a seller of plumbing hardware, but also as a provider of plumbing services such as repairs, installation of various equipment such as gas furnaces, electric furnaces, hot water heaters, extended maintenance contracts, etc.

Our plumber may be inclined to provide higher quality services in areas that benefit him most (e.g. installing electric water heaters) and of lesser quality in some other areas that are less lucrative, e.g. maintenance contracts or installing gas water heaters), even though an electric water heater may cost roughly the same as a gas water heater.

The point is that the plumber's reputation score acquired by providing one type of service should not be relevant when evaluating his/her trustworthiness in different service categories where he/she is either less competent or simply not interested in providing high quality services.

6.4.3 Discounting Old Trust Measures -- Levelling the Playing Field

Up to this point we have assumed that seller behavior is constant over time. For various reasons, sellers may well change their attitude and behave differently from the way they acted in the past. To accommodate this imponderable, in this Section we introduce a simple mechanism that allows us to discount older trust measures, giving more credence to recent reputation scores.

For an arbitrary integer r, consider r successive time epochs $(t_0,t_1]$, $(t_1,t_2]$, $\cdots$, $(t_{i-1},t_i]$, $\cdots$, $(t_{r-1},t_r]$ with $t_0 = 0$ and such that in epoch $(t_{i-1},t_i]$, $(1 \leq i \leq r)$, our seller was involved in n_i transactions and has fulfilled her contractual obligations in k_i of them. Recall that, given this information, the seller's reputation score at time t_r is $(\sum_{i=1}^{r} n_i, \sum_{i=1}^{r} k_i, (t_0,t_r))$, and, by Theorem 4,

her associated trust measure reads

$$\rho_S(0,t_r) = \frac{\sum_{i=1}^{r} k_i + 1}{\sum_{i=1}^{r} n_i + 2}. \tag{19}$$

In order to produce a weighted version of (19), consider weights $\lambda_1,\ \lambda_2,\ \cdots, \lambda_r$ such that each $\lambda_i,\ (1 \leq i \leq r)$, is either 0 or 1. Consider, further the weighted trust measure $\overline{\rho}_S(0,t_r)$, of S defined as

$$\overline{\rho}_S(0,t_r) = \frac{\sum_{i=1}^{r} \lambda_i k_i + 1}{\sum_{i=1}^{r} \lambda_i n_i + 2}. \tag{20}$$

Suppose that our seller was facing serious problems related to a steep learning curve, and her reputation scores in the first $i,\ (1 \leq i \leq r-1)$, transactions $(\sum_{j=1}^{i} k_j, \sum_{j=1}^{i} n_j, t_r)$, were very poor, in the sense that

$$\frac{\sum_{j=1}^{i} k_j}{\sum_{j=1}^{i} n_j} < \frac{\sum_{j=1}^{r} k_i + 1}{\sum_{j=1}^{r} n_i + 2} \tag{21}$$

To accommodate the seller, and to level the playing field, in the weighted version of her trust measure we take the weights:

$$\lambda_1 = \lambda_2 = \cdots = \lambda_i = 0$$

and

$$\lambda_{1+1} = \lambda_{i+2} = \cdots = \lambda_r = 1.$$

With these weights, the seller's weighted trust measure at time t_r is

$$\overline{\rho}_S(0,t_r) = \frac{\sum_{j=i+1}^{r} k_j + 1}{\sum_{j=i+1i}^{r} n_j + 2}.$$

Notice that by taking $a = \sum_{j=1}^{i} k_j$, $b = \sum_{j=1}^{i} n_j$, $a' = \sum_{j=i+1}^{r} k_j + 1$ and $b' = \sum_{j=i+1}^{r} n_j + 2$, Corollary 8 in the Appendix guarantees that

$$\rho_S(0,t_r) = \frac{\sum_{i=1}^{r} k_i + 1}{\sum_{i=1}^{r} n_i + 2} < \frac{\sum_{j=i+1}^{r} k_j + 1}{\sum_{j=i+1}^{r} n_j + 2} = \overline{\rho}_S(0,t_r).$$

In other words, as a result of discounting the first i transactions, the seller's weighted trust measure has increased, focusing attention on her more recent performance.

6.4.4 Predicting Trust Measure and Reputation Scores Over the Long Term

It is of great theoretical interest and practical relevance to be able to extrapolate the performance of a seller and predict her performance, far in the future. With this in mind, consider a seller that has completed n transactions and has fulfilled her obligations in k of them. Let A be the corresponding event. We wish to predict the *expected* reputation score of the seller by the time her total number of transactions has reached $n+m$ for some $m \geq 0$.

Let R be the random variable that keeps track of the number of black balls among the additional m balls extracted, and assume that the event $\{R = r\}$ has occurred.

Using the expression of H_i from (12), the conditional probability of the event $\{R = r\}$ given A is

$$\begin{aligned} \Pr[R = r|A] &= \sum_{i=0}^{N} \Pr[R = r|H_i] \Pr[H_i] \\ &= \frac{\binom{k+r}{k}\binom{n-k+m-r}{n-k}}{\binom{n+m+1}{n+1}}. \end{aligned} \tag{22}$$

Actually, this follows directly from (35) in Section A.0.1 of the Appendix by taking $r = k'$ and

$m = n'$.

We are interested in evaluating the *conditional expectation*, $E[R|A]$, of R given A. For this purpose, using the Law of Total Expectation, we write

$$
\begin{aligned}
E[R|A] &= \sum_{r=0}^{m} r \Pr[R = r|A] \\
&= \sum_{r=0}^{m} r \cdot \frac{\binom{k+r}{k}\binom{n-k+m-r}{n-k}}{\binom{n+m+1}{n+1}} \quad \text{[By (22)]} \\
&= \sum_{r=0}^{m} [(k+r+1)-(k+1)] \cdot \frac{\binom{k+r}{k}\binom{n-k+m-r}{n-k}}{\binom{n+m+1}{n+1}} \\
&= \sum_{r=0}^{m} (k+r+1) \frac{\binom{k+r}{k}\binom{n-k+m-r}{n-k}}{\binom{n+m+1}{n+1}} \\
&- \sum_{r=0}^{m} (k+1) \frac{\binom{k+r}{k}\binom{n-k+m-r}{n-k}}{\binom{n+m+1}{n+1}} \\
&= \sum_{r=0}^{m} (k+r+1) \frac{\binom{k+r}{k}\binom{n-k+m-r}{n-k}}{\binom{n+m+1}{n+1}} \qquad (23) \\
&- (k+1) \sum_{r=0}^{m} \frac{\binom{k+r}{k}\binom{n-k+m-r}{n-k}}{\binom{n+m+1}{n+1}}. \qquad (24)
\end{aligned}
$$

The two sums, (23) and (24), will be evaluated separately. We begin by evaluating the following sum:

$$
\begin{aligned}
\sum_{r=0}^{m} \frac{\binom{k+r}{k}\binom{n-k+m-r}{n-k}}{\binom{n+m+1}{n+1}} &= \frac{\sum_{r=0}^{m} \binom{k+r}{k}\binom{n-k+m-r}{n-k}}{\binom{n+m+1}{n+1}} \\
&= \frac{\binom{n+m+1}{n+1}}{\binom{n+m+1}{n+1}} = 1 \quad \text{[by (31) in Appendix A]}.
\end{aligned}
$$

This implies that the second sum, (24), evaluates to $k+1$.

Next, to evaluate the first sum, (23), we notice that

$$\begin{aligned}(k+r+1)\binom{k+r}{k} &= \tfrac{k+1}{k+1}(k+r+1)\tfrac{(k+r)!}{k!r!} \\ &= (k+1)\tfrac{(k+r+1)!}{(k+1)!r!} \\ &= (k+1)\tbinom{k+r+1}{k+1}. \end{aligned} \tag{25}$$

Using (25), the first sum, (23) can be written as

$$\begin{aligned}&\textstyle\sum_{r=0}^{m}(k+r+1)\frac{\binom{k+r}{k}\binom{n-k+m-r}{n-k}}{\binom{n+m+1}{n+1}} \\ &= \tfrac{k+1}{\binom{n+m+1}{n+1}}\textstyle\sum_{r=0}^{m}\tbinom{k+r+1}{k+1}\tbinom{n-k+m-r}{n-k} \\ &= \tfrac{k+1}{\binom{n+m+1}{n+1}}\tbinom{n+m+2}{n+2} \\ &= (k+1)\tfrac{n+m+2}{n+2}. \end{aligned} \tag{26}$$

By combining the intermediate results developed above, the expression of $E[R|A]$ becomes

$$\begin{aligned}E[R|A] &= \textstyle\sum_{r=0}^{m}(k+r+1)\frac{\binom{k+r}{k}\binom{n-k+m-r}{n-k}}{\binom{n+m+1}{n+1}} \\ &\quad -(k+1)\textstyle\sum_{r=0}^{m}\frac{\binom{k+r}{k}\binom{n-k+m-r}{n-k}}{\binom{n+m+1}{n+1}} \\ &= (k+1)\tfrac{n+m+2}{n+2} - (k+1) \\ &= (k+1)\left[\tfrac{n+m+2}{n+2} - 1\right] \\ &= m\cdot\tfrac{k+1}{n+2}. \end{aligned} \tag{27}$$

The intuition behind this simple result is as follows: since nothing is known about the future, in each of the m hypothetical extractions from the urn, the *success* probability, is the same, namely,

$\frac{k+1}{n+2}$. Thus, by a well know result, the expectation of the number of successes must be $m \cdot \frac{k+1}{n+2}$.

Let us translate (27) into the language of trust and reputation. Consider a seller with current reputation score (n,k,t). We are interested in predicting the reputation score of the seller by time T when her total number of transactions has reached $n+m$. By (27), it follows that out of a total of $n+m$ transactions, the *predicted* number of transactions in which our seller has fulfilled her obligations is $k+m\frac{k+1}{n+2}$.

To put it differently, the *expected reputation score* of the seller by time T, when she was involved in $n+m$ transactions, is $(n+m, k+m\frac{k+1}{n+2}, T)$. Interestingly, as the following derivation shows, the seller's predicted trust measure at time T is still $\frac{k+1}{n+2}$.

$$\begin{aligned}
\rho_S(0,T) &= \frac{k+m\frac{k+1}{n+2}+1}{n+m+2} \\
&= \frac{k(n+2)+m(k+1)+n+2}{(n+2)(n+m+2)} \\
&= \frac{k(n+m+2)+n+m+2}{(n+2)(n+m+2)} \\
&= \frac{(k+1)(n+m+2)}{(n+2)(n+m+2)} \\
&= \frac{k+1}{n+2}. \qquad (28)
\end{aligned}$$

6.5 SIMULATION RESULTS

The goal of this section is to present the results of our empirical evaluation of the trust and reputation service discussed analytically in Sections 6.2 – 6.4.

6.5.1 Simulation Model

For the purpose of empirical evaluation we have simulated a blockchain-based decentralized

marketplace with SC support, a feature of Society 5.0. The actors in the marketplace are the buyers and the sellers. We assume that a SC is associated with each transaction and, for simplicity, that each transaction involves one buyer and one seller. The SC in charge of the transaction is responsible for providing feedback at the end of the transaction, replacing notoriously unreliable buyer feedback by a more objective assessment of how well the buyer and the seller have fulfilled their contractual obligations towards each other.

The marketplace simulation model consists of a seller who was involved in transactions with multiple buyers. Each transaction can be either successful (indicating that the seller has fulfilled her contractual obligations) or failed otherwise. In the simulation, we tracked the number of successful transactions and the total transactions. The probability of a successful transaction is determined based on the goals of the experiment as we explain in the following sections. For each goal, we repeated the experiment a large number of times, as needed.

The remainder of this section is structured as follows. In Section 6.5.2 we turn our attention to a multi-segment marketplace (by dollar value of the goods transacted) and illustrate, by simulation, the reputation scores and trust measure of a generic seller in these market segments. Next, in Section 6.5.3 we present simulation results of seller performance in a marketplace segmented by service type, not price range. This is followed, in Section 6.5.4, by a simulation of the effect of a discounting strategy designed specifically to assist a seller facing a steep learning curve. Finally, in Section 6.5.5 we predict, by simulation, the future reputation scores and trust measure of a generic seller, using incomplete information.

6.5.2 Trust Measure in a Price-Range Based Multi-Segment Marketplace

The purpose of this Section is to illustrate, by simulation, the trust measure of a seller in dif-

ferent market segments defined by the dollar value of the goods transacted. For the simulation, we assume that the transactions in the marketplace are divided into four non-overlapping price ranges R_1, R_2, R_3, and R_4, based on the monetary value of the items transacted. These four price ranges determine four disjoint market segments—M_1, M_2, M_3, M_4, where market segment M_i includes all transactions falling within the price range R_i.

We have assumed that the seller has accumulated, over a time window of 250 units, the following performance in each of the four market segments:

- In market segment M_1 the seller had 88 successful transactions out of 100 total transactions;
- In market segment M_2 the seller had 3 successful transactions out of 3 total transactions;
- In market segment M_3 the seller had 1 successful transaction out of 1 total transactions; and,
- In market segment M_4 the seller had zero transactions;

Figure 29 illustrates the seller's trust measure in each of the four market segments using (1) from Theorem 1.

Not surprisingly, even though the trust measure of the seller in market segment M_1 is fairly high, 86/102, her trust measure in market segment M_3 is a meager 2/3, while in market segment M_4 the seller's performance is only 1/2, reflecting the fact that the seller has had no experience in the market segment. As a result, the seller cannot misrepresent her performance.

6.5.3 Trust Measure in a Service-Type Based Multi-Segment Marketplace

In Section 6.4.1 we argued that reputation scores and the trust measure of a seller should not be global but should, instead, be specific to individual price ranges. Specifically, we made the point

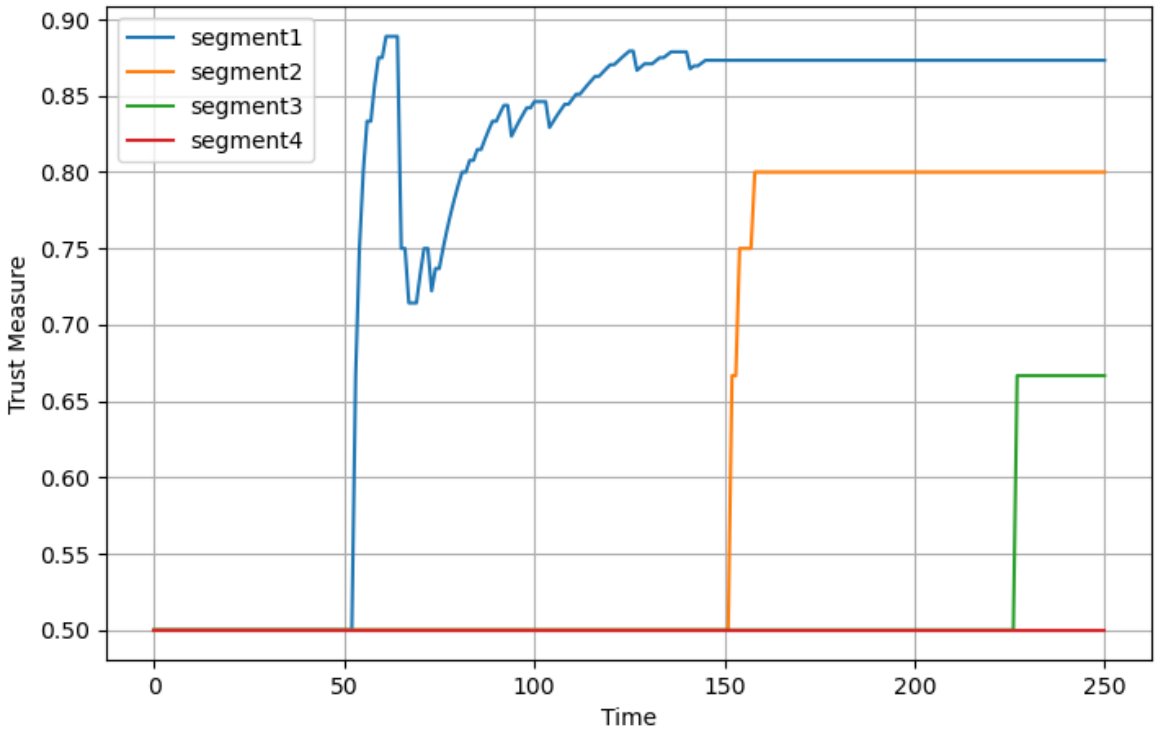

Figure 29. Illustrating the trust measure in a price-based multi-segment market.

that reputation scores acquired by conducting business in one market segment (by dollar amount) should not carry over to a different market segment. In Section 6.4.2 we extended the same idea to various types of services provided.

We have simulated the evolution of reputation scores and trust measure of a plumbing contractor who is offering the following services:

- general plumbing repairs;
- electric heater installation;
- gas heater installation;

- long-term maintenance contracts;
- sewer repairs;
- gas boiler service.

Some of these services are more lucrative than others and the plumber is more competent dealing with electric than with gas equipment. Thus, our plumber may be inclined to provide higher quality services in areas that benefit him most (e.g. installing electric water heaters and general plumbing repairs) and of lesser quality in some other areas that are less lucrative, e.g. installing gas water heaters or sewer repairs. even though an electric water heater may cost roughly the same as a gas water heater.

The point is that the plumber's reputation score acquired by providing one type of service should not be relevant when evaluating his/her trustworthiness in different service categories where he/she is either less competent or simply not interested in providing high quality services. Figure 30 illustrates the simulated lumber's trust measure in each of the service categories above.

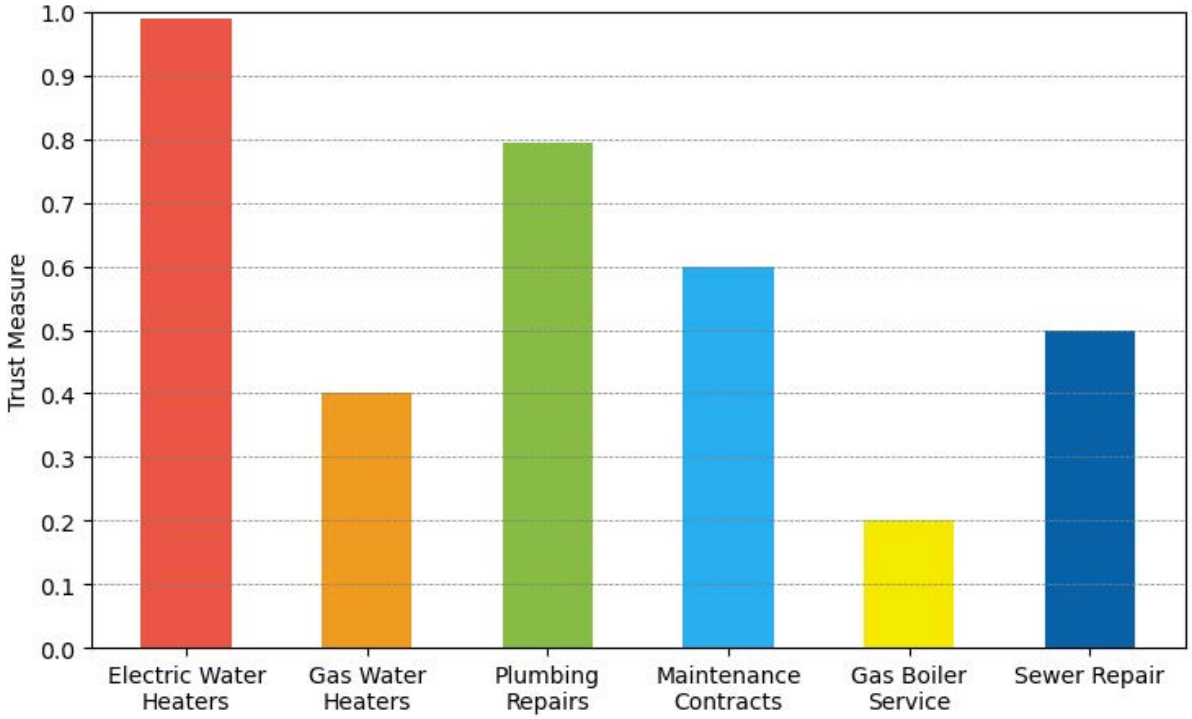

Figure 30. Illustrating a hypothetical plumber's trust measure in a service-based multi-segment market.

6.5.4 Illustrating the Effect of Discounting Strategies

We have simulated the reputation scores and associated trust measures of a generic seller in ten time epochs. Initially, the seller's reputation scores are low, perhaps because of her lack of experience. We have simulated the effect of the discounting strategy presented in Section 6.4. The results of the simulation are summarized in Figure 31 and 32. In the figures we have plotted, side by side, the seller's aggregate trust measure without discounting as well as her weighted trust measure. Figure 31 illustrates the trust measure for each epoch while Figure 32 illustrates the cumulative trust measure. It becomes obvious the effect of favoring recent performance over more

remote performance. As it turns out, selecting the weights that focus attention on the performance of the seller in the last week presents her trust measure in the best light, as it is, conceivably, the most accurate reflection of her improvement.

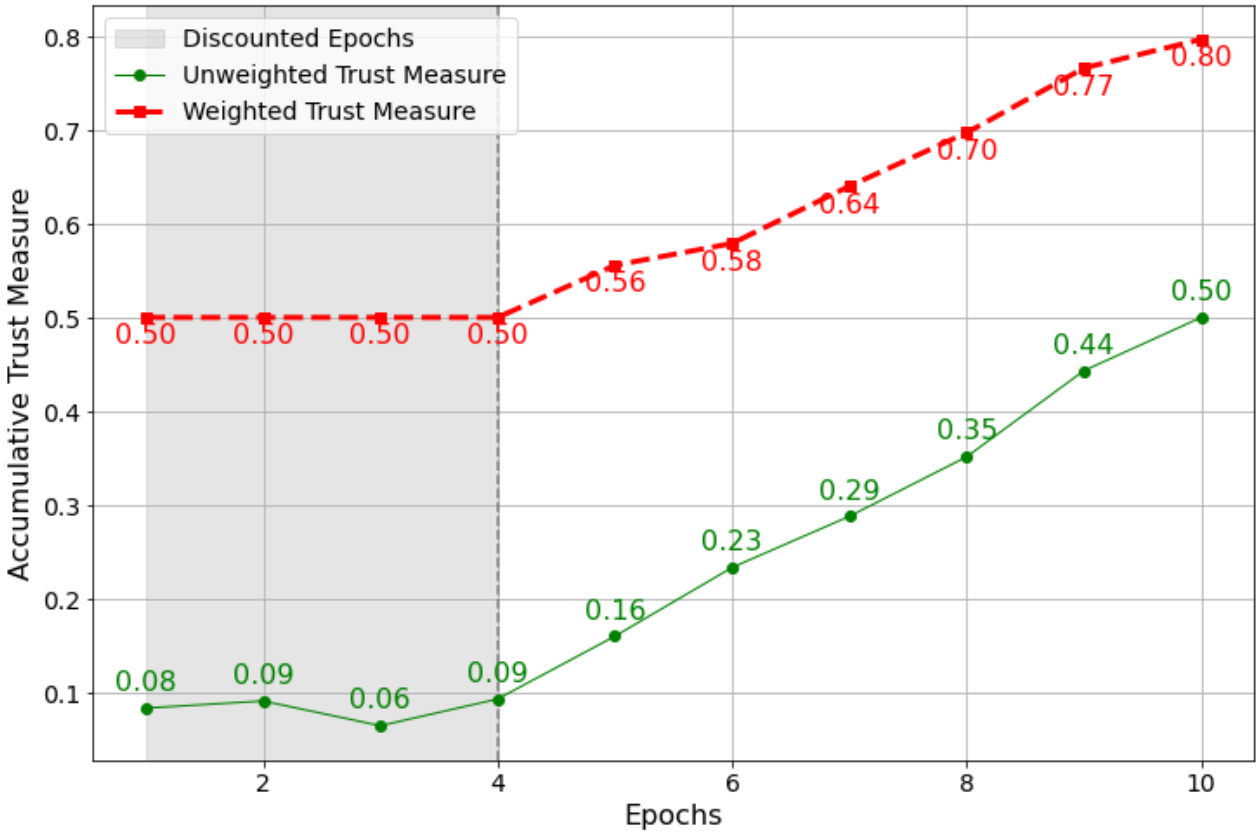

Figure 31. Illustrating the discounting strategies in Section 6.4.3, presenting the trust measure for each epoch.

6.5.5 Predicting Trust Measure and Reputation Scores Over the Long Term

In this Section, we are presenting the results of simulating the convergence of the predicted and simulated long-term trust measure of a seller. For this purpose, we have simulated the perfor-

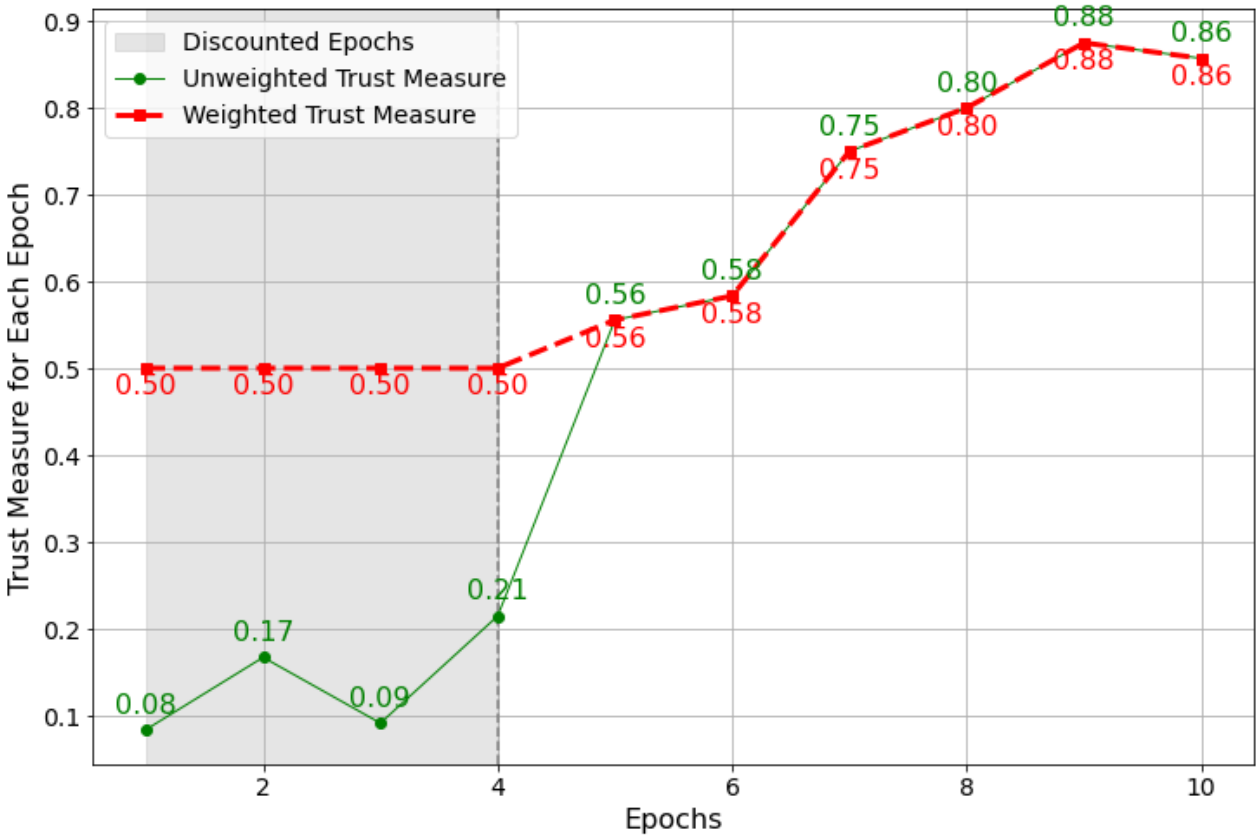

Figure 32. Illustrating the discounting strategies in Section 6.4.3, presenting the cumulative trust measure for all epochs

mance of a seller in her first 100 transactions. Our goal was to see how close the prediction of the expected number of her successful transactions among the next 100 transactions. The results of the simulation are plotted in Figure 33. The simulation was repeated 150 times. From the figure, it is clear that the seller's simulated long term performance, in terms of her reputation scores (and associated trust measure), converges to the theoretically predicted performance.

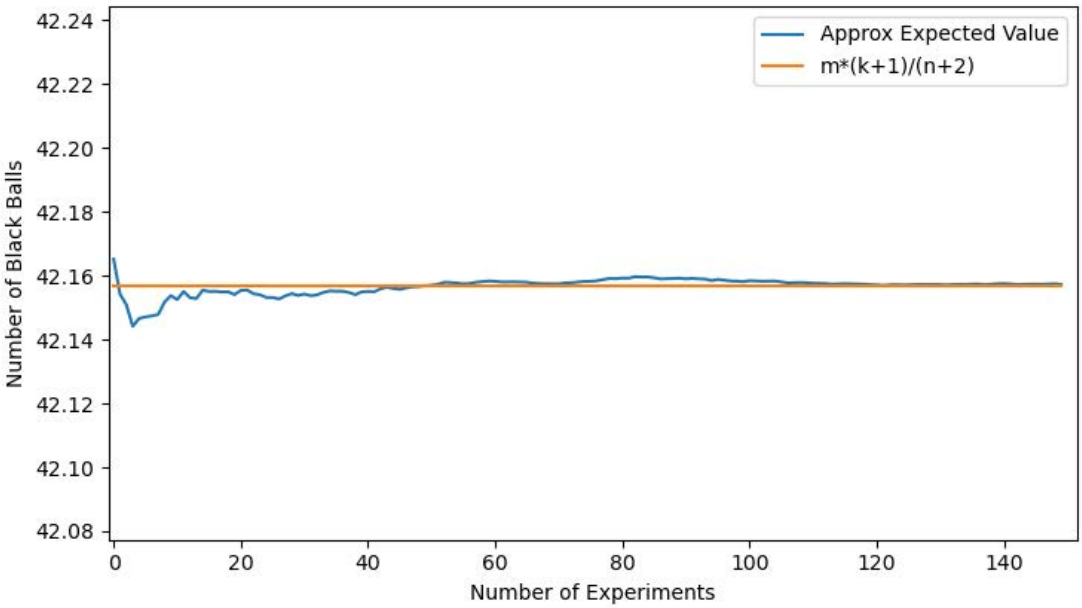

Figure 33. Illustrating the convergence of the simulated prediction of long-term trust measure to the theoretical prediction of Section 6.4.3.

6.6 SUMMARY

This chapter was motivated by the multifold challenges in implementing the vision of trusted and secure services in Society 5.0. The first focus was a novel trust and reputation service to reduce the uncertainty associated with buyer feedback in decentralized marketplaces. A classic result inspired our trust and reputation service in probability theory that can be traced back to Laplace.

The second focus of the chapter was to offer three applications of the proposed trust and reputation service. We discussed two applications to a multi-segment marketplace, where a malicious seller may establish a stellar reputation by selling cheap items or providing some specific service, only to use their excellent reputation score to defraud buyers in a different market segment. As

noted, our service can provide Sybil resistance, a much-desired attribute [60], [90]. Next, we applied the results of the effect of discounting strategies to assist a seller who tries to cope with an initial learning curve or other similar impediments. We provided a discounting scheme wherein less recent reputation scores are given less weight than more recent ones, and we showed how to use our trust and reputation service to predict future reputation scores based on fragmentary information.

CHAPTER 7

SMARTREVIEW: A BLOCKCHAIN-BASED TRANSACTION REVIEW SYSTEM FOR DECENTRALIZED MARKETPLACES

In this chapter, our goal is to answer the following research question: **RQ5:** H How does a SC-based review system address the shortcomings of traditional buyer-sourced reviews in marketplaces?

We begin by outlining the activities in the decentralized marketplace that are relevant to the transaction review 7.1. Following this, Section 7.2 presents SmartReview's multilayered architecture. Section 7.3 provides the tools that play the key role in automating the transaction review process, enabling it to be more objective, scalable, and timely. Section 7.4 introduces a system for efficiently managing reviews in order to predict seller performance for future transactions. In Section 5.4, we present and analyze the results obtained from our experiments and simulations, demonstrating the system's performance and effectiveness. Finally, Section 7.5 provides a summary of the chapter, highlighting the main findings and their implications for the field.

7.1 SYSTEM MODEL

SmartReview's system architecture is based on the following transaction execution model. Here, we only describe the activities in the decentralized marketplace that are relevant to the transaction review: Identity registration, Product registration, Order placement and management, Order delivery management, Returns management, Payment management, Review management, and Reputation management.

Identity registration is done as part of the initial stage of the proposed decentralized marketplace framework, where buyers and sellers complete the registration process before participating in the marketplace. This requires users to provide their credentials (e.g., Name, address, contact email, and phone#, and any other pre-authorized information such as bank account and/or credit card information, driver licenses, etc.). This is needed only during the onboarding process. In the product registration step, sellers register their products, providing the needed details. Buyers browse the available products, select a seller, inquire about their reputation scores, if necessary, and place an order. The payment management handles buyers' payments. The payments are initially held by the system and transferred to the sellers only at the end of a transaction. The system also keeps track of order dispatch at the sender end and order delivery at the buyer end. In case the buyer decides to return the merchandise, the returns management handles the return request.

The automated transaction review , the primary novelty and strength of SmartReview, is done at the end of the transaction, with inputs from the contract's terms and conditions, and the evidence sent by the buyer and the seller. The reviews as well as the underlying evidence are stored in the blockchain. Finally, the seller's reputation is computed based on transaction reviews where the seller was involved. These are dynamic scores using predictive algorithms, and not simple time-weighted averages.

7.2 SYSTEM ARCHITECTURE

In order to accomplish the stated goals, we have designed a multilayered architecture for SmartReview. It handles all the needed aspects of online transactions, from the user registration phase to the reputation management phase.

As shown in Figure 34, the architecture has six layers. The bottom layer is the blockchain

and SC layers where the data is securely stored and retrieved. It provides the needed transparency and immutability of records, thereby providing trust to users. It also supports the needed SCs to implement different functionalities in the system. The second layer handles user identity registrations. It validates user credentials and provides unique IDs (SSI) that are used throughout the system. The third layer handles product registrations. This is where a seller registers its products with the needed specifications, product details, and possibly prices. All registered products are assigned unique product IDs. The fourth layer is called the transaction processing layer. This is where all steps related to transaction execution take place—buyer choosing a product from a seller, both buyer and seller agreeing on the contract terms and conditions, buyer payment, order delivery, buyer inspection and initiation of return if necessary, and disbursement of money to the seller and/or buyer in case of a legitimate return—all subject to the agreed upon terms and conditions. The fifth layer is the transaction review layer, where the automated review process takes place. This is the unique contribution of the proposed SmartReview. Finally, the sixth and top layer manages user (seller/buyer) reputation based on the transaction reviews recorded in the blockchain by the transaction review layer.

The functionalities in the six layers are designed to be implemented as eight SCs. Each SC interacts with the users and the blockchain, and if necessary, with other SCs. The functionalities of each SC are summarized below.

1. Identity Registration: The user registration is orchestrated by **Identity Smart Contract** (ISC), ensuring a standardized and secure approach to onboarding individual buyers and sellers to the marketplace. Importantly, the captured identities are recorded within the blockchain, adopting a self-sovereign identity (SSI) approach [2]. This approach enables

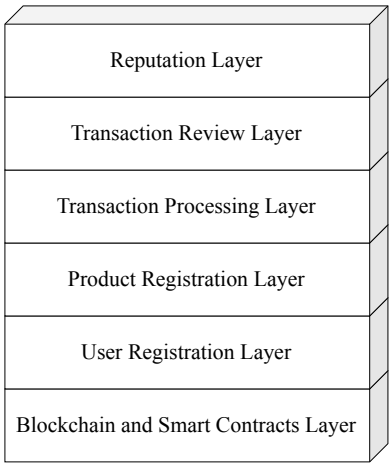

Figure 34. SmartReview layered architecture.

individuals to control their own identities and proofs, enhancing security and privacy.

2. Product Registration: This task is managed by **Product Registration Smart Contract** (PRSC). It involves a seller registering its product with product details (e.g., name, image, specification, manufacturer, etc.), price, shipping costs, delivery details, etc. Once registered, the product is assigned a unique ID by the marketplace. The provided product details are first verified with an external source and then stored on the blockchain.

3. Order Placement Management: This task is managed by **Order Placement Smart Contract** (OPSC). It consists of several subtasks, including product browsing, reputation/trust queries of the seller, any buyer-seller negotiations, seller-buyer confirmation, and order placement.

4. Order Delivery Management: **Order Delivery Smart Contract** (ODSC) manages the dispatch process at the seller and the receiving process at the buyer. Obviously, buyers and sellers are provided with APIs through which these can be accomplished by them.

5. Return Management: **Return Smart Contract** (RSC) manages the return tasks. In case a

buyer decides to return a product for various reasons, the buyer needs to first get approval from the seller or RSC and then return it based on the contractual terms and conditions. The return process, including verification of the terms and conditions, is managed by RSC.

6. Payment Management: The buyer payments are handled by the **Payment Smart Contract** (PSC). It validates the payment and holds the received payment with itself. The payment is recorded on the blockchain. When a transaction is completed, and it is determined that the seller needs to be paid the money, PSC transfers the money to the seller. In the case of a legitimate return, depending on the contractual terms, the appropriate funds are transferred to the buyer and/or seller.

7. Transaction Review Management: **Transaction Review Smart Contract** (TRSC) is the unique contribution of the proposed SmartReview system. This is responsible for evaluating a transaction based on the provided data. The data could have been automatically generated (e.g., shipping date/time, delivery date/time), evidence submitted by the buyer (e.g., evidence of received products, state of the products, etc.), or evidence from the seller (e.g., evidence of products sent, state of products, etc.). The SC, keeping the contractual terms as the basis, and after analyzing the received inputs using the technologies provided, provides the review for a transaction. The review has two parts. One is a quantitative review, a numerical evaluation of the seller's performance, and the other is a descriptive one, providing the details of the seller's performance. Both are important for buyers when choosing a seller. It also makes a decision on the return payments, in case of a return, based on the inputs provided and the terms and conditions, and informs PSC.

8. Seller (Buyer) Reputation Management: The **Reputation Management Smart Contract**

(RMSC) manages seller reputation and handles reputation queries from buyers and sellers. It retrieves the reviews, both quantitative and descriptive, maintained by TRSC on the blockchain, summarizes them, and provides them to the buyers. Optionally, it could handle sellers' queries regarding buyers' reputations. Several techniques have been proposed in the literature that describe ways to efficiently compute reputation scores on blockchains [6], [57], [59]. While it is simple to provide a time-averaged score, as in most traditional e-markets, RMSC goes a step further to predict success rates for future transactions based on the varying nature of sellers' performance.

The eight SCs and their roles in SmartReview system are illustrated in Figure 35. They also show the logical flow of tasks and information flow in the system.

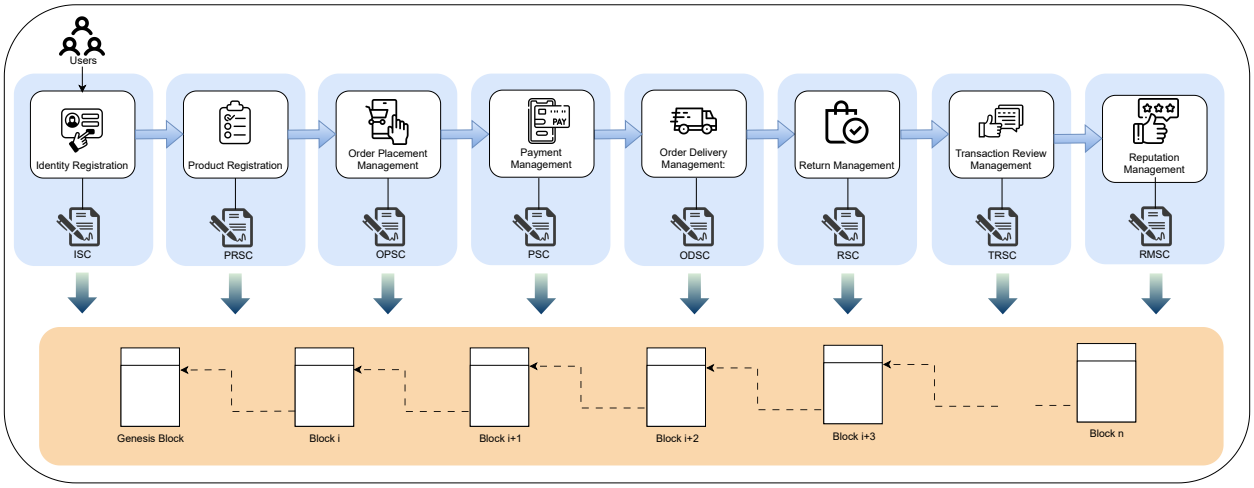

Figure 35. SCs employed in the SmartReview system.

7.3 TOOLS FOR TRANSACTION REVIEW

As mentioned above, in the SmartReview system, the Transaction Review Smart Contract (TRSC) plays a key role in automating the transaction review process, enabling it to be more objective, scalable, and timely. The reviews provided by TRSC are also used to evaluate the reputation and trust of sellers and buyers. While some information, such as the terms and conditions of the order, order shipping date/time, and the order received date/time are automatically recorded on the blockchain, when these events occur, other product-specific disputes need some special software for identification and resolution.

Besides the above standard information, one of the main inputs for TRSC in preparing a transaction review, especially when disputes arise, is the images provided by the buyer and/or seller. Computer vision methods are quite useful in extracting information from such images [67], [102]. Some of these methods use well-known tools such as OpenCV [73], YOLO (You Only Look Once)[49], Mask R-CNN[34], and Faster R-CNN (Region-based Convolutional Neural Networks)[18]. Libraries such as OpenCV have simple, pre-built functions that don't need additional training[1]. However, deep learning and machine learning models need to be trained for custom jobs that need to identify specific objects with custom labels[46], [63]. We describe a few computer vision tools that are considered in SmartReview to resolve buyer-seller disputes.

Color disputes

One of the frequent disputes is the mismatch in the color of the product that was received versus that was ordered. In such disputes, a buyer can upload an image of the product it received, with proof of the package, into the SmartReview system. Computer vision methods are then used

to automatically compare the product colors in both, i.e., the one in the contract or the seller's website versus what the buyer received, and make decisions on the discrepancy [91]. They can employ techniques such as setting color thresholds, noise reduction, and filling in any gaps[45], [72]. All of these techniques work together to help with color detection in pictures. Figure 36 illustrates an example where two images were compared for color using a color-matching algorithm (https://github.com/balajisrinivas/Color-Detection-OpenCV). The system identifies the image colors, identifies the discrepancies, compares them with the contractual terms, makes a decision, and writes a review for that transaction.

Figure 36. Color Detection

Size disputes

Another cause of dispute is the discrepancy in the dimensions of the received product. It can be hard to get exact measurements of objects in pictures [36]. AI technologies, such as computer vision and deep learning, can help enable TRSC to measure the product dimensions accurately by

employing object detection techniques such as YOLO and Faster R-CNN [83]. Depth estimation models and stereo vision methods get even more accurate measurements [69], [87]. Figure 37 illustrates an example where two water bottle images were compared for size (dimensions) using a sizing algorithm https://github.com/ashish1sasmal/Objects-Dimensions-Measurement). The system identifies the image sizes, identifies the discrepancies, compares them with the contractual terms, makes a decision, and writes a review for that transaction.

Figure 37. Size Measurement

Shape disputes

Shape is yet another point of contention. Shape detection techniques can solve this problem[37]. They include pre-processing, contour detection, and shape analysis [71]. Vittorio et al. [25] have a method that makes it easier to find models in images that are otherwise hard to read.

Count disputes

Some disputes may be related to an incorrect count of the number of items received. Simple computer vision methods can work amazingly well for counting objects in a picture. To separate interesting items from the background, methods like thresholding, edge detection, and contour finding are often used. Convolutional neural networks (CNNs) and other machine learning models can be trained to spot and count objects in complex scenes. Prithvijit et al. [17] used models that were specially trained to count things in a variety of natural settings. Figure 38 illustrates an example where the number of objects in the two images was compared using a counting algorithm https://github.com/niconielsen32/ComputerVision/tree/master/ OpenCVdnn). The roposed system identifies the number of objects in each image, identifies the discrepancies, compares them with the contractual terms, makes a decision, and writes a review for that transaction. In this example, it was able to identify six objects in the left image and four in the right image.

Figure 38. Object count

Item disputes

In some disputes, it may be necessary to compare a received item to an advertised image on a website. Image matching resolves these disputes by comparing the two images for consistency and accuracy. Ebrahim et al. [40] employed SIFT and ORB image-matching methods in a range of picture conditions, such as rotation, scaling, noise, fish-eye distortion, and shearing. ORB was found to be fast, while ORB was consistently accurate. Figure 39 illustrates an example where images of two toy figurines were compared using an image-matching algorithm (Image Comparison & Displaying Difference using Python's Opencv Library | OpenCv | Image Processing |). The system compares images, identifies the discrepancies, compares them with the contractual terms, makes a decision, and writes a review for that transaction.

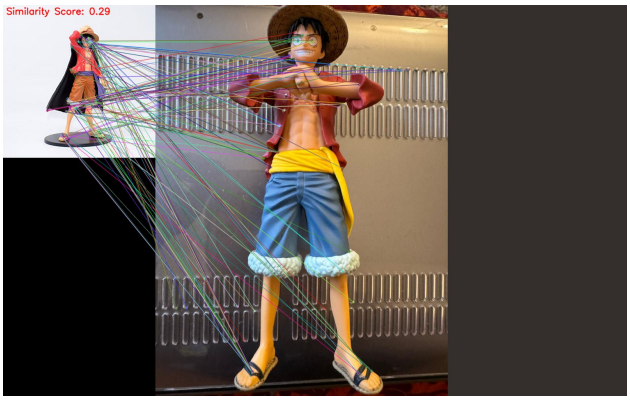

Figure 39. Image Matching

In other item disputes, it may be necessary to abstract text from images. For example, a customer ordered size 11 relaxed fit black shoes, but was delivered a shoe of size 10, and the buyer has uploaded an image of what it received. Optical Character Recognition (OCR) [85] tools such as

Easy OCR[16] and PyTesseract[80] extract text from the images. After the text is extracted, Natural Language Processing (NLP) methods, such as Named Entity Recognition (NER)[78], could be used to read, understand, and analyze the text [5]. Figure 40 illustrates an example where text from a soap box image was extracted by an OCR algorithm (https://github.com/nicknochnack/EasyOCR). The system extracts the keywords, compares them with those in the contract, makes a decision, and writes a review for that transaction.

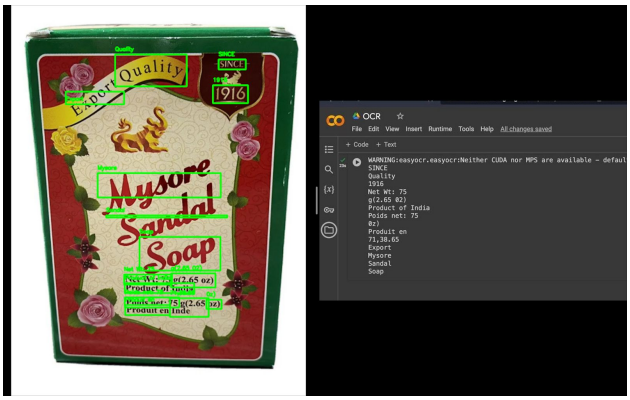

Figure 40. Text extraction using OCR

Complex disputes

For some disputes, more complicated models using both vision and language models may need to be combined, such as in ViLBERT (Vision and Language BERT) [52]. It improves understanding and interpretation of context, which lets the model do very well at tasks like describing images, asking questions, and having very accurate interactive conversations. This functionality is still being implemented.

While the above list of functionalities describes what has been implemented so far, we continue to look into ways to make the review process more accurate, comprehensive, and automatic. The question that is yet to be addressed is the data provenance of the evidence provided by the buyers and sellers. This work is still in progress.

7.4 REPUTATION MANAGEMENT

While SmartReview enables objective, cheap, and accurate reviews of transactions, we still need a system that can manage the reviews efficiently and use them to predict seller performance for future transactions. Both seller and product rankings have been shown to have a significant impact on e-sales [98]. In this chapter, we refer to seller rankings as reputation, in a generic way.

Seller (and product) reputation is computed based on the SmartReview-based reviews. These are important when a buyer is trying to make a decision on a seller, especially when the seller is new to the buyer. While today's e-markets provide simple 5-star ratings for seller reputation, these were found to be inadequate [14]. In particular, such metrics do not capture the variations in seller behavior due to factors such as volume of sales, seasonal variations, price range of products, etc. For example, a seller who sells well-selling products in the low or medium price range may not do well in high-price range products and vice versa. Similarly, if a seller has done very well in the past 10 years but has been slacking off in the last few months, it is important that a buyer knows this rather than a simple arithmetic average over the last several years.

Since transactions occur over time, SmartReview computes reputation using time-series predictions. Although conventional statistical models such as ARIMA (Autoregressive Integrated Moving-Average) [61] have played a major role in the past, advancements in machine learning have brought forward new approaches that provide complex methodologies for analyzing time se-

ries data. For example, Pavlyshenko et al. [68] have employed machine-learning models for sales predictive analytics, with a particular focus on sales forecasting. They highlight the significance of regression methods in contrast to conventional time series techniques when forecasting sales. Pao et al. [66], using retail sales data obtained from Walmart department stores, show that hybrid models comprising of STL (Seasonal-Trend Decomposition using Loess) [20], ARIMA and FFNN (feed-forward neural networks) [7] exhibit high accuracy in time-series predictions.

In the rest of the section, we describe a few prediction algorithms that we have experimented with to predict seller reputation and sales. The simple seller data that we have assumed is illustrated in Figures 41 and 42. While Figure 41 shows the pseudo seller's volume of transactions across different periods, Figure 42 shows (the dark line) the percentage of successful transactions. The pseudo seller's behavior incorporates time changing behavior. The pseudo seller starts with low sales and good transaction reviews. As its reputation grows, the sales grow, but then they grow beyond the seller's capacity. This results in increased unsuccessful transactions, resulting in a decrease in reputation and, thereby, a dramatic fall in sales. The seller puts in more resources and/or improves its processes to gradually improve its performance. These enhancements increase reputation as well as sales. But this cycle repeats as the seller learns to cope with high demand each time. To predict the reputation of this pseudo seller, we have used several algorithms, as discussed below.

Prophet algorithm

Facebook's Prophet [93] predictive model has become an established time series forecasting tool. It was designed as a decomposable model comprising three primary elements: trend, seasonality, and holidays. This time-series model frequently outperforms alternative approaches in terms

of precision and computational effectiveness. For simplicity, we assume that all sales are in one price range. While the past data is shown as a time series at different periods represented as black points joined by a thick black line, the Prophet's predictions are shown in blue with a cloud-like structure to indicate a range of values for prediction. the negative sales predictions in 41 should be taken as zero sales. As can be seen in both figures 41 and 42, the model accurately predicts seller performance. Such a prediction-based reputation is much more useful to a potential buyer than a simple weighted average of the past.

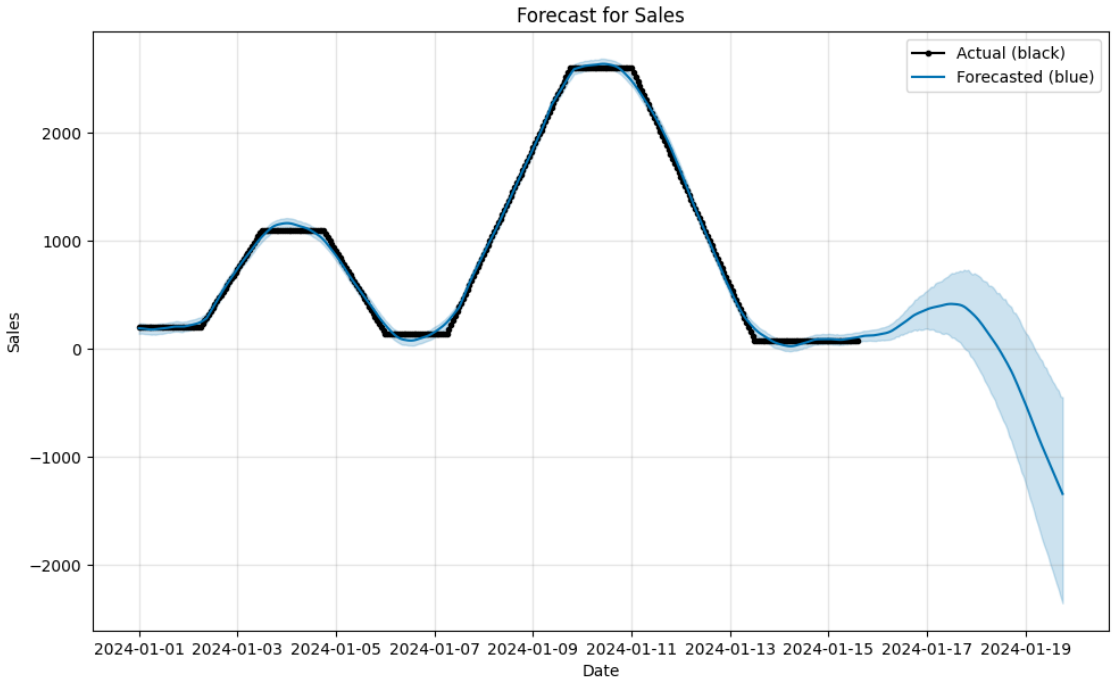

Figure 41. Volume of transactions (sales)

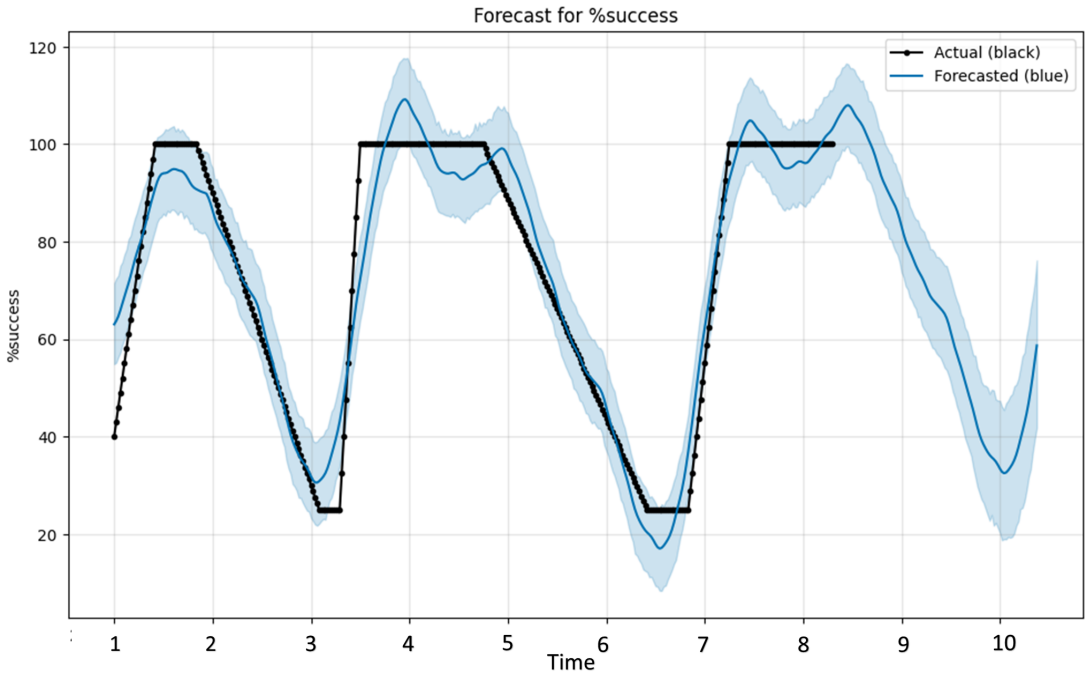

Figure 42. Reputation (% of Transaction success)

Laplace Estimator and other predictors

Based on Laplace's theory on predicting future events based on prior distribution [28], [64], we have calculated seller reputation. While the Laplace estimator is based on all prior reviews, we have also predicted based on the last 50 reviews (window of 50). We have applied these schemes to reputation predictions, and the results are summarized in Figure 43. It may be noticed that only the Prophet algorithm was able to predict seller's reputation much beyond the actual time. Other schemes can only predict the immediate future.

It is clear that the Prophet algorithm is the most accurate, closest to reality, and can predict the future better than the other schemes. Predictions with a window of 50 in the past are the next best. The Laplace predictor with the life time history is the least effective predictor among these since the pseudo seller we considered has a cyclic performance that is not captured by the Laplace

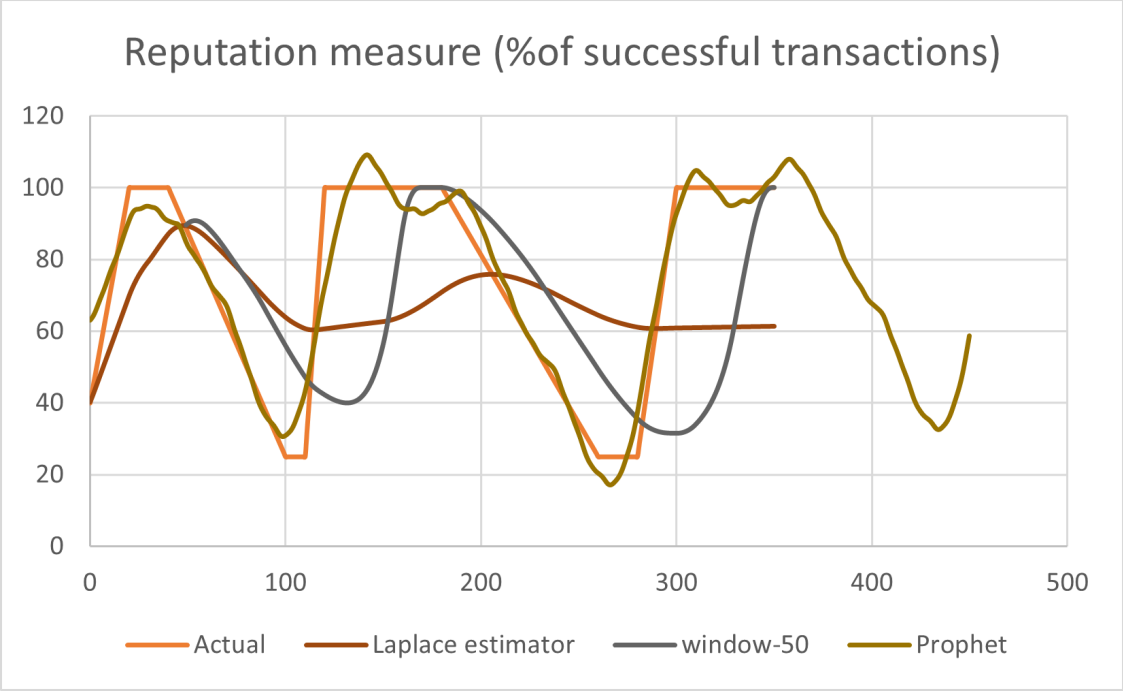

Figure 43. Reputation (% of Transaction success)

estimator. We are now developing alternate Laplace estimator schemes that can handle the time varying performance of sellers.

In SmartReview, we are thus able to provide predictive seller reputation so buyers can make proper choices for their purchases. The accuracy of these predictions is retained even when the seller's performance varies over seasons, product types, and price ranges. We are currently experimenting with expanding this to other predictive algorithms and reputation metrics.

7.5 SUMMARY

In this chapter, we have addressed an essential aspect of e-commerce: the accuracy and comprehensive reviews of transactions. The current review systems rely on buyer feedback, which is either infrequent or mostly subjective when given. The proposed SmartReview system attempts

to automate the review process. It is based on blockchain and SC technologies, several image processing techniques, and AI and machine learning techniques for predictive reputation. The system contains eight SCs to implement different functionalities of the system. It automates the transaction review process and provides a predictive reputation based on past reviews. The chapter illustrates the proposed methodologies through a simple proof-of-concept prototype.

CHAPTER 8

INNOVATIVE BLOCKCHAIN ARCHITECTURE FOR TAILORED APPLICATIONS

In this chapter, our goal is to answer the following research question: **RQ6:** How can a structured blockchain architecture optimize data integrity, security, efficiency, and query retrieval across various applications?

This section, 8.1, describes the proposed blockchain structure. Following this, Section 8.2 provides a detailed explanation of the technical specification of the proposed blockchain structure. Section 8.3 presents and analyzes the proposed blockchain structure, focusing on data integrity and security, as well as scalability and efficiency. Section 8.4 provides applications that use the proposed blockchain structure. Finally, Section 8.5 provides a summary of the chapter, highlighting the main findings and their implications for the field.

8.1 PROPOSED BLOCKCHAIN STRUCTURE

Blockchain technology has evolved from its traditional linear structure to accommodate more complex data management scenarios. The proposed structure introduces two distinct layers: the Physical Blockchain (Horizontal Blockchain) and the Logical Blockchain (Vertical Blockchain), each serving specific roles in enhancing data organization and accessibility.

8.1.1 Physical Blockchain (Horizontal Blockchain)

Each block in the Physical Blockchain layer represents a distinct user within the network. Formally, let B_i denote the i-th block in the Physical Blockchain, where $i = 1, 2, \ldots, n$. Each

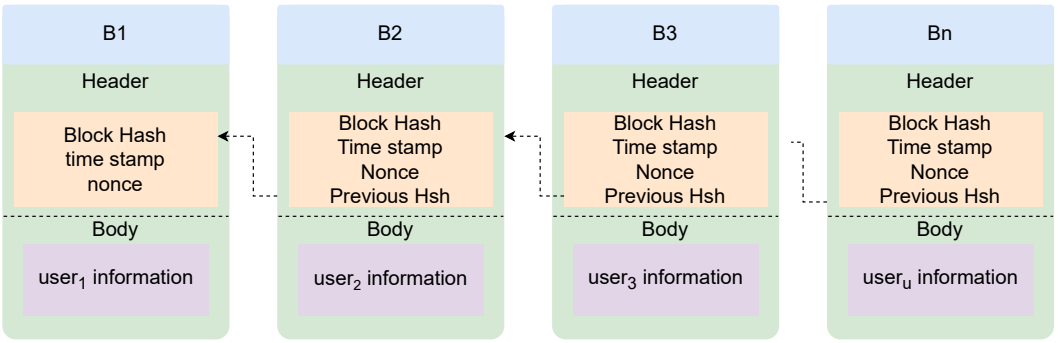

Figure 44. Illustrating the first physical blockchain

block B_i contains a cryptographic hash of the previous block B_{i-1} and user-specific data, thereby forming a chain of user registrations. This horizontal sequence ensures user records' immutability and sequential integrity across the network. Figure 44 shows the first physical blockchain in our structure.

8.1.2 Logical Blockchain (Vertical Blockchain)

The Logical Blockchain layer extends vertically from the Physical Blockchain, focusing on the detailed transactions or information associated with each registered user. For a given user u, let L_j denote the j-th block in the Logical Blockchain, where $j = 1, 2, \ldots, m$. $B_{u,j}$ denotes the j-th block in the vertical chain corresponding to user u. Each $B_{u,j}$ contains transactional data specific to the user u, linked sequentially based on the order of transactions. The linking mechanism ensures that each $B_{u,j}$ includes a hash pointer to $B_{u,j-1}$, establishing a chronological order of user-specific transactions. Figure 45 shows the first user logical blockchain in our structure.

Integrating these layers provides a structured approach to managing complex datasets, offering enhanced scalability, data retrieval efficiency, and security features. The Physical Blockchain establishes a foundational framework for user registration and identity management, while the Logical

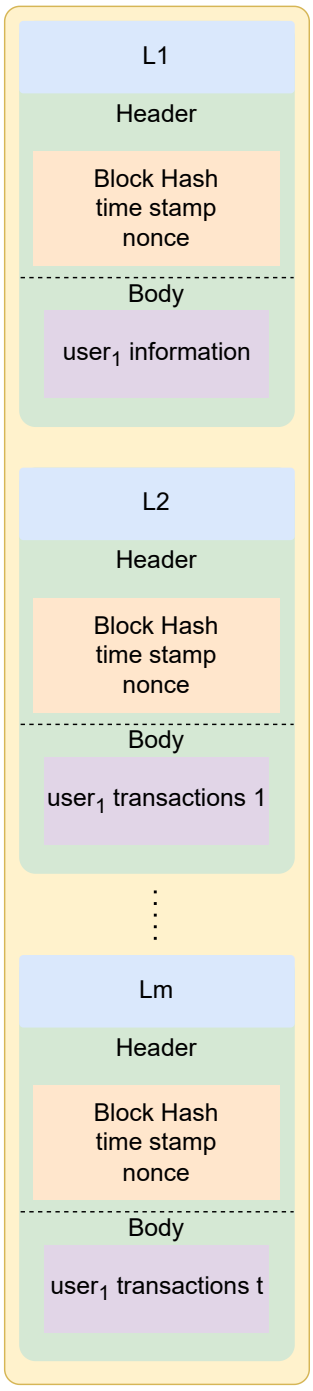

Figure 45. Illustrating the first logical blockchain

Blockchain enriches data granularity and transactional transparency for individual users. The notation B_iL_j represent a block in our blockchain structure where:

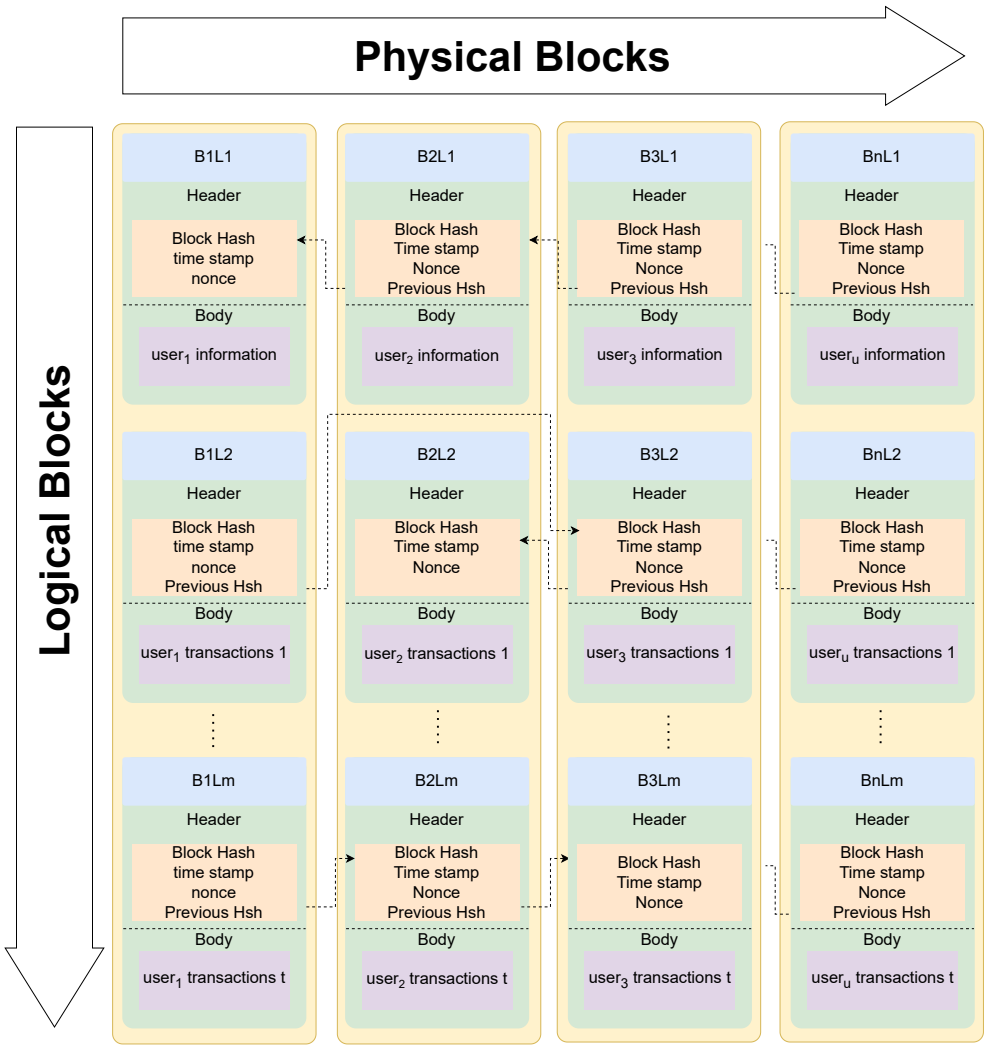

Figure 46. Illustrating the new blockchain structure

- B_i denotes the index of the block in the Physical (Horizontal) Blockchain.
- L_j denotes the index of the block in the Logical (Vertical) Blockchain.

Figure 46 shows the new structure of the proposed blockchain, where it represents the physical blockchain (Horizontal Blockchain) and the logical blockchain (Vertical Blockchain).

8.2 TECHNICAL DETAILS

In this section, we delve into the technical specifications of the proposed blockchain structure, detailing the block structure and linking mechanisms across its layers.

8.2.1 Physical Blockchain (Horizontal Blockchain)

The Physical Blockchain layer consists of two main layers: the initial layer for user registration and subsequent layers for user transactions.

User Registration (Layer 1)

In the first layer of the Physical Blockchain, each block B_i represents the registration of a new user in the network. Formally, each block B_i is structured as:

$$B_i = \langle \text{Block\_Header}, \text{User\_Data}, \text{Previous\_Hash} \rangle$$

where:

- **Block_Header**: Metadata containing a timestamp, nonce, and other relevant information.
- **User_Data**: Specific data related to the registered user.
- **Previous_Hash**: Cryptographic hash of the previous block B_{i-1}, ensuring the integrity and immutability of the blockchain.

Each user's registration block B_i is linked to the previous user's registration block through the **Previous_Hash**, establishing a sequential chain of user registrations.

User Transactions (Layers 2 to n)

In subsequent layers of the Physical Blockchain, each user u has a dedicated chain of transaction blocks. For a user u, the j-th block $B_{u,j}$ in the k-th layer (where $k > 1$) represents a transaction or data update related to user u. The structure of each transaction block $B_{u,j}$ is:

$$B_{u,j} = \langle \text{Block\_Header}, \text{Transaction\_Data}, \text{Previous\_Hash} \rangle$$

where:

- **Block_Header**: Metadata including timestamp and transaction ID.
- **Transaction_Data**: Specific transactional information related to user u.
- **Previous_Hash**: Cryptographic hash of the previous block $B_{u,j-1}$ in the same layer, ensuring the order and integrity of user transactions within the layer.

Each transaction block $B_{u,j}$ is linked to the previous transaction block $B_{u,j-1}$ within the same layer based on the order of confirmation by the network, maintaining the chronological sequence of user transactions.

8.2.2 Logical Blockchain (Vertical Blockchain)

The Logical Blockchain layer represents a vertical chain of blocks for each user, constructed from the horizontal blockchain layers.

Structure and Indexing

For each user u, the Logical Blockchain L_u consists of transaction blocks $B_{u,1}, B_{u,2}, \ldots, B_{u,m}$ organized vertically. An auxiliary indexing mechanism is implemented to facilitate efficient data retrieval. Each user's Logical Blockchain L_u includes:

- **User Information Block**: The first block $B_{u,1}$ contains metadata and user-specific information essential for direct access and identity verification.
- **Indexed Blocks**: Blocks $B_{u,j}$ for $j > 1$ are indexed using arrays. This indexing mechanism allows for rapid query retrieval within the user's transaction history by storing relevant identifiers, such as timestamps or transaction IDs, directly in the array. This enables efficient binary search operations to locate and access specific blocks within the user's vertical blockchain L_u.

The auxiliary index ensures efficient data management and retrieval within the user's vertical blockchain L_u, optimizing performance while maintaining the blockchain's security and integrity.

8.3 ANALYSIS OF DATA SECURITY AND SCALABILITY

8.3.1 Data Integrity and Security

The proposed blockchain structure significantly enhances data integrity and security compared to traditional methods. By implementing a layered approach—Physical Blockchain (Horizontal Blockchain) for user registration and Logical Blockchain (Vertical Blockchain) for transactional data—the system ensures that each transactional block is cryptographically linked to its predecessor. This linkage, using hash pointers, creates an immutable chain where any attempt to alter data

in a block would necessitate changing all subsequent blocks, thereby maintaining the integrity of the entire blockchain.

Moreover, the use of auxiliary indexes, implemented as arrays for each user in the Logical Blockchain, enhances security by enabling efficient data retrieval through binary search mechanisms. This indexing approach reduces the computational overhead typically associated with traditional blockchain searches, thus bolstering overall system security against unauthorized access and tampering.

8.3.2 Scalability and Efficiency

The structured blockchain architecture offers notable scalability features, particularly in managing large datasets and increasing transaction throughput. By segregating user registration (Physical Blockchain) and transactional data (Logical Blockchain), the system optimizes resource allocation and network performance. Each user's transaction history, organized vertically in the Logical Blockchain, allows for streamlined data management and faster access to specific transactional details.

Furthermore, the use of array-based auxiliary indexes enhances efficiency in data retrieval and transaction processing. This indexing mechanism supports rapid query operations, such as binary searches, which are crucial for scaling the blockchain to handle growing volumes of transactions without compromising performance. As a result, the proposed blockchain structure not only scales effectively but also enhances operational efficiency by minimizing latency in transaction verification and data access.

8.4 APPLICATION IN HEALTHCARE

8.4.1 Healthcare Use Case

The application of the proposed blockchain structure in healthcare demonstrates its transformative potential in enhancing medical data management, patient records, and overall healthcare operations. Consider a scenario where the blockchain is utilized to manage patient records and facilitate secure and efficient sharing of medical information among healthcare providers.

By leveraging the Physical Blockchain (Horizontal Blockchain) layer, each patient is registered with a unique block that contains comprehensive metadata and initial health data upon their entry into the healthcare system. This layer ensures the immutable recording of patient identities and medical histories, establishing a secure foundation for subsequent healthcare interactions.

In the Logical Blockchain (Vertical Blockchain) layer, patient transactions such as medical visits, treatments, prescriptions, and diagnostic results are recorded chronologically. Each patient's vertical blockchain enables seamless tracking of their healthcare journey, providing a transparent and auditable record accessible to authorized healthcare providers.

8.4.2 Benefits in Medical Data Management and Healthcare Operations

The adoption of this blockchain structure offers several benefits in healthcare settings. Firstly, it enhances data integrity and security by cryptographically linking each transactional block to its predecessor, thereby safeguarding against unauthorized modifications and ensuring the accuracy of medical records. This feature is crucial for maintaining patient confidentiality and complying with data privacy regulations such as HIPAA.

Furthermore, the structured blockchain architecture improves operational efficiency by streamlining access to patient information. Healthcare providers can securely retrieve relevant medical data through efficient query mechanisms enabled by the array-based auxiliary indexes in the Logical Blockchain. This capability not only reduces administrative burden but also enhances decision-making processes, leading to improved patient care outcomes.

Overall, the application of the proposed blockchain structure in healthcare demonstrates its capacity to revolutionize medical data management, promote interoperability among healthcare stakeholders, and elevate the standard of patient-centric care delivery.

8.5 SUMMARY

This chapter presents a new and innovative blockchain architecture that meets the unique needs of complicated data management situations. The suggested structure builds on the fundamental concepts of blockchain and includes two unique levels: physical (horizontal) and logical (vertical). These layers improve data organization, scalability, and operational efficiency. The suggested architecture enhances data integrity and security by unifying these layers. Additionally, it seeks to provide straightforward data access and administration across diverse applications. Moreover, this chapter examines the technical complexities of this structure, investigates its possible advantages through practical examples, and addresses implementation issues customized for various application domains, with a particular focus on healthcare.

CHAPTER 9

CONTRIBUTION, FUTURE WORK AND CONCLUSION

In this chapter, we review the research questions, describe the methods employed to address them, highlight the contributions made, propose future work, and summarize the conclusions.

9.1 REVIEW OF RESEARCH QUESTIONS

Our main research question is **"Can blockchain and SCs be used to build a strong, efficient, and secure reputation system in decentralized marketplaces?"**

Our approach involves utilizing blockchain technology and SCs to create new decentralized markets. This allows for the decentralization of transactions and ensures that reputation ratings are updated in real-time while maintaining user privacy. We improve and simplify managing reputation ratings in various marketplace situations by utilizing specific data structures. Our smart contract solution automates the review of transactions, reducing bias and improving the dependability of buyer feedback. Incorporating innovative technology like computer vision helps us to give unbiased assessments, supporting marketplace transparency and trustworthiness. We have designed our blockchain architecture to optimize data integrity, security, efficiency, and query retrieval. This demonstrates our goal of improving decentralized marketplace operations.

Our research questions are:

RQ1: How do blockchain-based SCs enhance the reliability and efficiency of feedback mechanisms in transaction systems in different marketplaces?

The framework proposes a decentralized blockchain-based marketplace designed to improve se-

curity and transparency in commercial transactions. This new methodology alters the dynamics between buyers, sellers, and miners, promoting a decentralized transaction ecosystem. The deployment of a permissioned blockchain, in which buyers and sellers interact directly for transactions, serves as the basis of this system. Miners, with substantial computational powers, protect the integrity of the blockchain. Their responsibilities go beyond simply handling transaction blocks; they play an important role in the real-time update of reputation scores, ensuring a strong and trustworthy system. This proposed framework not only decentralizes power but also promotes a greater sense of confidence and security in marketplace transactions, effectively altering old marketplace paradigms.

RQ2: What are the impacts of specialized data structures on the scalability and efficiency of computing and retrieving reputation scores within blockchain-based systems? The primary goal is to enhance the scalability and efficiency of reputation management in decentralized marketplaces through the use of specialized data structures. By integrating basic, adaptive and randomized schemes, our approach significantly reduces the average number of blocks accessed during queries, thus improving response times and ensuring reliable reputation scores. These methods address the problem of transaction outcome immutability using blockchain technologies and tackle the unreliability of buyer feedback through SCs. The framework demonstrates a substantial improvement over the basic approach. This integrated system supports scalable reputation management and ensures efficient data retrieval, setting a robust foundation for future enhancements and broader applications in decentralized marketplaces.

RQ3: How do SCs use multiple identities to promote reviewer anonymity in decentralized marketplaces, and what impact does this anonymity have on the quality of feedback?

The primary goal is to integrate user anonymity into the marketplace architecture, while also im-

plementing systems that encourage user feedback. The approach emphasizes the anonymity of the reviewer to reduce the possibility of bias and retaliation, two problems that frequently plague marketplaces. A new strategy is used to encourage customers to actively participate in offering feedback, which is essential to preserve a vibrant and trustworthy marketplace ecology. Advanced SCs, such as the Transaction and Review SCs, which manage a variety of tasks from listing things to processing review submissions, are essential to this system's functioning. The contracts have been carefully crafted to guarantee a smooth user experience in the marketplace, starting from the moment an item is discovered and ending with the completion of a transaction. This integrated system strategy builds the foundation for a long-lasting and dynamic marketplace while also improving the user experience.

RQ4: How do SCs within blockchain-based trust and reputation services specifically address and improve quality in buyer feedback in decentralized marketplaces, and what impact does this have on transaction reliability?

We proposed a solution for a decentralized blockchain-based marketplace that focuses on creating a trust and reputation service, which would leverage SCs to ensure independent feedback and transaction evaluation. Each transaction is accompanied by a Smart Contract, which automatically assesses how effectively the buyer and the seller have fulfilled their contractual obligations. This strategy dramatically reduces the subjectivity commonly involved with consumer feedback, resulting in a more reliable and trustworthy marketplace environment. Our solution relies heavily on Laplace's Law of Succession, a probabilistic model that assesses a seller's trustworthiness based on previous transaction performance. This model is capable of addressing a variety of marketplace scenarios, such as dealing with sellers who may attempt to manipulate their reputation across multiple segments or whose performance may fluctuate over time. We implement discounting tech-

niques that prioritize recent transactions, ensuring that reputation scores appropriately represent current seller behavior. Additionally, our approach is designed to anticipate future trust and reputation scores based on accessible data, providing useful information for buyers to make informed decisions. These qualities, which have been validated through extensive simulations, demonstrate the usefulness of our technology in improving the reliability and efficiency of decentralized marketplaces.

RQ5: How does a smart contract-based review system address the shortcomings of traditional buyer-sourced reviews in marketplaces?

We propose SmartReview, an automated review system that is built based on blockchain and SCs. SmartReview system is built as a multilayered architecture, with each layer handling different aspects of transaction execution in decentralized markets. The review module is conceived as a smart contract that takes the contract terms and conditions and the evidence provided by the buyer and seller as input and employs advanced computer vision and machine learning techniques to arrive at a quantitative and qualitative review for each transaction. These reviews are objective and do not suffer from reviewer bias. Furthermore, the reputation layer takes these as inputs and arrives at a dynamic predictive reputation for the sellers, by employing time-series-based prediction algorithms.

RQ6: How can a structured blockchain architecture optimize data integrity, security, efficiency, and query retrieval across various applications?

A structured blockchain architecture optimizes data integrity, security, efficiency, and query retrieval across various applications primarily through its innovative approach to data organization and indexing mechanisms. In this architecture, data is structured into a Physical Blockchain (Horizontal Blockchain) for user registration and a Logical Blockchain (Vertical Blockchain) for trans-

actional data. The focus on query retrieval involves implementing auxiliary indexing within the Logical Blockchain, enabling efficient data access and retrieval. By organizing transactional data vertically in the Logical Blockchain, each user's activity forms a chain of blocks, allowing for chronological tracking of transactions. Auxiliary indexing enhances query retrieval by structuring transactional data into arrays or indexed structures, facilitating rapid search and retrieval of specific user histories or transactional details. This indexing mechanism ensures that queries can efficiently access relevant data points without needing to traverse the entire blockchain, thereby optimizing performance and reducing query response times.

9.2 CONTRIBUTIONS

This dissertation contributes to the field of creating efficient and secure reputation systems in decentralized marketplaces using blockchain and SCs as follows:

- We introduced a blockchain-based trust and reputation system that utilizes SCs to manage every phase of a transaction, from the establishment of the contract to the interaction between parties, culminating in the final assessment and recording of feedback for both buyers and sellers (Section 4.1).

- We developed innovative data structures specifically tailored to store transaction data and compute reputation scores within a blockchain environment efficiently (Sections 4.2.1, 4.2.2 and 4.2.3).

- We developed two innovative blockchain-based schemes to manage user feedback and deliver reputation score information, which demonstrated up to an 80% improvement in query response times over existing methods (4.4).

- We introduced a secure and trusted review platform for decentralized marketplaces, utilizing blockchain and smart contract technology to promote reviewer anonymity without using cryptographic primitives (5.2). We also developed a method to encourage timely and frequent review submissions (5.1.2). Additionally, we tested this system as a proof-of-concept on the Ethereum test network using Remix IDE (5.3).

- We designed a blockchain-based trust and reputation service to mitigate uncertainties associated with buyer feedback in decentralized marketplaces, enhancing transaction reliability through secure and verifiable feedback (6.2).

- We developed a dynamic reputation scoring system that adjusts scores over time, prioritizing recent activities, and accommodating changes in seller performance (6.4.3).

- We employed methods to predict long-term trust and reputation using incomplete information, supported by a 'trust engine' that employs a modified version of Laplace's law of succession to predict the likelihood of sellers fulfilling future obligations (6.4.4).

- We designed SmartReview, an automated review system that is based on blockchain and SCs by taking contract terms, buyer and seller inputs and applying advanced computer vision and machine learning to provide both quantitative and qualitative reviews (7.1).

- We designed a novel structured blockchain architecture that enhances data integrity, security, and operational efficiency across diverse applications. This architecture integrates robust mechanisms for secure transaction recording and efficient query retrieval(8.1).

9.3 FUTURE WORK

Future work will address several open research issues to enhance the robustness and applicability of our blockchain-based trust and reputation system. One focus will be on extending the binary feedback provided by SCs to multi-valued feedback and allowing buyers and sellers to add optional personal annotations using natural language. Additionally, we will explore strategies to balance the cost of block addition with subsequent query efficiency and develop methods to probe the evolution of a seller's reputation scores over time. We aim to identify new applications for our trust and reputation system, including decentralized banking, inventory management, and other database systems. Moreover, exploring several methods to provide reviewers unlinkability, enforce buyer privacy, encourage honest feedback submission without using cryptographic primitives. Furthermore, we plan to explore applications in banking, inventory management, vehicular networks, peer-to-peer networking, and smart cities, where our reputation and trust service could have significant impact. Addressing data provenance and correctness for the automatic review process, incorporating advanced predictive techniques, and managing varying seller behavior across different contexts are additional priorities. Lastly, exploring AI techniques that integrate information from various sources to verify the accuracy of the provided evidence when buyer places a dispute.

9.4 CONCLUSIONS

This dissertation concludes with several significant contributions to the development of blockchain-based trust and reputation systems in decentralized marketplaces. We introduced a system utilizing SCs to manage every phase of a transaction, from contract establishment to the final feedback

recording for both buyers and sellers. Innovative data structures were developed to efficiently store transaction data and compute reputation scores within a blockchain environment. Two blockchain-based schemes were created to manage user feedback, demonstrating up to an 80% improvement in query response times. Additionally, we introduced a secure and trusted review platform that promotes reviewer anonymity without cryptographic primitives and encourages timely review submissions, tested as a proof-of-concept on the Ethereum test network. Our trust and reputation service mitigates uncertainties in buyer feedback, enhancing transaction reliability through secure and verifiable feedback. We developed a dynamic reputation scoring system that adjusts scores over time, prioritizing recent activities, and accommodating changes in seller performance. Furthermore, methods were employed to predict long-term trust using incomplete information, supported by a 'trust engine' employing a modified version of Laplace's law of succession. We also designed SmartReview, an automated review system that uses blockchain, SCs, and advanced technologies to provide comprehensive reviews. Finally, a novel structured blockchain architecture was designed to enhance data integrity, security, and operational efficiency across diverse applications, integrating mechanisms for secure transaction recording and efficient query retrieval. These contributions collectively advance the fields of blockchain technology and decentralized reputation management, providing a robust framework for secure and efficient reputation systems in decentralized marketplaces.

REFERENCES

[1] A. Abdessalem, "Opencv object tracking," 2022.

[2] A. Abid, S. Cheikhrouhou, S. Kallel, and M. Jmaiel, "A blockchain-based self-sovereign identity approach for inter-organizational business processes," in *17th Conference on Computer Science and Intelligence Systems (FedCSIS)*, 2022, pp. 685–694.

[3] *Abusive seller who got my negative comments remove... - the ebay community*, https://community.ebay.com/t5/Buying/Abusive-seller-who-got-my-negative-comments-removed/td-p/31597239, (Accessed on 11/16/2022).

[4] F. Adebesin and R. Mwalugha, "The mediating role of organizational reputation and trust in the intention to use wearable health devices: Cross-country study," *JMIR Mhealth Uhealth*, vol. 20, 6 2020. DOI: 10.2196/16721.

[5] S. Ali, K. Masood, A. Riaz, and A. Saud, "Named entity recognition using deep learning: A review," in *2022 International Conference on Business Analytics for Technology and Security (ICBATS)*, IEEE, 2022, pp. 1–7.

[6] M. Aljohani, R. Mukkamala, and S. Olariu, "A smart contract-based decentralized marketplace system to promote reviewer anonymity," in *2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 2023, pp. 524–532.

[7] H. Allende, C. Moraga, and R. Salas, "Artificial neural networks in time series forecasting: A comparative analysis," *Kybernetika*, vol. 38, no. 6, pp. 685–707, 2002.

[8] J. Arshad, M. A. Azad, A. Prince, J. Ali, and T. G. Papaioannou, "Reputable–a decentralized reputation system for blockchain-based ecosystems," *IEEE Access*, vol. 10, pp. 79 948–79 961, 2022.

[9] A. Avyukt, G. Ramachandran, and B. Krishnamachari, "A decentralized review system for data marketplaces," in *2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 2021, pp. 1–9.

[10] A. Avyukt, G. Ramachandran, and B. Krishnamachari, "A decentralized review system for data marketplaces," in *2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 2021, pp. 1–9. DOI: 10.1109/ICBC51069.2021.9461149.

[11] M. A. Azad, S. Bag, and F. Hao, "Privbox: Verifiable decentralized reputation system for online marketplaces," *Future Generation Computer Systems*, vol. 89, pp. 44–57, 2018.

[12] R. Bazin, A. Schaub, O. Hasan, and L. Brunie, "A decentralized anonymity-preserving reputation system with constant-time score retrieval," *Cryptology ePrint Archive*, 2016.

[13] E. Bellini, Y. Iraqi, and E. Damiani, "Blockchain-based distributed trust and reputation management systems: A survey," *IEEE Access*, vol. 8, pp. 21 127–21 151, 2020.

[14] J. Breinlinger, A. Hagiu, and J. Wright, "The problems with 5-star rating systems, and how to fix them," in *Harvard Business Review*, 2019.

[15] B. Brooks-Patton and S. Noor, "Blockplace: A novel blockchain-based physical marketplace system," in *SoutheastCon 2023*, 2023, pp. 927–934.

[16] Y. Chaitra, M. Roopa, M. Gopalakrishna, M. Swetha, and C. Aditya, "Text detection and recognition from the scene images using rcnn and easyocr," in *International Conference*

on Information and Communication Technology for Intelligent Systems, Springer, 2023, pp. 75–85.

[17] P. Chattopadhyay, R. Vedantam, R. R. Selvaraju, D. Batra, and D. Parikh, "Counting everyday objects in everyday scenes," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2017, pp. 1135–1144.

[18] Y. Chen, W. Li, C. Sakaridis, D. Dai, and L. Van Gool, "Domain adaptive faster R-CNN for object detection in the wild," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2018, pp. 3339–3348.

[19] A. Cheng and E. Friedman, "Sybilproof reputation mechanisms," in *SIGGCOM Workshops*, 2005, pp. 128–132.

[20] R. B. Cleveland, W. S. Cleveland, J. E. McRae, and I. Terpenning, "STL: A seasonal-trend decomposition," *J. Off. Stat*, vol. 6, no. 1, pp. 3–73, 1990.

[21] C. Dellarocas, "Immunizing online reputation reporting systems against unfair ratings and discriminatory behavior," in *Proceedings of the 2nd ACM Conference on Electronic Commerce*, 2000, pp. 150–157.

[22] R. Dennis and G. Owen, "Rep on the block: A next generation reputation system based on the blockchain," in *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, 2015, pp. 131–138.

[23] T. Dimitriou, "Decentralized reputation," in *Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy*, 2021, pp. 119–130.

[24] R. G. Engoulou, M. Bellaiche, T. Halabi, and S. Pierre, "A decentralized reputation management system for securing the internet of vehicles," in *2019 International Conference on Computing, Networking and Communications (ICNC)*, IEEE, 2019, pp. 900–904.

[25] V. Ferrari, F. Jurie, and C. Schmid, "From images to shape models for object detection," *International journal of computer vision*, vol. 87, no. 3, pp. 284–303, 2010.

[26] F. Gai, B. Wang, W. Deng, and W. Peng, "Proof of reputation: A reputation-based consensus protocol for peer-to-peer network," in *Database Systems for Advanced Applications: 23rd International Conference, DASFAA 2018, Gold Coast, QLD, Australia, May 21-24, 2018, Proceedings, Part II 23*, Springer, 2018, pp. 666–681.

[27] A. Gandini, I. Pais, and D. Beraldo, "Reputation and trust on online labor markets: The reputation economy of elance," *Work Organisation, Labour and Globalisation*, vol. 16, pp. 27–43, 1 2016. DOI: 0.13169/workorgalaboglob.10.1.0027.

[28] S. Geisser, "On prior distributions for binary trials," *The American Statistician*, vol. 38, no. 4, pp. 244–247, Nov. 1984.

[29] H. Ghiasi, M. Fathian Brojeny, and M. R. Gholamian, "A reputation system for e-marketplaces based on pairwise comparison," *Knowledge and Information Systems*, vol. 56, pp. 613–636, 2018.

[30] R. L. Graham, D. E. Knuth, and O. Patashnik, *Concrete Mathematics*, 2-nd. Addison-Wesley, 1994.

[31] G. Grankvist and P. Moustakas, "Towards engineering trustworthy distributed reputation systems over the blockchain," in *BS Thesis, Malmo University*, 2022, p. 34.

[32] O. Hasan, L. Brunie, and E. Bertino, "Privacy-preserving reputation systems based on blockchain and other cryptographic building blocks: A survey," *ACM Computing Surveys*, vol. 55, no. 2, p. 37, 2022.

[33] O. Hasan, L. Brunie, E. Bertino, and N. Shang, "A decentralized privacy preserving reputation protocol for the malicious adversarial model," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 6, pp. 949–962, 2013.

[34] K. He, G. Gkioxari, P. Dollár, and R. Girshick, "Mask r-cnn," in *Proceedings of the IEEE international conference on computer vision*, 2017, pp. 2961–2969.

[35] C. Huang, Y. Zhao, H. Chen, X. Wang, Q. Zhang, Y. Chen, H. Wang, and K.-Y. Lam, "Zkrep: A privacy-preserving scheme for reputation-based blockchain system," *IEEE Internet of Things Journal*, vol. 9, no. 6, pp. 4330–4342, 2022.

[36] K. Ikeuchi, *Computer vision: A reference guide*. Springer, 2021.

[37] A. R. Islam, "Machine learning in computer vision," in *Applications of Machine Learning and Artificial Intelligence in Education*, IGI Global, 2022, pp. 48–72.

[38] V. Jha, S. Ramu, P. D. Shenoy, and K. Venugopal, "Reputation systems: Evaluating reputation among all good sellers," *Data-Enabled Discovery and Applications*, vol. 1, pp. 1–13, 2017.

[39] A. Jøsang and R. Ismail, "The beta reputation system," in *Proceedings of 15-th Bled Electronic Commerce Conference, e-Reality: Constructing the e-Economy*, Bled, Slovenia, Jun. 2002.

[40] E. Karami, S. Prasad, and M. Shehata, "Image matching using SIFT, SURF, BRIEF and ORB: Performance comparison for distorted images," *arXiv preprint arXiv:1710.02726*, 2017.

[41] R. Kerr and R. Cohen, "Smart cheaters do prosper: Defeating trust and repuation systems," in *Proceedings of 8-th International Conference on Autonomous Agents and Multiagent Systems*, Budapest, Hungary, May 2009.

[42] S. Khezr, A. Yassine, R. Benlamri, and M. S. Hossain, "An edge intelligent blockchain-based reputation system for IIoT data ecosystem," *IEEE transactions on industrial informatics*, vol. 18, no. 11, pp. 8346–8355, 2022.

[43] V. Koutsos, D. Papadopoulos, D. Chatzoloulos, S. Tarkoma, and P. Hui, "Agora: A privacy-aware data marketplace," *IEEE Transactions on Dependable and Secure Computing*, 2021. DOI: 10.1109/TDSC.2021.3105099.

[44] M. P. Lamela, J. Rodríguez-Molina, M. Martínez-Núñez, and J. Garbajosa, "A blockchain-based decentralized marketplace for trustworthy trade in developing countries," *IEEE Access*, vol. 10, pp. 79 100–79 123, 2022.

[45] W. S. Lee and J. Blasco, "Sensors i: Color imaging and basics of image processing," *Fundamentals of Agricultural and Field Robotics*, pp. 13–37, 2021.

[46] J. Lemley, S. Bazrafkan, and P. Corcoran, "Deep learning for consumer devices and services: Pushing the limits for machine learning, artificial intelligence, and computer vision.," *IEEE Consumer Electronics Magazine*, vol. 6, no. 2, pp. 48–56, 2017.

[47] L. Li, "Reputation, trust, and rebates: How online auction markets can improve their feedback mechanisms," *Journal of Economics & Management Strategy*, vol. 19, no. 2, pp. 303–331, 2010.

[48] M. Li, L. Zhu, Z. Zhang, C. Lal, M. Conti, and M. Alazab, "Anonymous and verifiable reputation system for e-commerce platforms based on blockchain," *IEEE Transactions on Network and Service Management*, vol. 18, no. 4, pp. 4434–4449, 2021.

[49] C. Liu, Y. Tao, J. Liang, K. Li, and Y. Chen, "Object detection based on yolo network," in *2018 IEEE 4th Information Technology and Mechatronics Engineering Conference (ITOEC)*, 2018, pp. 799–803. DOI: 10.1109/ITOEC.2018.8740604.

[50] D. Liu, A. Alahmadi, J. Ni, X. Lin, and X. Shen, "Anonymous reputation system for IIoT-enabled retail marketing atop pos blockchain," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3527–3537, 2019.

[51] Y. Liu, Z. Xiong, Q. Hu, D. Niyato, J. Zhang, C. Miao, C. Leung, and Z. Tian, "Vrepchain: A decentralized and privacy-preserving reputation system for social internet of vehicles based on blockchain," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 12, pp. 13 242–13 253, 2022.

[52] J. Lu, D. Batra, D. Parikh, and S. Lee, "Vilbert: Pretraining task-agnostic visiolinguistic representations for vision-and-language tasks," *Advances in neural information processing systems*, vol. 32, 2019.

[53] J. Martins, M. Parente, M. Amorim-Lopes, L. Amaral, G. Figueira, P. Rocha, and P. Amorim, "Fostering customer bargaining and e-procurement through a decentralised marketplace on

the blockchain," *IEEE Transactions on Engineering Management*, vol. 69, no. 3, pp. 810–824, 2022.

[54] D. E. Mik, "Blockchains: A technology for decentralized marketplaces?" *Impact of Technology on International Contract Law: Smart Contracts and Blockchain Technologies, Forthcoming*, 2018.

[55] A. A. Monrat, O. Schelén, and K. Andersson, "A survey of blockchain from the perspectives of applications, challenges, and opportunities," *IEEE Access*, vol. 7, pp. 117 134–117 151, 2019.

[56] K. Mrabet, F. El Bouanani, and H. Ben-Azza, "Dynamic decentralized reputation system from blockchain and secure multiparty computation," *Journal of Sensor and Actuator Networks*, vol. 12, no. 1, p. 14, 2023.

[57] R. Mukkamala, S. Olariu, and M. Aljohani, "Improved schemes for managing reputation in a blockchain-based decentralized marketplace," in *2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 2023, pp. 1–2.

[58] R. Mukkamala, S. Olariu, M. Aljohani, and S. Kalari, "Managing reputation scores in a blockchain-based decentralized marketplace," in *Proc. Fourth IEEE International Conference on Trust, Privacy and Security, Intelligent Systems and Applications (TPS-2022)*, December 14-16, Dec. 2022.

[59] R. Mukkamala, S. Olariu, M. Aljohani, and S. Kalari, "Managing reputation scores in a blockchain-based decentralized marketplace," in *2022 IEEE 4th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA)*, 2022, pp. 77–86.

[60] B. Nasrulin, G. Ishmaev, and J. Pouwelse, "MeritRank: Sybil tolerant reputation for merit-based tokenomics," in *Proc. 4-th IEEE Conference on Blockchain Research and Applications for Innovative Networks and Services (BRAINS'22)*, 2022, pp. 95–102.

[61] B. K. Nelson, "Time series analysis using autoregressive integrated moving average (ARIMA) models," *Academic emergency medicine*, vol. 5, no. 7, pp. 739–744, 1998.

[62] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, "Blockchain," *Business & Information Systems Engineering*, vol. 59, no. 3, pp. 183–187, 2017.

[63] N. O'Mahony, S. Campbell, A. Carvalho, S. Harapanahalli, G. V. Hernandez, L. Krpalkova, D. Riordan, and J. Walsh, "Deep learning vs. traditional computer vision," in *Advances in Computer Vision: Proceedings of the 2019 Computer Vision Conference (CVC), Volume 1 1*, Springer, 2020, pp. 128–144.

[64] S. Olariu, R. Mukkamala, and M. Aljohani, "Towards trust and reputation as a service in a blockchain-based decentralized marketplace," in *arXiv:2403.04779v1*, 2024.

[65] E. Owiyo, Y. Wang, E. Asamoah, D. Kamenyi, and I. Obiri, "Decentralized privacy preserving reputation system," in *2018 IEEE Third International Conference on Data Science in Cyberspace (DSC)*, IEEE, 2018, pp. 665–672.

[66] J. J. Pao and D. S. Sullivan, "Time series sales forecasting," *Final year project, Computer Science, Stanford Univ., Stanford, CA, USA*, 2017.

[67] J. R. Parker, *Algorithms for image processing and computer vision*. John Wiley & Sons, 2010.

[68] B. M. Pavlyshenko, "Machine-learning models for sales time series forecasting," *Data*, vol. 4, no. 1, p. 15, 2019.

[69] R. Peng, R. Wang, Z. Wang, Y. Lai, and R. Wang, "Rethinking depth estimation for multi-view stereo: A unified representation," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2022, pp. 8645–8654.

[70] Y. Peng, M. Du, F. Li, R. Cheng, and D. Song, "FalconDB: Blockchain-based collaborative database," in *Proceedings of ACM SIGMOD'2020*, Portland, Oregon, Jun. 2020.

[71] J. F. Peters, *Foundations of computer vision: computational geometry, visual image structures and object shape detection*. Springer, 2017, vol. 124.

[72] K. Plataniotis and A. N. Venetsanopoulos, *Color image processing and applications*. Springer Science & Business Media, 2000.

[73] K. Pulli, A. Baksheev, K. Kornyakov, and V. Eruhimov, "Real-time computer vision with openCV," *Communications of the ACM*, vol. 55, no. 6, pp. 61–69, 2012.

[74] "Quarterly retail e-commerce sales 4th quarter 2023," in *U.S. Census Bureau News*, 2024.

[75] V. P. Ranganthan, R. Dantu, A. Paul, P. Mears, and K. Morozov, "A decentralized marketplace application on the ethereum blockchain," in *2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC)*, IEEE, 2018, pp. 90–97.

[76] P. Resnick, R. Zeckhauser, E. Friedman, and K. Kuwabara, "Reputation systems," *Communications of the ACM*, no. 12, pp. 45–48, 2000.

[77] P. Resnick and R. Zeckhauser, "Trust among strangers in internet transactions: Empirical analysis of ebay's reputation system," in *The Economics of the Internet and E-commerce*, Emerald Group Publishing Limited, 2002.

[78] A. Roy, "Recent trends in named entity recognition (ner)," *arXiv preprint arXiv:2101.11420*, 2021.

[79] C. Santana and L. Albareda, "Blockchain and the emergence of decentralized autonomous organizations (DAO): An integrative model and research agenda," *Technological Forecasting & Social Change*, vol. 182, 2022.

[80] S. Saoji, A. Eqbal, and B. Vidyapeeth, "Text recognition and detection from images using pytesseract," *J Interdiscip Cycle Res*, vol. 13, pp. 1674–1679, 2021.

[81] A. Schaub, R. Bazin, O. Hasan, and L. Brunie, "A trustless privacy-preserving reputation system," in *IFIP International Conference on ICT Systems Security and Privacy Protection*, Springer, 2016, pp. 398–411.

[82] U. K. Shakila and S. Sultana, "A decentralized marketplace application based on ethereum smart contract," in *2021 24th International Conference on Computer and Information Technology (ICCIT)*, IEEE, 2021, pp. 1–5.

[83] Y.-S. Shiu, R.-Y. Lee, and Y.-C. Chang, "Pineapples' detection and segmentation based on faster and mask R-CNN in uav imagery," *Remote Sensing*, vol. 15, no. 3, p. 814, 2023.

[84] T. W. Simpson, "E-trust and reputation," *Ethics and information technology*, vol. 13, no. 1, pp. 29–38, 2011.

[85] A. Singh, K. Bacchuwar, and A. Bhasin, "A survey of ocr applications," *International Journal of Machine Learning and Computing*, vol. 2, no. 3, p. 314, 2012.

[86] D. de Siqueira Braga, M. Niemann, B. Hellingrath, and F. B. de Lima-Neto, "Survey on computational trust and reputation models," *ACM Computing Surveys*, vol. 51, pp. 1–40, Nov. 2018.

[87] N. Smolyanskiy, A. Kamenev, and S. Birchfield, "On the importance of stereo for accurate depth estimation: An efficient semi-supervised deep neural network approach," in *Proceedings of the IEEE conference on computer vision and pattern recognition workshops*, 2018, pp. 1007–1015.

[88] *Solved: Why don't my buyers leave feedback? - the ebay community*, `https://community.ebay.com/t5/Archive-Buying-Selling-Basics-Q/Why-don-t-my-buyers-leave-feedback/qaq-p/27941602`, (Accessed on 12/02/2022).

[89] K. Soska, A. Kwon, N. Christin, and S. Devadas, "Beaver: A decentralized anonymous marketplace with secure reputation," *Cryptology ePrint Archive*, 2016.

[90] A. Stannat, C. U. Ileri, D. Gijswijt, and J. Pouwelse, "Achieving sybil-proofness in distributed work systems," in *Proc. 20-th International Conference on Autonomous Agents and Multiagent Systems, (AAMAS'21)*, 2021, pp. 1261–1271.

[91] D. T Joy, G. Kaur, A. Chugh, and S. B. Bajaj, "Computer vision for color detection," *International Journal of Innovative Research in Computer Science & Technology (IJIRCST) ISSN*, pp. 2347–5552, 2021.

[92] S. Tadelis, "The economics of reputation and feedback systems in e-commerce marketplaces," *IEEE Internet Computing*, vol. 20, no. 1, pp. 12–19, 2015.

[93] S. J. Taylor and B. Letham, "Forecasting at scale," *The American Statistician*, vol. 72, no. 1, pp. 37–45, 2018.

[94] W. T. Teacy, J. Patel, N. R. Jennings, and M. Luck, "TRAVOS: Trust and reputation in the context of inaccurate information sources," *Autonomous Agents and Multi-Agent Systems*, no. 2, pp. 183–198, 2006.

[95] A. Tenorio-Fornés, V. Jacynycz, D. Llop-Vila, A. Sánchez-Ruiz, and S. Hassan, "Towards a decentralized process for scientific publication and peer review using blockchain and ipfs," 2019.

[96] M. Travizano, C. Sarraute, G. Ajzenman, and M. Minnoni, "Wibson: A decentralized data marketplace," in *Proc. ACM Workshop on Blockchain and Smart Contracts*, San Francisco, CA, 2018.

[97] M. Travizano, C. Sarraute, G. Ajzenman, and M. Minnoni, "Wibson: A decentralized data marketplace," *arXiv preprint arXiv:1812.09966*, 2018.

[98] F. Watson and Y. Wu, "The impact of online reviews on the information flows and outcomes of marketing systems," in *Journal of Retailing and Consumer Services*, vol. 42, 2021, pp. 74–80.

[99] *What are smart contracts on blockchain? | ibm*, `https://www.ibm.com/topics/smart-contracts`, (Accessed on 07/08/2024).

[100] *What is an online marketplace? meaning, benefits, & examples*, `https://www.webfx.com/marketplaces/glossary/what-is-an-online-marketplace/`, (Accessed on 04/09/2024), Nov. 2021.

[101] Y. Xiao, L. Zhu, and X. Li, "A review on trust and reputation management systems in e-commerce and P2P network," in *2021 2nd International Conference on E-Commerce and Internet Technology (ECIT)*, 2021, pp. 58–62.

[102] S. Xu, J. Wang, W. Shou, T. Ngo, A.-M. Sadick, and X. Wang, "Computer vision techniques in construction: A critical review," *Archives of Computational Methods in Engineering*, vol. 28, pp. 3383–3397, 2021.

[103] X. Zhang, L. Cui, and Y. Wang, "Commtrust: Computing multi- dimensional trust by mining e-commerce feedback comments," *IEEE Transactions on Knowledge and Data Engineering*, no. 7, pp. 1631–1643, 2014.

[104] Z. Zhou, M. Wang, C.-N. Yang, Z. Fu, X. Sun, and Q. J. Wu, "Blockchain-based decentralized reputation system in e-commerce environment," *Future Generation Computer Systems*, vol. 124, pp. 155–167, 2021.

APPENDIX A

COMBINATORIAL PRELIMINARIES

In order to make this work as self-contained as possible, the goal of this first appendix is to review a few classic mathematical results about binomial coefficients that will be used heavily in the remainder of the paper.

Recall that for non-negative integers m and r,

$$\binom{m}{r} = \frac{m!}{r!(m-r)!} \tag{29}$$

counts the number of distinct r-element subsets of a collection of m distinguishable objects. By convention,

$$\binom{m}{0} = 1 \text{ and } \binom{m}{r} = 0 \text{ when } 0 < m < r.$$

For a wealth of results involving the binomial coefficients the reader is referred to the classic source [30].

We often use the following simple result that follows straight from the symmetry inherent in (29:

$$\binom{m}{r} = \binom{m}{m-r}. \tag{30}$$

Lemma 5. *For non-negative integers, r, s, t, the following holds*

$$\binom{r}{s}\binom{r-s}{t} = \binom{s+t}{s}\binom{r}{s+t}.$$

Proof. See [30], pp. 167–8. □

Next, we look at a more complicated combinatorial identity that turns out to be crucial in our derivations

Lemma 6. *For all non-negative integers k, r, s, m, n, with $0 \leq r \leq n$, the following equality holds*

$$\sum_{k=0}^{s}\binom{r+k}{n}\binom{s-k}{m} = \binom{r+s+1}{n+m+1}. \tag{31}$$

Proof. See [30], p. 169. □

A.0.1 Evaluating $\sum_j = 0^N \Pr[A'|H_j]\Pr[H_j]$

To simplify notation, we write $\Pr[H_i]$ instead of $\Pr[H_i|n,k]$. Obviously, Recall that by (12), $\Pr[H_i] = \frac{\binom{i}{k}\binom{N-i}{n-k}}{\binom{N+1}{n+1}}$ and that $\Pr[A'|H_i] = \frac{\binom{i-k}{k'}\binom{N-i-(n-k)}{n'-k'}}{\binom{N-n}{n'}}$. With this, the expression of $\sum_{j=0}^{N}\Pr[A'|H_j]\Pr[H_j]$ becomes:

$$\sum_{j=0}^{N}\Pr[A'|H_j]\Pr[H_j] = \frac{\sum_{i=0}^{N}\binom{i}{k}\binom{N-i}{n-k}\binom{i-k}{k'}\binom{N-i-(n-k)}{n'-k'}}{\binom{N-n}{n'}\binom{N+1}{n+1}} \tag{32}$$

By Lemma 5 in the Appendix A we can write

$$\binom{i}{k}\binom{i-k}{k'} = \binom{k+k'}{k}\binom{i}{k+k'} \tag{33}$$

$$\binom{N-i}{n-k}\binom{N-i-(n-k)}{n'-k'}=\binom{n-k+n'-k'}{n-k}\binom{N-i}{n-k+n'-k'} \tag{34}$$

On replacing (33) and (34) back into (32) we obtain

$$\begin{aligned}\sum_{j=0}^{N}\Pr[A'|H_j]\Pr[H_j] &= \frac{\binom{k+k'}{k}\binom{n-k+n'-k'}{n-k}}{\binom{N-n}{n'}\binom{N+1}{n+1}}\Sigma_{i=0}^{N}\binom{i}{k+k'}\binom{N-i}{n-k+n'-k'} \\ &= \frac{\binom{k+k'}{k}\binom{n-k+n'-k'}{n-k}\binom{N+1}{n+n'+1}}{\binom{N-n}{n'}\binom{N+1}{n+1}} \\ &= \frac{\binom{k+k'}{k}\binom{n-k+n'-k'}{n-k}}{\binom{n+n'+1}{n+1}}.\end{aligned} \tag{35}$$

A.0.2 A Simple Algebraic Inequality

Lemma 7. *Let a, a' be non-negative reals and let b, b' be positive reals. Then either*

$$\frac{a}{b} \leq \frac{a+a'}{b+b'} \leq \frac{a'}{b'} \tag{36}$$

or else

$$\frac{a'}{b'} \leq \frac{a+a'}{b+b'} \leq \frac{a}{b} \tag{37}$$

Proof. Assume, without loss of generality, that $\frac{a}{b} \leq \frac{a'}{b'}$. We write in stages

$$\begin{aligned}\frac{a}{b} \leq \frac{a'}{b'} \quad &\iff \quad \frac{a}{a'} \leq \frac{b}{b'} \\ &\iff \quad \frac{a+a'}{a'} \leq \frac{b+b'}{b'} \\ &\iff \quad \frac{a+a'}{b+b'} \geq \frac{a'}{b'}.\end{aligned} \tag{38}$$

Similarly,

$$\begin{aligned} \frac{a}{b} \leq \frac{a'}{b'} \quad &\Longleftrightarrow \quad \frac{b}{a} \geq \frac{b'}{b} \\ &\Longleftrightarrow \quad \frac{a+b}{a} \geq \frac{b+b'}{b} \\ &\Longleftrightarrow \quad \frac{a}{b} \leq \frac{a+a'}{b+b'}. \end{aligned} \tag{39}$$

Now, (38) and (39) imply (36). Equation (37) is proved similarly. This completes the proof of the lemma. □

Corollary 8. *Let a, a' be non-negative reals and let b, b' be positive reals. Then $\frac{a}{b} \leq \frac{a+a'}{b+b'}$ implies $\frac{a+a'}{b+b'} \leq \frac{a'}{b'}$*

Proof. Follows directly from Lemma 7 □

VITA

Meshari Mohammd Aljohani

Department of Computer Science

Old Dominion University

Norfolk, VA 23529

EDUCATION

2011-2013, Master of Science in Computer Science, California Lutheran University.

1998-2003, Bachelor of Education in Computer Science, Teachers College, Jeddah, KSA.

PROFESSIONAL EXPERIENCE

2015-Present, IT Supervisor, IT Department, Directorate of Education- Madinah, KSA.

2003-2015, Teacher of Computer Science, Directorate of Education- Madinah, KSA.

CONFERENCE PRESENTATIONS

1. 2024 Integrated Communications, Navigation and Surveillance Conference (ICNS).
2. 2022 EAI WiCON - 15th EAI International Conference on Wireless Internet.
3. 2022 IEEE 4th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA).

PUBLICATIONS

A complete list is available at: $scholar.google.com/citations?user=_Q Nop8gAAAAJ\&hl=en$.